FirePOWER 管理中心配置指南，版本 6.0

首次发布日期: 年 月 日

上次修改日期: 年 月 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

文本部件号： 仅提供在线版本

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 1 章

思科 Firepower 系统简介

思科 Firepower 系统是集成的网络安全和流量管理产品套件，部署在专用平台上或作为软件解决方案。

系统旨在帮助您以符合组织的安全策略（网络保护准则）的方式处理网络流量。安全策略可能还包括可接受的使用策略 (AUP)，该策略向员工提供他们可以如何使用贵组织的系统的准则。

在典型部署中，安装于各网段的多台流量感应受管设备监控流量以进行分析并向管理 *Firepower* 管理中心报告。内联部署的设备会影响流量。

提示

有多种型号的设备和 Firepower 管理中心，包括虚拟实施。有时，可将设备型号分组为系列。系统功能通常取决于型号和许可证。

Firepower 管理中心提供具有 Web 界面的集中管理控制台，可用于执行管理、分析和报告任务。大多数受管设备没有 FirePOWER 系统 Web 界面，您可以使用 CLI 执行初始设置。但是，7000 和 8000 系列设备具有受限的 Web 界面，您可以使用此 Web 界面执行初始设置以及基本的分析和配置任务。

受管设备简介

网段上安装的受管设备监控流量以进行分析。被动部署的受管设备收集有关组织资产的详细信息：主机、操作系统、应用、用户、发送的文件（包括恶意软件）、漏洞等等。Firepower 系统将此信息关联以供您进行分析，从而可以监控用户访问的网站及其使用的应用，评估流量模式，并获得入侵和其他攻击的通知。

内联部署的系统可以使用访问控制影响流量的传输，允许您以精细方式指定如何处理传入、传出和穿越网络的流量。您收集的有关网络流量的数据以及从中获取的所有信息都可用来基于以下条件过滤和控制该流量：

- 简单、易于确定的传输层和网络层特征：源和目标、端口和协议等
- 流量的最新情景信息，包括诸如信誉、风险、业务关联性、使用的应用或访问的 URL 等特征
- 组织中的 Microsoft Active Directory 和 LDAP 用户；可以向不同用户授予不同的访问级别
- 加密流量的特征；也可以解密此流量以进一步分析
- 未加密或已解密的流量包含禁止的文件、检测到的恶意软件还是入侵事件

注释 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向受管设备部署相关配置。

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。例如，基于信誉的黑名单因为使用简单的源和目标数据，可以在进程中较早阻止禁止的流量。相反，检测和阻止入侵和漏洞则是最后一道防线。

7000 和 8000 系列设备上的网络管理功能还允许其在交换式和路由式环境中工作，执行网络地址转换 (NAT)，以及在配置的虚拟路由器之间构建安全虚拟专用网 (VPN) 隧道。您还可以配置绕行接口、汇聚接口、8000 系列快速路径规则和严格 TCP 实施。

7000 和 8000 系列受管设备

思科 Firepower 7000 和 8000 系列设备是专为 Firepower 系统构建的物理设备。7000 和 8000 系列 设备具有各种吞吐量，但是共享大多数相同的功能。一般来说，8000 系列设备比7000 系列功能更强大；它们还支持其他功能，如8000 系列快速路径规则、链路汇聚和堆叠。

NGIPSv

可以使用 VMware vSphere 虚拟机监控程序或 vCloud Director 环境部署 NGIPSv（将 64 位虚拟设备部署为 ESXi 主机）。您也可以在所有受支持的 ESXi 版本上启用 VMware 工具。

默认情况下，NGIPSv 使用 e1000（1 千兆位/秒）接口。您也可以使用 VMware vSphere 客户端将默认传感和管理接口替换为 vmxnet3（10 千兆位/秒）接口。

无论许可证如何，NGIPSv 都不支持系统的任何基于硬件的功能：冗余和资源共享、交换、路由等等。

具备 FirePOWER 服务的思科 ASA

具备 FirePOWER 服务的思科 ASA（或 *ASA FirePOWER* 模块）的运作方式类似于 NGIPSv。在 ASA FirePOWER 部署中，ASA 设备提供最重要的系统策略，并将流量传递到 FirePOWER 系统进行发现和访问控制。

无论安装和应用的许可证如何，ASA FirePOWER 都不支持以下任何 Firepower 系统功能：

- ASA FirePOWER 不支持 Firepower 系统 7000 和 8000 系列的基于硬件的功能：设备高可用性、堆叠、交换，路由、VPN、NAT 等等。但是，ASA 平台确实提供这些功能，可以使用 ASA CLI 和 ASDM 配置这些功能。有关详细信息，请参阅 ASA 文档。
- 无法使用Firepower 管理中心网络界面配置ASA FirePOWER 界面。在 SPAN 端口模式下部署 ASA FirePOWER 时，Firepower 管理中心不显示 ASA 接口。
- 无法使用Firepower 管理中心关闭、重新启动或以其他方式管理 ASA FirePOWER 进程。

ASA FirePOWER 拥有 ASA 平台独有的软件和命令行界面 (CLI)）。使用这些特定于 ASA 的工具可安装系统以及执行其他特定于平台的管理任务，例如：

注释 如果编辑 ASA FirePOWER 并从多情景模式切换至单情景模式（或反之），设备会重命名其所有接口。**必须**重新配置所有 Firepower 系统的安全区域、关联规则和相关配置，才能使用更新的 ASA FirePOWER 接口名称。

按典型设备型号划分的网络管理功能

Firepower 系统典型设备的吞吐量和功能各异，取决于型号和许可证。下表将系统的网络管理功能与 7000 和 8000 系列设备以及必须启用的许可证相匹配。所有型号的典型设备都可以执行访问控制。

表 *1*：按设备型号支持的管理和网络管理功能

特性或功能	7000 和 8000 系列	ASA FirePOWER	NGIPSv	经典许可证
流量信道	是	否	否	任意
多个管理接口	是	否	否	任意
链路聚合	是	否	否	任意
Firepower 系统 Web 界面	有限	否	否	任意
受限制（辅助）命令行界面 (CLI)	是	是	是	任意

特性或功能	7000 和 8000 系列	ASA FirePOWER	NGIPSv	经典许可证
外部身份验证	是	否	否	任意
连接至 eStreamer 客户端	是	是	否	任意
自动应用旁路	是	是	是	任意
侧录模式	是	否	否	任意
8000 系列快速路径规则	8000 系列	否	否	任意
严格 TCP 实施	是	否	否	保护
内联集的旁路模式	因 NetMod/SFP 而异	否	否	保护
恶意软件存储包	是	否	否	恶意软件
交换、路由、交换式和路由式聚合接口	是	否	否	可控性
NAT 策略	是	否	否	可控性
设备堆叠	8140 82xx 系列 83xx 系列	否	否	任意
设备高可用性	是	否	否	可控性
设备堆栈高可用性	8140 82xx 系列 83xx 系列	否	否	可控性
VPN	是	否	否	VPN

Firepower 管理中心简介

Firepower 管理中心是一种容错专用网络设备，为 Firepower 系统部署提供集中管理控制台和数据库存储库。您还可以使用 VMware vSphere 和 KVM（基于内核的虚拟机）虚拟机监控程序环境，以及通过亚马逊 Web 服务 (AWS) 云平台部署 64 位虚拟虚拟 Firepower 管理中心。Firepower 管理中心具有各种设备管理、事件存储、主机监控和用户监控功能。任何 Firepower 管理中心都可以管理任何类型的 Firepower 系统设备。

Firepower 管理中心汇聚和关联网络流量信息和性能数据，进而评估事件对特定主机的影响。您可监控设备报告的信息，评估和控制网络中发生的总体活动。Firepower 管理中心还控制设备上的网络管理功能：交换、路由、NAT、VPN 等等。

Firepower 管理中心的主要功能包括：

- 设备、许可证和策略管理
- 在表格、图形和图表中显示事件和情景信息
- 运行状况与性能监控
- 外部通知和警报
- 关联、危害表现和补救功能（实现实时威胁响应）
- 自定义和基于模板的报告

Firepower 管理中心功能

在运行此版本时，所有Firepower管理中心都具有类似的功能，主要区别在于容量和速度。Firepower管理中心型号根据其可以管理的设备数、其可以存储的事件数及其可以监控的主机和用户数而异。

Firepower 管理中心 Web 界面中可用的功能配置可能会受到您正在管理的设备的许可证和型号的限制。

MC4000 将思科统一计算系统 (UCS) 平台引入到 Firepower 系统。MC4000 不支持使用基板管理控制器 (BMC) 上的工具的思科功能，如 UCS Manager 或思科集成管理控制器 (CIMC)。

版本 6.0 随附的设备

表 *2*: 版本 *6.0 Firepower* 系统管理中心和设备

型号/系列	系列/分组	Type
70xx 系列： • Firepower 7010、7020、7030、7050	Firepower 7000 系列、FirePOWER 软件、典型设备	设备
71xx 系列： • Firepower 7110、7120 • Firepower 7115、7125 • AMP7150	Firepower 7000 系列、FirePOWER 软件、典型设备	设备
81xx 系列： • Firepower 8120、8130、8140 • AMP8050 • AMP8150	Firepower 8000 系列、FirePOWER 软件、典型设备	设备

型号/系列	系列/分组	Type
82xx 系列： • Firepower 8250 • Firepower 8260、8270、8290	Firepower 8000 系列、FirePOWER 软件、典型设备	设备
83xx 系列： • Firepower 8350 • Firepower 8360、8370、8390 • AMP8350 • AMP8360/8370/8390	Firepower 8000 系列、FirePOWER 软件、典型设备	设备
NGIPSv 64 位虚拟设备	典型设备	设备
面向 ASA 5585-X 的 ASA FirePOWER	具备 FirePOWER 服务的 ASA	ASA FirePOWER 硬件模块
面向 ASA 5000-X 系列的 ASA FirePOWER • ASA 5506-X • ASA 5506H-X • ASA 5506W-X • ASA 5508-X • ASA 5512-X • ASA 5515-X • ASA 5516-X • ASA 5525-X • ASA 5545-X • ASA 5555-X	具备 FirePOWER 服务的 ASA	ASA FirePOWER 软件模块
Firepower 管理中心： • MC750、MC1500、MC3500 • MC2000、MC4000	管理中心s	管理中心
64 位虚拟Firepower 管理中心	管理中心s	管理中心

Firepower 系统组件

以下主题介绍Firepower系统的一些有助于组织安全性、可接受的使用策略和流量管理策略的关键功能。

提示 很多 Firepower 系统功能因设备型号、许可证和用户角色而异。本文档包含关于每个功能必需哪些 Firepower 系统许可证和设备以及哪些用户角色有权完成各操作步骤的信息。

冗余和资源共享

通过Firepower系统的冗余和资源共享功能，可以确保操作的连续性并组合多个7000和8000系列设备的处理资源。

设备堆叠

设备堆叠允许通过在堆叠配置中连接两至四个设备来增加在网段上检查到的流量。建立堆栈配置时，要将每个堆叠设备的资源集成到单个统一的共享配置中。

7000 和 8000 系列设备高可用性

通过7000 和 8000 系列设备高可用性，可以在两个或多个 7000 或 8000 系列设备或堆栈之间建立网络功能和配置数据的冗余。将两个或多个对等设备或堆栈配置为高可用性对会产生单个用于策略应用、系统更新和注册的逻辑系统。通过设备高可用性，系统可以手动或自动进行故障切换。

大多数情况下，可以使用 SFRP 在不配置高可用性对的情况下实现第 3 层冗余。SFRP 允许设备充当指定 IP 地址的冗余网关。通过网络冗余，可以配置两台或多台设备或堆栈来提供相同的网络连接，确保网络上其他主机的连接。

7000 和 8000 系列设备的网络流量管理

利用Firepower系统的网络流量管理功能，可将7000和8000系列设备用作阻止网络基础设施的一部分。可以配置 7000 和 8000 系列设备，使其在交换式、路由式或混合式（交换路由式）环境中提供服务；执行网络地址转换 (NAT) 以及创建安全虚拟专用网络 (VPN) 通道。

交换

可以在第 2 层部署中配置 Firepower 系统，使其在两个或多个网段提供数据包交换。在第 2 层部署中，在 7000 和 8000 系列设备上配置交换接口和虚拟交换机作为独立的广播域。虚拟交换机根据主机的 MAC 地址来确定数据包发送的目的地。您还可以将多个物理接口组成单个逻辑链路，用于在网络中的两个终端之间提供数据包交换。终端可以是两个 7000 和 8000 系列设备，也可以是连接到第三方接入交换机的受管设备。

路由

可以在第 3 层部署配置 Firepower 系统，使其在两个或多个接口之间路由流量。在第 3 层部署中，将 7000 和 8000 系列设备上的路由接口和虚拟路由器配置为接收和转发流量。系统通过根据目标 IP 地址制定数据包转发决策来路由数据包。路由器根据转发条件从传出接口获取目标位置，访问控制规则指定要应用的安全策略。

配置虚拟路由器时，可以定义静态路由。此外，还可以配置路由信息协议 (RIP) 和开放式最短路径优先 (OSPF) 动态路由协议。还可以配置静态路由与 RIP 或静态路由与 OSPF 的组合。可以为所配置的每个虚拟路由器设置 DHCP 中继。

如果在部署中同时使用虚拟交换机和虚拟路由器，则可以配置关联的混合接口以桥接它们之间的流量。这些实用程序将分析流量，确定流量类型和相应的响应措施（路由、交换或其他）。您还可以将多个物理接口组成单个逻辑链路，用于在网络中的两个终端之间路由流量。终端可以是两个 7000 和 8000 系列设备，也可以是连接到第三方路由器的受管设备。

NAT

在第 3 层部署中，可以使用 7000 和 8000 系列设备配置网络地址转换 (NAT)。可以将内部服务器暴露于外部网络，或者允许内部主机或服务器连接外部应用。还可以使用 IP 地址块或使用有限制的 IP 地址块和端口转换，从外部网络配置 NAT 来隐藏专用网络地址。

VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在终端之间建立安全隧道。可以配置 Firepower 系统以在 7000 和 8000 系列设备的虚拟路由器之间构建安全的 VPN 隧道。

多租户

域功能可通过划分用户对受管设备、配置和事件的访问权限，在 Firepower 系统部署中实现多租户。

除了您的用户角色所施加的任何限制之外，您当前的域级别可能也会限制您修改配置的能力。系统会将大多数管理任务（例如系统软件更新）限制于全局域。

发现和身份

思科的发现和身份技术可收集有关主机、操作系统、应用、用户、文件、网络、地理位置和漏洞的信息，帮助您全面了解网络：

- 网络发现策略监控网络中的流量并收集主机、应用和非授权用户数据。
- 身份策略将网络中的用户与领域和身份验证方法相关联，以收集授权用户数据。

除身份策略外，您还要配置领域才能与 LDAP 或 AD 服务器建立连接并执行用户数据下载。

您可以使用特定类型的发现和身份数据构建全面的网络资产映射，执行调查分析、行为剖析和访问控制并缓解和应对组织最易遭受的漏洞和攻击。

您也可以使用 Firepower 管理中心的 Web 界面来查看和分析系统收集的数据。

访问控制

访问控制是一项基于策略的功能，可用于指定、检查和记录可以流经网络的流量。访问控制策决定系统如何处理网络上的流量。

最简单的访问控制策略指导其目标设备使用其默认操作处理所有流量。可以将此默认操作设置为阻止或信任所有流量而不进一步检查，或者检查入侵和发现数据的流量。

更复杂的访问控制策略可以根据 IP、URL 和 DNS 安全情报数据将流量列入黑名单，以及使用访问控制规则对网络流量记录和处理进行精细控制。这些规则可以简单也可以复杂，从而使用多个条件来匹配和检查流量；可以按安全区域、网络或地理位置、VLAN、端口、应用、所请求的 URL 和用户来控制流量。高级访问控制选项包括解密、预处理和性能。

每个访问控制规则还具有一个操作，用于确定是否监控、信任、阻止或允许匹配的流量。当您允许流量时，可以指定在流量到达您的资产或退出您的网络之前，系统首先利用入侵或文件策略对其进行检查以阻止任何漏洞攻击、恶意软件或禁止的文件。

SSL 检查

SSL 检查是基于策略的功能，通过其可处理加密流量而不解密，或者解密加密流量以进一步进行访问控制检查。可以选择阻止不受信任加密流量的源而不解密或进一步分析流量，也可以选择不解密加密流量，而是通过访问控制对其进行检查。

为深入洞察加密流量，可以使用上传到系统的公钥证书和配对私钥来解密穿越网络的加密流量，然后通过访问控制检查解密流量，如同其从未加密一样。如果系统在分析已解密流量后未阻止该流量，则会重新对其加密，然后再将其传递到目标主机。系统可以在其处理加密连接时记录有关这些连接的详细信息。

入侵检测和防御

入侵检测和防御是系统在允许流量到达目的地之前的最后一道防线。入侵策略是访问控制策略调用的几组已定义的入侵检测和防御配置。使用入侵规则和其他设置，这些策略检查流量是否存在安全违规，以及在内联部署中可以阻止或修改恶意流量。

思科通过 Firepower 系统提供多种入侵策略。通过使用系统提供的策略，您可以利用Cisco Talos 安全情报和研究小组 (Talos) 的经验。对于这些策略，Talos 可设置入侵和预处理器规则状态（启用或禁用），以及提供其他高级设置的初始配置。启用的规则导致系统为匹配规则的流量生成入侵事件（或阻止该流量）。

如果系统提供的策略不能完全满足贵组织的安全需求，那么自定义策略可以改进环境中的系统性能，并且可以提供网络中发生的恶意流量和策略违规的集中视图。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

思科高级恶意软件防护和文件控制

为了帮助您识别和减轻恶意软件的影响，Firepower 系统的文件控制、网络文件轨迹和高级恶意软件防护 (AMP) 组件可以检测、跟踪、捕获、分析和阻止（可选）网络流量中的文件传输（包括恶意软件文件和存档文件中的嵌套文件）。

文件控制

文件控制允许受管设备检测并阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。可以配置文件控制，作为全局访问控制配置的一部分；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

面向 Firepower 的 AMP

面向 Firepower 的 AMP 是一个基于网络的 AMP 解决方案，系统可通过它检查几种类型的文件中的网络流量是否存在恶意软件。设备可以将检测文件存储到其硬盘或（针对某些型号）恶意软件存储包中以供进一步分析。

您可以使用本地恶意软件分析来分析设备上的本地文件，以对恶意软件进行预分类。无论是否存储受检测文件，您都可以使用文件的 SHA-256 散列值，将文件提交到 AMP 云，进行简单的已知处置情况查询。您还可以将文件提交到 AMP Threat Grid 云以进行动态分析，从而生成威胁评分。使用此上下文信息，可以配置系统来阻止或允许特定的文件。

您可在整体访问控制配置过程中配置面向 Firepower 的 AMP；与访问控制规则关联的文件策略可以检查符合规则条件的网络流量。

面向终端的 AMP 集成

面向终端的 AMP 是基于终端的企业级 AMP 解决方案。个人用户在其通过 AMP 云通信的计算机和移动设备上安装轻量级连接器。然后，Firepower 管理中心可导入扫描记录、恶意软件检测和隔离以及危害表现 (IOC)，并可显示已检测威胁的轨迹。

使用面向终端的 AMP 管理控制台配置面向终端的 AMP 部署。此控制台可帮助您快速识别和隔离恶意软件。可以识别恶意软件爆发，跟踪它们的发展轨迹，了解其影响，并学习如何成功恢复。您还可以使用面向终端的 AMP 创建自定义防护，根据组策略阻止执行某些应用，以及创建自定义白名单。

网络文件轨迹

网络文件轨迹功能可以跟踪网络中的文件传输路径。系统使用 SHA-256 哈希值跟踪文件；因此，要跟踪文件，系统必须执行以下一项操作：

- 计算文件的 SHA-256 散列值并使用该值查询 AMP 云
- 通过将 Firepower 管理中心与您的组织的面向终端的 AMP 部署集成，接收与该文件相关的基于终端的威胁和隔离数据

每个文件都有一个关联的轨迹映射，其中包含文件随着时间推移进行的传输的直观显示以及有关该文件的其他信息。

思科 AMP 私有云虚拟设备

如果您的组织的安全策略不允许系统直接连接到 AMP 云（无论是面向 Firepower 的 AMP 还是面向终端的 AMP），则您可以配置思科 AMP 私有云虚拟设备 (AMPv)。

AMPv 是一台虚拟机，用作 AMP 云的本地压缩版本或匿名代理。通常涉及与 AMP 云的直接连接的数据和操作（例如，来自面向终端的AMP的事件、文件处置情况查找、追溯性事件等）改为通过与 AMPv 的本地连接来处理。有了 AMPv，就无需通过外部连接共享终端事件数据。

思科 AMP Threat Grid 内部设备

如果您的组织担心提交文件到公共AMP Threat Grid云可能会造成隐私或安全问题，您可以部署内部 AMP Threat Grid 设备。如同公共云一样，内部设备在沙盒环境下运行合格文件，然后向 Firepower 系统传回威胁评分和动态分析报告。但是，内部设备不会与公共云或位于您的网络外部的任何其他系统通信。

应用编程接口

有几种方法可以使用应用程序编程接口 (API) 来与系统交互。

eStreamer

通过 Event Streamer (eStreamer)，您可以将几种事件数据从 Firepower 管理中心传输到自定义开发的客户端应用。创建客户端应用之后，您可以将其连接到 Firepower 管理中心上的 eStreamer 服务器，启动 eStreamer 服务，开始交换数据。

eStreamer集成需要自定义编程，但您可以向设备请求特定数据。如果在网络管理应用中显示网络主机数据，就可以写入一个程序来从Firepower管理中心检索主机重要性或漏洞数据并将该信息添加到显示中。

外部数据库访问

借助数据库访问功能，您可以通过支持 JDBC SSL 连接的第三方客户端，查询Firepower 管理中心中的多个数据库表。

可以使用 Crystal Reports、Actuate BIRT 或 JasperSoft iReport 等行业标准报告工具来设计和提交查询。也可以配置自定义应用来查询思科数据。例如，可以创建 servlet 来定期报告和发现事件数据或刷新警报控制面板。

主机输入

通过主机输入功能，您可以通过从使用脚本或命令行文件的第三方源导入数据来增加发现数据。

Web 界面还提供一些主机输入功能；您可以修改操作系统或应用协议身份，启用或禁用漏洞，同时从网络映射中删除各项目，包括客户端和服务器端口。

补救

该系统包含可用于创建补救 操作的 API，在网络状况违反相关关联策略或合规白名单时，Firepower 管理中心可以自动启动。补救可以在您无法立即处理攻击时自动减轻攻击，并确保系统仍符合贵公司的安全策略。除了用户自己创建的补救操作，Firepower 管理中心还提供预定义的补救模块。

联机帮助和相关文档

可以通过以下方式从 Web 界面访问联机帮助：

- 点击各页面上的上下文帮助链接
- 依次选择**帮助 (Help)** > **联机 (Online)**

联机帮助包含关于使用Firepower管理中心或设备 Web 界面可以完成的任务的信息，包括系统管理、策略管理和事件分析。

可以使用以下文档路线图查找与 Firepower 系统相关的其他文档：http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html。

许可证约定

节开头的许可证声明指示必须将哪个许可证分配到Firepower 系统中的受管设备以启用该节所述的功能。

许可证声明包括：

任意

任何受管设备都可执行该节所述的功能，只要为其分配了最高级别的许可证即可。通常，这表示典型受管设备的控制许可证。

保护（经典）或威胁（智能）

通过保护或威胁许可证，受管设备可以执行入侵检测和防御、文件控制和安全情报过滤。对于典型受管设备，此许可证对应于购买任何典型受管设备时自动包含的保护许可证。保护许可证是永久的，但是还必须购买威胁和应用 (TA) 订用以启用系统更新。

控制（仅经典）

通过控制许可证，典型受管设备可以执行主机、应用和用户发现，以及简单的基于网络的访问控制。（仅限 7000 和 8000 系列设备）通过该许可证，还可以配置交换和路由（包括 DHCP 中继）、NAT 以及将 7000 和 8000 系列设备和堆栈配置成高可用性对。此许可证对应于购买任何典型受管设备时包含的控制许可证。控制许可证是永久的，但是还必须购买威胁和应用 (TA) 订用以启用系统更新。

URL 过滤

通过 URL 过滤许可证，受管设备可以根据受监控主机请求的 URL，使用定期更新的威胁情报确定哪些流量可以流经网络。URL 过滤许可证需要保护许可证。对于典型设备，可以购买此许可证作为与保护（TAC 或 TAMC）相结合的服务订用，或者作为已启用保护 (TA) 的设备的附加订用 (URL)。

恶意软件

通过恶意软件许可证，受管设备可以使用面向 Firepower 的 AMP，即检测、捕获和阻止通过网络传输的文件中的恶意软件，并且将这些文件提交到 AMP 云进行动态分析。通过该许可证还可查看轨迹，从而跟踪通过网络发送的文件。恶意软件许可证需要保护许可证。对于典型设备，可以购买恶意软件许可证作为与保护（TAM 或 TAMC）相结合的服务订用，或者作为已启用保护 (TA) 的设备的附加订用 (AMP)。

VPN（仅限经典）

通过 VPN 许可证，可以在 7000 和 8000 系列设备的虚拟路由器之间构建安全 VPN 隧道。VPN 许可证需要保护和控制许可证。要购买 VPN 许可证，请与销售人员联系。

由于许可功能通常是累加的，因此许可证声明仅提供每项功能的最高要求许可证。例如，如果功能要求向受管设备分配保护和控制许可证，则仅会列出“控制”(Control)。

许可证声明中的“或”语句表明必须向受管设备分配特定许可证以启用该节所述的功能，但是附加许可证可以添加功能。例如，在文件策略中，某些文件规则操作要求向设备分配保护许可证，而其他操作则要求分配恶意软件许可证。

受支持设备约定

章节或主题开头的“受支持设备”声明指示仅在指定的设备序列、系列或型号上才支持相应的功能。例如，只有在 8000 系列设备上才支持堆栈。

有关此版本支持的平台的详细信息，请参阅版本说明。

访问约定

本文档中每个程序开头的“访问”声明表明执行此程序所需的预定义用户角色。所列的任何角色都可以执行此程序。下表定义了“访问”声明中出现的常用术语。

表 *3*：访问约定

访问术语	说明
访问管理员	用户必须具备访问控制管理员角色
管理	用户必须具备管理员角色
任意	用户可以是任何角色
任何角色/管理员	用户可以是任何角色，但是只有管理员角色可以不受限制地访问（例如可以查看保存为专用级别的其他用户数据）
任何安全分析师	用户可以是安全分析师角色或安全分析师（只读）角色
数据库	用户必须具备外部数据库角色

访问术语	说明
发现管理员	用户必须具备发现管理员角色
入侵管理员	用户必须具备入侵管理员角色
维护	用户必须具备维护人员角色
网络管理员	用户必须具备网络管理员角色
安全分析师	用户必须具备安全分析师角色
安全审批人	用户必须具备安全审批人角色

自定义角色的用户可以拥有不同于预定角色的权限。预定角色用于指示某个程序的访问要求时，具有相似权限的自定义角色也能访问。某些具有自定义角色的用户可以使用略有不同的菜单路径到达配置页面。例如，具有仅有入侵策略权限的自定义角色的用户通过入侵策略而非通过访问控制策略的标准路径来访问网络分析策略。

IP 地址约定

您可以使用 IPv4 无类域间路由选择 (CIDR) 表示法和类似的 IPv6 前缀长度表示法定义 Firepower 系统中很多位置的地址块。

CIDR 表示法使用网络 IP 地址结合位掩码来定义指定地址块中的 IP 地址。例如，下表列出了 CIDR 表示法中的 IPv4 地址空间。

表 *4*: *CIDR* 表示法语法示例

CIDR 块	CIDR 块中的 IP 地址	Subnet Mask	IP 地址数量
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同样，IPv6 使用网络 IP 地址结合前缀长度来定义指定块中的 IP 地址。例如，2001:db8::/32 指定的 IPv6 地址在 2001:db8:: 网络中，前缀长度为 32 位，即 2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，Firepower 系统**只**使用掩码或前缀长度指定的那部分网络 IP 地址。例如，如果键入 10.1.2.3/8，则 Firepower 系统使用 10.0.0.0/8。

换句话说，虽然思科建议您在使用 CIDR 或前缀长度表示法时采用使用位边界上网络 IP 地址的标准方法，但是 Firepower 系统并不要求必须这么做。

功能限制

以下功能不支持用于当前可由 Firepower 管理中心管理的任何设备：

- 威胁防御平台设置
- 威胁防御 NAT 策略
- 威胁防御路由
- 威胁防御接口管理
- 威胁防御设备管理
- 威胁防御设备注册
- 智能许可证
- AS 路径对象
- 社区列表对象
- 扩展访问列表对象
- 策略列表对象
- 前缀列表 IPv4 对象
- 前缀列表 IPv6 对象
- SLA 监控对象
- 标准访问列表对象

第 I 部分

用户帐户

第 2 章

登录 Firepower 系统

以下主题介绍如何登录 Firepower 系统：

Firepower 系统用户界面

在 Firepower 系统中，您可以使用 Web 界面或辅助命令行界面 (CLI) 登录设备。界面访问基于设备类型：

表 *5*：按设备分类的用户界面

设备	网络界面	辅助 CLI
Firepower 管理中心	可用于行政管理、普通管理和分析任务	not available

设备	网络界面	辅助 CLI
7000 和 8000 系列设备	可用于初始设置、基本分析和配置任务	可用于设置和支持部门指示的故障排除
NGIPSv	not available	
ASA FirePOWER	not available	

有关 Web 界面浏览器要求的信息，请参阅 Firepower 系统相应版本的版本说明。

注释 如果 ASA FirePOWER模块不通过 Firepower 管理中心管理，则您可以使用自适应安全设备管理器 (ASDM) 直接管理 ASA FirePOWER模块。有关详细信息，请参阅具备 *FirePOWER* 服务的思科 *ASA* 本地管理配置指南。

您必须提供用户名和密码才能访问设备的 Web 界面或 CLI。您在登录后可以访问的功能受制于您获得的用户帐户权限。

注释 由于系统根据用户帐户审核用户活动，因此请确保用户使用正确的帐户登录系统。

Web 界面注意事项

- 如果您的组织使用通用访问卡 (CAC) 进行身份验证，则您可以使用 CAC 凭证获得对设备 Web 界面的访问权限。
- 在网络会话期间首次访问设备主页时，可以查看您上一次登录该设备的登录会话相关信息。您可以查看与您上次登录相关的以下信息：

  登录的年、月、日和周

  用 24 小时制表示的登录设备本地时间

  上次用于访问设备的主机和域名

- 在默认主页顶部显示的菜单和菜单选项取决于用户帐户的权限。但是，默认主页上的链接包括适用于各种用户帐户权限范围的选项。如果点击的链接所需的权限与已授予帐户的权限不同，系统将显示警告消息并记录相关活动。
- 某些进程耗时较长，这可能会导致网络浏览器显示指明脚本无响应的消息。如果出现这种情况，请确保允许脚本继续运行，直至完成。

会话超时

默认情况下，除非您以其他方式配置为免除会话超时，否则在不活动达 1 小时之后 Firepower 系统会自动将您从会话中注销。

具有“管理员”(Administrator) 角色的用户可以通过以下设置更改设备的会话超时间隔：

设备	设置
Firepower 管理中心	**系统 (System)** > **配置 (Configuration)** > **外壳超时 (Shell Timeout)**
7000 和 8000 系列设备	**设备 (Devices)** > **平台设置 (Platform Settings)** > **外壳超时 (Shell Timeout)**

通过 Web 界面登录 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	管理中心	任何环境	任何环境

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户帐户登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 完成初始设置过程并创建用户帐户，如《*Firepower* 系统安装指南》和创建用户帐户，第 62 页中所述。

过程

步骤 1 将浏览器定向到 `https://hostname/`，其中 *hostname* 与 Firepower 管理中心的主机名对应。

步骤 2 在**用户名 (Username)** 和**密码 (Password)** 字段中，输入用户名和密码。请注意以下准则：

- 用户名不区分大小写。
- 在多域部署中，请在用户名前面附加在其中创建用户帐户的域。无需在用户名前面附加任何祖先域。例如，如果用户帐户在 SubdomainB 中创建（其祖先域为 DomainA），则请按以下格式输入用户名：

  ```
  SubdomainB\username
  ```

- 如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录 Firepower 系统。

步骤 3 点击 **Login**。

通过 Web 界面登录受管设备

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	7000 和 8000 系列	不适用	任意

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户帐户登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 完成初始设置过程并创建用户帐户，如《*Firepower* 系统安装指南》和创建用户帐户，第 62 页中所述。

过程

步骤 1 将浏览器定向到 `https://hostname/`，其中 *hostname* 与受管设备的主机名对应。

步骤 2 在**用户名 (Username)** 和**密码 (Password)** 字段中，输入用户名和密码。请注意以下准则：

- 用户名不区分大小写。
- 如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录 Firepower 系统。

步骤 3 点击 **Login**。

使用 CAC 凭证登录 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	管理中心	任何环境	任何环境

用户受限于单个活动会话。

注意 在浏览会话活动期间，**请勿**删除 CAC。在会话期间，如果删除或替换 CAC，网络浏览器会终止会话，且系统会退出网络界面。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 完成初始设置过程并创建用户帐户，如《*Firepower* 系统安装指南》和创建用户帐户，第 62 页中所述。
- 配置 CAC 身份验证和授权，如配置 CAC 身份验证，第 72 页中所述。

过程

步骤 1 按照您的组织的指示插入 CAC。

步骤 2 将浏览器定向到 `https://hostname/`，其中 *hostname* 与 Firepower 管理中心的主机名对应。

步骤 3 如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

步骤 4 如有提示，请从下拉列表中选择相应的证书。

步骤 5 点击**继续 (Continue)**。

通过 CAC 凭证登录受管设备

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	7000 和 8000 系列	不适用	任意

用户受限于单个活动会话。

注意 在浏览会话活动期间，**请勿**删除 CAC。在会话期间，如果删除或替换 CAC，网络浏览器会终止会话，且系统会退出网络界面。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。

- 完成初始设置过程并创建用户帐户，如《*Firepower* 系统安装指南》和创建用户帐户，第 62 页中所述。
- 配置 CAC 身份验证和授权，如配置 CAC 身份验证，第 72 页中所述。

过程

步骤 1 按照您的组织的指示插入 CAC。

步骤 2 将浏览器定向到 `https://hostname/`，其中 *hostname* 与要访问的设备的主机名对应。

步骤 3 如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

步骤 4 如有提示，请从下拉列表中选择相应的证书。

步骤 5 点击**继续 (Continue)**。

登录典型设备上的辅助命令行界面

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	传统	不适用	CLI 基本配置

可以直接登录典型受管设备上的辅助命令行界面（7000 和 8000 系列、NGIPSv 和 ASA FirePOWER）。

开始之前

- 完成初始设置过程并创建用户帐户，如《*Firepower* 系统安装指南》和创建用户帐户，第 62 页中所述。

过程

步骤 1 打开与设备的 SSH 连接：

- 对于 7000 系列、8000 系列和 NGIPSv，使用设备的主机名或其管理接口的 IP 地址进行连接。
- 对于 ASA FirePOWER，连接到管理地址上的 FirePOWER 服务软件。

步骤 2 在 `login as:` 命令提示符处，输入用户名并按 Enter 键。

步骤 3 在 `Password:` 提示符处，输入密码并按 Enter 键。
如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录 Firepower 系统。

步骤 4 在辅助 CLI 提示符处，使用命令行访问级别所允许的任何命令。

查看 Web 界面中的基本系统信息

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任何环境	任何环境	任何环境	任何环境

“关于”(About) 页面显示有关设备的信息，包括型号、序列号和 Firepower 系统各组件的版本信息。此页面还包含思科的版权信息。

过程

步骤 1 点击页面顶部工具栏中的**帮助 (Help)**。

步骤 2 选择**关于 (About)**。

在 Firepower 管理中心上切换域

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	管理中心	任何环境	任何环境

在多域部署中，用户角色权限确定用户可以访问哪些域，以及用户在其中每个域内具有哪些权限。可以将单个用户帐户与多个域相关联，并在每个域中为该用户分配不同的权限。例如，可以在全局域中为用户分配只读权限，但在后代域中分配管理员权限。

与多个域关联的用户可以在同一 Web 界面会话中的域之间进行切换。

在工具栏中的用户名下，系统会显示可用域的树。树：

- 显示祖先域，但是，可以根据分配给用户帐户的权限禁用对这些域的访问。
- 隐藏用户帐户无法访问的任何其他域，包括同代域和后代域。

在切换到域时，系统会显示：

- 仅与该域相关的数据。
- 由面向该域分配给您的用户角色确定的菜单选项。

过程

在您的用户名下的下拉列表中，选择要访问的域。

注销 Firepower 系统 Web 界面

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任何环境	任何环境	任何环境	任何环境

不再使用 Firepower 系统 Web 界面时，思科建议您注销，即使只是暂时离开 Web 浏览器。注销会结束您的 Web 会话并确保没有人可以通过您的凭证使用界面。

过程

从用户名下的下拉列表中，选择**注销 (Logout)**。

情景菜单

Firepower 系统 Web 界面中的某些页面支持右键点击上下文菜单（最常见）或左键点击上下文菜单，可供您用作访问 Firepower 系统中其他功能的快捷方式。上下文菜单的内容取决于您访问菜单时所处的位置 - 不仅是页面，还可以是特定数据。

例如：

- IP 地址热点，提供有关与该地址关联的主机的信息，包括任何可用的 whois 和主机配置文件信息。
- SHA-256 散列值热点，通过其可将文件的 SHA-256 散列值添加到干净列表或自定义检测列表中，或者查看要复制的完整散列值。

在不支持 Firepower 系统上下文菜单的页面或位置上，适用于浏览器的普通上下文菜单将会显示出来。

策略编辑器

许多策略编辑器都包含基于每个规则的热点。您可以插入新规则和类别，剪切、复制和粘贴规则，设置规则状态，以及编辑规则。

入侵规则编辑器

入侵规则编辑器包含基于每个入侵规则的热点。您可以编辑规则，设置规则状态，配置阈值和抑制选项，以及查看规则文档。

事件查看器

事件页面（向下钻取页面和表视图）包含基于每个事件、IP 地址、URL、DNS 查询以及某些文件的 SHA-256 散列值的热点。查看大多数事件类型时，您可以执行以下操作：

- 在情景管理器中查看相关信息。
- 在新窗口中向下展开到事件信息。
- 查看事件视图中的事件字段包含过长而无法完全显示的文本（例如文件的 SHA-256 散列值、漏洞说明或 URL）的位置的完整文本。

查看连接事件时，您可以将项目添加到默认安全情报白名单和黑名单：

- IP 地址热点中的 IP 地址。
- URL 热点中的 URL 或域名。
- DNS 查询热点中的 DNS 查询。

查看捕获的文件、文件事件和恶意软件事件时，您可以执行以下操作：

- 在干净列表或自定义检测列表中添加或删除文件。
- 下载文件的副本。
- 查看存档文件内的嵌套文件。
- 下载嵌套文件的父存档文件。
- 输入文件组成。
- 提交文件以进行本地恶意软件和动态分析。

查看入侵事件时，您可以执行与入侵规则编辑器或入侵策略中的任务类似的任务：

- 编辑触发规则。
- 设置规则状态（包括禁用规则）。
- 配置阈值和抑制选项。
- 查看规则文档。

入侵事件数据包视图

入侵事件数据包视图包含 IP 地址热点。数据包视图使用左键点击上下文菜单。

控制面板

许多控制板构件包含用于查看 Context Explorer 中相关信息的热点。控制面板构件还包含 IP 地址和 SHA-256 散列值热点。

Context Explorer

Context Explorer 包含其图表、表格和图形上的热点。如果您想要以超出 Context Explorer 允许的程度更为详细地查看图表或列表的数据，您可以向下钻取相关数据的表视图。您还可以查看相关的主机、用户、应用、文件和入侵规则信息。

情景管理器使用左键点击上下文菜单，该菜单也包含情景管理器独有的过滤选项及其他选项。

第 3 章

指定用户首选项

以下主题介绍如何指定用户首选项：

用户首选项简介

可以配置与单个用户帐户，例如主页、帐户密码、时区、控制面板和事件查看首选项相关联的首选项。

根据用户角色，可以指定用户帐户的一些首选项，包括密码、事件查看首选项、时区设置和主页首选项。

在多域部署中，用户首选项适用于您的帐户有权访问的所有域。当指定主页和控制面板首选项时，请记住某些页面和控制面板构件会受域限制。

更改您的密码

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何环境

所有用户帐户均采用密码保护。可以随时更改密码，根据用户帐户设置，可能需要定期更改密码。

如果密码强度检查已启用，则密码必须至少包含 8 个大小写混合的字母数字字符，并且至少包含一个数字字符。密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。

如果是 LDAP 或 RADIUS 用户，则不能通过网络界面更改密码。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项 (User Preferences)**。

步骤 2 请输入您的**当前密码 (Current Password)**，然后点击**更改 (Change)**。

步骤 3 在**新密码 (New Password)** 和**确认 (Confirm)** 字段中，输入新密码。

步骤 4 点击**更改**。

更改到期密码

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何环境

根据用户帐户设置，密码可能已过期。请注意，在帐户已创建且**不能**更改时，将会设置密码到期时间段。如果密码已过期，系统会显示 Password Expiration Warning 页面。

过程

在“密码到期警告”(Password Expiration Warning) 页面上，您有两种选择：

- 点击 **Change Password**，立即更改密码。如果警告天数为零，则**必须**更改密码。

  提示 如果密码强度检查已启用，则密码必须至少包含 8 个大小写混合的字母数字字符，并且至少包含一个数字字符。密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。

- 点击 **Skip**，稍后更改密码。

指定主页

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	除外部数据库用户以外的任何用户

可以将网络界面中的页面指定为该设备的主页。默认主页是“摘要控制面板”(Summary Dashboard)（**概述 (Overview)** > **控制面板 (Dashboards)**），没有控制面板访问权限的用户除外。

在多域部署中，您选择的主页适用于您的用户帐户具有访问权限的所有域。为经常访问多个域的帐户选择主页时，请记住某些页面限制为全局域。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项 (User Preferences)**。

步骤 2 点击 **Home Page**。

步骤 3 从下拉列表中选择要用作主页的页面。
下拉列表中的选项基于用户帐户的访问权限。有关详细信息，请参阅用户帐户权限，第 42 页。

步骤 4 点击**保存 (Save)**。

配置事件视图设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	因功能而异

使用“事件视图设置”(Event View Settings) 页面配置 Firepower 管理中心上事件视图的特征。请注意，一些事件查看配置仅对特定的用户角色可用。使用外部数据库用户角色的用户可以查看事件查看设置用户界面的某些部分，但是更改这些设置不会产生有意义的结果。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项 (User Preferences)**。

步骤 2 点击 **Event View Settings**。

步骤 3 在**事件首选项 (Event Preferences)** 部分，配置事件视图的基本特征；请参阅事件视图首选项，第 32 页。

步骤 4 在**文件首选项 (File Preferences)** 部分，配置文件下载首选项；请参阅文件下载首选项，第 33 页。

步骤 5 在**默认时间窗口 (Default Time Windows)** 部分，配置默认时间窗口；请参阅默认时间窗口，第 33 页。

步骤 6 在**默认工作流程 (Default Workflow)** 部分，配置默认工作流程；请参阅默认工作流程，第 35 页。

步骤 7 点击**保存 (Save)**。

事件视图首选项

使用“事件视图设置”(Event View Settings) 页面的“事件首选项”(Event Preferences) 部分可在 Firepower 系统中配置事件视图的基本特征。尽管此区域对无法查看事件的用户不重要，但所有用户角色均可使用。

以下字段显示在 Event Preferences 区域：

- **确认“所有”操作 (Confirm “All” Actions)** 字段控制设备是否强制确认影响事件视图中的所有事件的操作。

  例如，如果已启用此设置且点击事件查看上的**Delete All**，必须确认要删除的所有事件满足当前的限制条件（包括在当前页面未显示的活动），然后才可将其从数据库中删除。

- 通过**解析 IP 地址 (Resolve IP Addresses)** 字段，设备会尽可能在事件视图中显示主机名而非 IP 地址。

  请注意，如果事件查看包含大量IP地址，并且已启用该选项，则该视图可能缓慢显示。另请注意，为使此设置生效，必须使用管理接口配置在系统设置中建立 DNS 服务器。

- **Expand Packet View** 字段可供您配置入侵事件数据包视图的显示方式。默认情况下，设备以折叠方式显示数据包视图：

  None - 折叠数据包视图的 Packet Information 部分的所有子部分

  Packet Text - 仅展开 Packet Text 子部分

  Packet Bytes - 仅展开 Packet Bytes 子部分

  All - 展开所有部分

无论默认设置如何，您始终可以手动展开数据包视图中的部分查看有关已捕获数据包的详细信息。

- **Rows Per Page** 字段控制要在向下页面和表视图中显示的每页事件行数。
- **Refresh Interval** 字段设置事件查看的刷新时间间隔（以分钟为单位）。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **Statistics Refresh Interval** 控制事件摘要页面（例如，Intrusion Event Statistics 和 Discovery Statistics 页面）的刷新时间间隔。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **Deactivate Rules** 字段控制哪些链接显示在标准文本规则生成的入侵事件的数据包视图上：

  All Policies - 用于取消激活所有本地定义的自定义入侵规则中的标准文本规则的一个链接。

  当前策略 (Current Policy) - 用于仅停用当前部署的入侵规则中的标准文本规则的一个链接。请注意，您不能停用默认策略中的规则。

  Ask - 每一这些选项的链接

要在数据包视图上看到这些链接，您的用户帐户必须具有管理员或入侵管理员权限。

文件下载首选项

使用 Event View Settings 页面的 File Preferences 部分配置本地文件下载的基本特征。此部分仅适用于具有管理员、安全分析师或安全分析师（只读）用户角色的用户。

请注意，如果设备不支持下载捕获的文件，则这些选项会禁用。

以下字段显示在 File Preferences 区域：

- **Confirm ‘Download File’ Actions** 复选框控制 File Download 弹出窗口是否每次都显示下载文件，同时显示警告并提示继续或取消。

  注意 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

  请注意，在下载文件时，可随时禁用此选项。

- 当下载一个捕获的文件时，系统会创建包含该文件的密码保护的 .zip 归档文件。**Zip File Password** 字段定义要用于限制 .zip 文件的访问权限的密码。如果将此字段留空，系统会创建归档文件，不需要密码。
- **Show Zip File Password** 复选框会切换显示 **Zip File Password** 字段中的纯文本或模糊字符。当清除此字段时，**Zip File Password** 显示模糊字符。

默认时间窗口

时间段，有时称为时间范围，会对任何事件查看中的事件施加时间限制。使用 Event View Settings 页面的 Default Time Windows 区域控制时间段的默认行为。

此区域的用户角色访问权限列出如下：

- 管理员和维护人员可以访问完整的区域。
- 安全分析师和安全分析师（只读）可访问除 **Audit Log Time Window** 之外的所有选项。
- 访问管理员、发现管理员、外部数据库用户、入侵管理员、网络管理员和安全审批人只能访问**事件时间窗口 (Events Time Window)** 选项。

请注意，无论默认时间段设置如何，在事件分析期间，可以始终手动更改单个事件查看的时间段。另请注意，时间段设置仅对当前会话有效。在注销后重新登录时，时间段会重置为在此页面中配置的默认设置。

可为以下三种类型的事件设置默认时间段：

- **Events Time Window** 可为按时间限制的多数事件设置单个默认时间段。
- **Audit Log Time Window** 可为审核日志设置默认时间段。
- **Health Monitoring Time Window** 可为运行状况事件设置默认时间段。

仅可以为用户帐户可访问的事件类型设置时间段。所有用户类型都可设置事件事件段。管理员、维护人员和安全分析师可以设置运行状况监控时间段。管理员和维护人员可以设置审核日志时间段。

请注意，因为不是所有的事件查看都可以受时间限制，所以时间段设置对显示主机、主机属性、应用程序、客户端、漏洞、用户身份或白名单违规的事件查看没有影响。

可以使用**多个**时间段，每种事件类型一个，也可以使用适用于所有事件的**一个**时间段。如果使用一个时间段，则不会显示三种时间段类型的设置，会显示新的 **Global Time Window** 设置。

有以下三种类型的时间段：

- 静态，显示在某个特定开始时间和特定结束时间期间生成的所有事件
- 扩展，显示在某个特定开始时间和当前时间期间生成的所有事件；随着时间向前推进，时间段会扩展，新的事件会添加到事件查看
- 滑动，显示在某个特定开始时间（例如，一天前）和当前时间期间生成的所有事件；随着时间向前推进，时间段会“滑动”，以便只可以查看所配置范围内的事件（在本示例中，为最后一天）

所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。

以下选项显示在 **Time Window Settings** 下拉列表：

- **Show the Last - Sliding** 选项允许配置指定长度的默认滑动时间窗。

  设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。当更改事件查看，时间段会“滑动”，以便始终可查看最近一小时的事件。

- 通过**显示最后时间 - 静态/扩展式 (Show the Last - Static/Expanding)** 选项，可以配置指定长度的静态或扩展默认时间窗口。

  对于**静态**时间段，启用 **Use End Time** 复选框。设备会显示在某个特定开始时间（例如，1 小时前）和第一次查看事件时的时间期间生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。

  对于**扩展**时间段，禁用 **Use End Time** 复选框。设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。

- **Current Day - Static/Expanding** 选项允许为当日配置静态或扩展默认时间段。当日从午夜开始，基于当前会话的时区设置。

  对于**静态**时间段，启用 **Use End Time** 复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。

  对于**扩展**时间段，禁用 **Use End Time** 复选框。设备会显示在午夜到当前时间期间生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。请注意，如果分析在注销之前持续超过 24 小时，则时间段可能会超过 24 小时。

- **Current Day - Static/Expanding** 选项允许为当前星期配置静态或扩展默认时间段。当周从上一周日的午夜开始，基于当前会话的时区设置。

对于**静态**时间段，启用 **Use End Time** 复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件查看后，时间段会固定，以便只可查看在静态时间段内发生的事件。

对于**扩展**时间段，禁用 **Use End Time** 复选框。设备会显示在周日午夜到当前时间期间生成的所有事件。在更改事件查看后，时间段会扩展为当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间段可以超过 1 周。

默认工作流程

工作流程是一组页面，显示分析师评估事件所使用的数据。对于每个事件类型，设备附带了至少一个预定义工作流程。例如，作为安全分析师，根据执行分析的类型，可以在十种入侵事件工作流程中选择，每种类型都会以不同的方式显示入侵事件数据。

设备会使用每种事件类型的默认工作流程进行配置。例如，按优先级和分类事件的工作流程是入侵事件的默认值。这意味着，只要查看入侵事件（包括已审阅的入侵事件），设备都会显示按优先级和分类事件的工作流程。

但是，您可以更改每种事件类型的默认工作流程。可配置的默认工作流程取决于用户角色。例如，入侵事件分析师无法设置默认发现事件工作流程。

设置默认时区

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何环境

可以更改用于显示设备使用的标准 UTC 时间内事件的时间段。当配置时区时，它仅适用于用户帐户，并且在进一步更改时区之前有效。

注意 时区功能假设，默认系统时钟设置为 UTC 时间。如果更改设备的系统时钟使用本地时区，则必须将其更改回 UTC 时间，以查看设备的准确本地时间。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项 (User Preferences)**。

步骤 2 点击**时区首选项 (Time Zone Preference)** 选项卡。

步骤 3 从左侧列表框中，选择包含要使用时区的大洲或区域。

步骤 4 从右侧列表框中，选择与要使用的时区对应的时区（城市名）。

步骤 5 点击**保存 (Save)**。

指定默认控制面板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

当选择**概述 (Overview)** > **控制面板 (Dashboards)**时，系统将会显示默认控制面板。除非更改，否则所有用户的默认控制面板都是“摘要”(Summary) 控制面板。

在多域部署中，选择的默认控制面板适用于用户帐户具有访问权限的所有域。当选择频繁访问多个域的帐户的控制面板时，请记住，某些控制面板构件会受域限制。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项 (User Preferences)**。

步骤 2 点击 **Dashboard Settings**。

步骤 3 从下拉列表中选择要用作默认的控制面板。如果选择**无 (None)**，则选择**概述 (Overview)** > **控制面板 (Dashboards)**时，即可选择要查看的控制面板。

步骤 4 点击**保存 (Save)**。

第 II 部分

Firepower 系统管理

第 4 章

Firepower 系统用户管理

以下主题介绍具有管理员访问权限的用户如何在 Firepower 系统中管理用户帐户：

用户角色

通过Firepower系统，您可以根据用户的角色分配用户权限。例如，可以授予分析师预定义角色（如“安全分析师”[Security Analyst] 和“发现管理员”[Discovery Admin]），并为管理 Firepower 系统的安全管理员保留“管理员”(Administrator) 角色。也可以创建具有根据贵组织需求定制的访问权限的自定义用户角色。

在受管设备的平台设置策略中，为来自该设备的所有进行外部身份验证的用户设置默认访问角色。外部身份验证用户首次登录后，可以在 User Management 页面上添加或移除该用户的访问权限。如果没有修改用户权限，则用户仅具有默认授予的权限。由于是手动创建内部身份验证用户，因此在创建这些用户时设置访问权限。

如果通过 LDAP 组配置访问权限的管理，则用户的访问权限基于其在 LDAP 组中的成员资格。他们接收其所属的具有最高访问级别的组的默认访问权限。如果他们不属于任何组，并且您已配置组访问权，则他们会接收在 LDAP 服务器的身份验证对象中配置的默认用户访问权限。如果配置组访问权，则这些设置会覆盖平台设置策略中的默认访问设置。

同样，如果将用户分配到 RADIUS 身份验证对象中的特定用户角色列表，则除非其中一个或多个角色互不兼容，否则该用户会接收分配的所有角色。如果用户在两个互不兼容角色的列表上，则用户会接收具有最高访问级别的角色。如果用户不属于任何列表，并且您已在身份验证对象中配置默认

访问角色，则用户会接收该角色。如果已在身份验证对象中配置默认访问，则这些设置会覆盖平台设置策略中的默认访问设置。

在多域部署中，可以在多个域中分配用户角色。例如，可以在全局域中为用户分配只读权限，但在子域中分配“管理员”(Administrator) 权限。

预定义用户角色

Firepower 系统包含 10 个预定义用户角色，提供一系列访问权限集来满足您的组织的需求。请注意，7000 和 8000 系列设备仅有权访问 10 个预定义用户角色中的三个：“管理员”(Administrator)、“维护用户”(Maintenance User) 和“安全分析师”(Security Analyst)。

虽然无法编辑预定义用户角色，但是可以使用其访问权限集作为自定义用户角色的基础。此外，您无法对其进行配置以升级到其他用户角色。

下表简要描述可供使用的预定义角色。

访问管理员

提供对**策略 (Policies)** 菜单中访问控制策略和关联功能的访问权限。“访问管理员”(Access Admin) 无法部署策略。

管理员

提供对分析和报告功能、规则和策略配置、系统管理和所有维护功能的访问。“管理员”(Administrator) 也可对设备部署配置更改，包括策略的更改。Administrator 有权访问所有菜单选项；其会话如果受攻击会有更高安全风险，因此不能使其免于登录会话超时。

出于安全原因，应限制“管理员”(Administrator) 角色的使用。

发现管理员

提供对**策略 (Policies)** 菜单中网络发现、应用检测和关联功能的访问权限。“发现管理员”(Discovery Admin) 无法部署策略。

External Database User

使用支持 JDBC SSL 连接的应用对 Firepower 系统数据库的只读访问权限。为使第三方应用向 Firepower 系统设备进行身份验证，必须在系统设置中启用数据库访问权限。在网络界面上，External Database User 仅有权访问 **Help** 菜单中与联机帮助相关的选项。由于此角色的功能不涉及网络界面，因此提供访问只是为便于支持和密码更改。

Intrusion Admin

提供对**策略 (Policies)** 和**对象 (Objects)** 中所有入侵策略、入侵规则和网络分析策略功能的访问权限。“入侵管理员”(Intrusion Admin) 无法部署策略。

Maintenance User

提供对监控和维护功能的访问。Maintenance User 有权访问 **Health** 和 **System** 菜单中与维护相关的选项。

网络管理员

提供对**策略 (Policies)** 菜单中访问控制、SSL 检查、DNS 策略和身份策略功能以及**设备 (Devices)** 菜单中设备配置功能的访问权限。“网络管理员”(Network Admin) 可对设备部署配置更改。

安全分析师

提供对**概述 (Overview)**、**分析 (Analysis)**、**运行状况 (Health)** 和**系统 (System)** 菜单中安全事件分析功能的访问权限，以及对其中运行状况事件的只读访问权限。

Security Analyst (Read Only)

提供对**概述 (Overview)**、**分析 (Analysis)**、**运行状况 (Health)** 和**系统 (System)** 菜单中安全事件分析功能和运行状况事件的只读访问权限。

安全审批人

提供对**策略 (Policies)** 菜单中访问控制和关联策略以及网络发现策略的访问权限。“安全审批人”(Security Approver) 可以查看和部署这些策略，但不能进行策略更改。

除向用户分配事件分析师角色以外，可以限制该用户的删除权限，以仅允许删除由该用户创建的报告配置文件、搜索、书签、自定义表和自定义工作流程。

如果没有为外部身份验证用户分配其他角色，则根据 LDAP 或 RADIUS 身份验证对象中以及平台设置中的设置，他们仅有最低访问权限。可以向这些用户分配其他权限，但是要移除或更改最低访问权限，必须执行以下任务：

- 在身份验证对象中将用户从一个列表移至另一个列表，或者在外部身份验证服务器上更改用户的属性值或组成员资格。
- 更新平台设置。
- 使用 User Management 页面从该用户帐户中移除访问权。

自定义用户角色

除以上预定义角色外，还可以配置具有专用访问权限的自定义用户角色。自定义用户角色可以具有任何基于菜单的权限集和系统权限集，并且可能完全是原始的或基于预定义用户角色。与预定义用户角色类似，自定义角色可以充当外部身份验证用户的默认角色。与预定义角色不同，可以修改和删除自定义角色。

可选择的权限分层并且基于Firepower系统菜单布局。如果权限具有子页面，并且其具有比简单页面访问更精细的权限可用，则可以展开这些权限。在此情况下，父权限授予页面查看访问权以及对该页面的相关功能的子精细访问。包含单词“Manage”的权限授予编辑和删除其他用户创建的信息的能力。

提示 对于菜单中结构不包括的页面或功能，由父级或相关页面授予权限。例如，通过Modify Intrusion Policy 权限还您还可以修改网络分析策略。

可以对自定义用户角色应用受限搜索。这些会限制用户在事件查看器中可查看的数据。可以配置受限搜索，方法是先创建专用的已保存搜索，然后在适当的基于菜单的权限下从**受限搜索 (Restricted Search)** 下拉菜单中选择该搜索。

在Firepower管理中心上配置自定义用户角色时，所有基于菜单的权限都可供授予。在受管设备上配置自定义用户角色时，只有与设备功能相关的部分权限可用。

通过System Permissions下的可选选项，可以创建能够对外部数据库进行查询或升级到目标用户角色的权限的用户角色。

或者，可以从其他设备导出自定义用户角色，然后将其导入到您的设备上，而不是创建新的自定义用户角色。然后，在应用已导入的角色之前，可以对其进行编辑以满足需求。

示例：自定义用户角色和访问控制

您可以为与访问控制相关的功能创建自定义用户角色，以指定Firepower系统用户是否可以查看和修改访问控制和关联策略。

下表列出可以创建的自定义角色和为每个示例授予的用户权限。下表列出每个自定义角色所需的权限。在此示例中，策略审批人可以查看（但无法修改）访问控制和入侵策略。他们还可以将配置更改部署到设备。

表 *6*：访问控制自定义角色示例

自定义角色权限	示例：访问控制编辑器	示例：入侵和网络分析编辑器	示例：策略审批人
访问控制	是	否	yes
访问控制策略	是	否	yes
Modify Access Control Policy	是	否	否
入侵策略	否	是	是
Modify Intrusion Policy	否	是	否
将配置部署到设备	否	否	yes

用户帐户权限

以下各节提供Firepower系统中可配置用户权限的列表以及可以访问这些权限的预定义用户角色。并非所有权限在受管设备上都可用；仅在Firepower 管理中心上可用的权限相应进行了标记。

概述菜单

下表按顺序列出访问Overview菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。Security Approver、Discovery Admin、Intrusion Admin、Access Admin、Network Admin 和 External Database User 角色在 Overview 菜单中没有权限。

表 7：概述菜单

权限	管理	Maint User	安全分析师	Security Analyst (RO)
控制面板	是	是	是	是
Manage Dashboards	是	否	否	否
Appliance Information Widget	是	是	是	是
设备状态构件（仅限管理中心）	是	是	是	是
Correlation Events Widget	是	否	是	是
Current Interface Status Widget	是	是	是	是
Current Sessions Widget	是	否	否	否
自定义分析构件（仅限管理中心）	是	否	是	是
Disk Usage Widget	是	是	是	是
Interface Traffic Widget	是	是	是	是
入侵事件构件（仅限管理中心）	是	否	是	是
网络关联构件（仅限管理中心）	是	否	是	是
产品许可构件（仅限管理中心）	是	是	否	否
Product Updates Widget	是	是	否	否
RSS Feed Widget	是	是	是	是
System Load Widget	是	是	是	是
System Time Widget	是	是	是	是
白名单事件构件（仅限管理中心）	是	否	是	是

权限	管理	Maint User	安全分析师	Security Analyst (RO)
报告（仅限管理中心）	是	否	是	是
管理报告模板（仅限管理中心）	是	否	是	是
Summary	是	否	是	是
入侵事件统计信息（仅限管理中心）	是	否	是	是
Intrusion Event Performance	是	否	否	否
入侵事件图表（仅限管理中心）	是	否	是	是
发现统计信息（仅限管理中心）	是	否	是	是
发现性能（仅限管理中心）	是	否	否	否
连接摘要（仅限管理中心）	是	否	是	是

分析菜单

下表按顺序列出访问 Analysis 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。在不同标题下多次出现的权限将仅列于其第一次出现的表中，不同在于指示的是子菜单标题。Security Approver、Intrusion Admin、Access Admin、Network Admin 和 External Database User 角色在 Analysis 菜单中没有权限。Analysis 菜单仅在Firepower 管理中心上可用。

表 *8*：分析菜单

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
Context Explorer	是	否	否	是	是
连接事件	是	否	否	是	是
Modify Connection Events	是	否	否	是	否
Connection Summary Events	是	否	否	是	是
Modify Connection Summary Events	是	否	否	是	否
Security Intelligence Events	是	否	否	是	是
Modify Security Intelligence Events	是	否	否	是	否

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
入侵	是	否	否	是	是
入侵事件	是	否	否	是	是
Modify Intrusion Events	是	否	否	是	否
View Local Rules	是	否	否	是	是
Reviewed Events	是	否	否	是	是
剪贴板	是	否	否	是	是
突发事件	是	否	否	是	是
修改事故 (Modify Incidents)	是	否	否	是	否
文件	是	否	否	是	是
Malware Events	是	否	否	是	是
Modify Malware Events	是	否	否	是	否
File Events	是	否	否	是	是
Modify File Events	是	否	否	是	否
捕获的文件	是	否	否	是	是
Modify Captured Files	是	否	否	是	否
文件轨迹	是	否	否	是	是
File Download	是	否	否	是	是
Dynamic File Analysis	是	否	否	是	否
主机数	是	否	否	是	是
Network Map	是	否	否	是	是
主机数	是	否	否	是	是
Modify Hosts	是	否	否	是	否

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
危害表现	是	否	否	是	是
修改危害表现	是	否	否	是	否
服务器	是	否	否	是	是
Modify Servers	是	否	否	是	否
漏洞	是	否	否	是	是
Modify Vulnerabilities	是	否	否	是	否
Host Attributes	是	否	否	是	是
Modify Host Attributes	是	否	否	是	否
应用	是	否	否	是	是
应用详情	是	否	否	是	是
Modify Application Details	是	否	否	是	否
Host Attribute Management	是	否	否	否	否
Discovery Events	是	否	否	是	是
Modify Discovery Events	是	否	否	是	否
用户	是	是	否	是	是
用户活动	是	是	否	是	是
Modify User Activity Events	是	是	否	是	否
用户	是	是	否	是	是
Modify Users	是	是	否	是	否
漏洞	是	否	否	是	是
Third-party Vulnerabilities	是	否	否	是	是
Modify Third-party Vulnerabilities	是	否	否	是	否

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
互联	是	是	否	是	是
相关事件	是	是	否	是	是
Modify Correlation Events	是	是	否	是	否
White List Events	是	是	否	是	是
Modify White List Events	是	是	否	是	否
White List Violations	是	是	否	是	是
Remediation Status	是	是	否	否	否
Modify Remediation Status	是	是	否	否	否
自定义	是	否	否	是	是
自定义工作流程	是	否	否	是	是
Manage Custom Workflows	是	否	否	是	是
Custom Tables	是	否	否	是	是
Manage Custom Tables	是	否	否	是	是
搜索	是	否	是	是	是
管理搜索	是	否	否	否	否
书签	是	否	否	是	是
Manage Bookmarks	是	否	否	是	是
Application Statistics	是	否	否	是	是
Geolocation Statistics	是	否	否	是	是
User Statistics	是	否	否	是	是
URL Category Statistics	是	否	否	是	是
URL Reputation Statistics	是	否	否	是	是

菜单	管理	Discovery Admin	Maint User	安全分析师	Security Analyst (RO)
按记录类型划分的 DNS 查询 (DNS Queries by Record Types)	是	否	否	是	是
SSL statistics	是	否	否	是	是
Intrusion Event Statistics by Application	是	否	否	是	是
Intrusion Event Statistics by User	是	否	否	是	是
Security Intelligence Category Statistics	是	否	否	是	是
File Storage Statistics by Disposition	是	否	否	是	是
File Storage Statistics by Type	是	否	否	是	是
Dynamic File Analysis Statistics	是	否	否	是	是

Policies（策略）菜单

下表按顺序列出访问 Policies 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。External Database User、Maintenance User、Security Analyst 和 Security Analyst (Read Only) 角色在 Policies 菜单中没有权限。Policies 菜单仅在Firepower 管理中心上可用。

请注意，还可以通过 Intrusion Policy 和 Modify Intrusion Policy 权限创建和修改网络分析策略。

表 *9*: *Policies*（策略）菜单

菜单	Access Admin	管理	Discovery Admin	Intrusion Admin	网络管理员	Security Approver
访问控制	是	是	否	否	是	是
访问控制策略	是	是	否	否	是	是
Modify Access Control Policy	是	是	否	否	是	否
Modify Administrator Rules	是	是	否	否	是	否
Modify Root Rules	是	是	否	否	是	否
入侵策略	否	是	否	是	否	yes
Modify Intrusion Policy	否	是	否	是	否	否

菜单	Access Admin	管理	Discovery Admin	Intrusion Admin	网络管理员	Security Approver
恶意软件与文件策略 (Malware & File Policy)	是	是	否	否	否	yes
修改恶意软件和文件策略 (Modify Malware & File Policy)	是	是	否	否	否	否
DNS 策略 (DNS Policy)	是	是	否	否	是	是
修改 DNS 策略 (Modify DNS Policy)	是	是	否	否	是	否
身份策略 (Identity Policy)	是	是	否	否	是	否
修改身份策略 (Modify Identity Policy)	是	是	否	否	是	否
Modify Administrator Rules	是	是	否	否	是	否
Modify Root Rules	是	是	否	否	是	否
SSL 策略	是	是	否	否	是	是
Modify SSL Policy	是	是	否	否	是	否
Modify Administrator Rules	是	是	否	否	是	否
Modify Root Rules	是	是	否	否	是	否
网络发现	否	是	是	否	否	yes
Custom Fingerprinting	否	是	是	否	否	否
修改自定义指纹 (Modify Custom Fingerprinting)	否	是		否	否	否
Custom Topology	否	是	是	否	否	否
修改自定义拓扑 (Modify Custom Topology)	否	是	否	否	否	否
Modify Network Discovery	否	是	是	否	否	否
Application Detectors	否	是	是	否	否	否
修改应用检测器 (Modify Application Detectors)	否	是	是	否	否	否

菜单	Access Admin	管理	Discovery Admin	Intrusion Admin	网络管理员	Security Approver
User 3rd Party Mappings	否	是	是	否	否	否
修改用户第三方映射 (Modify User 3rd Party Mappings)	否	是	否	否	否	否
Custom Product Mappings	否	是	是	否	否	否
修改自定义产品映射 (Modify Custom Product Mappings)	否	是	否	否	否	否
互联	否	是	否	否	否	否
策略管理	否	是	否	否	否	否
修改策略管理 (Modify Policy Management)	否	是	是	否	否	否
规则管理	否	是	否	否	否	否
修改规则管理 (Modify Rule Management)	否	是	是	否	否	否
White List	否	是	否	否	否	否
修改白名单 (Modify White List)	否	是	是	否	否	否
Traffic Profiles	否	是	否	否	否	否
修改流量量变曲线 (Modify Traffic Profiles)	否	是	是	否	否	否
操作	否	是	是	否	否	yes
风险通告	否	是	是	否	否	yes
Impact Flag Alerts	否	是	是	否	否	否
修改影响标志警报 (Modify Impact Flag Alerts)	否	是	是	否	否	否
Discovery Event Alerts	否	是	是	否	否	否
修改发现事件警报 (Modify Discovery Event Alerts)	否	是	是	否	否	否

菜单	Access Admin	管理	Discovery Admin	Intrusion Admin	网络管理员	Security Approver
电子邮件	否	是	否	是	否	否
修改邮件 (Modify Email)	否	是	否	是	否	否
修改警报 (Modify Alerts)	否	是	是	否	否	否
Scanners	否	是	是	否	否	否
Scan Results	否	是	是	否	否	否
Modify Scan Results	否	是	是	否	否	否
修改扫描工具 (Modify Scanners)	否	是	是	否	否	否
组	否	是	否	否	否	否
修改组 (Modify Groups)	否	是	是	否	否	否
模块	否	是	否	否	否	否
修改模块	否	是	是	否	否	否
Instances	否	是	否	否	否	否
修改实例 (Modify Instances)	否	是	是	否	否	否

设备菜单

Devices 菜单表按顺序列出访问 Devices 菜单中的各选项及其中的子权限所需的用户角色权限。“发现管理员”(Discovery Admin)、“外部数据库用户”(External Database User)、“入侵管理员”(Intrusion Admin)、“维护用户”(Maintenance User)、“安全分析师”(Security Analyst) 和“安全分析师（只读）”(Security Analyst [Read Only]) 在“设备”(Devices) 菜单中没有任何权限。Devices 菜单仅在 Firepower 管理中心上可用。

表 *10*：设备菜单

菜单	Access Admin	管理	网络管理员	Security Approver
设备管理	否	是	是	是
Modify Devices	否	是	是	否

菜单	Access Admin	管理	网络管理员	Security Approver
NAT	是	是	是	是
NAT List	是	是	是	是
Modify NAT Policy	是	是	是	否
VPN	否	是	是	是
Modify VPN	否	是	是	否
平台设置 (Platform Settings)	否	是	是	是
修改平台设置 (Modify Platform Settings)	否	是	是	否

对象管理器菜单

“对象管理器”(Object Manager) 菜单表按顺序列出访问“对象管理器”(Object Manager) 菜单中的各选项及其中的子权限所需要的用户角色权限。“发现管理员”(Discovery Admin)、“安全审批人”(Security Approver)、“维护用户”(Maintenance User)、“外部数据库用户”(External Database User)、“安全分析师”(Security Analyst) 以及“安全分析师（只读）”(Security Analyst [Read Only]) 在“对象管理器”(Object Manager) 菜单中没有权限。“对象管理器”(Object Manager) 菜单仅在 Firepower 管理中心上可用。

表 *11*：对象管理器菜单

菜单	Access Admin	管理	Intrusion Admin	网络管理员
对象管理员	是	是	否	yes
Rule Editor	否	是	是	否
修改规则编辑器 (Modify Rule Editor)	否	是	是	否
NAT List	是	是	否	yes
修改对象管理器 (Modify Object Manager)	否	是	否	否

思科 AMP

思科 AMP 权限仅可供“管理员”(Administrator) 用户角色使用。此权限仅在 Firepower 管理中心上可用。

将配置部署到设备

“将配置部署到设备”(Deploy Configuration to Devices) 权限可用于“管理员”(Administrator)、“网络管理员”(Network Admin) 和“安全审批人”(Security Approver) 角色。此权限仅在 Firepower 管理中心上可用。

系统菜单

下表按顺序列出访问 System 菜单中的各选项所需的用户角色权限以及用户角色是否有权访问其中的子权限。“外部数据库用户”(External Database User) 角色在“系统”(System) 菜单中没有权限。

表 *12*: 系统菜单

菜单	Access Admin	管理	Discovery Admin	入侵管理员	Maint User	网络管理员	Security Approver	安全分析师	Security Analyst (RO)
配置	否	是	否	否	否	否	否	否	否
域	否	是	否	否	否	否	否	否	否
集成	否	是	否	否	否	是	是	否	否
思科 CSI	是	是	否	否	否	是	是	否	否
身份领域（仅限管理中心）	是	是	否	否	否	是	是	否	否
修改身份领域（仅限管理中心）	是	是	否	否	否	是	否	否	否
身份源（仅限管理中心）	是	是	否	否	否	是	是	否	否
修改身份源（仅限管理中心）	是	是	否	否	否	是	否	否	否
eStreamer	否	是	否	否	否	否	否	否	否
主机输入客户端（仅限管理中心）	否	是	否	否	否	否	否	否	否
智能软件卫星（仅限管理中心）	是	是	否	否	否	是	是	否	否
修改智能软件卫星（仅限管理中心）	是	是	否	否	否	是	否	否	否

菜单	Access Admin	管理	Discovery Admin	入侵管理员	Maint User	网络管理员	Security Approver	安全分析师	Security Analyst (RO)
用户管理	否	是	否	否	否	否	否	否	否
用户	否	是	否	否	否	否	否	否	否
用户角色	否	是	否	否	否	否	否	否	否
外部身份验证（仅限管理中心）	否	是	是	否	否	否	否	否	否
更新	否	是	否	否	否	否	否	否	否
规则更新（仅限管理中心）	否	是	否	是	否	否	否	否	否
规则更新导入日志（管理中心仅限）	否	是	否	否	否	否	否	否	否
许可证	否	是	否	否	否	否	否	否	否
智能许可证	否	是	否	否	否	否	否	否	否
修改智能许可证	否	是	否	否	否	否	否	否	否
经典许可证	否	是	否	否	否	否	否	否	否
运行状况 (Health)（仅限管理中心）	否	是	否	否	是	否	否	是	是
运行状况策略（仅限管理中心）	否	是	否	否	是	否	否	是	否
修改运行状况策略（仅限管理中心）	否	是	否	否	是	否	否	是	否
应用运行状况策略（仅限管理中心）	否	是	否	否	是	否	否	是	否
运行状况事件（仅限管理中心）	否	是	否	否	是	否	否	是	是
修改运行状况事件（仅限管理中心）	否	是	否	否	是	否	否	是	否
监控	否	是	否	否	是	是	是	是	否
审计	否	是	否	否	否	否	否	否	否

菜单	Access Admin	管理	Discovery Admin	入侵管理员	Maint User	网络管理员	Security Approver	安全分析师	Security Analyst (RO)
Modify Audit Log	否	是	否	否	否	否	否	否	否
系统日志	否	是	否	否	是	否	否	否	否
统计信息	否	是	否	否	是	否	否	否	否
工具	否	是	否	否	是	否	否	是	否
Backup Management	否	是	否	否	是	否	否	否	否
Restore Backup	否	是	否	否	是	否	否	否	否
安排	否	是	否	否	是	否	否	否	否
Delete Other Users' Scheduled Tasks	否	是	否	否	否	否	否	否	否
Import/Export	否	是	否	否	否	否	否	否	否
发现数据清除（仅限管理中心）	否	是	否	否	否	否	否	是	否
Whois（仅限 管理中心）	否	是	否	否	是	否	否	是	是

帮助菜单

Help 菜单及其权限可供所有用户角色访问。不能限制 Help 菜单选项。

管理用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

每个Firepower系统用户与一个或多个用户访问角色相关联。这些用户角色被分配的权限可确定对系统中菜单和其他选项的访问权限。例如，分析师需要访问事件数据以分析网络的安全性，但是可能无需访问 Firepower 系统本身的管理功能。您可以向分析师授予“安全分析师”(Security Analyst) 访问权限，同时为管理 Firepower 系统的一个或多个用户保留“管理员”(Administrator) 角色。

Firepower 系统系统提供 10 个专为各种管理员和分析师设计的预定义用户角色。这些预定义用户角色拥有一套预定的访问权限。

您还可以创建具有更精细访问权限的自定义用户角色。

也可以通过对用户角色应用受限搜索来限制该角色在事件查看器中可查看的数据。要创建具有受限访问权限的自定义角色，必须从“基于菜单的权限”(Menu Based Permissions) 列表中选择要限制的表，然后从“限制性搜索”(Restrictive Search) 下拉列表中选择专用的已保存搜索。

您无法删除预定义用户角色，但可以删除不再需要的自定义角色。如果要禁用自定义角色而不完全将其移除，可以改为将其停用。请注意，不能删除自己的用户角色或在平台设置策略中设置为默认用户角色的角色。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击**用户角色**选项卡。

步骤 3 管理用户角色：

- 激活 - 激活或停用预定义用户角色，如激活和停用用户角色，第 56 页中所述。
- 创建 - 创建自定义用户角色，如 中所述 创建自定义用户角色，第 57 页
- 复制 - 复制现有用户角色以创建新的自定义用户角色，如复制用户角色，第 58 页中所述。
- 编辑 - 编辑自定义用户角色，如编辑自定义用户角色，第 58 页中所述。
- 删除 - 点击要删除的自定义角色旁边的删除图标 ( )。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

注释 如果已删除的角色是分配给指定用户的唯一角色，则该用户可以登录并访问“用户首选项”(User Preferences) 菜单，但是无法以其他方式访问 Firepower 系统。

激活和停用用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

不能删除预定义用户角色，但是可以将其停用。停用角色会从已分配有该角色的任何用户从移除该角色和所有关联权限。

在多域部署中，系统会显示在当前域中创建的自定义用户角色，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义用户角色，您不可以对其进行编辑。要查看和编辑较低域中的自定义用户角色，请切换至该域。

注意 如果已停用的角色是分配给指定用户的唯一角色，则该用户可以登录并访问“用户首选项”(User Preferences) 菜单，但是无法以其他方式访问 Firepower 系统。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击**用户角色**选项卡。

步骤 3 点击要激活或停用的用户角色旁边的滑块。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

如果在具有某个角色的用户已登录时通过远端控制管理停用，然后重新启用该角色，或者在该用户的登录会话期间从备份恢复用户或用户角色，则该用户必须重新登录到Web 界面中才能重新获取对 IPMItool 命令的访问。

创建自定义用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击**用户角色**选项卡。

步骤 3 点击 **Create User Role**。

步骤 4 在**名称 (Name)** 字段中，输入新用户角色的名称。用户角色名称区分大小写。

步骤 5 或者，添加**说明 (Description)**。

步骤 6 为新角色选择基于菜单的权限。
选择权限时，会选择其所有子级，且多值权限使用第一个值。如果清除选择高级权限，则也会清除其所有子级。如果您选择权限但没有选择其所有子级，则权限以斜体文本显示。

复制要用作自定义角色基础的预定义用户角色将预先选择与该预定义角色关联的权限。

步骤 7 或者，通过选中或取消选中**外部数据库访问 (External Database Access)** 复选框设置新角色的数据库访问权限。

步骤 8 或者，在 Firepower 管理中心上，设置新用户角色的升级权限，如为升级配置自定义用户角色，第 60 页中所述。

步骤 9 点击**保存 (Save)**。

复制用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可以复制现有角色以用作新的自定义角色的基础。这会在 User Role Editor 中预先选择现有角色的权限，从而可以对角色进行相互建模。

您可以复制任何现有角色，包括从祖先域继承的预定义用户角色和自定义用户角色。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击**用户角色**选项卡。

步骤 3 点击要复制的用户角色旁边的复制图标 ( )。

步骤 4 在**名称 (Name)** 中输入新名称。
系统通过将原始角色的名称与 `(copy)` 后缀组合在一起，为新用户角色创建默认名称。

步骤 5 在**说明 (Description)** 中输入新说明。
如果不覆盖原始用户角色的说明，系统将保留该说明。

步骤 6 或者，修改从源用户角色继承的基于菜单的权限。
选择权限时，会选择其所有子级，且多值权限使用第一个值。如果清除选择高级权限，则也会清除其所有子级。如果您选择权限但没有选择其所有子级，则权限以斜体文本显示。

步骤 7 或者，通过选中或取消选中**外部数据库访问 (External Database Access)** 复选框设置新角色的数据库访问权限。

步骤 8 或者，设置新用户角色的升级权限，如为升级配置自定义用户角色，第 60 页中所述。

步骤 9 点击**保存 (Save)**。

编辑自定义用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

不能编辑预定义用户角色。

在多域部署中，系统会显示在当前域中创建的自定义用户角色，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义用户角色，您不可以对其进行编辑。要查看和编辑较低域中的自定义用户角色，请切换至该域。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击**用户角色**选项卡。

步骤 3 点击要修改的自定义用户角色旁边的编辑图标 ( )。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 修改**名称 (Name)** 和**说明 (Description)** 字段。用户角色名称区分大小写。

步骤 5 为用户角色选择基于菜单的权限。
选择权限时，会选择其所有子级，且多值权限使用第一个值。如果清除选择高级权限，则也会清除其所有子级。如果您选择权限但没有选择其所有子级，则权限以斜体文本显示。

步骤 6 或者，通过选中或取消选中**外部数据库访问 (External Database Access)** 复选框设置角色的数据库访问权限。

步骤 7 或者，在 Firepower 管理中心上，设置用户角色的升级权限，如为升级配置自定义用户角色，第 60 页中所述。

步骤 8 点击**保存 (Save)**。

用户角色升级

可以通过密码为自定义用户角色提供权限，以除基本角色的权限以外，暂时获取其他目标用户角色的权限。借此可以在用户缺勤期间将一个用户替换为另一个用户，或者更密切地跟踪高级用户权限的使用。

例如，其基本角色的权限非常有限的用户可以升级到 Administrator 角色以执行管理操作。可以配置此功能，以便用户可以使用其自己的密码，或者因此使用所指定的其他用户的密码。通过第二个选项，可以轻松管理所有适用用户的一个升级密码。

请注意，一次仅有一个用户角色可以是升级目标角色。可以使用自定义或预定义用户角色。每次升级持续时长为登录会话的持续时间，并会记录在审计日志中。

设置升级目标角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可以分配任何用户角色（预定义或自定义）来充当系统范围的升级目标角色。这是任何其他角色可升级到的角色（如果其有能力）。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 点击 **Configure Permission Escalation**。

步骤 4 从下拉列表中选择一个用户角色。

步骤 5 点击 **OK**，保存更改。

注释 更改升级目标角色立即生效。已升级会话中的用户现在具有新升级目标的权限。

为升级配置自定义用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

为自定义角色配置升级密码时，请考虑贵组织的需求。如果要轻松管理多个升级用户，可能需要选择其密码充当升级密码的其他用户。如果更改该用户的密码或停用该用户，则需要该密码的所有升级用户都会受影响。借此可以更高效地管理用户角色升级，尤其是在选择可以集中管理的外部身份验证用户的情况下。

过程

步骤 1 开始配置自定义用户角色，如创建自定义用户角色，第 57 页中所述。

步骤 2 在“系统权限”(System Permissions) 中，选择**设置此角色以升级至：(Set this role to escalate to:)** 复选框。
当前升级目标角色列于复选框旁边。

步骤 3 选择此角色用于升级的密码。此时您有两种选择：

- 如果希望具有此角色的用户在升级时使用其自己的密码，请选择**使用分配的用户密码进行身份验证 (Authenticate with the assigned user’s password)**。
- 如果希望具有此角色的用户使用其他用户的密码，请选择**使用指定的用户密码进行身份验证 (Authenticate with the specified user’s password)** 并输入该用户名。

  注释 在使用其他用户的密码进行验证时，可以输入任何用户名，甚至是已停用或不存在的用户的用户名。停用其密码用于升级的用户会使具有需要该密码的角色的用户无法升级。如有必要，可以使用此功能快速移除升级能力。

步骤 4 点击**保存 (Save)**。

具有此角色的用户现在可以升级到目标用户角色。

升级用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	任何环境	任何环境

当用户具有带升级权限的已分配自定义用户角色时，该用户可以随时升级到目标用户的权限。请注意，升级对用户首选项没有影响。

开始之前

- 确认系统管理员是否已配置升级目标角色或自定义用户角色进行升级，如设置升级目标角色，第 59 页或为升级配置自定义用户角色，第 60 页中所述。

过程

步骤 1 从用户名下的下拉列表中，选择**升级权限 (Escalate Permissions)**。

步骤 2 输入身份验证密码。

步骤 3 点击 **Escalate**。除当前角色以外，您现在具有升级目标角色的所有权限。

注释 升级持续至登录会话结束。要仅返回到基本角色的权限，必须注销，然后开始新会话。

用户帐户

管理员帐户以及 Firepower 管理中心或 Firepower 7000 和 8000 系列设备上的可选自定义用户帐户允许用户登录这些设备中。对于内部身份验证的用户，必须手动创建帐户。对于外部身份验证的用户，将会自动创建帐户。

管理用户帐户

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 管理用户帐户：

- 激活/停用 - 点击用户旁边的滑块以重新激活已停用的用户，或者禁用活动用户帐户而不将其删除。只能激活和停用内部身份验证用户。
- 创建 - 创建新用户帐户；请参阅创建用户帐户，第 62 页。
- 编辑 - 编辑现有用户帐户；请参阅编辑用户帐户，第 63 页。
- 删除 - 如果要删除用户，请点击删除图标( )。除无法删除的管理员帐户以外，可以随时从系统中删除用户帐户。

创建用户帐户

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

设置新用户帐户时，可以控制帐户能够访问的系统部分。可以在创建期间设置用户帐户的密码到期和强度设置。对于 7000 或 8000 系列设备上的本地帐户，还可以配置用户将具有的命令行访问级别。

在多域部署中，可以在已为您分配管理员访问权限的任何域中创建用户帐户。也可以在较高级别域中创建帐户并仅为用户分配较低级别访问权限。例如，您可能想让一位用户成为两个域的管理员，但要拒绝他们访问祖先域。只有切换到分配访问权限所在的子域才可以修改此类用户帐户。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **Create User**。

步骤 3 输入**用户名 (User Name)**。

步骤 4 修改登录选项；请参阅用户帐户登录选项，第 64 页。

步骤 5 在**密码 (Password)** 和**确认密码 (Confirm Password)** 中输入值。
必须根据您之前设置的密码选项来创建值。

步骤 6 如果您在 7000 或 8000 系列设备上创建用户帐户，请分配适合级别的**命令行界面访问权限 (Command-Line Interface Access)**，如命令行访问级别，第 66 页中所述。

步骤 7 分配用户角色：

- 选中或取消选中要分配用户的用户角色旁边的复选框。

- 在多域部署中，如果您将用户帐户添加到带有后代域的域中，请点击显示的**添加域 (Add Domains)**按钮而不是用户角色复选框。如在多个域中分配用户角色，第 63 页中所述继续操作。

注释　用户角色决定用户的访问权限。有关详细信息，请参阅管理用户角色，第 55 页。

步骤 8　点击**保存 (Save)**。

编辑用户帐户

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

将用户帐户添加到系统中后，可以随时修改访问权限、帐户选项或密码。请注意，密码管理选项不适用于向外部目录服务器身份验证的用户。请在外部服务器上管理这些设置。但是，必须配置所有帐户的访问权限，包括进行外部身份验证的帐户。

注释　对于外部身份验证用户，由于 LDAP 组或 RADIUS 列表成员身份或属性值，不能通过 Firepower 系统用户管理页面删除已分配有访问角色的用户的最低访问权限。但是，可以分配其他权限。修改外部身份验证用户的访问权限时，User Management 页面上的 Authentication Method 列提供状态 **External - Locally Modified**。

如果将用户的身份验证从外部身份验证更改为内部身份验证，则必须为该用户提供新密码。

过程

步骤 1　选择**系统 (System)** > **用户 (Users)**。

步骤 2　点击要修改的用户旁边的编辑图标 ( )。

步骤 3　修改创建用户帐户，第 62 页中所述的设置。

步骤 4　点击**保存 (Save)**。

在多个域中分配用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在多域部署中，可以在祖先域和后代域中分配用户角色。例如，可以在全局域中分配用户只读权限，但在后代域中分配管理员权限。

过程

步骤 1 在用户帐户编辑器中，点击**添加域 (Add Domain)**。

步骤 2 从**域 (Domain)** 下拉列表中选择域。

步骤 3 选中要为用户分配的用户角色。

步骤 4 点击**保存 (Save)**。

将用户从内部转换为外部身份验证

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

注释 将用户从内部身份验证转换为外部身份验证时，用户帐户会保留该帐户中已存在的权限。现有权限会覆盖与平台设置策略中的相关身份验证对象组或默认用户角色集相关联的任何权限。

开始之前

- 具有相同用户名的用户记录必须存在于外部身份验证服务器上。

过程

步骤 1 启用 LDAP（带有或不带 CAC）或 RADIUS 身份验证。有关详细信息，请参阅LDAP 身份验证，第 69 页或RADIUS 身份验证，第 91 页。

步骤 2 指示用户使用在外部服务器上为该用户存储的密码进行登录。

用户帐户登录选项

下表介绍可用于管理 Firepower 系统用户的密码和帐户访问权限的某些选项。

注释

- 密码管理选项不适用于向外部目录服务器进行身份验证的用户。请在外部身份验证服务器上管理这些设置。在启用**使用外部身份验证方法 (Use External Authentication Method)** 后，系统不显示密码管理选项。
- 如果在设备上启用 STIG 合规性或无人值守管理 (LOM)，则适用不同的密码限制。有关 STIG 合规性的详细信息，请参阅启用 STIG 合规性，第 463 页。

表 13: 用户帐户登录选项

选项	说明
Use External Authentication Method	如果希望此用户的凭证进行外部身份验证，请选择此复选框。如果启用此选项，则不再显示密码管理选项。 注释 • 为使用户向外部目录服务器进行身份验证，还必须为要使用的服务器创建身份验证对象，然后部署已启用身份验证的平台设置策略。 • 请注意，对于外部身份验证用户，如果禁用服务器的身份验证对象，则“用户”(Users) 列表中的**身份验证方法 (Authentication Method)** 列会显示**外部（已禁用）(External [Disabled])**。 • 如果为用户选择此选项，并且外部身份验证服务器不可用，则该用户可以登录到 Web 界面中，但无法访问任何功能。
最大登录失败次数	输入不含空格的整数，用于确定每个用户在登录尝试失败后且帐户锁定之前可以尝试的最大次数。默认设置为五次尝试；使用 0 允许失败登录数不受限制。
Minimum Password Length	输入不含空格的整数，用于确定用户密码的最小所需长度（以字符数为单位）。默认设置为 8。值为 0 指示无需最小长度。 如果启用**检查密码长度 (Check Password Strength)** 选项，并为**最小密码长度 (Minimum Password Length)** 设置超过 8 个字符的值，则更高的值适用。
Days Until Password Expiration	输入用户密码到期之前经过的天数。默认设置为 0，指示密码永不过期。如果设置此选项，则“用户”(Users) 列表的**密码生存期 (Password Lifetime)** 列指示每个用户的密码的剩余有效天数。
密码过期前警告天数	输入在用户密码实际到期之前警告用户必须更改其密码的警告天数。默认设置为 0 天。 注释 警告天数必须**小于**密码截止天数。
登录时强制重置密码	选择此选项可强制用户在下次登录时更改密码。

选项	说明
检查密码强度	选择此选项以要求设置强密码。强密码必须为至少八个大小写混合的字母数字字符，并且必须包含至少一个数字字符和一个特殊字符。它不能是字典中出现的单词或包含连续的重复字符。
Exempt from Browser Session Timeout	如果不希望用户的登录会话由于不活动而终止，请选择此选项。具有管理员角色的用户无法获得豁免。

命令行访问级别

可以使用 7000 或 8000 系列设备上的本地 Web 界面将命令行界面访问分配给本地设备用户。请注意，也可以在 NGIPSv 上为用户分配命令行访问，但是要从命令行界面使用命令。

用户可以运行的命令取决于分配给用户的访问级别。**命令行界面访问 (Command-Line Interface Access)** 设置的可能值包括：

无

用户无法在命令行上登录设备。当用户提供凭证时，用户启动的任何会话都将关闭。创建用户时，访问级别默认为 **None**。

配置

用户可以访问任何命令行选项。请谨慎将此访问级别分配给用户。

注意 向外部身份验证用户授予的外壳访问默认为 **Configuration** 级别的命令行访问，从而将权限授予所有命令行实用程序。

基本

用户可以运行一组特定的命令，如下所列。

表 *14*: 基本命令行命令

`configure password`	接口
`end`	`lcd`
`exit`	`link-state`
`help`	`log-ips-connection`
`history`	`managers`
`logout`	`memory`

?	model
??	mpls-depth
access-control-config	NAT
alarms	网络
arp-tables	network-modules
audit-log	ntp
bypass	perfstats
high-availability	portstats
cpu	power-supply-status
数据库	process-tree
device-settings	processes
disk	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	time
fastpath-rules	traffic-statistics
gui	版本
主机名	virtual-routers
hyperthreading	virtual-switches
inline-sets	

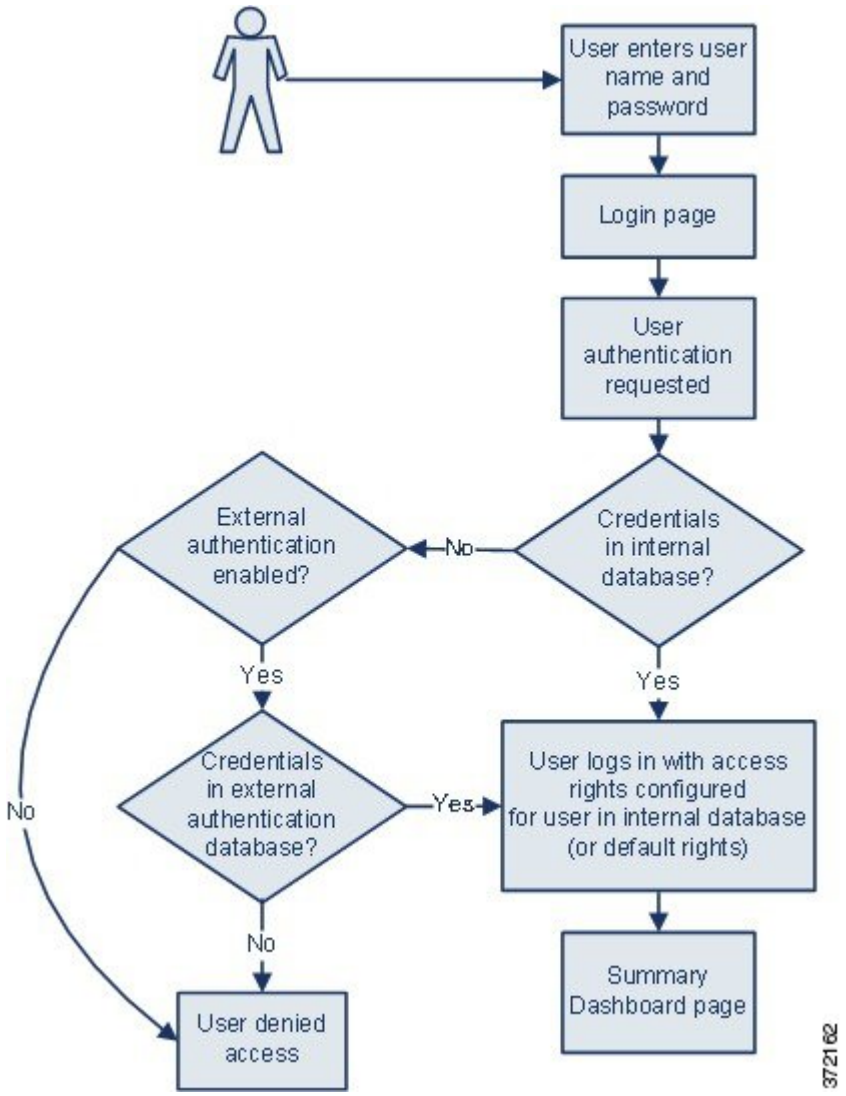
Firepower 系统用户身份验证

当用户登录 Firepower 管理中心或受管设备上的 Web 界面时，设备会在用户的本地列表中查找用户名和密码的匹配项。此过程称为身份验证。

有两种类型的身份验证：

- 内部身份验证 - 系统检查本地数据库的列表中是否存在该用户。
- 外部身份验证 - 系统检查本地数据库的列表中是否存在该用户，如果用户不存在于该列表中，则查询外部身份验证服务器以获取其用户列表。

身份验证过程在下方进行了展示。



当创建用户帐户时，您可以为该用户指定内部或外部身份验证。

内部身份验证

在内部身份验证中，将根据内部Firepower系统数据库中的记录验证用户凭证。这是默认的身份验证类型。

当您创建用户帐户时，将为内部身份验证用户设置访问权限。

注释 当内部身份验证用户转换为外部身份验证时，您无法将其恢复为内部身份验证。

外部身份验证

在外部身份验证中，Firepower管理中心或受管设备从外部服务器上的存储库检索用户凭证。外部服务器可以是轻量级目录访问协议(LDAP)目录服务器或远程身份验证拨入用户服务(RADIUS)身份验证服务器。

可通过平台设置策略和个人用户帐户设置来启用外部身份验证。只能为设备使用一种形式的外部身份验证。

当用户首次登录设备时，该设备通过创建本地用户记录将外部凭证与权限集相关联。系统根据以下任一条件向用户分配权限：

- 权限所属的组或访问列表
- 在设备的平台设置策略中设置的默认用户访问角色

如果通过组或列表成员身份授予权限，则无法修改这些权限。但是，如果默认情况下为其分配了用户角色，则可以在用户帐户中修改权限，并且进行的修改会覆盖默认设置。例如：

- 如果外部身份验证用户帐户的默认角色设置为特定访问角色，则用户可以使用其外部帐户凭证登录到设备中，而无需系统管理员进行任何其他配置。
- 如果帐户已进行外部身份验证并在默认情况下没有接收任何访问权限，则用户可以登录但无法访问任何功能。然后，您（或您的系统管理员）可以更改权限以授予对用户功能的适当访问。

不能通过Firepower系统界面管理外部身份验证用户的密码或停用外部身份验证用户。对于外部身份验证用户，由于 LDAP 组或 RADIUS 列表成员身份或属性值，不能通过 Firepower 系统用户管理页面删除已分配有访问角色的用户的最低访问权限。在外部身份验证用户的 Edit User 页面上，由于外部身份验证服务器上的设置而授予的权限以状态 **Externally Modified** 进行标记。

但是，可以分配其他权限。修改外部身份验证用户的访问权限时，User Management 页面上的 Authentication Method 列提供状态 **External - Locally Modified**。

LDAP 身份验证

通过LDAP（或轻量目录访问协议），可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置进行更改。

您必须在 Firepower 管理中心上创建 LDAP 身份验证对象，但可以在具备 Web 界面的任何受管设备上（即 7000 和 8000 系列设备上）使用外部身份验证对象，方法是将已启用此对象的平台设置策略部署到该设备。部署策略时，系统会将对象复制到设备上。

注释 在 7000 和 8000 系列设备上启用外部身份验证之前，请删除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

请注意，可以将 LDAP 命名标准用于地址规范以及用于身份验证对象中的过滤器和属性语法。有关详细信息，请参阅轻量目录访问控制协议 (v3) 中列出的 RFC：“Technical Specification, RFC 3377”（技术规范，RFC 3377）。本过程各处提供了语法示例。请注意，如果将身份验证对象设置为连接到 Microsoft Active Directory Server，可以在引用包含域的用户名时使用互联网 RFC 822（ARPA 互联网文本消息格式的标准）规范中记录的地址规范语法。例如，为引用用户对象，可能会在使用 Microsoft Active Directory Server 时键入 `JoeSmith@security.example.com` 而不是等效的用户基础可分辨名称 `cn=JoeSmith,ou=security, dc=example,dc=com`。

注释 当前，Firepower 系统在 LDAP 服务器（在 Windows Server 2008 上运行 Microsoft Active Directory，在 Windows Server 2008 上运行 Oracle Directory Server Enterprise Edition 7.0，或在 Linux 上运行 OpenLDAP）上支持 LDAP 外部身份验证。但是，Firepower 系统不支持 NGIPSv 或 ASA FirePOWER 设备的外部身份验证。

创建 LDAP 身份验证对象的必要信息

在配置与 LDAP 服务器的连接之前，应该收集创建 LDAP 身份验证对象所需的信息。

注释 您必须具有从本地设备对要连接的身份验证服务器进行 TCP/IP 访问的权限。

创建基本身份验证对象至少需要以下信息：

- 计划连接的服务器的服务器名称或 IP 地址
- 计划连接的服务器的服务器类型
- 具有浏览 LDAP 树的足够权限的用户帐户的用户名和密码；思科建议为此使用域管理员用户帐户
- 防火墙中用于允许传出连接的条目（如果设备和 LDAP 服务器之间存在防火墙）
- 用户名驻留所在的服务器目录的基础可分辨名称（如有可能）

提示 可以使用第三方 LDAP 客户端浏览 LDAP 树和查看基础 DN 和属性描述。还可以使用该客户端确认所选用户是否可以浏览选择的基础 DN。请求 LDAP 管理员为 LDAP 服务器推荐已批准的 LDAP 客户端。

根据计划如何定制高级 LDAP 身份验证对象配置，还可能需要下表中的信息。

表 *15*：其他 *LDAP* 配置信息

所需的操作…	您需要.....
通过除 389 以外的端口进行连接	端口号
通过加密连接进行连接	用于连接的证书
根据属性值过滤可以访问设备的用户	进行过滤所依据的属性-值对
使用一个属性作为UI访问属性，而不是检查用户可分辨名称	属性的名称
使用一个属性作为外壳登录属性，而不是检查用户可分辨名称	属性的名称
根据属性值过滤可以通过外壳访问设备的用户	进行过滤所依据的属性-值对
将组与特定用户角色关联	各组的可分辨名称以及组成员属性（如果组是静态组）或组成员 URL 属性（如果组是动态组）
使用 CAC 进行身份验证和授权	CAC、由发行 CAC 的同一 CA 签名的服务器证书，以及两个证书的证书链

CAC 身份验证

如果贵组织使用通用访问卡 (CAC)，则可以配置 LDAP 身份验证来对登录到 Web 界面中的用户进行身份验证，并根据组成员资格或默认访问权限来授权访问特定功能。在已配置CAC身份验证和授权的情况下，用户可以选择直接登录，而不用为设备提供单独的用户名和密码。

注释 您**必须**在浏览器中具有有效的用户证书（在这种情况下，即通过您的 CAC 传递至您的浏览器的证书），才能在CAC配置流程中启用用户证书。配置CAC身份验证和授权之后，网络上的用户**必须**在其浏览会话的持续时间内维持 CAC 连接。如果在会话期间移除或替换 CAC，则网络浏览器会终止该会话，并且系统会注销网络界面。

CAC 身份验证用户在系统中通过其电子数据交换个人标识符 (EDIPI) 号码进行识别。用户使用其 CAC 凭证首次登录后，可以在 User Management 页面上手动添加或移除这些用户的访问权限。如果未使用组控制的访问角色预配置用户的权限，则该用户仅具有平台设置策略中默认授予的权限。

提示 当系统在经过 CAC 身份验证的用户处于不活动状态 24 小时后从“用户管理”(User Management) 页面中将其清除时，将会清除手动配置的访问权限。每次后续登录后会将用户恢复到该页面，但是必须重新配置对其访问权限的所有手动更改。

配置 CAC 身份验证

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，但虚拟设备、 除外	任意	管理员/网络管理员

具有适当权限的用户必须完成CAC身份验证和授权的多步配置过程，然后网络上的用户才能使用其 CAC 凭证进行登录。

开始之前

- 收集创建 LDAP 身份验证对象的必要信息， 第 70 页中所述的信息。

过程

步骤 1 按照您的组织的指示插入 CAC。

步骤 2 将浏览器定向到 `https://hostname/`，其中 hostname 与 Firepower 管理中心的主机名对应。

步骤 3 如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

步骤 4 如有提示，请从下拉列表中选择相应的证书。

步骤 5 在“登录”(Login) 页面的**用户名 (Username)** 和**密码 (Password)** 字段中，以具备管理员权限的用户身份登录。用户名区分大小写。

提示 **不能**使用 CAC 凭证进行登录，直到已完全配置 CAC 身份验证和授权为止。

步骤 6 导航至**系统 (System)** > **用户 (Users)**，然后点击**外部身份验证 (External Authentication)** 选项卡。遵循创建高级 LDAP 身份验证对象， 第 76 页中的程序，专门为 CAC 身份验证和授权创建 LDAP 身份验证对象。必须配置以下内容：

- **LDAP-Specific Parameters** 部分的高级选项中的 **User Name Template**。
- **Attribute Mapping** 部分中的 **UI Access Attribute**。
- **组控制访问角色 (Group Controlled Access Roles)** 部分中现有 LDAP 组的可分辨名称（如果要通过 LDAP 组成员身份预配置访问权限）。

提示 请注意，**不能**在同一身份验证对象中配置 CAC 身份验证和外壳访问。如果还要授权用户访问外壳的权限，请创建并启用单独的身份验证对象。

步骤 7 点击**保存 (Save)**。

步骤 8 启用外部身份验证和 CAC 身份验证，如启用外部身份验证，第 489 页所述。

注意 所做的更改在应用系统策略之前**不会**生效。

步骤 9 导航至**系统 (System)** > **配置 (Configuration)**并点击 **HTTPS 证书 (HTTPS Certificate)**。如有必要，请遵循上传服务器证书，第 432 页中概括的过程导入 HTTPS 服务器证书。

注释 同一身份验证中心 (CA) **必须**在 CAC 上发行计划用于身份验证和授权的 HTTPS 服务器证书和用户证书。

步骤 10 在 **HTTPS 用户证书设置 (HTTPS User Certificate Settings)** 下，选择**启用用户证书 (Enable User Certificates)**。有关详细信息，请参阅需要有效的用户证书，第 433 页。

接下来的操作

- 在用户首次登录后，可以手动添加或删除用户的访问权限。如果没有修改权限，则用户仅具有默认授予的权限。有关详细信息，请参阅编辑用户帐户，第 63 页。

创建基本 LDAP 身份验证对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可以设置用于定制许多值的 LDAP 身份验证对象。但是，如果只希望对特定目录中的所有用户进行身份验证，则可以使用该目录的基础 DN 创建基本身份验证对象。如果将默认值设置为适用于服务器类型的默认值，并为用于从服务器检索用户数据的帐户提供身份验证凭证，则可以快速创建身份验证对象。请遵循以下步骤执行此操作。

注释 如果在创建身份验证对象（例如，以授予外壳访问权限）时首选考虑并可能自定义各身份验证设置，请使用高级程序创建对象。如果计划加密与服务器的连接，设置用户超时，自定义用户名模板或根据 LDAP 组成员身份分配 Firepower 系统用户角色，则也应使用高级程序。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

开始之前

- 收集创建 LDAP 身份验证对象的必要信息，第 70 页中所述的信息。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 从**身份验证方法 (Authentication Method)** 下拉列表中选择 **LDAP**。

步骤 5 在**名称 (Name)**、**说明 (Description)**、**服务器类型 (Server Type)** 和**主服务器主机名/IP 地址 (Primary Server Host Name/IP Address)** 中输入相应内容，如识别 LDAP 身份验证服务器，第 80 页中所述。

提示 如果点击“设置默认值”(Set Defaults)，系统会使用默认值填写**用户名模板 (User Name Template)**、**UI 访问属性 (UI Access Attribute)**、**外壳访问属性 (Shell Access Attribute)**、**组成员属性 (Group Member Attribute)** 和**组成员 URI 属性 (Group Member URL Attribute)** 字段。

步骤 6 选择**获取 DN (Fetch DNs)** 以指定基本可分辨名称，以及提供**基本过滤器 (Base Filter)**（可选），如配置 LDAP 特定参数，第 83 页中所述。

步骤 7 输入可分辨名称作为具有足够凭证来浏览 LDAP 服务器的用户的**用户名 (User Name)** 和**密码 (Password)**，如配置 LDAP 特定参数，第 83 页中所述。

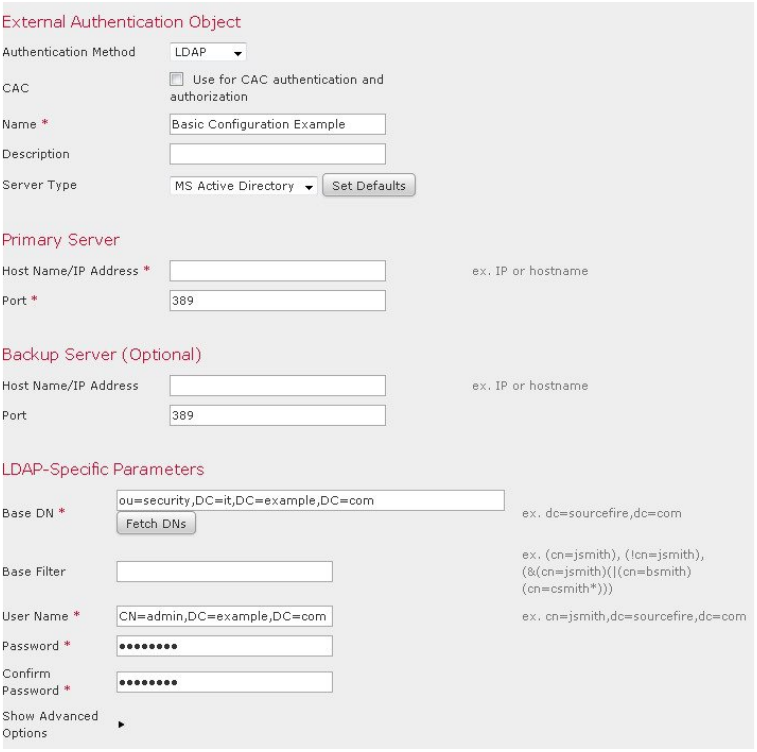
步骤 8 在**确认密码 (Confirm Password)** 字段中重新输入密码。

步骤 9 测试连接，如测试 LDAP 身份验证连接，第 89 页中所述。

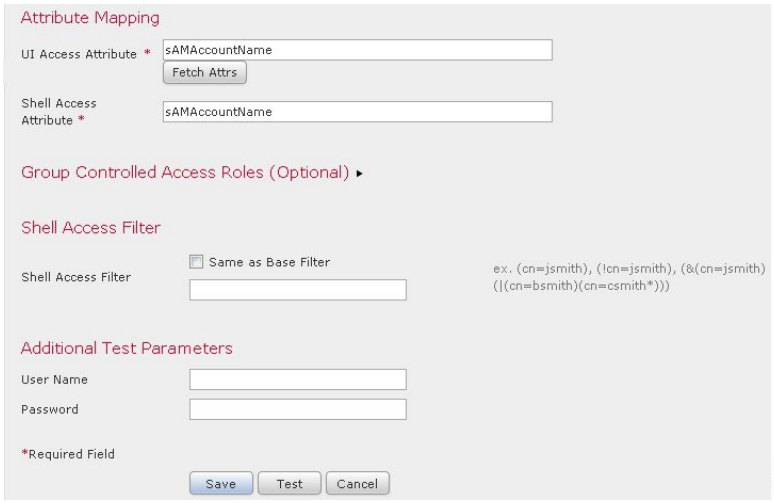
步骤 10 点击**保存 (Save)**。

示例

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。



此示例显示对于 Example 公司的信息技术领域中的 Security 组织使用基本可分辨名称 `OU=security,MC=it,MC=example,MC=com` 的连接。



但是，由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。选择 MS Active Directory 服务器类型并点击**设置默认值 (Set Defaults)** 会将“UI 访问属性”(UI Access Attribute) 设置为 `sAMAccountName`。因此，当用户尝试登录 Firepower 系统时，Firepower 系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的外壳帐户中时，Shell Access Attribute 为 `sAMAccountName` 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

请注意，由于未对此服务器应用基本过滤器，因此Firepower系统会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

接下来的操作

- 如果要启用 LDAP 身份验证，请启用身份验证对象，如启用外部身份验证，第 489 页中所述。
- 如果要优化检索到的用户列表，请参阅LDAP 身份验证连接故障排除，第 90 页以了解详细信息。

创建高级 LDAP 身份验证对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

创建基本身份验证对象时，可定义用于连接到身份验证服务器的基本设置。创建高级身份验证对象时，可定义基本设置，还可以选择要用于从服务器检索用户数据的目录情景和搜索条件。或者，可以配置外壳访问身份验证。

尽管可以使用服务器类型的默认设置快速设置 LDAP 配置，但也可以定制高级设置，以控制设备是否与 LDAP 服务器建立加密连接，连接超时，以及服务器会检查哪些属性来获取用户信息。

对于特定于 LDAP 的参数，可以使用 LDAP 命名标准和过滤器及属性语法。有关详细信息，请参阅轻量目录访问控制协议 (v3) 中列出的 RFC：“Technical Specification, RFC 3377”（技术规范，RFC 3377）。本过程各处提供了语法示例。请注意，如果将身份验证对象设置为连接到 Microsoft Active Directory Server，可以在引用包含域的用户名时使用互联网 RFC 822（ARPA 互联网文本消息格式的标准）规范中记录的地址规范语法。例如，为引用用户对象，可能会在使用 Microsoft Active Directory Server 时输入 `JoeSmith@security.example.com` 而不是等效的用户基本可分辨名称 `cn=JoeSmith,ou=security, dc=example,dc=com`。

注释 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，**请勿**移除在计算机中插入的 CAC。启用用户证书后，**必须**一直插入 CAC。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

开始之前

- 收集创建 LDAP 身份验证对象的必要信息，第 70 页中所述的信息。
- 请删除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 识别验证服务器，如识别 LDAP 身份验证服务器，第 80 页中所述。

步骤 5 配置身份验证设置，如配置 LDAP 特定参数，第 83 页中所述。

步骤 6 或者，配置 LDAP 组以用作默认访问角色分配的基础，如按组配置访问权限，第 86 页中所述。

提示 如果计划将此对象用于 CAC 身份验证和授权，思科建议配置 LDAP 组以管理访问角色分配。

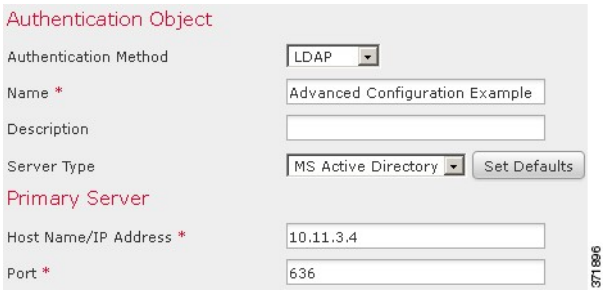
步骤 7 或者，配置外壳访问的身份验证设置，如配置 LDAP 外壳访问，第 87 页中所述。

步骤 8 测试配置，如测试 LDAP 身份验证连接，第 89 页中所述。

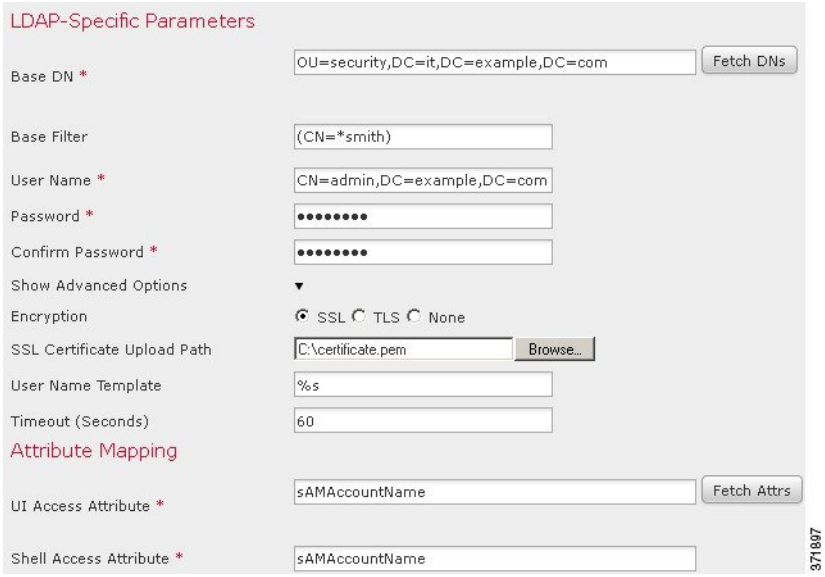
步骤 9 点击**保存 (Save)**。

示例

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。



此示例显示对于 Example 公司的信息技术领域中的 Security 组织使用基本可分辨名称 `OU=security,MC=it,MC=example,MC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。过滤器将从服务器检索的用户限制为具有以 `smith` 结尾的常见名称的用户。

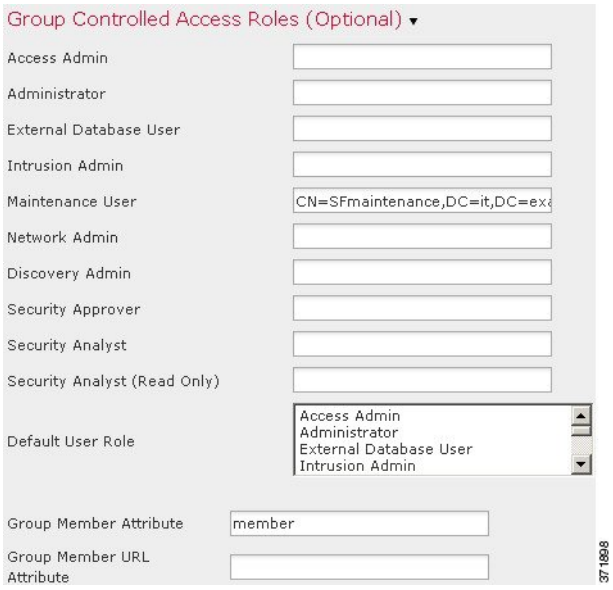


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于 **Timeout** 设置，与服务器的连接在 60 秒后将超时。

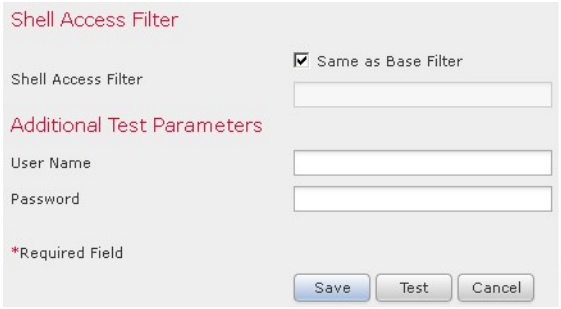
由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。请注意，配置包括 UI Access Attribute `sAMAccountName`。因此，当用户尝试登录 Firepower 系统时，Firepower 系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的外壳帐户中时，Shell Access Attribute 为 `sAMAccountName` 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

此示例还具有相应的组设置。“维护用户”(Maintenance User) 角色会自动分配给具有 `member` 组属性且基本域名为 `CN=SFmaintenance,MC=it,MC=example,MC=com` 的组的所有成员。



外壳访问过滤器设置为基本过滤器相同，因此相同用户可以通过外壳访问设备，如同通过Web 界面进行访问一样。



接下来的操作

- 如果要启用 LDAP 身份验证，请启用启用外部身份验证，第 489 页中的身份验证对象。

LDAP 身份验证服务器字段

CAC

如果要使用 CAC 进行身份验证和授权，请选中此复选框。

Name

身份验证服务器的名称。

说明

身份验证服务器的说明。

服务器类型

计划连接的 LDAP 服务器的类型。选择一个类型时，您有以下选择：

- 如果是连接到 Microsoft Active Directory Server，请选择 **MS Active Directory**。
- 如果是连接到 Sun Java Systems Directory Server 或 Oracle Directory Server，请选择 **Oracle Directory**。
- 如果是连接到 OpenLDAP 服务器，请选择 **OpenLDAP**。
- 如果是连接到除上述所列以外的 LDAP 服务器并要清除默认设置，请选择**其他 (Other)**。

提示 如果点击“设置默认值”(Set Defaults)，系统会使用默认值填写**用户名模板 (User Name Template)**、**UI 访问属性 (UI Access Attribute)**、**外壳访问属性 (Shell Access Attribute)**、**组成员属性 (Group Member Attribute)** 和**组成员 URI 属性 (Group Member URL Attribute)** 字段。

主服务器主机名/IP 地址 (Primary Server Host Name/IP Address)

要在其中获取身份验证数据的主服务器的 IP 地址或主机名。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

主服务器端口 (Primary Server Port)

主身份验证服务器使用的端口。

备用服务器主机名/IP 地址 (Backup Server Host Name/IP Address)

要在其中获取身份验证数据的备用服务器的 IP 地址或主机名。

备用服务器端口 (Backup Server Port)

备用身份验证服务器使用的端口。

识别 LDAP 身份验证服务器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

创建身份验证对象时，首先指定希望受管设备或Firepower管理中心连接以进行身份验证的主服务器和备用服务器及服务器端口。

注释 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，**请勿**移除在计算机中插入的 CAC。启用用户证书后，**必须**一直插入 CAC。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 从**身份验证方法 (Authentication Method)** 下拉列表中选择 **LDAP**。

步骤 5 或者，如果计划将此身份验证对象用于 CAC 身份验证和授权，请选择 **CAC** 的对应复选框。

注释 必须遵循配置 CAC 身份验证，第 72 页中的程序，以完全配置 CAC 身份验证和授权。

步骤 6 在**名称 (Name)** 和**说明 (Description)** 字段中输入身份验证服务器的名称和说明。

步骤 7 从下拉列表中选择**服务器类型 (Server Type)**，如LDAP 身份验证服务器字段，第 79 页中所述。或者，点击**设置默认值 (Set Defaults)**。

步骤 8 输入**主服务器主机名/IP 地址 (Primary Server Host Name/IP Address)**。

注释 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 9 或者，输入**主服务器端口 (Primary Server Port)**。

步骤 10 或者，输入**备用服务器主机名/IP 地址 (Backup Server Host Name/IP Address)**。

步骤 11 或者，输入**备用服务器端口 (Backup Server Port)**。

接下来的操作

- 继续创建 LDAP 身份验证对象，如创建高级 LDAP 身份验证对象，第 76 页中所述。

LDAP 特定字段

下表描述每个特定于 LDAP 的参数。

表 *16*: *LDAP* 特定参数

设置	说明	示例
Base DN	提供设备搜索有关LDAP服务器的用户信息所在的目录的基础可分辨名称。 通常，基础 DN 具有指示公司领域和运营单位的基础结构。 请注意，识别主服务器之后，可以从该服务器自动检索可用基础 DN 列表并选择相应的基础 DN。	例如，Example 公司的 Security 部门的基础 DN 可能为 `ou=security, dc=example,dc=com`
Base Filter	通过仅检索基础 DN 中具有过滤器中设置的属性-值对的对象来专注搜索。基本过滤器是要用作过滤器的属性类型、比较运算符和属性值（用括号括起来）。	要仅对具有以 F 开头的公共名称的用户进行过滤，请使用过滤器 `(cn=F*)`。
User Name/ Password	允许本地设备访问用户对象。为对于要检索的身份验证对象具有适当权限的用户提供用户凭证。所指定用户的可分辨名称对于LDAP服务器的目录信息树必须唯一。与 Microsoft Active Directory Server 关联的服务器用户名不能以字符 `$` 结尾。	Example 公司的 Security 部门中 `admin` 用户的用户名可能为 `cn=admin, ou=security, dc=example,dc=com`

设置	说明	示例
加密	确定通信是否加密及如何加密。可以选择不加密、传输层安全 (TLS) 或安全套接字层 (SSL) 加密。请注意，如果在通过 TLS 或 SSL 进行连接时使用证书进行身份验证，则证书中 LDAP 服务器的名称**必须**与您提供的**用户名**匹配。 如果在指定端口后更改加密方法，则端口重置为所选服务器类型的默认值。	如果在外部身份验证设置中输入 `10.10.10.250`，并在证书中输入 `computer1. example.com`，则连接失败，即使 `computer1. example.com` 的 IP 地址为 `10.10.10.250` 时也是如此。将外部身份验证设置中的服务器名称更改为 `computer1. example.com` 可成功连接。
SSL Certificate Upload Path	指示本地计算机上要用于加密的证书的路径。	`c:/server.crt`
User Name Template	通过将字符串转换字符 (`%s`) 映射到用户的 **UI 访问属性 (UI Access Attribute)** 值，指示应如何格式化在登录时输入的用户名。用户名模板是用于身份验证的可分辨名称的格式。当用户将用户名输入到登录页面中时，设备会将名称替换为字符串转换字符，并使用产生的可分辨名称搜索用户凭证。 如果要将此对象用于 CAC 身份验证和授权，**必须**输入**用户名模板 (User Name Template)**。	`%s@security.example.com`、 `%s@mail.com`、 `%s@mil`、 `% s@smil.mil`、
Timeout	为对主服务器进行的连接尝试设置超时，以使连接滚动转移到备份服务器。如果在经过此字段中指示的秒数（或 LDAP 服务器上的超时）后主身份验证服务器没有响应，则设备将查询备份服务器。 但是，如果 LDAP 是在主 LDAP 服务器的端口上运行，并且因某种原因而拒绝服务请求，则不会故障转移到备份服务器。	如果主服务器已禁用 LDAP，则设备将查询备份服务器。
UI Access Attribute	告知本地设备与特定属性的值而不是用户可分辨名称值匹配。如果属性的值是 Firepower 系统 Web 界面的有效用户名，则可以使用任何属性。如果其中一个对象具有匹配的用户名和密码，表明用户登录请求已进行身份验证。 选择服务器类型并设置默认值将会使用通常适合于该类型的服务器的值预填充 **UI Access Attribute**。 如果将此字段留空，则本地设备会检查 LDAP 服务器上各用户记录的用户可分辨名称值，以查看其是否与用户名匹配。 如果要将此对象用于 CAC 身份验证和授权，**必须**输入与**用户名模板 (User Name Template)** 值对应的值。	`sAMAccountName`、 `userPrincipalName`、 邮件

配置 LDAP 特定参数

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

特定于 LDAP 的参数部分中的设置确定设备搜索用户名所在的 LDAP 目录区域，并且控制有关设备如何连接到 LDAP 服务器的详细信息。

有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。

此外对于大多数特定于 LDAP 的设置而言，可以使用 LDAP 命名标准和过滤器及属性语法。有关详细信息，请参阅轻量目录访问控制协议 (v3) 中列出的 RFC：“Technical Specification, RFC 3377”（技术规范，RFC 3377）。本过程各处提供了语法示例。请注意，如果将身份验证对象设置为连接到 Microsoft Active Directory Server，可以在引用包含域的用户名时使用互联网 RFC 822（ARPA 互联网文本消息格式的标准）规范中记录的地址规范语法。例如，为引用用户对象，可能会在使用 Microsoft Active Directory Server 时输入 `JoeSmith@security.example.com` 而不是等效的用户基本可分辨名称 `cn=JoeSmith,ou=security, dc=example,dc=com`。

注释 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，**请勿**移除在计算机中插入的 CAC。启用用户证书后，**必须**一直插入 CAC。

过程

步骤 1 在“创建外部身份验证对象”(Create External Authentication Object) 页面的 **LDAP 特定参数 (LDAP-Specific Parameters)** 部分中，有两个用于设置基本 DN 的选项：

- 点击**获取 DN (Fetch DNs)**，然后从下拉列表中选择相应的基本可分辨名称。
- 在**基本 DN (Base DN)** 字段中输入要访问的 LDAP 目录的基本可分辨名称。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。

步骤 2 或者，输入**基本过滤器 (Base Filter)**。

示例：
例如，如果目录树中的用户对象具有 physicalDeliveryOfficeName 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。

步骤 3 输入一个可分辨名称作为有足够凭证浏览 LDAP 服务器的用户的**用户名 (User Name)** 和**密码 (Password)**。

示例：

例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司的 Security 部门中管理员的对象的 `uid` 值为 `NetworkAdmin`，则可能会输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

注意 如果是连接到 Microsoft Active Directory Server，则不能提供以 `$` 字符结尾的服务器用户名。

步骤 4 在**确认密码 (Confirm Password)** 字段中重新输入密码。

步骤 5 配置特定于 LDAP 的基本参数后，有若干选项：

- 要访问高级选项，请点击 **Show Advanced Options** 旁边的箭头并继续执行下一步。
- 如果要根据 LDAP 组成员资格配置用户默认角色，请进入下一节按组配置访问权限，第 86 页。
- 如果不是使用 LDAP 组进行身份验证，请进入下一节配置 LDAP 外壳访问，第 87 页。

步骤 6 或者，为 LDAP 连接选择**加密 (Encryption)** 模式。

注释 请注意，如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于 None 或 TLS，端口使用默认值 389。如果选择 SSL 加密，则端口使用默认值 636。

步骤 7 如果选择 TLS 或 SSL 加密并且要使用证书进行身份验证，请点击**浏览 (Browse)** 以浏览至有效 TLS 或 SSL 证书的位置。

注释 如果之前已上传证书并要将其替换，请上传新证书并将配置重新部署到设备来复制转移新证书。

步骤 8 或者，提供与 **UI 访问属性 (UI Access Attribute)** 对应的**用户名模板 (User Name Template)**。

示例：

例如，要通过连接到 UI 访问属性为 `uid` 的 OpenLDAP 服务器来对 Example 公司的 Security 组织中工作的所有用户进行身份验证，可能会在**用户名模板 (User Name Template)** 字段中输入 `uid=%s,ou=security,dc=example,dc=com`。对于 Microsoft Active Directory Server，可以输入 `%s@security.example.com`。

注释 如果要使用 CAC 凭证进行身份验证和授权，**必须**在 **User Name Template** 字段中输入值。

步骤 9 或者，在**超时 (Timeout)** 字段中，输入在滚动到备份连接之前应经过的秒数。

步骤 10 或者，要根据属性而不是 Base DN 和 Base Filter 检索用户，有两个选项：

- 点击**获取属性 (Fetch Attrs)** 以检索可用属性的列表，然后选择相应的属性。
- 输入 **UI 访问属性 (UI Access Attribute)**。例如，在 Microsoft Active Directory Server 上，可能要使用 UI Access Attribute 检索用户，因为在 Active Directory Server 用户对象上可能没有 `uid` 属性。相反，可以通过在 **UI Access Attribute** 字段中键入 `userPrincipalName` 来搜索 `userPrincipalName` 属性。

注释 如果要使用 CAC 凭证进行身份验证和授权，**必须**在 **User Access Attribute** 字段中输入值。

接下来的操作

- 继续创建 LDAP 身份验证对象，如创建高级 LDAP 身份验证对象，第 76 页中所述。

LDAP 组字段

引用的任何组都必须存在于 LDAP 服务器上。可以引用静态 LDAP 组或动态 LDAP 组。静态 LDAP 组是成员资格由指向特定用户的组对象属性确定的组，动态 LDAP 组是通过创建根据用户对象属性检索组用户的 LDAP 搜索来确定成员资格的组。角色的组访问权限仅影响身为组成员的用户。

用户登录 Firepower 系统中时授予的访问权限取决于 LDAP 配置：

- 如果没有为 LDAP 服务器配置组访问权限，则在新用户登录时，Firepower 系统会利用 LDAP 服务器对用户进行身份验证，然后根据平台设置策略中设置的默认最低访问角色授予用户权限。
- 如果配置任何组设置，则属于指定组的新用户将继承其所属的组的最低访问设置。
- 如果新用户不属于任何指定组，则会为用户分配在身份验证对象的 Group Controlled Access Roles 部分中指定的默认最低访问角色。
- 如果用户属于多个已配置组，则用户会接收具有最高访问的组的访问角色作为最低访问角色。

由于 LDAP 组成员身份，不能使用 Firepower 系统用户管理页面删除已分配到访问角色的用户的最低访问权限。但是，可以分配其他权限。修改外部身份验证用户的访问权限时，User Management 页面上的 Authentication Method 列提供状态 **External - Locally Modified**。

注释 如果使用动态组，则完全按照 LDAP 查询在 LDAP 服务器上的配置来使用 LDAP 查询。因此，Firepower 系统将搜索的递归数限制为 4，以防止搜索语法错误导致无限循环。如果在这些递归中未建立用户的组成员资格，则会向用户授予 Group Controlled Access Roles 部分中定义的默认访问角色。

Firepower 系统用户角色 (Firepower System User Roles)

包含应分配有每个用户角色的用户的 LDAP 组的可分辨名称。

默认用户角色 (Default User Role)

不属于任何指定组的用户的默认最低访问角色。

组成员属性 (Group Member Attribute)

在静态组中包含 LDAP 搜索字符串的 LDAP 属性。

组成员 URL 属性 (Group Member URL Attribute)

在动态组中指定成员身份的 LDAP 属性

按组配置访问权限

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果首选将默认访问权限基于 LDAP 组中的用户成员身份，则可以为 Firepower 系统使用的各访问角色指定 LDAP 服务器上现有组的可分辨名称。执行此操作时，可以为 LDAP 检测到的不属于任何指定组的用户配置默认访问设置。当用户登录时，Firepower 系统会动态检查 LDAP 服务器并根据用户的当前组成员身份分配默认访问权限。

如果不使用组控制的访问角色配置用户的权限，则用户仅具有平台设置策略中默认授予的权限。

如果计划将对象用于 CAC 身份验证和授权，则思科建议配置 LDAP 组以管理经过 CAC 身份验证的用户的访问角色分配。

注释 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，**请勿**移除在计算机中插入的 CAC。启用用户证书后，**必须**一直插入 CAC。

开始之前

- 确认计划引用的组是否存在于 LDAP 服务器上。

过程

步骤 1 在 Create External Authentication Object 页面上，点击 **Group Controlled Access Roles** 旁边的向下箭头。

步骤 2 或者，在与 Firepower 系统用户角色对应的 **DN** 字段中，输入包含应向其分配这些角色的用户的 LDAP 组的可分辨名称。

示例：
例如，可能会在**管理员 (Administrator)** 字段中输入以下内容来对 `Example` 公司的信息技术部门中的名称进行身份验证：

```
cn=itgroup,ou=groups, dc=example,dc=com
```

步骤 3 选择**默认用户角色 (Default User Role)**。

步骤 4 如果使用静态组，请输入**组成员属性 (Group Member Attribute)**。

示例：
例如，如果 `member` 属性用于指示为默认“安全分析师”(Security Analyst) 访问权限引用的静态组中的成员身份，请输入 `member`。

步骤 5 如果使用动态组，请输入**组成员 URL 属性 (Group Member URL Attribute)**。

示例：
例如，如果 `memberURL` 属性包含用于检索为默认“管理员”(Admin) 访问权限指定的动态组的成员的 LDAP 搜索，请输入 `memberURL`。

接下来的操作

- 继续创建 LDAP 身份验证对象，如创建高级 LDAP 身份验证对象，第 76 页中所述。

LDAP 外壳访问字段

除管理员帐户以外，外壳访问完全通过所设置的外壳访问属性进行控制。所设置的外壳访问过滤器确定 LDAP 服务器上可登录到外壳中的用户集。

请注意，各外壳用户的主目录是在登录时创建的，并且禁用 LDAP 外壳访问用户帐户后（通过禁用 LDAP 连接），该目录仍然保留，但是用户外壳在 `/etc/password` 中设置为 `/bin/false` 以禁用外壳。如果之后重新启用用户，则会使用同一主目录重置外壳。

外壳用户可以使用小写、大写或大小写字母混合的用户名进行登录。外壳的登录身份验证区分大小写。

Shell Access Attribute

要用于过滤的访问属性。如果属性的值是外壳访问的有效用户名，则可以使用任何属性。

如果将此字段留空，则用户可分辨名称用于外壳访问身份验证。

提示 选择服务器类型并设置默认值将会使用通常适合于该类型的服务器的属性预填充此字段。

外壳访问过滤器 (Shell Access Filter)

要用于检索外壳访问的管理用户条目的属性值。过滤器是属性名称、比较操作符和属性值。

如果基础 DN 中限定的所有用户也有资格获取外壳访问权限，则通过 **Same as Base Filter** 复选框可更高效地进行搜索。通常，用来检索用户的LDAP查询会将基本过滤器与外壳访问过滤器进行组合。如果外壳访问过滤器与基本过滤器相同，则同一查询会运行两次，从而不必要地耗时。可以使用 **Same as Base Filter** 选项仅运行一次查询来实现两个目的。

如果将此字段留空，则可以阻止对外壳访问的 LDAP 身份验证。

配置 LDAP 外壳访问

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

还可以使用 LDAP 服务器对受管设备或Firepower管理中心上的外壳访问帐户进行身份验证。指定用于为要向其授予外壳访问的用户检索条目的搜索过滤器。

请注意，**不能**在同一身份验证对象中配置CAC身份验证和授权及外壳访问。相反，请创建并启用单独的身份验证对象。

外壳访问的身份验证对象必须是 Firepower 管理中心上的第一个身份验证对象。

思科不支持 NGIPSv 设备的外部身份验证。此外，外壳访问身份验证不支持 IPv6。

注意 在物理 Firepower 管理中心上，所有外壳用户都具有 `sudoers` 权限。请确保适当地限制具有外壳访问的用户列表。在 7000 和 8000 系列和 NGIPSv 设备上，授予外部身份验证用户的外壳访问权限默认为**配置 (Configuration)** 级别的命令行访问权限，它还授予 `sudoers` 权限。

请注意，**不能**在同一身份验证对象中配置 CAC 身份验证和授权及外壳访问。选中 **CAC** 复选框会禁用页面上的外壳访问配置选项。相反，请创建并启用单独的身份验证对象。

开始之前

- 请删除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

过程

步骤 1 在“创建外部身份验证对象”(Create External Authentication Object) 页面上，如果要使用除用户可分辨以外的外壳访问属性，请键入**外壳访问属性 (Shell Access Attribute)**。

示例：
例如，在 Microsoft Active Directory Server 上，通过在**外壳访问属性 (Shell Access Attribute)** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` 外壳访问属性检索外壳访问用户。

步骤 2 设置外壳访问帐户过滤器。您有多个选择：

- 要根据属性值检索管理用户条目，请在**外壳访问过滤器 (Shell Access Filter)** 字段中输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。
- 要使用配置身份验证设置时指定的同一过滤器，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 要防止对外壳访问进行 LDAP 身份验证，请将此字段留空。

接下来的操作

- 继续创建 LDAP 身份验证对象，如创建高级 LDAP 身份验证对象，第 76 页中所述。

测试 LDAP 身份验证连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在配置 LDAP 服务器和身份验证设置后，可以为应该能够进行身份验证以测试这些设置的用户指定用户凭证。

对于**用户名 (User Name)**，可以为要进行测试的用户输入 `uid` 属性的值。如果是连接到 Microsoft Active Directory Server 并提供 UI 访问属性来代替 `uid`，请使用该属性的值作为用户名。还可以为用户指定完全限定的可分辨名称。

为该用户输入**密码 (Password)**。

测试输出列出有效和无效的用户名。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。

请注意，由于网络界面页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅返回 1000 个用户。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。请首先测试没有其他测试参数的服务器配置。如果成功，请提供要通过特定用户进行测试的用户名和密码。

过程

步骤 1 在“添加外部身份验证对象”(Add External Authentication Object) 页面上，输入**用户名 (Username)** 和**密码 (Password)**。

示例：
例如，要测试以了解是否可以在 Example 公司检索 `JSmith` 用户凭证，请输入 `JSmith` 和 `password`。

步骤 2 点击 **Test**。此时您有两种选择：

- 如果测试成功，则页面底部会显示测试输出。点击**保存 (Save)**。
- 如果测试失败，请参阅LDAP 身份验证连接故障排除，第 90 页，以获取有关对连接进行故障排除的建议。

接下来的操作

- 如果要启用 LDAP 身份验证，请启用身份验证对象，如启用外部身份验证，第 489 页中所述。

LDAP 身份验证连接故障排除

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效。

  检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基础可分辨名称中指示的目录。

  检查用户名对于 LDAP 服务器的目录信息树是否唯一。

  如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用向服务器身份验证，以了解通过该连接进行的绑定是否也失败。

- 检查是否已正确识别服务器：

  检查服务器 IP 地址或主机名是否正确。

  检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问。

  检查对服务器的访问是否未被防火墙阻止，以及已在对象中配置的端口是否打开。

  如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。

  如果是对外壳访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。

  如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击 **Set Defaults** 以重置默认值。

- 如果键入了基础可分辨名称，请点击 **Fetch DNs** 以检索服务器上的所有可用基础可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。
- 如果使用的是基本过滤器或外壳访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符。
- 要测试受限更多的基本过滤器，请尝试将其设置为基础可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：

  检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。

  检查是否未对加密服务器连接使用 IPv6 地址。

- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过要从中进行连接的设备上的命令行使用以下语法连接到 LDAP 服务器来测试所使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

例如，如果是尝试使用 `domainadmin@myrtle.example.com` 用户和基本过滤器 (`cn=*`) 连接到 `myrtle.example.com` 上的安全域，则可以使用以下语句测试连接：

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

如果可以成功测试连接，但在部署平台设置策略后身份验证不起作用，请检查在应用到设备的系统策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或外壳访问过滤器，或者使用限制较多或较少的基本 DN。

RADIUS 身份验证

远程身份验证拨入用户服务 (RADIUS) 是用于身份验证、授权和阐释对网络资源的用户访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

在 RADIUS 服务器上进行身份验证的用户首次登录时，该用户会接收在身份验证对象中为其指定的角色。如果没有为任何用户角色列出该用户，则会接收在身份验证对象中选择的默认访问角色。如果在身份验证对象中未选择默认访问角色，则会接收在平台设置策略中设置的默认访问角色。除非通过身份验证对象中的用户列表对设置进行授权，否则在需要时可以修改用户的角色。请注意，在 RADIUS 服务器上使用属性匹配进行身份验证的用户首次尝试登录时，会因已创建该用户帐户而被拒绝登录。用户必须再次登录。

注释 在 7000 或 8000 系列设备上启用外部身份验证之前，请删除与外壳访问过滤器中包含的外部身份验证用户具有相同用户名的所有内部身份验证外壳用户。

RADIUS 的 Firepower 系统实施支持使用 SecurID® 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并在其登录到思科系统中时将此代码用作其密码。只要 SecurID 正确配置为在 Firepower 系统外部对用户进行身份验证，这些用户即可使用其 PIN 以及 SecurID 令牌登录到 Firepower 管理中心或 7000 或 8000 系列设备中，而无需在设备上进行任何其他配置。

创建 RADIUS 身份验证对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

创建 RADIUS 身份验证对象时，可定义用于连接到身份验证服务器的设置。另外将用户角色授予特定用户和默认用户。如果 RADIUS 服务器为计划进行身份验证的任何用户返回自定义属性，必须定义这些自定义属性。或者，也可以配置外壳访问身份验证。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

开始之前

- 确认您具有从本地设备对要连接的身份验证服务器进行 TCP/IP 访问的权限。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 从**身份验证方法 (Authentication Method)** 下拉列表中选择 **RADIUS**。

步骤 5 识别验证服务器，如配置 RADIUS 连接设置，第 94 页中所述。

步骤 6 配置用户角色，如配置 RADIUS 用户角色，第 96 页中所述。

步骤 7 或者，配置外壳访问，如配置 RADIUS 外壳访问，第 97 页中所述。

步骤 8 或者，定义自定义属性，如定义自定义 RADIUS 属性，第 98 页中所述。

步骤 9 测试配置，如测试 RADIUS 身份验证连接，第 99 页中所述。

示例

下图说明 IP 地址为 10.10.10.98 的运行 FreeRADIUS 的服务器的样本 RADIUS 登录身份验证对象。请注意，连接使用端口 1812 进行访问，并请注意，与服务器的连接在停用 30 秒后将超时，然后重试三次后会尝试连接到备份身份验证服务器。

此示例说明 RADIUS 用户角色配置的重要方面：

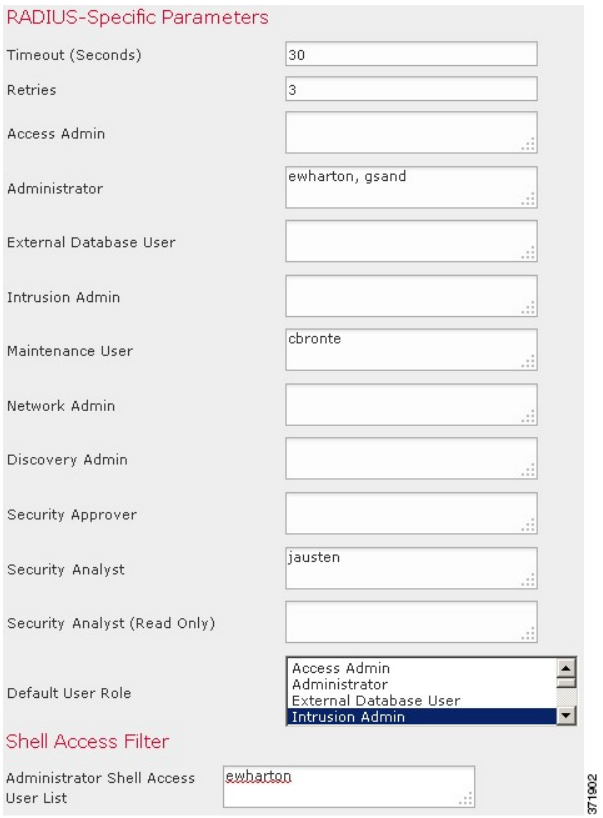
用户 `ewharton` 和 `gsand` 被授予对已启用此身份验证对象的设备的管理访问权限。

用户 `cbronte` 被授予对已启用此身份验证对象的设备的“维护用户”(Maintenance User) 访问权限。

用户 `jausten` 被授予对已启用此身份验证对象的设备的“安全分析师”(Security Analyst) 访问权限。

用户 `ewharton` 可以使用外壳帐户登录到设备中。

下图说明示例的角色配置：

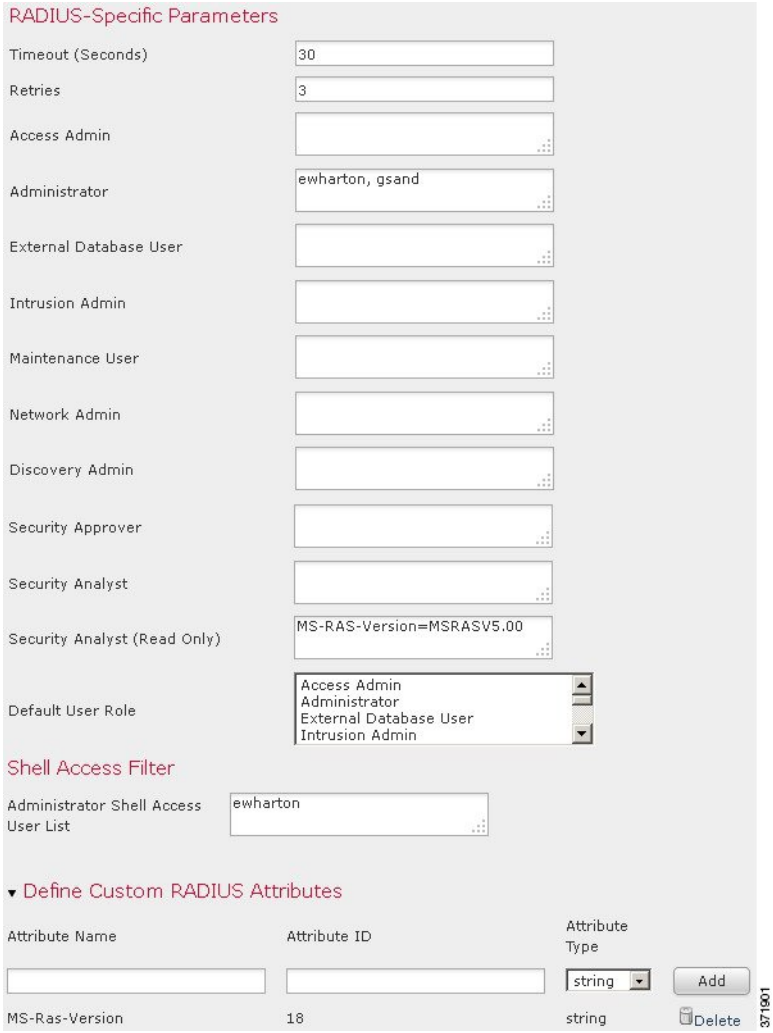


示例

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 FreeRADIUS 服务器的样本 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v. 5.00 远程访问服务器登录 RADIUS 的所有用户都应得到“安全分析师（只读）”(Security Analyst [Read Only]) 角色，因此请在**安全分析师（只读）(Security Analyst [Read Only]** 字段中输入属性-值对 `MS-RAS-Version=MSRASV5.00`。



接下来的操作

- 如果要启用 RADIUS 身份验证，请启用身份验证对象，如启用外部身份验证，第 489 页中所述。

配置 RADIUS 连接设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

创建RADIUS身份验证对象时，首先指定希望受管设备或Firepower管理中心连接以进行身份验证的主服务器和备用服务器及服务器端口。

注释 为使 RADIUS 正常工作，必须在防火墙上打开其身份验证和记帐端口（默认情况下为1812 和 1813）。

如果指定备份身份验证服务器，则可以为对主服务器进行的连接尝试设置超时。如果在经过 **Timeout** 字段中指示的秒数（或 LDAP 服务器上的超时）后主身份验证服务器没有响应，则设备将重新查询主服务器。

在设备按照 **Retries** 字段中指示的次数重新查询身份验证服务器，并且再次经过 **Timeout** 字段中指示的秒数而主身份验证服务器没有响应后，设备将滚动转移到备份服务器。

例如，如果主服务器已禁用 RADIUS，则设备将查询备份服务器。但是，如果 RADIUS 是在主 RADIUS 服务器的端口上运行，并且因某种原因而拒绝服务请求（由于配置错误或其他问题），则不会故障转移到备份服务器。

过程

步骤 1 选择**系统 (System)** > **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击**创建外部 (Create External)** > **身份验证对象 (Authentication Object)**。

步骤 4 从**身份验证方法 (Authentication Method)** 下拉列表中选择 **RADIUS**。

步骤 5 为身份验证服务器输入**名称 (Name)** 和**说明 (Description)**。

步骤 6 在**主服务器主机名/IP 地址 (Primary Server Host Name/IP Address)** 字段中输入要在其中获取身份验证数据的主 RADIUS 服务器的 IP 地址或主机名。

注释 外壳身份验证不支持 IPv6 地址。要在对主 RADIUS 服务器使用 IPv6 地址时允许外壳身份验证，请使用服务器的 IPv4 地址设置身份验证对象，并使用该 IPv4 对象作为 Firepower 管理中心上的第一个身份验证对象。

步骤 7 或者，在 **Primary Server Port** 字段中修改主 RADIUS 身份验证服务器使用的端口。

注释 如果身份验证端口号和记帐端口号不连续，请将此字段留空。然后，系统根据设备的 `/etc/services` 文件中的 `radius` 和 `radacct` 数据确定 RADIUS 端口号。

步骤 8 为主 RADIUS 身份验证服务器输入 **RADIUS 密钥 (RADIUS Secret Key)**。

步骤 9 或者，在**备用服务器主机名/IP 地址 (Backup Server Host Name/IP Address)** 字段中输入要在其中获取身份验证数据的备用 RADIUS 身份验证服务器的 IP 地址或主机名。

步骤 10 如果设置备用服务器，请修改**备用服务器端口 (Backup Server Port)**、**RADIUS 密钥 (RADIUS Secret Key)** 和**超时 (Timeout)**，并在**重试次数 (Retries)** 字段中输入应在滚动到备用连接之前尝试主服务器连接的次数。

注释 如果身份验证端口号和记帐端口号不连续，请将此字段留空。然后，系统根据设备的 `/etc/services` 文件中的 `radius` 和 `radacct` 数据确定 RADIUS 端口号。

接下来的操作

- 继续创建 RADIUS 身份验证对象，如创建 RADIUS 身份验证对象，第 91 页中所述。

配置 RADIUS 用户角色

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

当用户登录时，Firepower 系统会根据 RADIUS 配置检查 RADIUS 服务器并授予访问权限：

- 如果没有为用户配置特定访问权限且未指定默认访问角色，则当新用户登录时，Firepower 系统会按照 RADIUS 服务器对用户进行身份验证，然后根据平台设置策略中设置的一个或多个默认访问角色授予用户权限。
- 如果未在任何列表上指定新用户，且在身份验证对象的**默认用户角色 (Default User Role)** 列表中指定了默认访问角色，则会为该用户分配这些访问角色。
- 如果为一个或多个特定角色向列表中添加用户，则该用户会接收所有已分配的访问角色。

也可以使用属性-值对而不是用户名来识别应接收特定用户角色的用户。例如，如果您知道所有本应为“安全分析师”(Security Analyst) 的用户的 `User-Category` 属性值为 `Analyst`，则可以在“安全分析师列表”(Security Analyst List) 字段中输入 `User-Category=Analyst`，以将该角色授予这些用户。

可以分配一个或多个要分配给已进行外部身份验证但没有为特定角色列出的任何用户的默认用户角色。可以指定**默认用户角色 (Default User Role)** 列表中的多个角色。

由于具备 RADIUS 用户列表成员身份，无法通过 Firepower 系统用户管理页面移除已为其分配访问角色的用户的最低访问权限。但是，可以分配其他权限。

注意 如果要更改用户的最低访问设置，则不仅必须在 RADIUS“特定参数”(Specific Parameters) 部分中将用户从一个列表移至另一个列表或在 RADIUS 服务器上更改用户属性，还必须将配置重新部署到受管设备，并且必须在用户管理页面上移除已分配的用户权限。

开始之前

- 如果您计划使用自定义属性来设置用户角色成员身份，请进行定义，如定义自定义 RADIUS 属性，第 98 页中所述。

过程

步骤 1 在“创建外部身份验证对象”(Create External Authentication Object) 页面上与 Firepower 系统用户角色对应的字段中，输入各用户的名称或应分配给这些角色的标识属性-值对。
将用户名和属性-值对以逗号分隔。

示例：

例如，要将“管理员”(Administrator) 角色授予用户 `jsmith` 和 `jdoe`，请在**管理员 (Administrator)** 字段中输入 `jsmith, jdoe`。又例如，要将“维护用户”(Maintenance User) 角色授予 `User-Category` 值为 `Maintenance` 的所有用户，请在**维护用户 (Maintenance User)** 字段中输入 `User-Category=Maintenance`。

步骤 2 从**默认用户角色 (Default User Role)** 列表中为不属于任何指定组的用户选择默认最低访问角色。

接下来的操作

- 继续创建 RADIUS 身份验证对象，如创建 RADIUS 身份验证对象，第 91 页中所述。

配置 RADIUS 外壳访问

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

也可以使用RADIUS服务器对本地设备（受管设备或Firepower管理中心）上的外壳访问帐户进行身份验证。指定要向其授予外壳访问的用户的用户名。

注释 外壳身份验证不支持 IPv6 地址。如果使用 IPv6 地址配置主 RADIUS 服务器，并且还配置管理外壳访问，则会忽略外壳访问设置。要在对主RADIUS服务器使用IPv6地址时允许外壳身份验证，请使用服务器的 IPv4 地址设置其他身份验证对象，并使用该对象作为 Firepower 管理中心上的第一个身份验证对象。

除管理帐户以外，在 RADIUS 身份验证对象上设置的外壳访问列表完全控制设备上的外壳访问。部署平台设置策略后，外壳用户配置为设备上的本地用户。请注意，在 RADIUS 服务器上使用属性匹配进行身份验证的用户首次尝试登录时，会因已创建该用户帐户而被拒绝登录。用户必须再次登录。

请注意，各外壳用户的主目录是在登录时创建的，并且禁用 RADIUS 外壳访问用户帐户后（通过禁用 RADIUS 连接），该目录仍然保留，但是用户外壳在 `/etc/password` 中设置为 `/bin/false` 以禁用外壳。如果之后重新启用用户，则会使用同一主目录重置外壳。

外壳用户可以使用小写、大写或大小写字母混合的用户名进行登录。外壳的登录身份验证区分大小写。

注意 在物理 Firepower 管理中心上，所有外壳用户都具有 `sudoers` 权限。请确保适当地限制具有外壳访问的用户列表。在 7000 和 8000 系列和 NGIPSv 设备上，授予外部身份验证用户的外壳访问权限默认为**配置 (Configuration)** 级别的命令行访问权限，它还授予 `sudoers` 权限。

过程

在“创建外部身份验证对象”(Create External Authentication Object) 页面的**管理员外壳访问用户列表 (Administrator Shell Access User List)** 字段中，输入以逗号分隔的用户名。

注释 如果选择不指定外壳访问过滤器，则在保存身份验证对象时会显示警告，要求确认是否意图将过滤器留空。

接下来的操作

- 继续创建 RADIUS 身份验证对象，如创建 RADIUS 身份验证对象，第 91 页中所述。

定义自定义 RADIUS 属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果 RADIUS 服务器返回 `/etc/radiusclient/` 中 `dictionary` 文件内不包含的属性值，并且计划使用这些属性来设置具有这些属性的用户的用户角色，则需要在登录身份验证对象中定义这些属性。可以通过查看 RADIUS 服务器上的用户配置文件来查找为用户返回的属性。

定义属性时，请提供属性的名称，其中包含字母数字字符。请注意，属性名称中的单词应以破折号而不是空格进行分隔。另请提供属性 ID，它应为整数且不应与 `etc/radiusclient/dictionary` 文件中的任何现有属性 ID 冲突。还请指定属性的类型：字符串、IP 地址、整数或日期。

在创建 RADIUS 身份验证对象时，会在设备上的 `/var/sf/userauth` 目录中创建该对象的新目录文件。添加到身份验证对象的所有自定义属性都会添加到字典文件。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

过程

步骤 1 在“添加外部身份验证对象”(Add External Authentication Object) 页面上，点击箭头以展开“定义自定义 RADIUS 属性”(Define Custom RADIUS Attributes) 部分。

步骤 2 在 **属性名称 (Attribute Name)** 字段中输入属性名称。

步骤 3 在**属性 ID (Attribute ID)** 字段中以整数形式输入属性 ID。

步骤 4 从**属性类型 (Attribute Type)** 下拉列表中选择属性的类型。

步骤 5 点击 **Add** 以将自定义属性添加到身份验证对象。

提示 可以通过点击自定义属性旁边的 **Delete** 从身份验证对象中移除该属性。

示例

如果在含有思科路由器的网络上使用 RADIUS 服务器，则可能要使用 `Ascend-Assign-IP-Pool` 属性向从特定 IP 地址池登录的所有用户授予特定角色。`Ascend-Assign-IP-Pool` 是一个整数属性，用于定义允许用户登录的地址池，其中整数指示已分配的 IP 地址池的编号。

要声明自定义属性，请创建属性名称为 `Ascend-IP-Pool-Definition`、属性 ID 为 `218` 且属性类型为 `integer` 的自定义属性。

然后，可以在**安全分析（只读）(Security Analyst [Read Only])** 字段中输入 `Ascend-Assign-IP-Pool=2`，将只读安全分析师权限授予 `Ascend-IP-Pool-Definition` 属性值为 `2` 的所有用户。

接下来的操作

- 继续创建 RADIUS 身份验证对象，如创建 RADIUS 身份验证对象，第 91 页中所述。

测试 RADIUS 身份验证连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在配置 RADIUS 连接、用户角色和自定义属性设置后，可以为应该能够进行身份验证以测试这些设置的用户指定用户凭证。

对于用户名，可以输入要测试的用户的用户名。

请注意，由于 UI 页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅返回 1000 个用户。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置正确，请点击 **Test**，而无需首先在 **Additional Test Parameters** 字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

过程

步骤 1 在“添加外部身份验证对象”(Add External Authentication Object) 页面上的**用户名 (User Name)** 和**密码 (Password)** 字段中，输入其凭证应该用于验证对 RADIUS 服务器的访问的用户的用户名和密码。

示例：
例如，要测试以了解是否可以在 example 公司检索 `jsmith` 用户凭证，请输入 `jsmith`。

步骤 2 选择**显示详细信息 (Show Details)**，然后点击 **测试 (Test)**。

步骤 3 如果测试成功，请点击 **Save**。

接下来的操作

- 如果要启用 RADIUS 身份验证，请启用身份验证对象，如启用外部身份验证，第 489 页中所述。

单点登录 (SSO)

单点登录 (SSO) 支持思科安全管理器 (CSM) V4.7 或更高版本与 Firepower 管理中心之间的集成，让您可以从 CSM 访问 Firepower 管理中心，而无需进行其他身份验证以进行登录。当管理 ASA FirePOWER模块时，您可能要修改部署到该模块的策略。可以选择 CSM 中的主管Firepower 管理中心并在网络浏览器中将其启动。

如果您根据用户角色具有访问权限，则对于CSM中从中交叉启动的设备，系统会将您导航到Device Management 页面的 Device 选项卡。否则，系统会将您导航到“摘要控制面板”(Summary Dashboard) 页面（**概述 (Overview)** > **控制面板 (Dashboards)**），但没有控制面板访问权的用户帐户除外，这些帐户使用“欢迎”(Welcome) 页面。

为Firepower 管理中心启用 STIG 合规性后，系统会禁用 SSO。.

注释 如果贵组织使用 CAC 进行身份验证，则无法通过单点登录进行登录。

配置 SSO

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	ASA FirePOWER	任意	管理

在配置单点登录之前，必须设置从 CSM 到 Firepower 管理中心的单向、加密身份验证路径。

在 NAT 环境中，Firepower 管理中心和 CSM 必须驻留在 NAT 边界的同一侧。必须提供特定条件才能启用 CSM 和 Firepower 管理中心之间的通信。

注释 如果贵组织使用 CAC 进行身份验证，则无法通过单点登录进行登录。

过程

步骤 1 从 CSM 中，生成用于识别连接的 SSO 共享加密密钥。有关详细信息，请参阅 CSM 文档。

步骤 2 从 Firepower 管理中心中，选择**系统 (System)** > **用户 (Users)**。

步骤 3 选择 **CSM 单点登录 (CSM Single Sign-on)**。

步骤 4 输入 **CSM 主机名**或 **IP** 地址和服务器**端口**。

步骤 5 输入从 CSM 生成的**共享密钥**。

步骤 6 或者，如果要使用 Firepower 管理中心的代理服务器与 CSM 进行通信，请选择**使用代理进行连接 (Use Proxy For Connection)** 复选框。

步骤 7 点击 **Submit**。

步骤 8 点击 **Confirm Certificate** 以保存证书。
您现在可以从 CSM 登录到Firepower 管理中心而无需其他登录。

第 5 章

许可 Firepower 系统

以下主题介绍如何许可 Firepower 系统：

Firepower 系统许可

您可以许可各种功能，为您的组织创建最佳 Firepower 系统部署。您可使用Firepower 管理中心为其本身及其管理的设备管理许可证Firepower 系统提供的许可证类型取决于您要管理的设备类型：

- 对于 7000 和 8000 系列、ASA FirePOWER 和 NGIPSv 设备，必须使用经典许可证。使用使用经典许可证的设备有时也称为典型设备。

Firepower 功能的服务订用

服务订用在设置的时间长度内启用Firepower系统受管设备上的特定功能。可以购买为期一年、三年或五年的服务订用。如果订用到期，则思科会通知您必须更新订用。如果典型设备的订用到期，根据功能类型，可能无法使用相关功能。

服务订用对应于分配到 Firepower 系统中的受管设备的许可证，如下所示：

表 *17*：服务订用和对应的经典许可证

您购买的订用	您在 **Firepower** 系统中分配的经典许可证
TA	控制 + 保护（也称为“威胁与应用”，对于系统更新是必需的）

您购买的订用	您在 Firepower 系统中分配的经典许可证
思科技术支持中心 (TAC)	控制 + 保护 + URL 过滤
TAM	控制 + 保护 + 恶意软件
TAMC	控制 + 保护 + URL 过滤 + 恶意软件
URL	URL 过滤（已存在 TA 的附加设备）
AMP	恶意软件（已存在 TA 的附加设备）

您购买的自动使用经典许可证的受管设备包括控制和保护许可证。这些许可证是永久的，但是您还必须购买 TA 服务订用才能启用系统更新。其他服务订用是可选的。

经典许可证类型和限制

本节介绍Firepower系统部署中可用的经典许可证类型。可在某设备上启用的许可证取决于其型号、版本和已启用的其他许可证。

对于 7000 和 8000 系列设备、NGIPSv 设备和 ASA FirePOWER 模块，许可证是特定于型号的。无法在受管设备上启用许可证，除非许可证与设备的型号完全相符。例如，无法使用 Firepower 8250 恶意软件许可证 (FP8250-TAM-LIC=) 在 8140 设备上启用恶意软件功能；必须购买一个 Firepower 8140 恶意软件许可证 (FP8140-TAM-LIC=)。

注释 对于 NGIPSv 或 ASA FirePOWER，可以通过控制许可证执行用户和应用控制，但这些设备不支持交换、路由、堆叠或 7000 和 8000 系列设备高可用性。

有多种方式可能让您失去对 Firepower 系统中许可功能的访问权限。

- 可以从 Firepower 管理中心移除经典许可证，这将影响其所有受管设备。
- 可以在特定受管设备上禁用已许可的功能。

虽然有一些例外情况，但不能使用与已到期或删除的许可证关联的功能。

下表总结了 Firepower 系统中的经典许可证。

表 *18*: *Firepower* 系统经典许可证

在 Firepower 系统中分配的许可证	购买的订用服务	平台	授予的功能	另外要求	支持到期？
任意	TA、TAC、TAM 或 TAMC	7000 和 8000 系列 ASA FirePOWER NGIPSv	主机、应用和用户发现 解密和检查通过 SSL 和 TLS 加密的流量	none	取决于许可证

在 Firepower 系统中分配的许可证	购买的订用服务	平台	授予的功能	另外要求	支持到期？
保护	TA（设备随附）	7000 和 8000 系列 ASA FirePOWER NGIPSv	入侵检测和阻止 文件控制 安全情报过滤	none	否
可控性	无（设备随附）	7000 和 8000 系列	用户和应用控制 交换和路由 7000 和 8000 系列设备高可用性 7000 和 8000 系列网络地址转换 (NAT)	保护	否
可控性	无（设备随附）	ASA FirePOWER NGIPSv	用户和应用控制	保护	否
恶意软件	TAM、TAMC 或 AMP	7000 和 8000 系列 ASA FirePOWER NGIPSv	面向 Firepower 的 AMP（基于网络的高级恶意软件防护）	保护	yes
URL 过滤	TAC、TAMC 或 URL	7000 和 8000 系列 ASA FirePOWER NGIPSv	基于类别和信誉的 URL 过滤	保护	yes
VPN	无（联系销售部门了解详细信息）	7000 和 8000 系列	部署虚拟专用网络	可控性	yes

保护许可证

通过保护许可证，可以执行入侵检测和防御、文件控制和安全情报过滤。

- 入侵检测和阻止可用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。
- 文件控制可用于检测且或者阻止用户通过特定应用程序协议上传（发送）或下载（接收）特定类型的文件。面向 *Firepower* 的 *AMP*，需要恶意软件许可证，允许您根据文件处置情况检查并阻止这些文件类型的受限集合。
- 安全情报过滤，允许您在流量接受访问控制规则的分析之前，拒绝发送到特定 IP 地址、URL 和 DNS 域名或从其发送的流量，即，将其列入黑名单。动态源可用于根据最新智能立即拉黑连接。或者，可将“仅监控”设置用于安全情报过滤。

购买任何典型受管设备时自动包含保护许可证（以及控制许可证）。此许可证是永久的，但还必须购买 TA 订用才能启用系统更新。

虽然可以将访问控制策略配置为在没有许可证的情况下执行与保护相关的检查，但是不能部署策略，直至先向 Firepower 管理中心添加保护许可证，然后在策略所针对的设备上启用该许可证为止。

如果从 Firepower 管理中心中删除保护许可证或在受管设备上禁用保护，则 Firepower 管理中心会停止确认来自受影响设备的入侵和文件事件。因此，使用这些事件作为触发器条件的关联规则停止开启。此外，Firepower管理中心将不会访问互联网以获取思科提供的或第三方安全情报信息。重新启用保护之前，无法重新部署现有策略。

由于保护许可证对于URL过滤许可证、恶意软件许可证和控制许可证是必需的，因此删除或禁用保护许可证与删除或禁用 URL 过滤许可证、恶意软件许可证或控制许可证的效果相同。

控制许可证

控制许可证使您能够通过向访问控制规则添加用户和应用条件来实施用户和应用控制。（仅限 7000 和 8000 系列设备）通过此许可证，还可以配置交换和路由（包括 DHCP 中继和 NAT）以及设备高可用性对。要在受管设备上启用控制许可证，还必须启用保护许可证。购买任何典型受管设备自动包含控制许可证（连同保护许可证）。此许可证是永久的，但还必须购买 TA 订用才能启用系统更新。

如果未启用典型托管设备的控制许可证，则可以向访问控制策略中的规则添加用户和应用条件，但是不能将该策略部署到该设备。如果未专门启用 7000 或 8000 系列设备的控制许可证，则也无法执行以下操作：

- 创建交换、路由或混合接口
- 创建 NAT 条目
- 配置虚拟路由器的 DHCP 中继
- 将包含交换或路由的设备配置部署到设备
- 在设备之间建立高可用性

注释 尽管可在没有控制许可证的情况下创建虚拟交换机和路由器，但是如果没有交换和路由接口来对其进行填充，则这些虚拟交换机和路由器无用。

如果从Firepower管理中心删除控制许可证或在单个设备上禁用该许可证，则受影响设备不会停止执行交换或路由，设备高可用性对也不会中断。可以继续编辑和删除现有配置，但是不能将这些更改部署到受影响设备。不能添加新的交换、路由或混合接口，也不能添加新的 NAT 条目，配置 DHCP 中继或建立 7000 或 8000 系列设备高可用性。最后，如果现在访问控制策略包含具有用户或应用条件的规则，则无法重新部署该策略。

典型设备的 URL 过滤许可证

URL 过滤可用于编写访问控制规则，该规则可根据受监控主机请求的 URL 确定可横越网络且与那些 URL 的相关信息关联的流量。要启用 URL 过滤许可证，还必须启用保护许可证。您可以购买典

型设备的 URL 过滤许可证作为与威胁和应用 (TAC) 或威胁和应用及恶意软件 (TAMC) 订用相结合的服务订用，或者作为已启用威胁和应用 (TA) 的系统的附加订用 (URL)。

提示 如果没有 URL 过滤许可证，则可以指定要允许或阻止的单个 URL 或 URL 组。这将对网络流量进行精细和自定义控制，但是，不允许使用 URL 类别和信誉数据来过滤网络流量。

虽然无需 URL 过滤许可证即可将基于类别和信誉的 URL 条件添加到访问控制规则，但 Firepower 管理中心将不会下载 URL 信息。只有先将 URL 过滤许可证添加到 Firepower 管理中心，才能部署访问控制策略，然后在该策略所针对的设备上启用。

如果从 Firepower 管理中心删除许可证或在受管设备上禁用 URL 过滤，则可能会失去对 URL 过滤的访问权限。此外，URL 过滤许可证还可能过期。如果许可证到期，或者如果删除或禁用该许可证，则具有 URL 条件的访问控制规则会立即停止过滤 URL，并且 Firepower 管理中心无法再下载 URL 数据更新。如果现有访问控制策略包括的规则带有基于类别和信誉的URL条件，则不能重新部署该等策略。

典型设备的恶意软件许可证

通过恶意软件许可证，您可以使用面向 Firepower 的 AMP 和 AMP Threat Grid 执行思科高级恶意软件防护 (AMP)。您可以使用受管设备检测并阻止通过网络传输的文件中的恶意软件。要启用恶意软件许可证，还必须启用保护许可证。您可以购买恶意软件许可证作为与威胁及应用 (TAM) 或威胁及应用和 URL 过滤 (TAMC) 订用相结合的订用，或者作为已启用威胁及应用 (TA) 的系统的附加订用 (AMP)。

注释 已启用恶意软件许可证的 7000 和 8000 系列受管设备会定期尝试连接到 AMP 云，即使尚未配置动态分析也如此。因此，设备的接口流量控制面板构件显示传输的流量；这是预期行为。

请将面向 Firepower 的 AMP 配置为文件策略的一部分，然后可将该文件策略与一个或多个访问控制规则相关联。文件策略可以通过特定应用协议检测用户是否上传或下载特定类型的文件。通过面向 Firepower 的 AMP，您可以使用本地恶意软件分析和文件预分类来检查一组受限的文件类型中是否存在恶意软件。您也可以将特定文件类型下载并提交到 AMP Threat Grid 云进行动态和 Spero 分析，从而确定其是否包含恶意软件。对于这些文件，您可以查看网络文件轨迹，其中详述文件通过网络所采用的路径。通过恶意软件许可证，您还可以将特定文件添加到文件列表并在文件策略中启用该文件列表，从而在检测时自动允许或阻止这些文件。

在可部署包含面向 Firepower 的 AMP 的访问控制策略之前，**必须**添加恶意软件许可证，然后在作为该策略目标的设备上启用该许可证。如果稍后禁用设备上的许可证，则无法向这些设备重新部署现有访问控制策略。

如果删除所有恶意软件许可证或这些许可证全都过期，则系统会停止查询AMP云，并且还会停止确认从 AMP 云发送的追溯性事件。如果现有访问控制策略包含面向 Firepower 的 AMP 配置，则无法对其重新部署。请注意，在删除恶意软件许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗口到期后，系统会向这些文件分配处置情况 `Unavailable`。

仅在部署面向 Firepower 的 AMP 和 AMP Threat Grid 时，才需要恶意软件许可证。如果没有恶意软件许可证，则 Firepower 管理中心可以从 AMP 云接收面向终端的 AMP 恶意软件事件和危害表现 (IOC)。

VPN 许可证

VPN 可用于在终端之间通过公共资源建立安全隧道，例如互联网或其他网络。可以配置 Firepower 系统以在 7000 和 8000 系列设备的虚拟路由器之间构建安全的 VPN 隧道。要启用 VPN，还必须启用保护和控制许可证。要购买 VPN 许可证，请与销售人员联系。

没有 VPN 许可证，就不能用 7000 和 8000 系列设备配置 VPN 部署。虽然可创建部署，但不用至少启用一个支持 VPN 的路由接口填充部署，则部署无用。

如从 Firepower 管理中心删除 VPN 许可证，或在各台设备上禁用 VPN，则受影响设备将**不**中断当前 VPN 部署。尽管可编辑和删除现有部署，但不能对受影响设备部署更改。

设备堆栈和高可用性对中的经典许可证

单台设备必须具有等效许可证后才能堆叠或配置到 7000 或 8000 系列设备高可用性对中。堆栈设备后，可更改整个堆栈的许可证。但是，无法在 7000 或 8000 系列设备高可用性对中更改已启用的许可证。

查看经典许可证

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	传统	仅全局	管理

使用“经典许可证”(Classic Licenses) 页面查看已添加到 Firepower 管理中心的经典许可证。对于部署中的每种类型的受管设备，该页面会列出您所拥有的许可证总数以及那些在使用中的许可证部分。

Licenses 页面还提供了每个许可证的详细信息。对于每种型号，均可看到您拥有的每种类型许可证的数量，以及用每种类型许可证许可的受管设备数量。针对有期限的许可证，该页面向您提供过期日期。

您还可以查看许可证和许可证限制，如下所示：

- Product Licensing 控制面板构件提供了许可证概览。
- “设备管理”(Device Management) 页面（**设备 (Devices)** > **设备管理 (Device Management)**）列出应用于每个受管设备的许可证。
- 经典许可证监控运行状况模块在运行状况策略中使用时传达许可证状态。

过程

选择**系统 (System)** > **许可证 (Licenses)** > **经典许可证 (Classic Licenses)**。

识别许可证密钥

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	传统	仅全局	管理

许可证密钥可唯一地识别思科许可证注册门户中的 Firepower 管理中心。它由 Firepower 管理中心的产品代码 (66) 和 MAC 地址组成；例如，66:00:00:77:FF:CC:88。

必须使用思科许可证注册门户中的许可证密钥获取向 Firepower 管理中心添加许可证所需的许可证文本。

过程

步骤 1 选择**系统 (System)** > **许可证 (Licenses)** > **经典许可证 (Classic Licenses)**。

步骤 2 点击 **Add New License**。

步骤 3 请记下**添加功能许可证 (Add Feature License)** 对话框顶部的**许可证密钥 (License Key)** 字段中的值。

接下来的操作

- 将许可证添加到 Firepower 管理中心；请参阅将经典许可证添加到 Firepower 管理中心，第 109 页。

将经典许可证添加到 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	传统	仅全局	管理

注释 如果在备份完成后添加许可证，即使备份恢复，这些许可证不会删除也不会被覆盖。为防止恢复时出现冲突，请在恢复备份之前移除这些许可证，记住许可证使用位置，并在恢复备份之后添加和重新配置它们。如果发生冲突，请与技术支持部门联系。

提示 在登录支持网站后，还可在**许可证 (Licenses)** 选项卡上申请许可证。

开始之前

- 请确保您有思科在您购买许可证时提供的软件索赔证书中的产品激活秘钥(PAK)。如果有延迟，请在获取思科许可证之前联系支持部门。
- 识别 Firepower 管理中心的许可证密钥；请参阅识别许可证密钥，第 109 页。

过程

步骤 1 选择**系统 (System)** > **许可证 (Licenses)** > **经典许可证 (Classic Licenses)**。

步骤 2 点击 **Add New License**。

步骤 3 根据情况继续操作：

- 如果您已经获取许可证文本，请跳至步骤 8。
- 如果您仍需要获取许可证文本，请跳至下一步骤。

步骤 4 点击**获取许可证 (Get License)**，打开思科许可证注册门户。

注释 如果无法使用当前的计算机访问互联网，请切换至可访问互联网的计算机，并浏览至http://cisco.com/go/license。

步骤 5 从许可证注册门户中的 PAK 生成一个许可证。有关详细信息，请参阅 https://www.cisco.com/web/fw/tools/swift/xui/html/help.html。
此步骤需要您在购买过程中收到的 PAK 以及 Firepower 管理中心的许可证密钥。

步骤 6 复制许可证注册门户显示或许可证注册门户发送给您的邮件中的许可证文本。

步骤 7 返回 Firepower 管理中心的 Web 界面中的**添加功能许可证 (Add Feature License)** 页面。

步骤 8 将许可证文本粘贴到**许可证 (License)** 字段。

步骤 9 点击**验证许可证 (Verify License)**。
如果许可证无效，请确保您复制的许可证文本正确无误。

步骤 10 点击**提交许可证 (Submit License)**。

接下来的操作

- 将许可证分配到受管设备，请参阅将许可证分配到受管设备，第 110 页。**必须**将许可证分配到受管设备后，才能在那些设备上使用许可的功能。

将许可证分配到受管设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员

尽管有一些例外，但如果在受管设备上禁用许可证，就无法使用与该许可证关联的功能。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要分配或禁用许可证的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 点击 License 部分旁边的编辑图标 ( )。

步骤 5 选中或清除相应的复选框，以便为设备分配或禁用许可证。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 6 章

系统软件更新

以下主题介绍如何更新 Firepower 系统软件：

系统软件更新简介

思科以电子形式分发多种不同类型的更新，包括：

- 对系统软件本身的主要和次要更新
- 入侵规则更新
- 地理位置数据库 (GeoDB) 更新
- 漏洞数据库 (VDB) 更新

对于大多数更新类型，可以安排其下载和安装。

注意 本章包含有关更新 Firepower 系统的常规信息。在更新 Firepower 系统的任何部分（包括 VDB、GeoDB 或入侵规则）之前，**必须**阅读更新随附的版本说明或建议性文本。版本说明提供重要信息，包括支持的平台、兼容性、先决条件、警告以及具体安装和卸载说明。

表 *19*: *Firepower* 系统更新类型

更新类型	说明	安排？	卸载？	Tab	域
Firepower 系统补丁	补丁包括数量有限的修复程序（通常更改版本号中的第四位数字；例如，6.0.0.1）。	是	是	Product Updates	仅全局
Firepower 系统的功能更新	功能更新比补丁更全面，通常包括新功能（并且通常更改版本号中的第三位数字；例如，6.0.1）。	是	是	Product Updates	仅全局
Firepower 系统的主要更新（主要和次要版本发布）	主要更新（有时称为升级）包括新功能，并且可能需要对产品进行大规模更改（通常改变版本号中的第一位或第二位数字；例如，6.1 或 6.2）。主要更新可能要求再次接受思科最终用户许可证协议 (EULA)。	否	否	Product Updates	仅全局
漏洞数据库 (VDB)	VDB 更新会影响 Firepower 系统报告的漏洞以及检测到的操作系统、应用和客户端。	是	否	Product Updates	仅全局
入侵规则	入侵规则更新提供新的和更新后的入侵规则和预处理器规则、现有规则的修改后状态以及修改后的默认入侵策略设置。规则更新还可以删除规则，提供新规则类别和默认变量，以及修改默认变量值。	是	否	规则更新	• 入侵规则更新：仅全局 • 本地规则导入：任意
地理定位数据库 (GeoDB)	GeoDB 提供有关系统可通过可路由 IP 地址与之关联的物理位置、连接类型等等方面的更新信息。地理定位数据可用作访问控制规则中的条件。必须安装 GeoDB 才能查看地理定位详细信息。	是	否	地理位置更新	仅全局

请注意，虽然可以卸载Firepower系统的补丁和其他次要更新，但不能卸载主要更新，也不能恢复到VDB、GeoDB 或入侵规则的先前版本。如果已将设备更新为 Firepower 系统的新的主要版本，并且需要恢复为旧版本，请联系支持部门。

除非版本说明或建议性文本另有说明，否则，更新设备不会修改其配置；设备设置将保持不变。

Firepower 系统软件更新

更新Firepower系统部署要执行几个基本步骤。首先，**必须**为更新做好准备，包括阅读版本说明以及完成必要的更新前任务。然后，即可开始更新 - 首先更新 Firepower 管理中心，然后更新其管理的设备。必须监控更新进度直至更新完成，然后验证更新是否成功。最后，完成必要的更新后步骤。

Firepower 系统软件更新准备

开始更新之前，必须仔细阅读并理解版本说明（可从支持网站下载）。版本说明介绍支持的平台、新功能、已知问题、已解决的问题以及产品兼容性。版本说明还包含有关先决条件、警告以及具体安装和卸载说明的重要信息。

Firepower 系统版本要求

必须确保设备（包括基于软件的设备）运行的是正确版本的Firepower系统。版本说明指明所需的版本。如果运行的是早期版本，可从支持网站获取更新。

操作系统要求

确定安装了基于软件的设备的计算机运行的是正确的操作系统版本。版本说明指明所需的版本。有关 NGIPSv 设备的受支持操作系统的信息，请参阅《《*Firepower* 系统虚拟安装指南》》。

时间和磁盘空间方面的要求

确定有足够的可用磁盘空间并且更新时间足够。更新受管设备时，要求Firepower管理中心上有额外磁盘空间。版本说明指明磁盘空间和时间方面的要求。

配置和事件备份准则

在开始主要更新之前，思科建议在将位于设备上的任何备份复制到外部位置后删除这些备份。此外，不管更新类型如何，都应该将当前事件和配置数据备份到外部位置。更新过程中**不**会备份事件数据。

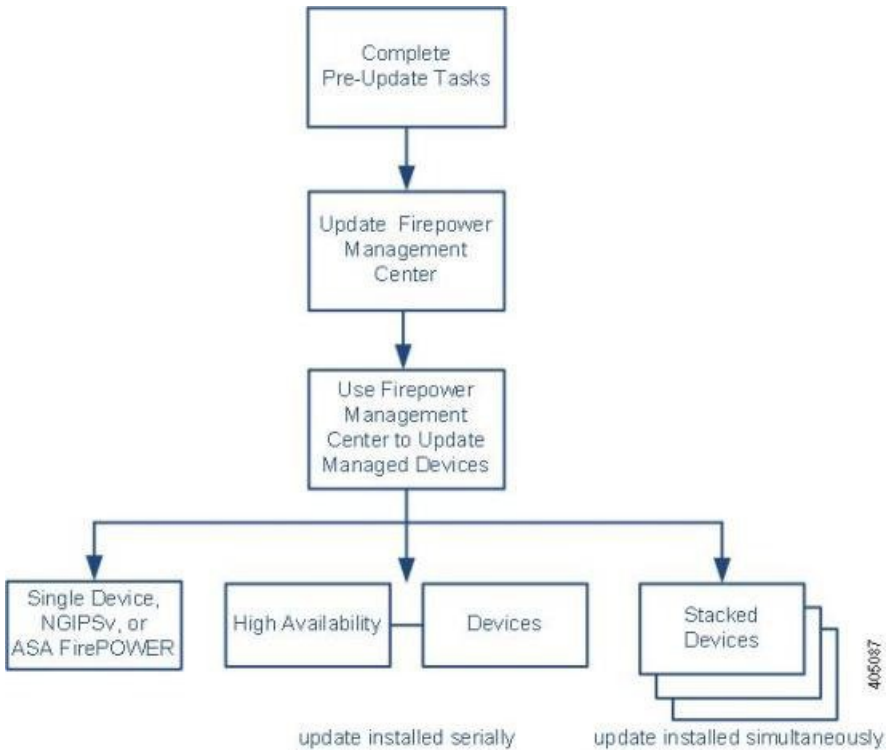
可以使用 Firepower 管理中心备份其自身及其管理的设备的事件和配置数据。

何时执行更新

注意 由于更新过程可能会影响流量检查、流量和链路状态，并且数据相关器在更新过程中处于禁用状态，因此思科建议在维护窗口中或者在中断对部署造成的影响最小时执行更新。

Firepower 系统软件更新过程

以下流程图显示 Firepower 系统的更新过程：



更新顺序

必须先更新Firepower 管理中心，再更新其管理的设备。

使用Firepower 管理中心进行更新

使用 Firepower 管理中心的 Web 界面更新其本身以及其管理的设备。

提示 对于补丁和功能更新，可以利用自动更新功能。

更新受管设备分两步进行。首先，从支持站点下载更新，并将其上传到管理 Firepower 管理中心：http://www.cisco.com/cisco/web/support/index.html。

接着，安装软件。

注意 在更新过程中，流量检查、流量和链路状态可能会受到影响，具体取决于设备的配置和部署方式、受更新影响的组件以及更新时是否会重新启动设备。有关特定更新如何和何时影响网络流量的详细信息，请参阅更新的版本说明。

更新高可用性对中的 7000 和 8000 系列设备

在 7000 或 8000 系列设备上或高可用性对中的设备堆栈上安装更新时，系统会逐一在每台设备或堆栈上进行更新。更新开始后，系统首先将更新应用到备份设备或堆栈；此时，备份设备或堆栈会进入维护模式，当有必要的进程重新启动后，备份设备或堆栈会重新开始处理流量。然后，系统以同样的方式将更新应用到活动设备或堆栈。

要更新高可用性对中的堆栈设备，您必须同时更新所有高可用性对成员上的管理 Firepower 管理中心；不能直接从设备进行升级。

更新堆叠 8000 系列设备

在堆叠设备上安装更新时，系统同时进行更新。更新完成后，每台设备都会恢复正常运行。请注意：

- 如果主设备先于所有辅助设备完成更新，在所有设备完成更新之前，堆栈以受限的混合版本状态运行。
- 如果主设备晚于所有辅助设备完成更新，堆栈在主设备完成更新后恢复正常运行。

流量和检查

从受管设备安装或卸载更新时，以下功能可能会受到影响：

- 流量检查，包括应用和用户感知与控制、URL 过滤、安全情报过滤、入侵检测与防御以及连接日志记录
- 流量，包括交换、路由及相关功能
- 链路状态
- VPN
- NAT

数据相关器在系统更新期间不运行。更新完成后，它会恢复正常运行。

网络流量中断的方式和持续时间取决于受更新影响的Firepower系统组件、设备的配置和部署方式，以及更新是否会重新启动设备。有关特定更新如何和何时影响网络流量的详细信息，请参阅版本说明。

提示 更新高可用性对中的 7000 或 8000 系列设备时，系统一次更新一台设备，以避免流量中断。

在更新过程中使用 Web 界面

不管更新类型如何，请**勿**在进行更新时使用设备的网络界面执行除监控更新以外的任何其他任务。

为避免在主要更新期间使用设备，并方便监控主要更新进度，系统简化了设备的网络界面。您可以在消息中心监控次要更新的进度。尽管在进行次要更新时并未禁止您使用 Web 界面，但思科并不建议执行此操作。

提示 要监控其受管设备的更新，可使用 Firepower 管理中心上的消息中心。

即使对于次要更新，进行更新时也可能无法使用正在更新的设备的网络界面，或者设备可能会注销您的登录。这是预期行为。如果发生这种情况，请再次登录以查看消息中心（对于次要更新）或“更新状态”(Update Status) 页面（对于主要更新）。如果仍在进行更新，**必须**避免使用网络界面，直至更新完成。请注意，在更新过程中，受管设备可能会重新启动两次；这也是预期行为。

注意 如果更新出现问题（例如，Web 界面指示更新失败；再如，消息中心或“更新状态”[Update Status] 页面不显示进度），请**勿**重新开始更新。而应联系支持部门。

更新后

必须完成版本说明中列出的所有更新后任务，以确保部署正常运行。

注意 在更新 Firepower 管理中心**以及**更新其受管设备后，您必须部署配置。

此外，还应：

- 确认更新是否成功。
- 确保部署中的所有设备都能够成功通信
- 如有必要，更新入侵规则、VDB 和 GeoDB
- 根据版本说明中的信息更改任何必要的配置
- 进行版本说明中列出的任何其他更新后任务

Firepower 系统软件更新说明

根据更新类型以及 Firepower 管理中心是否具有互联网访问权限，您可以通过以下两种方式之一在 Firepower 管理中心上更新 Firepower 系统软件：

- 如果 Firepower 管理中心具有互联网访问权限，则直接从支持站点获取更新。这种方法**不**适用于主要更新。
- 从支持站点手动下载更新，然后将其上传到 Firepower 管理中心。如果 Firepower 管理中心不具有互联网访问权限或者您执行的是主要更新，请使用此方法。

注释 使用上述方法之一获取更新。如果通过邮件传输更新文件，可能会损坏该文件。

“产品更新”(Product Updates) 页面（**系统 (System)** > **更新 (Updates)**）显示每个更新的版本及其生成日期和时间。此外，该页面还指明更新过程中是否需要重新启动。

将从支持部门获得的更新上传到设备后，这些更新会显示在该页面中。此外，还会显示补丁和功能更新的卸载程序。在Firepower 管理中心上，该页面可能列出 VDB 更新。

对于主要更新，更新Firepower 管理中心会删除之前更新的卸载程序。

在 Firepower 管理中心上更新软件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

开始之前

- 完成 Firepower 管理中心上的长期任务。
- 将更新上传到Firepower 管理中心。有关详细信息，请参阅下载 Firepower 系统软件更新，第 120 页和将软件更新上传到 Firepower 管理中心，第 121 页。

过程

步骤 1 阅读版本说明并完成必要的更新前任务。

步骤 2 确定部署中的设备可成功通信，且运行状况监控器没有报告任何问题。

步骤 3 选择**系统 (System)** > **更新 (Updates)**。

步骤 4 点击上传的更新旁边的安装图标。

步骤 5 选择 Firepower 管理中心并点击**安装 (Install)**。如果出现提示，请确认是否要安装更新并重新启动 Firepower 管理中心。

步骤 6 或者，也可以监控更新状态：

- 对于次要更新，请参阅查看任务消息，第 239 页。
- 对于主要更新，请参阅监控主要 Firepower 系统软件更新，第 122 页。

注意 不管更新类型如何，请**勿**在更新完成前使用网络界面执行除监控更新以外的任何其他任务；如有必要，Firepower 管理中心会重新启动。

如果更新出现问题（例如，“消息中心”[Message Center] 指出更新失败；再如，消息不显示进度），请**勿**重新开始更新。而应联系支持部门。

步骤 7 更新完成后，若有必要，重新登录 Firepower 管理中心。

步骤 8 在完成主要更新后，如果您是第一个登录的用户，请阅读并接受用户软件授权协议(EULA)以继续。

步骤 9 清除浏览器缓存并强制浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 10 依次选择**帮助 (Help)** > **关于 (About)** 以查看系统信息。

步骤 11 在系统信息页面中，确认已正确列出软件版本，然后记下 Firepower 管理中心上的规则更新和 VDB 的版本，稍后您需要使用这些信息。

步骤 12 验证所有受管设备都能够成功地与Firepower 管理中心进行通信。

接下来的操作

- 如果存在新的入侵规则更新，请导入该更新；请参阅入侵规则更新，第 127 页。
- 如果支持站点上的 VDB 比 Firepower 管理中心上的 VDB 要新，请安装新 VDB；请参阅漏洞数据库更新，第 125 页。
- 在受管设备上更新系统软件；请参阅更新受管设备上的软件，第 121 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

下载 Firepower 系统软件更新

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

可以将主要更新之外的所有软件更新都下载到 Firepower 管理中心。为此，Firepower 管理中心必须具有互联网访问权限。

开始之前

- 确保 Firepower 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 1717 页。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击**下载更新 (Download Updates)** 以检查思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 上的最新更新。

步骤 3 安装更新。有关详细信息，请参阅在 Firepower 管理中心上更新软件，第 119 页和更新漏洞数据库，第 126 页。

将软件更新上传到 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

在下列情况下，必须将更新上传到 Firepower 管理中心：

- 执行主要更新。
- Firepower 管理中心没有互联网访问权限。
- 更新受管设备。

过程

步骤 1 从思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 手动下载更新。

步骤 2 选择**系统 (System)** > **更新 (Updates)**。

步骤 3 点击**上传更新 (Upload Update)**。

步骤 4 浏览到更新并点击**上传 (Upload)**。

接下来的操作

- 安装更新。有关详细信息，请参阅在 Firepower 管理中心上更新软件，第 119 页和更新漏洞数据库，第 126 页。

更新受管设备上的软件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

除非另行说明，否则此过程中的所有步骤均在 Firepower 管理中心上进行。

开始之前

- 更新 Firepower 管理中心上用于管理设备的 Firepower 系统软件。有关详细信息，请参阅Firepower 系统软件更新说明，第 118 页。
- 将更新上传到Firepower 管理中心。有关详细信息，请参阅将软件更新上传到 Firepower 管理中心，第 121 页。

过程

步骤 1 阅读版本说明并完成必要的更新前任务；请参阅Firepower 系统软件更新说明，第 118 页和Firepower 系统软件更新准备，第 115 页。

步骤 2 确定部署中的设备可成功通信，且运行状况监控器没有报告任何问题。

步骤 3 选择**系统 (System)** > **更新 (Updates)**。

步骤 4 点击要安装的更新旁边的安装图标。

步骤 5 选择要安装更新的设备，然后点击**安装 (Install)**。
如果多台设备使用相同更新，可一次性对这些设备进行更新。如果出现提示，请确认是否要安装更新并重新启动设备。

在所有设备上安装更新可能需要一些时间，具体取决于文件大小。在更新过程中，受管设备可能会重新启动两次；这是正常现象。

步骤 6 或者，也可以监控更新状态：

- 对于次要更新，请参阅查看任务消息，第 239 页。
- 对于主要更新，请参阅监控主要 Firepower 系统软件更新，第 122 页。

注意 不管更新类型如何，请**勿**在更新完成前使用 Web 界面执行除监控更新以外的任何其他任务；如有必要，受管设备会重新启动。

如果更新出现问题（例如，消息中心指示更新失败；再如，消息不显示进度），请**勿**重新开始更新。而应联系支持部门。

步骤 7 清除浏览器缓存并强制浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 8 选择**设备 (Devices)** > **设备管理 (Device Management)**并确认更新的设备是否列出正确的版本。

步骤 9 验证更新的设备能够成功地与Firepower 管理中心进行通讯。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。
- 或者在完成 7000 或 8000 系列设备的主要更新后，登录设备的本地 Web 界面。在完成主要更新后，如果是第一次登录，可能会显示最终用户许可证协议 (EULA)。必须阅读并接受 EULA 才能继续。请注意，如果第一次登录是通过命令行界面而非网络界面进行的，也可能显示EULA；必须接受 EULA。

监控主要 Firepower 系统软件更新

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

必须使用设备的本地 Web 界面执行此程序。

过程

步骤 1 监控消息中心内主要软件更新的进度，直至设备完成其必要的更新前检查为止。
此时，系统会从 Web 界面中注销您和所有其他用户。只有管理员或维护人员方才可以在更新完成前重新登录。

步骤 2 如果您是管理员，请重新登录 Web 界面。系统将显示精简的更新页面。

步骤 3 点击 **show log for current script** 可查看更新日志。点击 **hide log for current script** 可隐藏更新日志。

注意 如果遇到任何更新问题（例如，如果手动刷新精简的更新页面后长时间没有显示进度），请**勿**重新启动更新。而应联系支持部门。

接下来的操作

- 如果更新由于任何原因而失败，该页面会显示错误消息，其中指明失败的时间和日期、更新失败时正在运行的脚本，并提供有关如何联系支持部门的说明。请**不要**重新开始更新。
- 如果更新成功完成，则页面将显示成功消息，并且设备会重启。设备重新启动后，请刷新页面进行登录，并完成必要的更新后步骤。

Firepower 系统软件更新卸载

应用补丁或功能更新时，更新过程中会创建卸载程序，让您可通过设备的 Web 界面从该设备移除更新。

卸载更新时，产生的版本取决于设备的更新路径。例如，假设您直接将设备从版本 6.0 更新为版本 6.0.0.2。卸载版本 6.0.0.2 补丁可能会产生运行版本 6.0.0.1 的设备，尽管您从未安装版本 6.0.0.1 更新。有关卸载更新时产生的 Firepower 软件版本的信息，请参阅版本说明。

注意 主要更新不支持从网络界面卸载。如果已将设备更新为 Firepower 系统的新的主要版本，但需要恢复为旧版本，请联系支持部门。

卸载顺序

按照与安装相反的顺序卸载更新；即首先从受管设备卸载更新，然后从 Firepower 管理中心卸载。

使用本地网络界面卸载更新

必须使用本地网络界面卸载更新；不得使用Firepower管理中心从受管设备卸载更新。有关从没有本地 Web 界面的设备（例如，NGIPSv 设备）卸载补丁的信息，请参阅版本说明。

从高可用性对中的 7000 和 8000 系列设备卸载更新

高可用性对中的 7000 或 8000 系列设备必须运行相同版本的 Firepower 系统。虽然卸载过程会触发自动故障切换，但错配的高可用性对中的 7000 或 8000 系列设备不会共享配置信息，也不会在同步过程中安装或卸载更新。如果需要从冗余设备卸载更新，应紧接着上一个过程进行。

如果卸载会导致这些设备恢复为不支持将堆栈配置到高可用性中的版本，则无法从配置为高可用性对的堆栈中的 7000 或 8000 系列设备卸载更新。

为确保操作的连续性，请逐一从高可用性对中的设备卸载更新。首先，从辅助设备卸载更新。等待卸载过程完成，然后立即从主设备卸载更新。

注意 如果高可用性对中的设备的卸载过程失败，请**不要**重新开始卸载或更改其对等设备上的配置，而应联系支持部门。

从堆叠设备卸载更新

堆栈中的所有设备必须运行相同版本的 Firepower 系统。从任何堆叠设备卸载更新，都会导致该堆栈中的设备进入受限的混合版本状态。

为最大程度降低对部署的影响，应同时从堆叠设备卸载更新。堆栈中所有设备的更新完成，堆栈会恢复正常运行。

如果卸载会导致这些设备恢复为不支持将堆栈配置到高可用性中的版本，则无法从配置为高可用性对的堆栈中的 7000 或 8000 系列设备卸载更新。

流量和检查

从受管设备卸载更新可能会影响流量检查、流量和链路状态。有关特定更新如何和何时影响网络流量的详细信息，请参阅版本说明。

卸载后

卸载更新后，应执行多个步骤来确保部署正常运行。这些步骤包括验证卸载是否成功以及部署中的所有设备是否能够成功地进行通信。有关每项更新的详细信息，请参阅版本说明。

卸载 Firepower 系统软件更新

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

可以在 Firepower 管理中心和 7000 和 8000 系列设备上执行此程序。

开始之前

- 如果已将设备更新为 Firepower 系统的新的主要版本，并且需要恢复为旧版本，请联系支持部门。主要更新不支持从网络界面卸载。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击要移除的更新的卸载程序旁边的安装图标。如果出现提示，请确认是否要安装更新并重启设备。

- 在 Firepower 管理中心上，Install Update 页面显示。选择 Firepower 管理中心并点击**安装 (Install)**。
- 在受管设备上，不会显示干预页面。

注意 在卸载完成之前，请**勿**使用网络界面执行除监控更新以外的任何其他任务；如有必要，设备会重新启动。

步骤 3 或者，监控任务状态；请参阅查看任务消息，第 239 页。

步骤 4 卸载完成后，若有必要，登录设备。

步骤 5 清除浏览器缓存并强制浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 6 依次选择**帮助 (Help)** > **关于 (About)** 并确认是否正确列出软件版本。

接下来的操作

- 验证卸载了补丁的设备是否能够成功地与其受管设备（对于Firepower 管理中心）或其管理 Firepower 管理中心（对于受管设备）进行通信。
- 验证卸载是否成功，以及部署中的所有设备是否在成功地进行通信。有关每项更新的详细信息，请参阅版本说明。

漏洞数据库更新

思科漏洞数据库 (VDB) 是可能容易影响主机的已知漏洞以及操作系统指纹、客户端指纹和应用指纹的数据库。Firepower 系统将指纹与漏洞相关联，以帮助确定特定主机是否会增加网络危害的风险。Cisco Talos 安全情报和研究小组 (Talos) 定期发布 VDB 更新。

要更新 VDB，请使用Firepower 管理中心上的 Product Updates 页面。将从支持部门获得的 VDB 更新上传到设备后，这些更新连同 Firepower 系统的更新和卸载程序更新都会显示在该页面上。

注释 可直接从支持网站下载更新（手动下载，或者点击 **Download Updates**）。如果通过邮件传输更新文件，可能会损坏更新文件。

更新漏洞映射所需的时间取决于网络映射中主机的数量。您可能想将更新安排在系统不繁忙的时间进行，以最大程度减少系统停机造成的影响。一般来说，可以用网络上主机的数量除以 1000 来确定进行更新的适当时间。

在更新 VDB 后，您必须先部署配置，然后已更新的应用检测器和操作系统指纹才会生效。

注意 安装 VDB 更新在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

您可以利用自动化的更新功能来计划 VDB 更新。

更新漏洞数据库

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

此程序仅在可 Firepower 管理中心上执行。

开始之前

- 将更新上传到Firepower 管理中心。有关详细信息，请参阅下载 Firepower 系统软件更新，第 120 页和将软件更新上传到 Firepower 管理中心，第 121 页。

注意 安装 VDB 更新在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 阅读适用于具体更新的 VDB 更新建议性文本。建议性文本包括有关在更新过程中对 VDB 所做更改的信息以及产品兼容性信息。

步骤 2 选择**系统 (System)** > **更新 (Updates)**。

步骤 3 在**产品更新 (Product Updates)** 选项卡上，点击 VDB 更新旁边的安装图标。

步骤 4 选中 Firepower 管理中心条目旁边的复选框。

步骤 5 点击**安装**。安装更新可能需要一些时间，具体取决于网络映射中主机的数量。

步骤 6 或者，监控任务状态；请参阅查看任务消息，第 239 页。

注意 在完成更新之前，请**勿**使用网络界面执行与映射的漏洞相关的任务。如果更新出现问题（例如，如果消息中心不显示进度或指示更新失败）,请**勿**重新开始更新。而应联系支持部门。

步骤 7 更新完成后，选择**帮助 (Help)** > **关于 (About)** 确认 VDB 内部版本号是否与安装的更新相匹配。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。
- 或者，安排 VDB 更新；请参阅漏洞数据库更新自动化，第 166 页。

入侵规则更新

随着新漏洞的暴露，Cisco Talos 安全情报和研究小组 (Talos) 会发布可以导入到 Firepower 管理中心上的入侵规则更新，然后通过将已更改的配置部署到受管设备进行实施。这些更新会影响入侵规则、预处理器规则和使用规则的策略。

入侵规则更新是累加性的，并且思科建议始终导入最新的更新。不能导入与当前安装的规则的版本匹配或早于该版本的入侵规则更新。

入侵规则更新可能提供以下内容：

- **新的和修改的规则和规则状态** - 规则更新提供新的和更新的入侵和预处理器规则。对于新的规则，每个系统提供的入侵规则中的规则状态可能不同。例如，一个新规则在 Security over Connectivity 入侵策略中可能是启用状态，在 Connectivity over Security 入侵策略中则可能是禁用状态。规则更新也可以更改现有规则的默认状态，或者完全删除现有规则。
- **新规则类别** - 规则更新可能包括始终添加的新规则类别。
- **修改的预处理程序和高级设置** - 规则更新可能更改系统提供的入侵策略中的高级设置以及系统提供的网络分析策略中的预处理器设置。它们也可以更新访问控制策略中的高级预处理和性能选项的默认值。
- **新的和修改的变量** - 规则更新可能修改现有默认变量的默认值，但不会覆盖您的更改。始终会添加新变量。

在多域部署中，可以在任何域中导入本地入侵规则，但是，只能在全局域中从 Talos 导入入侵规则更新。

了解入侵规则更新何时修改策略

入侵规则更新可以影响系统提供的和自定义网络分析策略，以及所有访问控制策略：

- **系统提供** - 对系统提供的网络分析和入侵策略的更改以及对高级访问控制设置的任何更改将在您更新后重新部署策略时自动生效。
- **自定义** - 因为每个自定义网络分析和入侵策略都使用系统提供的策略作为其基础，或作为策略链中的事件基础，所以规则更新可以影响自定义网络分析和入侵策略。但是，您可以阻止规则更新自动执行这些更改。这使您能够在独立于规则更新导入的计划中手动更新系统提供的基本策略。无论您的选择（在每个自定义策略基础上实施）如何，更新系统提供的策略**都不会**覆盖您定制的任何设置。

请注意，导入规则更新会丢弃对网络分析和入侵策略所做的所有已缓存更改。为了方便起见，Rule Updates 页面列出了包含已缓存更改的策略以及做出这些更改的用户。

部署入侵规则更新

为使入侵规则更新所做的更改生效，必须重新部署配置。在导入规则更新时，可以将系统配置为自动重新部署到受影响设备。如果允许入侵规则更新修改系统提供的基本入侵策略，则此方法尤其有用。

注意 导入新的或已更新的共享对象规则（二进制）的规则更新，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。请确保下载和安装规则更新的过程符合您的安全策略。此外，入侵规则更新可能很大，因此，请在网络使用较少的期间导入规则。

周期性入侵规则更新

可以在 Rule Updates 页面上设置为按日、周或月导入规则更新。

入侵规则更新导入中的适用子任务按以下顺序出现：下载、安装、基本策略更新和策略部署。完成一个子任务后，才会开始下一个子任务。

在计划的时间，系统按照在先前步骤中所指定，安装规则更新并部署已更改的配置。在导入之前或导入过程中，可注销或使用网络界面执行其他任务。在导入期间访问时，“规则更新日志”(Rule Update Log) 显示红色状态图标 ( )，您可以在“规则更新日志”(Rule Update Log) 详细视图中出现消息时查看这些消息。根据规则更新大小和内容，可能几分钟之后才会显示状态消息。

导入本地入侵规则

本地入侵规则是从本地计算机以采用 ASCII 或 UTF-8 编码的纯文本文件形式导入的自定义标准文本规则。可以使用 Snort 用户手册（可在 http://www.snort.org 上获取）中的说明创建本地规则。

在多域部署中，可以在任何域中导入本地入侵规则。可以查看在当前域和祖先域中导入的本地入侵规则。

一次性手动更新入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

如果 Firepower 管理中心没有互联网访问权限，请手动导入新的入侵规则更新。

过程

步骤 1 从思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 手动下载更新。

步骤 2 选择**系统 (System)** > **更新 (Updates)**，然后点击**规则更新 (Rule Updates)** 选项卡。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，则必须点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选择**要上传并安装的规则更新或文本规则文件 (Rule Update or text rule file to upload and install)**，然后点击**浏览 (Browse)** 以浏览并选择规则更新文件。

步骤 5 如果要在更新完成后自动将策略重新部署到受管设备，请选择**在规则更新导入完成后重新应用所有策略 (Reapply all policies after the rule update import completes)**。

步骤 6 点击 **Import**。系统将安装规则更新并显示“规则更新日志”(Rule Update Log) 详细视图。

注释 如果在安装规则更新时出现错误消息，请联系支持部门。

一次性自动更新入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

要自动导入新的入侵规则更新，设备必须具有互联网访问权限以连接到支持站点。

开始之前

- 确保 Firepower 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 1717 页。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击**规则更新 (Rule Updates)** 选项卡。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，请点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选择**从支持站点下载新规则更新 (Download new Rule Update from the Support Site)**。

步骤 5 如果要在更新完成后自动将已更改的配置部署到受管设备，请选中**在规则更新导入完成后重新应用所有策略 (Reapply all policies after the rule update import completes)** 复选框。

步骤 6 点击 **Import**。

系统将安装规则更新并显示“规则更新日志”(Rule Update Log) 详细视图。

注意 如果在安装规则更新时出现错误消息，请联系支持部门。

配置周期性入侵规则更新

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击**规则更新 (Rule Updates)** 选项卡。

步骤 3 如果要将已创建或导入的所有用户定义的规则都移至已删除的文件夹，请点击工具栏中的**删除所有本地规则 (Delete All Local Rules)**，然后点击**确定 (OK)**。

步骤 4 选中**启用周期性规则更新导入 (Enable Recurring Rule Update Imports)** 复选框。
导入状态消息显示在 **Recurring Rule Update Imports** 部分下方。

步骤 5 在**导入频率 (Import Frequency)** 字段中，指定：

- 更新频率（**每天 [Daily]**、**每周 [Weekly]** 或**每月 [Monthly]**）
- 要发生更新的周日期或月日期
- 要开始更新的时间

步骤 6 如果要在更新完成后自动将已更改的配置重新部署到受管设备，请选中**在规则更新完成后将已部署的策略部署到目标设备 (Deploy updated policies to targeted devices after rule update completes)** 复选框。

步骤 7 点击**保存 (Save)**。

注意 如果在安装入侵规则更新时收到错误消息，请联系支持部门。

Recurring Rule Update Imports 部分下方的状态信息会发生变化，以指明尚未运行规则更新。

本地入侵规则文件导入

导入本地规则文件时，请遵循以下准则：

- 规则导入程序要求以 ASCII 或 UTF-8 编码的纯文本文件导入所有自定义规则。
- 文本文件名称可包含字母数字字符和空格，不可包含除下划线 (_)、句号 (.) 和破折号 (-) 以外的其他特殊字符。
- 系统会导入以一个井号 (#) 开头的本地规则，但它们被标记为已删除。
- 系统会导入以一个井号 (#) 开头的本地规则，但不会导入以两个井号 (##) 开头的本地规则。

- 规则不能包含任何转义字符。
- 导入本地规则时，不必指定生成器 ID (GID)。如果要执行此操作，可以仅为标准文本规则指定 GID 1，为敏感数据规则指定 GID 138。
- 首次导入规则时，请**勿**指定 Snort ID (SID) 或修订版本号。这可避免与其他规则的 SID 发生冲突，包括已删除的规则。系统会自动为规则分配下一个可用的自定义规则 SID（1000000 或更高） 以及版本号 1。

  在多域部署中，系统会从 Firepower 管理中心上所有域使用的共享池将 SID 分配给已导入的规则。如果多个管理员同时导入本地规则，则单个域中的 SID 可能不连续，因为系统已将该序列的中间编号分配给其他域。
- 导入之前已导入的本地规则的更新版本时，或者重新安装已删除的本地规则时，**必须**包含由系统分配的 SID 以及高于当前编号的修订版本号。您可以通过编辑规则确定当前或已删除规则的修订版本号。

  注释 删除本地规则时，系统会自动增加修订版本号；这样方便恢复本地规则。所有已删除的本地规则从会从本地规则类别转移到已删除规则类别。
- 如果规则包含以下任意一项，则导入失败：

  大于 2147483647 的 SID

  多于 64 个字符的源或目的端口列表
- 如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。
- 所有导入的本地规则都会自动保存在本地规则类别中。
- 系统始终将导入的本地规则设置为禁用状态。必须手动设置本地规则的状态后，才能将其用于入侵策略中。

导入本地入侵规则文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

按如下所述导入的入侵规则保存在本地规则类别中。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击**规则更新 (Rule Updates)** 选项卡。

步骤 3 选择**要上传并安装的规则更新或文本规则文件 (Rule Update or text rule file to upload and install)**，然后点击**浏览 (Browse)** 以浏览到您的规则文件。

步骤 4 点击 **Import**。

接下来的操作

- 确保在入侵策略中启用适当的规则。
- 部署配置更改；请参阅部署配置更改，第 254 页。

规则更新日志

Firepower 管理中心会为导入的规则更新和本地规则文件生成记录。

每个记录都包含时间戳、导入文件的用户名称以及指明导入成功或失败的状态图标。可保留导入的所有规则更新和本地规则文件的列表，删除列表中的任何记录，以及访问有关所有导入的规则和规则更新组成部分的详细记录。

Rule Update Import Log 详细视图列出导入到规则更新或本地规则文件中的每个对象的详细记录。此外，还可以根据列出的记录创建仅包含符合特定需求的信息的自定义工作流程或报告。

入侵规则更新日志表

表 *20*：入侵规则更新日志字段

字段	说明
摘要	导入文件的名称。如果导入失败，文件名称下方会显示有关导入失败原因的简要说明。
Time	导入开始的时间和日期。
用户 ID	触发导入的用户的用户名。

字段	说明
状态	导入有以下状态： • 成功 ( ) • 失败或当前在进行中 ( ) 导入过程中，Rule Update Log 页面上会显示红色状态图标，表示导入失败或未完成；成功完成导入后，该红色状态图标会变为绿色状态图标。

提示 可以在入侵规则更新导入正在进行中时查看显示的导入详细信息。

查看入侵规则更新日志

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

提示 您也可以点击入侵规则编辑器页面 (**对象 (Objects)** > **入侵规则 (Intrusion Rules)**) 上的**导入规则 (Import Rules)**。

步骤 2 点击**规则更新 (Rule Updates)** 选项卡。

步骤 3 点击 **Rule Update Log**。

步骤 4 此时您有两种选择：

- 查看详细信息 - 要查看规则更新或本地规则文件中导入的每个对象的详细信息，请点击要查看的文件旁边的图标 ( )；请参阅查看入侵规则更新导入日志的详细信息，第 135 页。
- 删除 - 要删除导入日志中的导入文件记录（包括文件中包含的所有对象的详细记录），请点击导入文件名旁边的删除图标 ( )。

  注释 删除日志中的文件并不会删除导入到导入文件中的任何对象，而只是删除导入日志记录。

规则更新导入日志详细视图

提示 即使是通过在仅显示单个导入文件的记录的 Rule Update Import Log 详细视图中工具栏上点击 **Search** 发起搜索，也可以搜索整个规则更新导入日志数据库。确保将时间限制条件设置为包含所有搜索中要包含的对象。

表 *21*：规则更新导入日志详细视图字段

字段	说明
操作	指明对对象类型执行了以下其中一项操作： • `new`（对于规则而言，是指第一次把规则存储在设备上） • `changed`（对于规则更新组成部分或规则而言，规则更新组成部分已被修改，或者规则的版本号更高且 GID 和 SID 相同） • `collision`（对于规则更新组成部分或规则而言，由于版本与设备上的现有组成部分或规则冲突，因此跳过导入） • `deleted`（对于规则而言，已从规则更新删除规则） • `enabled`（对于规则更新编辑而言，已在系统提供的默认策略中启用了预处理器、规则或其他功能） • `disabled`（对于规则而言，已在系统提供的默认策略中禁用规则） • `drop`（对于规则而言，已在系统提供的默认策略中将规则设置为“丢弃并生成事件”[Drop and Generate Events]） • `error`（对于规则更新或本地规则文件而言，导入失败） • `apply`（为导入启用了**在规则更新导入完成后重新应用所有策略 [Reapply all policies after the rule update import completes]** 选项）
默认操作	规则更新定义的默认操作。当导入对象类型是 `rule` 时，默认操作是 `Pass`、`Alert` 或 `Drop`。对于所有其他导入对象类型，没有默认操作。
Details	组成部分或规则独有的字符串。对于规则、GID、SID 以及已更改规则的上一个版本号，此字段显示为 `previously (GID:SID:Rev)`。对于未更改的规则，此字段为空白。
域	其入侵策略可使用更新规则的域。后代域中的入侵策略也可以使用该规则。此字段只存在于多域部署中。
GID	规则的生成器 ID。例如，`1`（标准文本规则）或 `3`（共享对象规则）。
Name	导入对象的名称（对于规则，对应的是规则Message字段；对于规则更新，对应的是组成部分名称）。

字段	说明
策略	对于导入的规则而言，此字段显示为 `All`，表示导入的规则包含在所有默认入侵策略中。对于其他导入对象类型，此字段为空白。
Rev	规则的版本号。
Rule Update	规则更新文件名。
SID	规则的 SID。
Time	导入开始的时间和日期。
Type	导入对象的类型，可以是以下类型之一： • `rule update component`（已导入的组成部分，例如规则包或策略包） • `rule`（对于规则而言，是指新的或更新后的规则；请注意，在版本 5.0.1 中，此值替换为 `update` 值，后者已被弃用） • `policy apply`（为导入启用了**在规则更新导入完成后重新应用所有策略 [Reapply all policies after the rule update import completes]** 选项）
计数	记录数 (`1`)。当表受限时，Count 字段显示在表视图中，而且在默认情况下，Rule Update Log 详细视图受限于规则更新记录。此字段不可搜索。

查看入侵规则更新导入日志的详细信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击**规则更新 (Rule Updates)** 选项卡。

步骤 3 点击 **Rule Update Log**。

步骤 4 点击要查看的详细记录的文件的旁边的视图图标 ( )。

步骤 5 可以采取以下任何操作：

- 书签 - 要将当前页面加入书签，请点击**将此页面加入书签 (Bookmark This Page)**。

- 编辑搜索 - 要打开使用当前单一限制预填充的搜索页面，请选择“搜索限制”(Search Constraints)旁边的**编辑搜索 (Edit Search)** 或**保存搜索 (Save Search)**。
- 管理书签 - 要导航至书签管理页面，请点击**报告设计器 (Report Designer)**。
- 报告 - 要根据当前视图中的数据生成报告，请点击**报告设计器 (Report Designer)**。
- 搜索 - 要搜索整个规则更新导入日志数据库以查找规则更新导入记录，请点击**搜索 (Search)**。
- 排序 - 要对当前工作流程页面上的记录进行排序和限制，请参阅使用向下钻取页面，第 1450 页以了解详细信息。
- 切换工作流程 - 要暂时使用其他工作流程，请点击（**切换工作流程**）**([switch workflows])**。

地理位置数据库更新

思科地理位置数据库 (GeoDB) 是与可路由 IP 地址关联的地理数据（例如国家/地区、城市、坐标）以及与连接相关的数据（例如互联网运营商、域名、连接类型）的数据库。系统检测与已经检测到的 IP 地址匹配的 GeoDB 信息时，可查看与 IP 地址相关的地理定位信息。要查看除国家/地区或大洲以外的任何地理定位详细信息，必须在系统上安装 GeoDB。思科定期发布 GeoDB 更新。

要更新 GeoDB，请使用 Firepower 管理中心上的“地理位置更新”(Geolocation Updates) 页面（**系统 [System] > 更新 [Updates] > 地理位置更新 [Geolocation Updates]**）。将从支持部门获得的 GeoDB 更新上传到设备后，这些更新会显示在该页面中。

注释 手动或通过点击“地理位置更新”(Geolocation Updates) 页面上的**从支持站点下载并安装地理位置更新 (Download and install geolocation update from the Support Site)**，直接从支持站点下载更新。如果通过邮件传输更新文件，可能会损坏该文件。

更新 GeoDB 所需的时间取决于设备；安装过程一般需要30 到 40 分钟。虽然 GeoDB 更新不会中断任何其他系统功能（包括持续收集地理定位信息），但是，这个过程确实会耗用系统资源。制定更新计划时需要考虑这一点。

GeoDB 更新将会覆盖之前的所有 GeoDB 版本并立即生效。更新 GeoDB 时，Firepower 管理中心会自动更新其受管设备上的相关数据。GeoDB 更新可能需要几分钟时间才能在整个部署中生效。更新后，无需重新部署。

手动更新 GeoDB（互联网连接）

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

仅当设备可访问互联网时才能通过自动连接到支持站点来导入新的 GeoDB 更新。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击 **Geolocation Updates** 选项卡。

步骤 3 选择**从支持站点下载并安装地理位置更新 (Download and install geolocation update from the Support Site)**。

步骤 4 点击 **Import**。
系统对地理位置更新任务排队，该任务会检查思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 上的最新更新。

步骤 5 或者，监控任务状态；请参阅查看任务消息，第 239 页。

步骤 6 完成更新后，返回到“地理位置更新”(Geolocation Updates) 页面，或者选择**帮助 (Help)** > **关于 (About)** 以确认 GeoDB 内部版本号与所安装的更新相匹配。

手动更新 GeoDB（无互联网连接）

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

如果 Firepower 管理中心没有互联网访问权限，则可以将 GeoDB 更新从思科支持站点下载到网络上的本地计算机，然后手动将它上传到 Firepower 管理中心。

过程

步骤 1 从思科支持站点 (http://www.cisco.com/cisco/web/support/index.html) 手动下载更新。

步骤 2 选择**系统 (System)** > **更新 (Updates)**。

步骤 3 点击 **Geolocation Updates** 选项卡。

步骤 4 选择**上传并安装地理位置更新 (Upload and install geolocation update)**。

步骤 5 浏览到已下载的更新，然后点击**上传 (Upload)**。

步骤 6 点击 **Import**。

步骤 7 或者，监控任务状态；请参阅查看任务消息，第 239 页。

步骤 8 完成更新后，返回到“地理位置更新”(Geolocation Updates) 页面，或者选择**帮助 (Help)** > **关于 (About)** 以确认 GeoDB 内部版本号与所安装的更新相匹配。

安排 GeoDB 更新

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理

可自动运行周期性地理位置数据库 (GeoDB) 更新。周期性 GeoDB 更新每 7 天（每周）运行一次；可配置每周更新运行时间。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击 **Geolocation Updates** 选项卡。

步骤 3 在**周期性地理位置更新 (Recurring Geolocation Updates)** 下，选择**启用周期性每周更新 (Enable Recurring Weekly Updates)** 复选框。

步骤 4 在 **Update Start Time** 字段中，指定想要每周 GeoDB 更新运行的周日和时间。

步骤 5 点击**保存 (Save)**。

第 7 章

备份和还原

以下主题介绍如何在 Firepower 系统中使用备份和还原功能：

备份和恢复简介

备份和恢复是所有系统维护计划的重要部分。当每个组织的备份计划极具个性化时，Firepower 系统会提供数据存档机制，以便在灾难情况下可以恢复来自 Firepower 管理中心或物理受管设备的数据。

备份和恢复操作

可以将备份文件保存到设备或本地计算机。如果您是使用 Firepower 管理中心来执行备份，则可以使用远程存储。

注释 当系统收集备份数据时，在数据关联过程中可能会临时暂停，并且系统可能会阻止您更改与备份相关的配置。

请注意有关备份和恢复的以下限制：

- 仅当两个设备是同一型号且运行相同版本的 Firepower 系统软件时，才能将备份恢复到替换设备上。
- 备份不包括捕获的文件数据。
- 您**不能**创建或恢复 NGIPSv或 ASA FirePOWER 模块的备份文件。要备份事件数据，请对管理 Firepower 管理中心执行备份。
- 请勿使用备份和恢复过程在设备之间复制配置。备份文件包含唯一识别设备的信息，并且不能共享。
- 在恢复 Firepower 管理中心后，必须应用最新的入侵规则更新。
- 与 PKI 对象关联的私有密钥在存储到设备时生成随机加密密钥。如果执行包含与 PKI 对象关联的私人密钥的备份，在被纳入未加密备份文件之前密钥将解密。在安全的位置存储备份文件。
- 如果恢复包含与 PKI 对象关联的私钥的备份，则系统会使用随机生成的密钥加密这些密钥，然后再将其存储在设备上。
- 如果恢复包含已启用干净的列表或自定义检测列表的文件策略的备份，则系统会将任何现有文件列表与要恢复的文件列表合并。
- 如果执行备份，再删除已审核的入侵事件，然后使用该备份进行恢复，则系统会恢复已删除的入侵事件，但不恢复其已审核状态。应在 Intrusion Event 下，而不是在 Reviewed Events 下查看这些恢复的入侵事件。
- 如果在已经包含数据的设备上恢复包含入侵事件数据的备份，将创建重复事件。为避免这种情况，仅限在不包含以往恢复入侵事件数据的设备上恢复入侵事件备份。
- 如果已配置与安全区域的任何接口关联，则不会备份这些关联。在恢复后，必须重新配置它们。
- 在 Firepower 管理中心上，备份和恢复功能仅在全局域中可用。您可以在子域范围内使用导出和导入功能作为备份和恢复的替换。

备份文件

系统根据您执行备份的类型备份不同数据。请注意系统**不会**备份捕获的文件数据。使用下表确定要执行哪种备份。

表 *22*：按备份类型存储的数据

备份类型	包括配置数据？	包括事件数据？	包括统一文件？
Firepower 管理中心	是	是	否
7000 和 8000 系列，从设备本身执行	是	否	否
7000 和 8000 系列，从管理 Firepower 管理中心执行	是	否	是

注释 您**不能**创建或恢复 NGIPSv 设备或 ASA FirePOWER 模块的备份文件。要备份事件数据，请对管理Firepower 管理中心执行备份。

除事件数据外，还应定期保存包含恢复设备所需的所有配置文件的备份文件。在测试配置更改时也可能需要备份系统，以便可以根据需要还原已保存的配置。可以选择将备份文件保存到设备或本地计算机。

此外，或者如果备份文件超过4GB，还可以通过SCP将其复制到远程主机。从本地计算机上传的备份文件不能超过 4 GB，因为网络浏览器不支持这样大的上传文件。在 Firepower 管理中心上，备份文件可以保存到远程位置。

备份 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

开始之前

- 请确保您的设备具有足够的磁盘空间；如果备份进程使用90%以上的可用磁盘空间，则备份可能会失败。如有必要，请删除旧备份文件，将旧备份文件从设备中转移或使用远程存储；请参阅远程存储管理，第 446 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 点击 **Firepower 管理备份 (Firepower Management Backup)**。

步骤 3 键入**名称 (Name)**。

步骤 4 您有两个其他选择：

- 要归档配置，请选择 **Back Up Configuration**。在多域部署中，不能禁用此选项。
- 要归档整个事件数据库，请选择 **Back Up Events**。

步骤 5 如果要在备份完成时收到通知，请选中**邮件 (Email)** 复选框并在随附文本框中键入邮箱地址。

注释 要接收邮件通知，您必须配置中继主机，如配置邮件中继主机和通知地址，第 458 页中所述。

步骤 6 要使用安全复制 (SCP) 将备份存档复制到其他计算机，请选中**完成时复制 (Copy when complete)** 复选框，然后在随附的文本框中键入以下信息：

- 在 **Host** 字段中，键入要复制备份的机器的主机名或 IP 地址
- 在 **Path** 字段中，键入要复制备份目录路径
- 在 **User** 字段中，键入要用于登录 Telnet 远程机器的用户名
- 在**密码 (Password)** 字段中，键入该用户名的密码。如果希望使用 SSH 公共密钥而不是密码来访问远程机器，则必须将 **SSH Public Key** 字段中的内容到该机器上指定用户的 `authorized_keys` 文件中。

提示 在此选项处于清除状态时，系统在远程服务器上存储备份期间使用的临时文件；选择此选项时，**不**在远程服务器上存储临时文件。思科建议定期将备份保存到远程位置，以便可以在系统故障时恢复设备。

步骤 7 您有以下选择：

- 要将备份文件保存到设备，请点击 **Start Backup**。备份文件会保存到 `/var/sf/backup` 目录中。
- 要将此配置保存为可供以后使用的备份配置文件，请点击 **Save As New**。

接下来的操作

- 如果备份文件包含 KPI 对象数据，请将其存储在安全位置中，因为私钥在备份中以未加密形式存储。

本地备份受管设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	不适用	管理员/维护人员

必须使用设备的本地 Web 界面执行此程序。

开始之前

- 请确保您的设备具有足够的磁盘空间；如果备份进程使用90%以上的可用磁盘空间，则备份可能会失败。如有必要，请删除旧备份文件，或者将旧备份文件从设备中转移。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 点击 **Device Backup**。

步骤 3 在 **Name** 字段中，键入一个备份文件名称。

步骤 4 如果要在备份完成时收到通知，请选中**邮件 (Email)** 复选框并在随附文本框中键入邮箱地址。

注释 要接收邮件通知，您必须配置中继主机，如配置邮件中继主机和通知地址，第 458 页中所述。

步骤 5 如果要使用安全复制 (SCP) 将备份存档复制到其他计算机，请选中**完成时复制 (Copy when complete)** 复选框，然后在随附文本框中键入以下信息：

- 在**主机 (Host)** 字段中，键入要复制备份的计算机的主机名或 IP 地址。
- 在**路径 (Path)** 字段中，键入要复制备份的目录的路径。
- 在**用户 (User)** 字段中，键入要用于登录到远程计算机中的用户名。
- 在**密码 (Password)** 字段中，键入该用户名的密码。如果希望使用 SSH 公共密钥而不是密码来访问远程机器，则必须将 **SSH Public Key** 字段中的内容到该机器上指定用户的 `authorized_keys` 文件中。

提示 在此选项处于清除状态时，系统在远程服务器上存储备份期间使用的临时文件；选择此选项时，**不**在远程服务器上存储临时文件。思科建议定期将备份保存到远程位置，以便可以在系统故障时恢复设备。

步骤 6 您有以下选择：

- 要将备份文件保存到设备，请点击 **Start Backup**。备份文件会保存到 `/var/sf/backup` 目录中。
- 要将此配置保存为可供以后使用的备份配置文件，请点击 **Save As New**。

接下来的操作

- 如果备份文件包含 KPI 对象数据，请将其存储在安全位置中，因为私钥在备份中以未加密形式存储。

从 Firepower 管理中心备份受管设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	仅全局	管理员/维护人员

开始之前

- 请确保您的设备具有足够的磁盘空间；如果备份进程使用 90% 以上的可用磁盘空间，则备份可能会失败。如有必要，请删除旧备份文件，将旧备份文件从设备中转移或使用远程存储；请参阅远程存储管理，第 446 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 选择 **Managed Device Backup**。

步骤 3 在 **Managed Devices** 字段，选择一个或多个受管设备。

步骤 4 除配置数据外，如果还要包含统一文件，请选择 **Include All Unified Files** 复选框。统一文件是受管设备尚未发送到 Firepower 管理中心进行分析和存储的事件数据的二进制文件。

步骤 5 要将备份文件的副本保存在 Firepower 管理中心上，请选中**检索到管理中心 (Retrieve to Management Center)** 复选框。要将每个设备的备份文件仅保存在设备自身上，请保持不选中此复选框。

注释 如果选中**检索到管理中心 (Retrieve to Management Center)**，但是 Firepower 管理中心配置用于备份的远程存储，则系统会将设备备份文件保存到所配置的远程位置。

步骤 6 点击 **Start Backup**。备份文件会保存到 `/var/sf/backup` 目录中。

接下来的操作

- 如果备份文件包含 KPI 对象数据，请将其存储在安全位置中，因为私钥在备份中以未加密形式存储。

创建备份配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	仅全局	管理员/维护人员

必须使用设备的 Web 用户界面执行此程序。

可以创建包含要用于不同备份类型的设置的备份配置文件。稍后可以在设备上备份文件时，选择这两个配置文件。

提示 使用新文件名创建Firepower管理中心的备份文件时，系统自动创建具有该名称的备份配置文件。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 点击 the **Backup Profiles** 选项卡。

步骤 3 点击 **Create Profile**。

步骤 4 键入一个备份配置文件名称。

步骤 5 配置备份配置文件。请参阅备份 Firepower 管理中心 ， 第 141 页。

步骤 6 点击 **Save As New** 来保存备份配置文件。

从本地主机上传备份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	仅全局	管理员/维护人员

可以将备份文件从本地主机上传到某台设备。必须使用设备的 Web 界面执行此程序。

如果备份文件包含 PKI 对象，在上传时，系统将重新加密与内部 CA 关联的私钥以及具有随机生成密钥的内部证书对象。

开始之前

- 使用下载功能将备份文件下载到本地主机，如备份管理页面 ， 第 146 页中所述。

- 通过 SCP 将大于 4GB 的备份从本地主机上复制到远程主机，并从远程主机将它检索到您的 Firepower 管理中心，因为浏览器不支持上传如此大的文件。有关详细信息，请参阅远程存储管理，第 446 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 点击 **Upload Backup**。

步骤 3 点击**浏览 (Browse)**，然后导航至要上传的备份文件并将其选定。

步骤 4 点击**上传备份 (Upload Backup)**。

步骤 5 点击 **Backup Management** 以返回 Backup Management 页面。

接下来的操作

- 在设备验证文件完整性之后，刷新“备份管理”(Backup Management) 页面以显示详细文件系统信息。

备份管理页面

如果备份文件包含 PKI 对象，在上传时，系统将重新加密与内部 CA 关联的私钥以及具有随机生成密钥的内部证书对象。

如果使用本地存储，备份文件将保存到 `/var/sf/backup`，`/var` 分区中使用的磁盘空间将在“备份管理”(Backup Management) 页面底部列出。在 Firepower 管理中心中，选择“备份管理”(Backup Management) 页面顶部的**远程存储 (Remote Storage)** 来配置远程存储选项；然后为了启用远程存储，请在“备份管理”(Backup Management) 页面选择**为备份启用远程存储 (Enable Remote Storage for Backups)** 复选框。如果使用远程存储，协议、备份系统和备份目录将列在页面底部。

下表说明在 Backup Management 页面的各列和图标。

表 23: Backup Management

功能	说明
系统信息	原始设备名称、类型和版本。注意只能将备份恢复到同样的设备类型和版本。
创建日期	备份文件创建的日期和时间
文件名	备份文件的全名
VDB Version	备份时在设备上运行的漏洞数据库 (VDB) 版本。
位置	备份文件的位置

功能	说明
Size (MB)	备份文件的大小，以兆字节计算
Events?	“是”表示包括事件数据的备份
查看	点击备份文件的名称可查看压缩备份文件中的文件列表。
恢复	点击所选的备份文件可将其恢复其到设备。如果 VDB 版本与备份文件中的 VDB 版本不相符，将禁用此选项。
下载	点击所选的备份文件可将其保存到本地计算机。
Delete	点击所选的备份文件可将其删除。
升级	在Firepower 管理中心中，当选择先前创建的本地备份时，点击可将备份发送到指定的远程备份位置。

从备份文件恢复设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	仅全局	管理员/维护人员

使用 Backup Management 页面，可以从备份文件恢复设备。必须使用设备的 Web 界面执行此程序。

注意

- 此操作会覆盖所有配置文件，并在受管设备上覆盖所有事件数据。
- 请勿将在虚拟Firepower管理中心上创建的备份恢复到物理Firepower管理中心中，这可能会对系统资源造成压力。如果必须在物理Firepower 管理中心上恢复虚拟备份，请与技术支持部门联系。

注释

如果在备份完成后添加许可证，即使备份恢复，这些许可证不会删除也不会被覆盖。为防止恢复时出现冲突，请在恢复备份之前移除这些许可证，记住许可证使用位置，并在恢复备份之后添加和重新配置它们。如果发生冲突，请与技术支持部门联系。

开始之前

- 确认备份文件中的 VDB 版本与设备上的当前 VDB 版本相匹配。有关详细信息，请参阅查看仪表板 ， 第 198 页。

- 在备份完成后删除添加到设备的任何许可证，然后再恢复该备份，以避免在恢复时发生冲突。有关详细信息，请参阅Firepower 系统许可，第 103 页。
- 如果需要在物理 Firepower 管理中心上恢复虚拟备份，请与技术支持部门联系。
- 由于在此类情况下恢复备份会创建重复事件，请确认设备没有与备份中所存储相同的入侵事件数据。有关详细信息，请参阅入侵事件，第 1539 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**。

步骤 2 点击备份文件以查看其内容。详细信息包括文件所有者、文件权限、文件大小和日期。

步骤 3 选择**系统 (System)** > **工具 (Tools)** > **备份/恢复 (Backup/Restore)**以返回到“备份管理”(Backup Management) 页面。

步骤 4 选择要恢复的备份文件。

步骤 5 点击 **Restore**。

注释 如果备份中的 VDB 版本与设备上当前安装的 VDB 版本不匹配，则**恢复 (Restore)** 按钮会灰显。

步骤 6 要恢复文件，请选择以下任一选项或同时选择两个选项：

- **Replace Configuration Data**

  注释 从备份文件恢复受管设备的配置时，从设备的管理 Firepower 管理中心进行的任何设备配置更改也将恢复。恢复备份文件将会覆盖在创建该备份文件后进行的更改。

- **Restore Event Data**

步骤 7 点击 **Restore**。

步骤 8 重新启动设备。

接下来的操作

- 导入最新的思科规则更新；请参阅一次性手动更新入侵规则，第 128 页。如果在导入过程中重新部署策略，则无需部署配置更改（见下文）。
- 部署配置更改；请参阅部署配置更改，第 254 页。
- 在恢复备份之前，添加并重新配置已从设备中删除的任何许可证。
- 如果设备显示在恢复时发生许可证冲突，请联系支持人员。

第 8 章

配置导入和导出

以下主题介绍如何使用导入/导出功能：

配置导入/导出简介

可以使用导入/导出功能在设备之间复制配置。导入/导出不是备份工具，但可简化将新设备添加到部署的过程。

您可导出单项配置，也可立即导出一组（相同类型或不同类型的）配置。当您稍后将软件包导入另一台设备时，您可选择要导入软件包中的哪些配置。

注释 如果导出使用包含私钥的PKI对象的配置，系统会在导出之前解密私钥。导入时，系统会使用随机生成的密钥加密密钥。

导出的数据包包含该配置的版本信息，从而确定是否可以将该配置导入到另一设备上。当设备兼容但数据包包含重复配置时，系统会提供解决方法选项。您还必须将导入的配置中使用的任何安全区域映射到导入 Firepower 管理中心管理的匹配类型区域。

注释 导入和导出设备必须运行相同版本的 Firepower 系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。如果版本不匹配，导入将失败。您可以使用导入/导出功能更新入侵规则。相反，请下载并应用最新的规则更新版本。

导出关联的配置

当导出配置时，系统也会导出其他所需的配置。例如，导出访问控制策略也会导出策略调用的任何子策略、策略使用的对象、祖先策略（在多域部署中），等等。又例如，如果导出启用了外部身份验证的平台设置策略，则也会导出身份验证对象。但是，也有一些例外：

- 系统提供的数据库和源 - 系统不会导出 URL 过滤类别和信誉数据、思科情报源数据或地理位置数据库 (GeoDB)。确保部署中的所有设备可从思科获取最新信息。
- 全局安全情报列表 - 系统会导出与导出的配置关联的全局安全情报黑名单和白名单。（在多域部署中，不管当前域如何，都会发生此情况。系统**不**导出后代域列表。）导入过程将这些黑名单和白名单转换为用户创建的列表，然后将这些新列表用于导入的配置中。这可确保导入的列表不会与现有全局黑名单和白名单发生冲突。要在导入的配置中对导入 Firepower 管理中心使用全局列表，请手动添加这些列表。
- 入侵策略共享层 - 导出过程会中断入侵策略共享层。以前共享的层包含在数据包中，而导入的入侵策略不包含共享层。
- 入侵策略默认变量集 - 导出数据包包含一个默认变量集，此变量集包含自定义变量及带用户定义值的系统提供的变量。导入过程会使用导入的值更新导入 Firepower 管理中心上的默认变量集。但是，导入过程**不**会删除不存在于导出数据包中的自定义变量。对于在导出数据包中未设置的值，导入过程也不会恢复导入Firepower管理中心上的用户定义值。因此，如果导入Firepower管理中心具有配置不同的默认变量，则导入的入侵策略的行为可能会与预期大不相同。
- 对象 - 系统会导出与导出的配置关联的对象和对象组。导入过程始终会将这些从属对象和对象组作为新对象和对象组导入。您无法替换现有对象和对象组。如果需要，系统会将自动生成的编号附加到新对象和对象组以使其唯一。

支持导入/导出的配置

以下配置支持导入/导出：

- 访问控制策略及其调用的策略：网络分析、入侵、SSL、文件
- 入侵策略，与访问控制无关
- 平台设置
- 运行状况策略
- 警报响应
- 应用检测器（用户定义的检测器以及那些由思科专业服务提供的检测器）
- 控制面板
- 自定义表
- 自定义工作流程
- 保存的搜索
- 自定义用户角色
- 报告模板

- 第三方产品和漏洞映射

导出配置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

导出过程可能需要几分钟，取决于正在导出的配置数量以及这些配置引用的对象数量。

提示

Firepower 系统中的许多列表页面的列表项旁均包括导出图标 ()。如果该图标存在，您可将其作为下列导出步骤的快速替代项。

开始之前

- 确认导入和导出设备运行的是同一版本的 Firepower 系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **导出/导出 (Import/Export)**。

点击折叠 () 和展开 () 图标以折叠和展开可用配置列表。

步骤 2 选中要导出的配置并点击**导出 (Export)**。

步骤 3 按照网页浏览器提示将已导出软件包保存至计算机。

导入配置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

视乎正在导入的配置数量以及这些配置所引用的对象数量，导入过程可能需要几分钟。

开始之前

- 确认导入和导出设备运行的是同一版本的 Firepower 系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

- 在类型与要导入的访问控制策略中的区域类型相匹配的导入 Firepower 管理中心上创建安全区域。有关信息，请参阅安全区域，第 309 页。

过程

步骤 1 在导入设备上，选择**系统 (System)** > **工具 (Tools)** > **导出/导出 (Import/Export)**。

步骤 2 点击 **Upload Package**。

步骤 3 输入已导出的软件包的路径或浏览到其位置，然后点击**上传 (Upload)**。

步骤 4 如果没有版本不匹配情况或其他问题，请选择要导入的配置，然后点击**导入 (Import)**。
如果无需执行任何冲突解决方案或安全区域映射，则表明导入完成，并会显示成功消息。跳过此程序的其余步骤。

步骤 5 如果提示，请在访问控制导入解决方案 (Access Control Import Resolution) 页面上，将已导入的配置中使用的安全区域映射到具有由导入 Firepower 管理中心管理的匹配接口类型的区域。

步骤 6 点击 **Import**。

步骤 7 如果提示，请在“导入解决方案”(Import Resolution) 页面上，展开每项配置并选择相应的选项，如解决导入冲突，第 152 页中所述。

步骤 8 点击 **Import**。

解决导入冲突

当您尝试导入配置时，系统会确定设备上是否已存在同一名称和类型的配置。在多域部署中，系统还会确定某个配置是在当前域还是在其任何祖先域或后代域中定义的配置的重复。（您无法查看后代域中的配置，但如果后代域中存在具有重复名称的配置，则系统会通知您发生冲突。）当导入包含重复配置时，系统会提供适合于您的部署的解决方法选项，其中包括：

- **保持现有配置 (Keep existing)**

  系统不导入该配置。

- **替换现有配置 (Replace existing)**

  系统使用选择用于导入的配置覆盖当前配置。

- **保留最新配置 (Keep newest)**

  仅在所选配置的时间戳比设备上的当前配置中的时间戳更新时，系统才会导入所选配置。

- **导入为新配置 (Import as new)**

  系统导入所选重复配置，将系统生成的编号附加到名称以使其唯一。（可以在完成导入过程之前更改此名称。）设备上的原始配置保持不变。

系统提供的解决方法选项取决于部署是否使用域，以及导入的配置是在当前域中定义的配置的重复，还是在当前域的祖先或后代中定义的配置的重复。下表列出系统何时提供或不提供解决方法选项。

解决方法选项	Firepower 管理中心		受管设备
	在当前域中重复	在祖先域或后代域中重复	
保持现有配置 (Keep existing)	是	是	是
替换现有配置 (Replace existing)	是	否	是
保留最新配置 (Keep newest)	是	否	是
导入为新配置 (Import as new)	是	是	是

当导入包含使用干净或自定义检测文件列表的文件策略的访问控制策略，并且文件列表出现重复名称冲突时，系统会提供上表中所述的冲突解决方法选项，但是系统对策略和文件列表执行的操作会有所差异，如下表所述：

解决方法选项	系统操作	
	访问控制策略及其关联的文件策略导入为新策略，并且合并文件列表	现有访问控制策略及其关联的文件策略和文件列表保持不变
保持现有配置 (Keep existing)	否	是
替换现有配置 (Replace existing)	是	否
导入为新配置 (Import as new)	是	否
保持最新配置 (Keep newest)，并且导入的访问控制策略为最新策略	是	否
保持最新配置 (Keep newest)，并且现有访问控制策略为最新策略	否	是

如果修改设备上的已导入配置，然后将该配置重新导入到同一设备，则必须选择要保留的配置版本。

第 9 章

任务安排

以下主题介绍如何安排任务：

任务安排简介

可安排许多不同类型的管理任务在指定时间运行一次或反复运行。

注释 有些任务（例如，那些涉及自动化软件更新的任务，或者要求将更新推送到受管设备的任务）可能会显著增加低带宽网络的负载。应安排此类任务在网络使用量较低的时段运行。

配置周期性任务

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任务相关	任务相关	管理员/维护人员

使用相同流程为所有类型的任务设置周期性任务的频率。

请注意，网络界面上大多数页面中显示的时间为本地时间，由您在本地配置中指定的时区决定。此外，在适当时候，Firepower 管理中心自动针对夏时令 (DST) 调整其本地时间显示。然而，跨越从 DST 到标准时间以及从标准时间到 DST 的过渡日期的周期性任务不因过渡而自行调整。也就是说，如果创建一个任务，预定在标准时间的凌晨 2:00 运行，则它将在 DST 期间的凌晨 3:00 运行。同样，如果创建一个任务，预定在 DST 期间的凌晨 2:00 运行，则它将在标准时间的凌晨 1:00 运行。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择要安排的任务类型。

步骤 4 点击**安排要运行的任务 (Schedule task to run)** 选项旁边的**周期性 (Recurring)** 单选按钮。

步骤 5 在 **Start On** 字段中，指定想要开始周期性任务的日期。

步骤 6 在 **Repeat Every** 字段中，指定想要任务重复的频率。
可键入数字，或者点击向上图标 (▲) 和向下图标 (▼) 指定时间间隔。例如，键入 2 并点击**天数 (Days)** 单选按钮，让任务每两天运行一次。

步骤 7 在 **Run At** 字段中，指定想要开始周期性任务的时间。

步骤 8 如需每周或每月运行一次任务，请在**重复日期 (Repeat On)** 字段中选择要运行任务的天数。

步骤 9 为正在创建的任务类型选择其余选项：

- “备份”(Backup) - 安排备份作业，如自动执行Firepower 管理中心备份，第 157 页中所述。
- “下载 CRL”(Download CRL) - 安排证书撤销列表下载，如配置证书撤销列表下载，第 158 页中所述。
- “部署策略”(Deploy Policies) - 安排策略部署，如自动执行策略部署，第 159 页中所述。
- “Nmap 扫描”(Nmap Scan) - 安排 Nmap 扫描，如安排 Nmap 扫描，第 160 页中所述。
- “报告”(Report) - 安排报告生成，如 中所述 自动执行报告生成，第 161 页
- “Firepower 建议规则”(Firepower Recommended Rules) - 安排 Firepower 建议规则的自动更新，如 中所述 自动生成 Firepower 建议，第 162 页
- “下载最新更新”(Download Latest Update) - 安排软件或 VDB 更新下载，如自动执行软件下载，第 164 页或自动执行 VDB 更新下载，第 167 页中所述。
- “安装最新更新”(Install Latest Update) - 安排在 Firepower 管理中心或受管设备上安装软件或 VDB 更新，如自动执行软件安装，第 165 页或中所述 自动执行 VDB 更新安装，第 167 页
- “推送最新更新”(Push Latest Update) - 安排将软件更新推送到受管设备，如自动执行软件推送，第 165 页中所述。
- “更新 URL 过滤数据库”(Update URL Filtering Database) - 安排 URL 过滤数据的自动更新，如中所述 自动执行 URL 过滤更新，第 168 页

备份任务自动化

可以使用调度程序自动化 Firepower 管理中心或物理受管设备的备份。

要在物理受管设备上执行配置数据的计划备份，请使用设备自身的 Web 界面。

要在 Firepower 管理中心上执行配置和事件数据的计划备份或只执行配置数据的计划备份，请使用 Firepower 管理中心的 Web 界面。安排任务时所选择的备份配置文件决定了备份的数据类型。

不能从受管设备管理的 Firepower 管理中心安排受管设备的备份，但是可以从 Firepower 管理中心执行某些型号的受管设备的按需备份。

自动执行Firepower 管理中心备份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

开始之前

- 创建备份配置文件。请参阅创建备份配置文件，第 145 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表中，选择 **Backup**。

步骤 4 指定要如何安排备份，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**备份配置文件 (Backup Profile)** 列表中，选择相应的备份配置文件。

步骤 7 或者，输入**注释 (Comment)**。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中。请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

自动执行受管设备备份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	不适用	管理员/维护人员

必须使用 7000 或 8000 系列设备的本地 Web 界面执行此程序。

开始之前

创建备份配置文件。请参阅 创建备份配置文件，第 145 页

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表中，选择 **Backup**。

步骤 4 指定要如何安排备份，**一次性 (Once)** 或**周期性 (Recurring)**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**备份配置文件 (Backup Profile)** 列表中，选择相应的备份配置文件。

步骤 7 或者，输入**注释 (Comment)**。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中。请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

配置证书撤销列表下载

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	设备相关	管理员/维护人员

必须使用 Firepower 管理中心或 7000 或 8000 系列设备的本地 Web 界面执行此程序。在多域部署中，仅在 Firepower 管理中心的全局域中支持此任务。

当支持在启用用户证书或审核日志证书的设备上的本地配置中下载证书吊销列表 (CRL) 时，系统会自动创建下载 CRL 任务。可以使用计划程序来编辑任务以设置更新频率。

开始之前

- 启用并配置用户证书，并且设置 CRL 下载 URL。有关详细信息，请参阅需要有效的用户证书，第 433 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择**下载 CRL (Download CRL)**。

步骤 4 指定想要如何安排 CRL 下载，**Once** 或 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 7 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须在Firepower管理中心上配置一台有效的邮件中继服务器，以发送状态消息。

步骤 8 点击**保存 (Save)**。

自动执行策略部署

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

在管理中心中修改配置设置后，必须将这些更改部署到受影响的设备。

在多域部署中，只能为当前域安排策略部署。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表，选择 **Nmap 扫描 (Nmap Scan)**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**设备 (Device)** 字段中，选择要部署策略的设备。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

Nmap 扫描自动化

可在网络上安排定期 Nmap 目标扫描。自动化扫描允许您刷新 Nmap 扫描之前提供的信息。由于 Firepower 系统无法更新 Nmap 提供的数据，因此需要定期重新扫描以保持数据为最新。还可安排扫描，使其自动在网络主机上测试未识别的应用或服务器。

请注意，发现管理员也可使用 Nmap 扫描作为补救。例如，主机上发生的操作系统冲突可能会触发 Nmap 扫描。运行扫描可以获取主机的最新操作系统信息，解决冲突。

如果之前未曾使用 Nmap 扫描功能，则在定义计划扫描之前，需要配置 Nmap 扫描。

安排 Nmap 扫描

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

Nmap 使用 Nmap 扫描结果替换系统检测到的主机操作系统、应用或服务器之后，系统不再更新 Nmap 替换的主机信息。Nmap 提供的服务和操作系统数据保持不变，直至运行另一次 Nmap 扫描。如果计划使用 Nmap 扫描主机，则可能要设置定期安排的扫描，以使 Nmap 提供的操作系统、应用或服务器保持最新。如从网络删除主机并重新添加，则将丢弃任何 Nmap 扫描结果，系统假设监控主机的所有操作系统和服务数据。

在多域部署中：

- 只能为当前域安排扫描
- 选择的补救和 Nmap 目标必须存在于当前域或祖先域中。
- 选择对非枝叶域执行 Nmap 扫描将会扫描该域的每个后代中的相同目标。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Nmap Scan**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在 **Nmap 补救 (Nmap Remediation)** 字段中，选择 Nmap 补救。

步骤 7 在 **Nmap 目标 (Nmap Target)** 字段中，选择扫描目标。

步骤 8 在**域 (Domain)** 字段中，选择要扩充其网络映射的域。

步骤 9 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

提示 注释字段显示在日历计划页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 10 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 11 点击**保存 (Save)**。

自动执行报告生成

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

可自动生成报告，以使它们按固定间隔运行。

在多域部署中，只能为当前域安排报告。

开始之前

- 使用报告设计程序创建报告模板。有关详细信息，请参阅报告模板，第 1342 页。
- 如果要使用调度程序分发邮件报告，请配置邮件中继主机并指定报告收件人和消息信息。请参阅配置邮件中继主机和通知地址，第 458 页和在生成时通过邮件分发报告，第 1365 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Report**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**报告模板 (Report Template)** 字段中，选择报告模板。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Tasks Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。
注释 配置此选项**不会**分发报告。

步骤 9 如果不想在报告没有数据（例如，当报告期间未发生特定类型的事件时）时接收报告邮件附件，请选择 **If report is empty, still attach to email** 复选框。

步骤 10 点击**保存 (Save)**。

自动生成 Firepower 建议

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/维护人员

可使用自定义入侵策略中最近保存的配置设置，根据网络发现数据，自动生成规则状态建议。

注释 如果系统自动为入侵策略生成预定建议并且不保存更改，则必须丢弃在入侵策略中所做出的更改，而且如果想要策略反映自动生成的建议，还必须执行此策略。

当任务运行时，系统自动生成建议规则状态，并且根据策略的配置修改入侵规则的状态。已修改的规则状态在下次部署入侵策略时生效。

在多域部署中，可以在当前域级别自动生成入侵策略的建议。系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶

域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

开始之前

- 在入侵策略中配置 Firepower 建议规则，如 中所述 生成和应用 Firepower 建议，第 848 页
- 如果要通过邮件发送任务状态消息，请配置有效的邮件中继服务器。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从**作业类型 (Job Type)** 列表中，选择 **Firepower 建议规则 (Firepower Recommended Rules)**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中输入名称。

步骤 6 在**策略 (Policies)** 旁边，选择要在其中生成建议的一个或多个入侵策略。选中**所有策略 (All Policies)** 复选框以选择所有策略。

步骤 7 （可选）在**注释 (Comment)** 字段中输入备注。
请保持注释简短。注释显示在计划日历页面的“任务详细信息”(Task Details) 部分中。

步骤 8 （可选）要通过邮件发送任务状态消息，请在**邮件状态收件人：(Email Status To:)** 字段中输入邮件地址（或以逗号分隔的多个邮件地址）。

步骤 9 点击**保存 (Save)**。

软件更新自动化

可自动下载大多数补丁和主要版本，并将其应用到 Firepower 系统。

必须安排安装软件更新的任务因正在更新管理中心还是正在使用管理中心更新受管设备而异。

注释 思科强烈建议使用管理中心更新其管理的设备。

- 要更新管理中心，请使用 Install Latest Update 任务安排软件安装。
- 要使用管理中心自动对其受管设备执行软件更新，必须安排两个任务：

  使用 Push Latest Update 任务将更新推送（复制）至受管设备。

  使用 Install Latest Update 任务在受管设备上安装更新。

对受管设备安排更新时，请连续安排推送和安装任务；必须首先将更新推送到设备，然后才能进行安装。在各任务之间留出足够的时间，以便完成相关过程；安排任务的时间间隔至少应为30分钟。如果安排一个更新安装任务，且更新尚未完成从管理中心到设备的复制，则安装任务将不成功。然而，如果安排的安装任务每天重复一次，它将在第二天运行时安装推送的更新。

注释 在两种情况下，必须手动上传和安装更新。第一，无法安排 Firepower 系统的主要更新。第二，无法为不能访问支持网站的管理中心安排更新，或者无法安排来自这些设备的推送。如果管理中心未直接连接到互联网，应使用管理接口配置设置一个代理，以便其从支持网站下载更新。

请注意，为在设备组上安装更新而安排的任务会将推送的更新同时安装到设备组内的每台设备。请留出足够的时间，以便设备组内的每台设备都可完成安排的任务。

如果想要加大对此过程的控制，可在得知更新已发布之后，在非高峰时段使用 **Once** 选项下载和安装更新。

自动执行软件下载

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

可创建一个预定任务，自动从思科下载最新软件更新。可使用此任务安排下载计划手动安装的更新。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Download Latest Update**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务 ， 第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 选中**更新项目 (Update Items)** 旁边的**软件 (Software)** 复选框。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

自动执行软件推送

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

如果想要在受管设备上自动安装软件更新，必须先将更新推送至设备，然后再安装。

创建向受管设备推送软件更新的任务时，确保在推送任务与预定安装任务之间预留充分时间，以便将更新复制至设备。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Push Latest Update**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**设备 (Device)** 下拉列表中，选择要更新的设备。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

自动执行软件安装

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

请确保在向受管设备推送更新的任务与安装更新的任务之间预留充分的时间。

注意 视乎正在安装的更新，设备可能在安装软件之后重新启动。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Install Latest Update**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**设备 (Device)** 下拉列表中，选择要在其上安装更新的设备（包括 Firepower 管理中心）。

步骤 7 选中**更新项目 (Update Items)** 旁边的**软件 (Software)** 复选框。

步骤 8 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

漏洞数据库更新自动化

思科使用漏洞数据库 (VDB) 更新扩展 Firepower 系统识别的网络资产、流量和漏洞列表。可以使用安排功能更新 VDB，从而确保正在使用最新信息评估网络主机。

自动更新 VDB 时，必须自动完成两个独立的步骤：

- 下载 VDB 更新。
- 安装 VDB 更新。

注意 安装 VDB 更新在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

在任务之间预留充分的时间，以便完成相关过程。例如，如果安排一个更新安装任务，并且更新尚未完全下载，安装任务将不成功。然而，如果安排的安装任务每天重复一次，它将在第二天运行时安装已下载的 VDB 更新。

注意：

- 不能为无法访问支持网站的设备安排更新。如果管理中心未直接连接到互联网，应使用管理接口配置设置一个代理，以便其从支持网站下载更新。
- 如想加大对此过程的控制，可在得知更新已发布之后，在非高峰时段使用 **Once** 选项下载和安装 VDB 更新。
- 在多域部署中，只能为全局域安排 VDB 更新。重新部署策略时，更改才会生效。

自动执行 VDB 更新下载

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Download Latest Update**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

步骤 7 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在日历计划页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 8 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 9 点击**保存 (Save)**。

自动执行 VDB 更新安装

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

在 VDB 更新下载任务与更新安装任务之间预留足够的时间。

注意 安装 VDB 更新在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Install Latest Update**。

步骤 4 指定想要如何安排任务，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 从**设备 (Device)** 下拉列表中，选择管理中心。

步骤 7 在**更新项目 (Update Items)** 旁边，选中**漏洞数据库 (Vulnerability Database)** 复选框。

步骤 8 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。

提示 Comment 字段显示在页面的 View Tasks 部分，因此，应当尽量使其保持简短。

步骤 9 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 10 点击**保存 (Save)**。

自动执行 URL 过滤更新

智能许可证	经典许可证	支持的设备	支持的域	Access
URL 过滤	URL 过滤	任意	仅全局	管理员/维护人员

可使用调度程序，自动从思科综合安全智能 (CSI) 更新 URL 过滤数据。

请注意，启用 URL 过滤时，也可启用自动更新。这会强制管理中心每 30 分钟联系一次 CSI，以获取 URL 过滤数据更新。

注释 如果在启用 URL 过滤时已启用自动更新，则请**勿**创建预定任务来更新 URL 过滤数据。只有在要严格控制 URL 过滤更新时，才应安排任务。

尽管每日更新往往较小，如果距离上次更新已超过五天，新 URL 过滤数据可能需要 20 分钟才能下载完成，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

开始之前

- 确保 Firepower 管理中心能够访问互联网；请参阅安全、互联网接入和通信端口，第 1717 页。
- 启用 URL 过滤。有关详细信息，请参阅配置与综合安全情报的通信，第 773 页。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 点击 **Add Task**。

步骤 3 从 **Job Type** 列表，选择 **Update URL Filtering Database**。

步骤 4 指定想要如何安排更新，**Once** 或者 **Recurring**：

- 对于一次性任务，请使用下拉列表指定开始日期和时间。
- 有关周期性任务，请参阅配置周期性任务，第 155 页以了解详细信息。

步骤 5 在**作业名称 (Job Name)** 字段中键入名称。

步骤 6 如果要对任务进行注释，请在**注释 (Comment)** 字段中输入注释。
注释字段显示在计划日历页面的“任务详细信息”(Task Details) 部分中；请保持注释简短。

步骤 7 如果要通过邮件发送任务状态消息，请在**状态收件人：(Email Status To:)** 字段中输入邮箱地址（或以逗号分隔的多个邮箱地址）。必须配置有效的邮件中继服务器，才能发送状态消息。

步骤 8 点击**保存 (Save)**。

预定任务审核

添加预定任务后，即可查看这些任务，评估它们的状态。在页面的 View Options 部分，查使用日历和预定任务列表查看预定任务。

Calendar 视图选项可用于查看哪些预定任务在哪天发生。

Task List 显示一列任务及其状态。打开日历时，任务列表出现在日历下方。此外，也可通过从日历中选择日期或任务来查看它。

可编辑先前创建的预定任务。如果想要测试一次预定任务，确保参数正确，此功能特别有用。稍后，任务成功完成后，即可将其更改为周期性任务。

可从 Schedule View 页面执行两类删除。可删除尚未运行的特定一次性任务，也可删除周期性任务的每个实例。如果删除周期性任务的一个实例，该任务的所有实例均将删除。如果删除预定运行一次的任务，则仅删除该任务。

任务列表详细信息

表 *24*: 任务列表列

列	说明
Name	显示预定任务的名称及与其关联的注释。
Type	显示预定任务的类型。
开始时间	显示预定任务的开始日期和时间。
频率	显示任务的运行频率。
上次运行时间	显示实际开始日期和时间。 对于周期性任务，这适用于最近执行。
上次运行状态	描述预定任务的当前状态。 • 对号图标 () 指明任务已成功运行。 • 问号图标 () 指明任务处于未知状态。 • 感叹号图标 () 指明任务已失败。 对于周期性任务，这适用于最近执行。
下次运行时间	显示周期性任务的下次执行时间。 为一次性任务显示“不适用”(N/A)。
创建者	显示创建预定任务的用户的名称。
Edit	编辑预定任务。
Delete	删除预定任务。

在日历中查看预定任务

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

在多域部署中，只能查看当前域的预定任务。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 可使用日历视图执行以下任务：

- 点击左向双箭头图标 (<<)，向后移动一年：
- 点击左向单箭头图标 (<)，向后移动一个月。
- 点击右向单箭头图标 (>)，向前移动一个月。
- 点击右向双箭头图标 (>>)，向前移动一年。
- 点击 **Today**，返回当前月份和年份。
- 点击 **Add Task**，安排新任务。
- 点击一个日期，在日历下方的任务列表中查看所有预定任务的特定日期。
- 点击在某个日期发生的特定任务，在日历下方的任务列表中查看此任务。

编辑预定任务

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

在多域部署中，只能为当前域编辑预定任务。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 在日历上，点击要编辑的任务，或者任务出现的日期。

步骤 3 在**任务详细信息 (Task Details)** 表中，点击要编辑的任务表旁边的编辑图标 ()。

步骤 4 编辑任务。

步骤 5 点击**保存 (Save)**。

删除预定任务

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

在多域部署中，只能删除当前域的预定任务。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **安排 (Scheduling)**。

步骤 2 在日历中，点击要删除的任务。对于周期性任务，请点击任务的实例。

步骤 3 在**任务详情 (Task Details)** 表中，点击删除图标 ( )，然后确认您的选择。

第 10 章

管理中心数据库清除

以下主题介绍如何从管理中心清除发现数据：

从管理中心数据库清除数据

智能许可证	经典许可证	支持的域	Access
任何环境	任何环境	仅全局	管理员/安全分析师

可以使用数据库清除页面从管理中心数据库清除发现、身份、连接和安全情报数据文件。请注意，清除数据库时，会重新启动相应的进程。

注意 清除数据库会从Firepower 管理中心中移除指定的数据。删除数据后，该数据无法恢复。

过程

步骤 1 选择**系统 (System)** > **工具 (Tools)** > **数据清除 (Data Purge)**。

步骤 2 在 **Network Discovery** 下，执行以下任一或所有步骤：

- 选中**网络发现事件 (Network Discovery Events)** 复选框以从数据库删除所有网络发现事件。
- 选中**主机 (Hosts)** 复选框以从数据库删除所有主机和危害表现标志。
- 选中**用户活动 (User Activity)** 复选框以从数据库删除所有用户活动事件。
- 选中**用户身份 (User Identities)** 复选框以从数据库删除所有用户登录信息和用户历史记录数据。

步骤 3 在 **Connections** 下，执行以下任一或所有步骤：

- 选中**连接事件 (Connection Events)** 复选框以从数据库删除所有连接数据。
- 选中**连接摘要事件 (Connection Summary Events)** 复选框以从数据库删除所有连接摘要数据。
- 选中**安全情报事件 (Security Intelligence Events)** 复选框以从数据库删除所有安全情报数据。

注释 选中**连接事件 (Connection Events)** 复选框不会删除安全情报事件。与安全情报数据的连接将显示在安全情报事件查看器中。同样，选中**安全情报事件 (Security Intelligence Events)** 复选框不会删除具有关联安全情报数据的连接事件。

步骤 4 点击 **Purge Selected Events**。
项目清除成功并重新启动相应的进程。

第 III 部分

系统监控

第 11 章

控制面板

以下主题介绍如何在 Firepower 系统中使用控制面板：

控制面板简介

Firepower 系统控制面板为您提供当前系统状态的概览视图，包括有关系统收集和生成的事件的数据。您还可以使用控制面板了解有关部署中的设备的状态和整体运行状况的信息。请记住，控制面板提供的信息取决于如何许可、配置和部署系统。

提示 控制面板是一种复杂、高度可定制的监控功能，用于提供详尽的数据。要了解受监控网络的广泛、简短和多种多样的概况，请使用情景管理器。控制面板在 Firepower 管理中心和 7000 和 8000 系列设备上可用。

控制面板使用选项卡显示构件：提供对系统的不同方面的见解的小型独立组件。例如，预定义的“设备信息”(Appliance Information) 构件指示设备名称、型号以及当前运行的 Firepower 系统软件版本。系统通过控制面板时间范围限制构件，可以将其更改为反映短至前一小时或长至前一年的时间段。

系统随附若干可以使用和修改的预定义控制面板。如果用户角色具有控制面板访问权限（“管理员”[Administrator]、“维护用户”[Maintenance User]、“安全分析师”[Security Analyst]、“安全分析师（只读）”[Security Analyst (Read Only)] 和具有控制面板权限的自定义角色），则默认情况下主页是预定义的“摘要控制面板”(Summary Dashboard)。但是，可以配置其他默认主页，包括非控制面板。您还可以更改默认控制面板。请注意，如果用户角色无法访问控制面板，则默认主页与角色相关；例如，发现管理员可以查看“网络发现”(Network Discovery) 页面。

您还可以使用预定义控制面板作为自定义控制面板的基础，可以将其共享或限制为专用。除非您具有管理员访问权限，否则无法查看或修改其他用户创建的专用控制面板。

注释 某些事件的深入查看页面和表视图包含一个 **Dashboard** 工具栏链接，您可以点击查看相关的预定义控制面板。如果删除预定义控制面板或选项卡，则关联的工具栏链接将不起作用。

在多域部署中，无法从祖先域查看控制面板；但是，可以创建新控制面板，这些控制面板是较高级别控制面板的副本。

Firepower 系统控制面板构件

控制面板有一个或多个选项卡，每个选项卡都会以三列布局显示一个或多个构件。Firepower 系统附有许多预定义的控制面板构件，每个构件均提供对 Firepower 系统不同方面的洞察。构件分为三类：

- 分析和报告构件：显示有关 Firepower 系统收集和生成的事件的数据。
- 其他构件：不显示事件数据和运营数据。目前，该类别中仅有的一个构件显示 RSS 源。
- 运行构件：显示有关 Firepower 系统的状态和整体运行状况的信息。

可以查看的控制面板构件取决于：

- 使用的设备类型
- 用户角色
- 当前的域（在多域部署中）

此外，每个控制面板都有一组可确定其行为的首选项。

您可以将构件最小化和最大化，向选项卡添加和从选项卡移除构件，以及在选项卡上重新排列构件。

注释 对于显示某个时间范围内的事件数的构件而言，事件的总数可能无法反映可在事件查看器中查看其详细数据的事件数量。因为系统有时会删掉较旧的事件详情以管理磁盘空间使用情况，所以会发生这种情况。要将事件详情删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。

构件可用性

您可以查看的控制面板构件取决于使用的设备类型、用户角色和当前域（在多域部署中）。

构件可以通过两种方式不可用：

- 无效构件是由于使用错误类型的设备而无法查看的构件。
- 未授权构件是由于用户帐户没有必要的权限而无法查看的构件。

例如，“设备状态”(Appliance Status) 构件仅在管理中心上对于具有管理员、维护用户、安全分析师或安全分析师（只读）帐户权限的用户可用。

虽然无法将未授权或无效的构件添加到控制面板，但是已导入的控制面板可能包含未授权或无效的构件。例如，如果已导入的控制面板满足以下条件，则此类构件可能存在：

- 由具有不同访问权限的用户创建，或者
- 属于祖先域。

不可用构件处于禁用状态，并且显示表明无法查看这些构件的原因的错误消息。

当此类构件超时或出现其他问题时，各个构件也会显示错误消息。

注释 您可以删除或最小化未授权和无效的构件，以及不显示数据的构件。请注意，在共享控制面板中对某个构件的修改会对该设备的所有用户适用。

按平台划分的控制面板构件可用性

构件的内容因使用的平台而异。

下表列出每个平台可以显示的有效构件。

表 *25*: *Firepower* 平台和控制面板构件可用性

构件	管理中心	7000 和 8000 系列设备
Appliance Information	是	是
设备状态	是	否
相关事件	是	否
Current Interface Status	是	是
Current Sessions	是	是
Custom Analysis	是	否
磁盘使用情况	是	是
Interface Traffic	是	是
入侵事件	是	否
Network Compliance	是	否
Product Licensing	是	否
Product Updates	是	是

构件	管理中心	7000 和 8000 系列设备
RSS 源	是	是
系统负载	是	是
系统时间	是	是
White List Events	是	否

按用户角色划分的控制面板构件可用性

下表列出了查看各个构件所需的用户帐户权限。只有具备管理员、维护人员、安全分析师或安全分析师（只读）权限的用户帐户才能使用控制面板。

自定义角色的用户可能访问构件的任何组合，也可能完全不能，具体取决于其用户角色是否许可。

表 *26*：用户角色和控制面板构件可用性

构件	管理员	维护人员	安全分析师	安全分析师（只读）
Appliance Information	是	是	是	是
设备状态	是	是	是	否
相关事件	是	否	是	是
Current Interface Status	是	是	是	是
Current Sessions	是	否	否	否
Custom Analysis	是	否	是	是
磁盘使用情况	是	是	是	是
Interface Traffic	是	是	是	是
入侵事件	是	否	是	是
Network Compliance	是	否	是	是
Product Licensing	是	是	否	否
Product Updates	是	是	否	否

构件	管理员	维护人员	安全分析师	安全分析师（只读）
RSS 源	是	是	是	是
系统负载	是	是	是	是
系统时间	是	是	是	是
White List Events	是	否	是	是

按域划分的控制面板构件可用性

在多域部署中，某些构件在Firepower管理中心全局域中有效，但在子域中无效。下表列出每个域可以显示的有效构件。

表 *27*：域和控制面板构件可用性

构件	支持的域
设备信息	任意
设备状态	任意
相关事件	任意
Current Interface Status	仅全局
Current Sessions	任意
Custom Analysis	任意
磁盘使用情况	仅全局
Interface Traffic	仅全局
入侵事件	任意
Network Compliance	任意
Product Licensing	仅全局
Product Updates	仅全局
RSS 源	任意

构件	支持的域
系统负载	仅全局
系统时间	任意
White List Events	任意

预定义控制面板构件

Firepower 系统随附若干预定义构件，当在控制面板上使用时，可以为您提供当前系统状态的概览视图。这些视图包括：

- 有关系统收集和生成的事件的数据
- 有关部署中的设备的状态和整体运行状况的信息

注释 可以查看的控制面板构件取决于使用的设备、用户角色以及在多域部署中的当前域。

设备信息构件

Appliance Information 构件可提供设备的快照。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。该构件提供：

- 设备名称、IPv4 地址、IPv6 地址和型号
- 在带控制面板的设备上安装的 Firepower 系统软件、操作系统、Snort、规则更新、规则包、模块包、漏洞数据库 (VDB) 和地理位置更新的版本信息，虚拟 Firepower 管理中心除外
- 受管设备与管理设备的通信链路的名称和状态

通过修改构件首选项以显示简单或高级视图，您可以配置构件显示更多或更少信息；首选项还可控制构件的更新频率。

设备状态构件

Appliance Status 构件指示设备及其所管理的任何设备的运行状况。请注意，由于Firepower 管理中心不会自动将运行状况策略应用于受管设备，您必须将运行状况策略手动应用于设备上，否则设备状态会显示为禁用。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

通过修改构件首选项，您可以配置构件以饼形图或表格形式显示设备状态。

首选项还可控制构件的更新频率。

您可以点击饼形图上的某个部分或设备状态表的一个数字转到 Health Monitor 页面，并查看设备及其所管理的任何设备的编译后的运行状况状态。

关联事件构件

Correlation Events 构件按照优先级显示控制面板时间范围内每秒发生关联事件的平均次数。默认情况下，该构件在 Detailed Dashboard 的 Correlation 选项卡中显示。

通过修改构件首选项，可以配置构件以显示不同优先级的关联事件，并选择线性（增量）或对数（十倍）比例。

选中一个或多个**优先级 (Priorities)** 复选框，以分别显示特定优先级事件的图形，包括不具有优先级的事件。选择**全部显示 (Show All)** 以显示所有关联事件的图形，无论其优先级如何。首选项还可控制构件的更新频率。

您可以点击某个图形查看特定优先级的关联事件，或者点击 **All** 图形查看所有关联事件。在任何一种情况下，事件均受到控制面板时间范围的限制；通过控制面板访问关联事件可更改设备的事件（或全球）时间段。

当前接口状态构件

Current Interface Status 构件显示设备上所有接口的状态，已启用或未使用。在Firepower管理中心上，您可以显示管理（`eth0`、`eth1`等等）接口。在受管设备上，可以选择仅显示感知（`s1p1` 等）接口或同时显示管理和感知接口。接口按类型分组：管理、内联、被动、已交换、已路由、已堆栈和未使用。

对于每个接口，该构件都会提供：

- 接口的名称
- 接口的链路状态
- 接口的链路模式（例如，100Mb 全双工或 10Mb 半双工）
- 接口类型，例如，铜或光纤
- 接口接收 (Rx) 和发送 (Tx) 的数据量

代表链路状态的球的颜色指明当前状态，如下所示：

- 绿色：链路正常并且全速运行
- 黄色：链路正常，但未全速运行
- 红色：链路不正常
- 灰色：链路通过管理方式禁用
- 蓝色：链路状态信息不可用（例如，ASA）

构件首选项可控制构件的更新频率。

当前会话构件

Current Sessions 构件显示哪些用户目前已经登录设备、与发起会话的机器相关的 IP 地址，以及各用户最近一次访问设备页面的时间（基于设备的本地时间）。代表用户，也就是说，当前查看构件的

用户，会以用户图标()标记并渲染为粗体。在注销或变成不活动状态后一小时内，会话会从构件数据中删除。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

在 Current Sessions 构件上，您可以：

- 点击任何用户名以管理“用户管理”(User Management) 页面上的用户帐户。
- 点击任何 IP 地址旁边的主机图标 () 或受损主机图标 () 以查看关联计算机的主机配置文件。
- 点击任何 IP 地址或访问时间以查看该 IP 地址以及与该 IP 地址关联的用户登录 Web 界面的时间所限制的审核日志。

构件首选项可控制构件的更新频率。

自定义分析构件

“自定义分析”(Custom Analysis) 构件是一款高度可自定义的构件，可用于显示 Firepower 系统收集和生成的事件的详细信息。

该构件随附多个预设，可用于快速访问有关部署的信息。预定义控制面板对这些预设进行广泛使用。您可以使用这些预设或创建自定义配置。至少，自定义配置可指定您感兴趣的数据（表和字段），以及该数据的汇聚方法。您还可以设置其他与显示相关的首选项，包括是否要以相对发生率（条形图）或随时间推移（曲线图）的形式显示事件。

该构件基于本地时间显示其最近更新的时间。构件的更新频率取决于控制面板的时间范围。例如，如果您将控制面板时间范围设置为 1 小时，则构件每五分钟更新一次。另一方面，如果将控制面板时间范围设置为一年，则构件每周更新一次。要确定控制面板何时进行下次更新，请将光标停留在构件左下角 **Last updated** 通知处。

注释 以红色阴影显示的“自定义分析”(Custom Analysis) 构件表示其正在危害系统性能。如果构件继续保持红色，请移除该构件。也可以在系统配置中的“控制面板”(Dashboard) 设置禁用所有“自定义分析”(Custom Analysis) 构件（**系统 [System] > 配置 [Configuration] > 控制面板 [Dashboard]**）

显示事件的相对发生率（条形图）

对于“自定义分析”(Custom Analysis) 构件中的条形图，构件背景中的彩色条显示每个事件的相对出现次数。请从右到左阅读彩色条。

方向图标 () 指示和控制显示的排序顺序。向下指向的图标表示降序；向上的图标表示升序。要更改排序顺序，请点击图标。

在每个事件旁边，构件可以显示三个图标中的其中一个，以显示最近结果中的任何更改：

- 新的事件图标 () 表示该事件对结果而言是第一次发生。

- 向上箭头图标()表示该事件自上次构件更新以来已经上移。指示事件上移了多少个位置的数字在图标旁边显示。
- 向下箭头图标()表示该事件自上次构件更新以来已经下移。指示事件下移了多少个位置的数字在图标旁边显示。

显示一段时间内的事件（曲线图）

如果您想了解时间范围内的事件或其他所收集数据的信息，您可以配置 Custom Analysis 构件显示一个线形图，例如显示时间范围内配置中所生成的入侵事件总数的线形图。

“自定义分析”(Custom Analysis) 构件的限制

“自定义分析”(Custom Analysis) 构件可能会指示您无权查看配置显示的数据。例如，“维护用户”(Maintenance Users) 无权查看发现事件。又例如，构件不会显示与未许可的功能相关的信息。但是，您（以及共享控制面板的任何其他用户）可以修改构件的首选项以显示您可以看到的数据，或者甚至是删除构件。如果您希望确保不发生这种情况，请将控制面板另存为专用控制面板。

当查看用户数据时，系统只会显示授权用户。

当查看 URL 类别信息时，系统不会显示未归类的 URL。

当查看由**计数 (Count)** 汇聚的入侵事件时，计数包含已审核的入侵事件；如果在事件查看器中查看计数，则计数不包含已审核的事件。

注释 在多域部署中，系统会为每个枝叶域构建单独的网络映射。因此，枝叶域可以包含这样一个 IP 地址，该地址在它的网络内是唯一的，但与另一枝叶域中的 IP 地址完全相同。查看祖先域中的“自定义分析”(Custom Analysis) 构件时，可显示该重复 IP 地址的多个实例。初看上去，似乎是重复条目。但是，如果向下展开到每个 IP 地址的主机配置数据，则系统会显示它们属于不同的枝叶域。

示例：证书配置

通过将“自定义分析”(Custom Analysis) 构件配置为显示**入侵事件 (Intrusion Events)** 表中的数据，可以将该构件配置为显示最近入侵事件的列表。选择**分类 (Classification)** 字段并通过**计数 (Count)** 来汇聚此数据，以便了解生成的每种类型的事件数量。

另外，通过 **Unique Event** 合计可以了解每种类型有多少个入侵事件已经发生（例如，检测到多少网络木马、可能违反公司政策的情况、试图拒绝服务攻击，等等）。

您还可以使用已保存的搜索（无论是设备随附的其中一个预定义搜索还是您创建的自定义搜索）来进一步限制构件。例如，使用 **Dropped Events** 搜索限制第一个示例（使用 **Classification**，通过 **Count** 合计的入侵事件）可帮助您了解每一种类型中有多少个入侵事件已丢弃。

自定义分析构件首选项

下表介绍可以在“自定义分析”(Custom Analysis) 构件中设置的首选项。

不同的首选项根据构件的配置方式进行显示。例如，如果将构件配置为显示事件的相对发生次数（条形图）与一段时间内的图形（曲线图），则会显示一组不同的首选项。仅在选择从中显示数据的特定表时，才会显示某些首选项，例如过滤器。

表 *28*：自定义分析构件首选项

偏好	Details
职位	如果不指定构件的标题，则设备使用已配置的事件类型作为标题。
Preset	“自定义分析”(Custom Analysis) 预设提供有关部署的信息的快速访问。预定义控制面板对这些预设进行广泛使用。您可以使用这些预设或创建自定义配置。
表 (Table)（必要）	包含构件显示的数据的事件或资产的表。
字段 (Field)（必要）	要显示的事件类型的特定字段。要显示一段时间内的数据（曲线图），请选择**时间 (Time)**。要显示事件的相对发生次数（条形图），请选择其他选项。
汇聚 (Aggregate)（必要）	汇聚方法配置构件对显示数据的分组方法。对于大多数事件类型，默认选项为**计数 (Count)**。
Filter	可以使用应用过滤器限制“应用统计信息”(Application Statistics) 表和“按应用划分的入侵事件统计信息”(Intrusion Event Statistics by Application) 表中的数据。
搜索	可以使用已保存的搜索限制构件显示的数据。您必须指定搜索，不过，有些预设使用预定义搜索。 只有您才能访问另存为专用的搜索。如果在共享控制面板上配置构件，并使用专用搜索限制其事件，则构件会重置为当其他用户登录时不使用搜索。这也会影响构件的视图。如果您希望确保不发生这种情况，请将控制面板另存为专用控制面板。 只有限制连接摘要的字段才能基于连接事件限制“自定义分析”(Custom Analysis) 控制面板构件。无效的已保存搜索会灰显。 如果您使用已保存的搜索限制 Custom Analysis 构件，该构件在下一次更新之前不会反映更改。
显示	选择是要显示最频繁（**顶部**）还是最不频繁（**底部**）发生的事件。
结果	选择要显示的结果行数。
Show Movers	选择是否要显示表示最新结果中的更改的图标。
时区	选择要用于显示结果的时区。
颜色	可以更改构件的条形图中的条形颜色。

从自定义分析构件查看关联事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

在自定义分析构件中，可以调用事件视图（工作流程），其中提供有关该构件中显示的事件的详细信息。事件显示在该事件类型的默认工作流程中，受到控制面板时间范围限制。根据所配置的时间窗口数量和事件类型，这还会更改 Firepower 管理中心上的相应时间窗口。

例如：

- 如果配置多个时间窗口，然后从自定义分析构件访问运行状况事件，则事件会显示在默认运行状况事件工作流程中，并且运行状况监控时间窗口会更改为控制面板时间范围。
- 如果配置单个时间窗，然后从自定义分析构件访问任意类型的事件，则事件会显示在该事件类型的默认工作流程中，并且全局时间窗口会更改为控制面板时间范围。

过程

有以下选项可供选择：

- 在任意自定义分析构件上，点击构件右下角的查看所有图标( )，以查看构件首选项限制的所有关联事件。
- 在显示事件的相对发生（条形图）的自定义分析构件上，点击任意事件以查看构件首选项以及该事件所限制的关联事件。

磁盘使用率构件

根据磁盘使用类别，Disk Usage 构件显示硬盘驱动器的空间使用比例。它还会显示设备硬盘驱动器上的空间使用比例及其每个分区的容量。Disk Usage 构件如果被安装在设备中，或者如果Firepower 管理中心管理某个包含恶意软件包的设备，则其会显示相同的恶意软件存储包信息。默认情况下，该构件在 Default Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

By Category 堆积条形图显示每个磁盘使用情况类别在使用的总可用磁盘空间中的比例。下表列出了可用的类别。

表 *29*：磁盘使用率类别

磁盘使用情况类别	说明
活动	系统记录的所有事件
文件	系统存储的所有文件

磁盘使用情况类别	说明
备用	所有备份文件
更新	与更新相关的所有文件，例如规则更新和系统更新
其他	系统故障排除文件和其他文件
免费	设备上剩余的可用空间

您可以将指针悬停在By Category堆积条形图中的磁盘使用情况类别上，以查看该类别使用的可用磁盘空间的比例、磁盘上的实际存储空间，以及该类别的总可用磁盘空间。请注意，如果您安装了一个恶意软件存储包，Files 类别的总可用磁盘空间为恶意软件包上的可用磁盘空间。

如果您安装了恶意软件存储包，您可以通过修改构件首选项配置构件仅显示By Category堆积条形图和管理员 (/)、/Volume、/boot分区使用情况，以及/var/storage分区。

构件首选项还可以控制构件的更新频率，及其显示的是当前磁盘使用情况还是控制面板时间范围内收集的磁盘使用情况统计数据。

接口流量构件

“接口流量”(Interface Traffic) 构件显示在设备的管理接口上接收的流量速率 (Rx) 和传输的流量速率 (Tx)。对于 7000 和 8000 系列设备，该构件还显示有关传感接口的信息。默认情况下，该构件不会在任何预定义控制面板上显示。

出站（已传输）流量包括流量控制数据包。因此，7000 和 8000 系列设备上的被动传感接口可能会显示已传输的流量；这是预期行为。已启用恶意软件许可证的设备会定期尝试连接到AMP云，即使尚未配置动态分析也如此。因此，这些设备会显示已传输流量；这也是预期行为。

构件首选项可控制构件的更新频率。在 7000 和 8000 系列设备上，首选项还控制构件是否显示未使用的接口的流量速率（默认情况下，该构件仅显示主动接口的流量速率）。

入侵事件构件

Intrusion Events 构件可显示发生在控制面板时间范围内的入侵事件（按优先级组织）。这包括有丢弃数据包和不同影响的入侵事件的统计数据。默认情况下，该构件在Summary Dashboard的Intrusion Events 选项卡中显示。

在构件首选项中，您可以选择：

- **事件标志 (Event Flags)**，以便为包含已丢弃数据包、本应丢弃数据包或产生特定影响的事件显示单独的图表。选择**全部 (All)** 以显示所有入侵事件的额外图表，无论影响或规则状态如何。
- **显示 (Show)** 以指定**每秒平均事件 (Average Events Per Second)** 或**事件总数 (Total Events)**。
- **垂直比例 (Vertical Scale)** 以指定**线性 (Linear)**（增量）或**对数 (Logarithmic)**（十倍）比例
- 构件的更新频率。

在构件上，您可以：

- 点击与已丢弃数据包、本应丢弃数据包或特定影响相对应的图形以查看该类型的入侵事件。
- 点击对应于已丢弃事件的图形可查看已丢弃事件。
- 点击与本应丢弃事件相对应的图形可查看本应丢弃事件。
- 点击**全部 (All)** 图形可查看所有入侵事件。

所发生的事件视图受到控制面板时间范围的限制；通过控制面板访问入侵事件可能会更改设备的事件（或全球）时间段。请注意，被动部署的数据包不会丢弃，无论入侵规则状态或入侵策略的内联丢包行为如何。

网络合规性构件

“网络合规性”(Network Compliance) 构件总结主机符合您配置的白名单的情况。默认情况下，该构件会显示有关活跃关联策略中的所有合规白名单列出的合规、不合规，以及未评估的主机数量的饼形图。默认情况下，该构件在 Detailed Dashboard 的 Correlation 选项卡中显示。

您可以通过修改构件首选项配置构件显示所有白名单或具体白名单的合规性。

如果您选择显示所有白名单的网络合规性，而一旦其不符合某个有效的关联策略中的任何白名单，则构件会将主机视为不合规。

您还可以使用构件首选项以指定您想使用三种不同风格中的哪一种来显示网络合规性。

Network Compliance 风格（默认）显示有关合规、不合规及尚未评估的主机数量的饼形图。您可以点击该饼形图以查看主机违规数，它会列出至少违反一个白名单的主机。

Network Compliance over Time (%) 风格会显示有关控制面板时间范围内合规，不合规，未评估的主机相对比例的堆积区域图。

Network Compliance over Time 风格会显示有关控制面板时间范围内合规，不合规，未评估的主机数量的线形图。

首选项可控制构件的更新频率。您可以选中 **Show Not Evaluated** 框以隐藏未评估的活动。

产品许可构件

Product Licensing 构件可显示当前安装于Firepower 管理中心上的设备和功能许可证。它还指示获得许可的项目数以及允许的剩余许可项目数。默认情况下，该构件不会在任何预定义控制面板上显示。

构件的顶部显示在Firepower管理中心上安装的所有设备和功能许可证，包括临时许可证，而 Expiring Licenses 部分则显示临时及已到期许可证。

构件背景中的长条显示正在使用的各种许可证的比例；您应该从右到左阅读这些长条。已到期许可证标标记有一条删除线。

您可以通过修改构件首选项配置构件显示所有当前许可的功能，或者您可许可的所有功能。首选项还可控制构件的更新频率。

您可以点击任何一种许可证类型发往本地配置的 License 页面并添加或删除功能许可证。

产品更新构件

“产品更新”(Product Updates) 构件为您提供当前安装在设备上的软件摘要和您已经下载但未安装的更新的信息摘要。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

由于构件使用预定任务确定最新版本，因此会显示`Unknown`，直到您将预定任务配置为下载、推送或安装更新。
通过修改构件首选项，您可以配置构件以隐藏最新版本。首选项还可控制构件的更新频率。

构件也会为您提供可以更新软件的页面链接。您可以执行以下操作：

- 通过点击当前版本来手动更新设备。
- 通过点击最新版本来创建预定任务以下载更新。

RSS 源构件

RSS Feed 构件可向控制面板添加一个 RSS 源。默认情况下，该构件可显示思科安全新闻的信息源。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

您还可以配置构件显示公司新闻的预配置摘要、Snort.org 博客，或思科威胁研究博客，或者也可以指定其在构件首选项的 URL 以创建任何其他 RSS 源的自定义连接。

信息源每24小时（但您可以手动更新摘要）更新一次，而且，构件会根据设备的本地时间显示最近一次更新信息源的时间。请记住，设备必须访问（两个预配置摘要的）网站或您配置的任何自定义信息源。

当您配置构件时，您还可以选择您想要在构件中显示多少个案例，以及是否想要在标题下显示案例说明；记住，并非所有的 RSS 源都会使用说明。

在 RSS Feed 构件中，您可以：

- 点击信息源中的某个案例查看案例
- 点击 **more** 链接转到信息源的网站
- 点击更新图标 () 手动更新信息源

系统负载构件

System Load 构件可显示设备当前及控制面板时间范围内的（每个 CPU）CPU 使用率、内存 (RAM) 使用情况和系统负载（又称为平均负载，通过等待运行的进程数量衡量）。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

您可以通过修改构件首选项以配置构件显示或隐藏平均负载。首选项还可控制构件的更新频率。

系统时间构件

System Time 构件可显示本地系统时间、正常运行时间和设备启动时间。默认情况下，该构件在 Detailed Dashboard 和 Summary Dashboard 的 Status 选项卡中显示。

通过修改构件首选项，您可以配置构件以隐藏启动时间。首选项还会控制构件与设备的时钟同步的频率。

白名单事件构件

White List Events 构件按照优先级显示控制面板时间范围内每秒内事件发生的平均次数。默认情况下，该构件在 Default Dashboard 的 Correlation 选项卡中显示。

通过修改构件首选项，您可以配置构件以显示不同优先级的白名单事件。

在构件首选项中，您可以：

- 选择一个或多个**优先级 (Priorities)** 复选框，以显示特定优先级事件的图形，包括不具备优先级的事件
- 选择**全部显示 (Show All)** 以显示所有白名单事件的其他图形，无论其优先级如何
- 选择**垂直刻度 (Vertical Scale)** 以选择**线性 (Linear)**（增量）或**对数 (Logarithmic)**（十倍）比例

首选项还可控制构件的更新频率。

您可以点击某个图形查看特定优先级的白名单事件，或者点击 **All** 图形查看所有白名单事件。在任何一种情况下，事件均受到控制面板时间范围的限制；通过控制面板访问关联事件可更改Firepower管理中心的事件（或全球）时间段。

管理控制面板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

过程

步骤 1 选择**概述 (Overview)** > **控制面板 (Dashboards)**，然后从菜单中选择要修改的控制面板。

步骤 2 管理控制面板：

- 创建控制面板 - 创建自定义控制面板；请参阅创建自定义控制面板 ， 第 194 页。
- 删除控制面板 - 要删除控制面板，请点击要删除的控制面板旁边的删除图标 ()。如果删除默认控制面板，则必须定义新的默认控制面板，否则设备会在您每次尝试查看控制面板时提示您选择控制面板。
- 编辑选项 - 编辑自定义控制面板选项；请参阅编辑控制面板选项 ， 第 196 页。

- 修改时间限制 - 修改时间显示或暂停/取消暂停控制面板，如修改控制面板时间设置，第 196 页中所述。

步骤 3 管理控制面板选项卡：

- 添加选项卡 - 向控制面板中添加选项卡；请参阅添加控制面板选项卡，第 192 页。
- 删除选项卡 - 要删除控制面板选项卡，请点击选项卡右上角的关闭图标 ( )，然后通过点击**确定 (OK)** 进行确认。您无法从控制面板中删除最后一个选项卡；每个控制面板必须至少有一个选项卡。
- 重命名选项卡 - 重命名控制面板中的选项卡；请参阅重命名控制面板选项卡，第 197 页。

注释 不能更改控制面板选项卡的顺序。

步骤 4 管理控制面板构件：

- 添加构件 - 向控制面板中添加构件；请参阅将构件添加到控制面板，第 193 页。
- 配置首选项 - 配置构件首选项；请参阅配置构件首选项，第 194 页。
- 自定义显示 - 自定义构件显示；请参阅自定义构件显示，第 195 页。
- 查看事件 - 查看“自定义分析”(Custom Analysis) 构件中的关联事件；请参阅从自定义分析构件查看关联事件，第 187 页。

提示 思科预定义控制面板中的“自定义分析”(Custom Analysis) 构件的每个配置都与该构件的系统预设相对应。如果您更改或删除了其中一个构件，您可以通过根据适当的预设创建一个新的 Custom Analysis 来恢复它。

添加控制面板选项卡

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

过程

步骤 1 查看要修改的控制面板；请参阅查看仪表板，第 198 页。

步骤 2 点击最后一个现有选项卡旁边的添加图标 ( )。

步骤 3 输入选项卡的名称。

步骤 4 点击 **OK**。

将构件添加到控制面板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

每个选项卡都可以三列布局显示一个或多个构件。向控制面板添加构件时，必须选择要向其添加构件的选项卡。系统会自动将其添加到构件最少的一列。如果所有列的构件数量均相同，新的构件会被添加到最左边的一列。您最多可以添加 15 个构件到控制面板选项卡中。

提示 在添加构件后，您可以将其移到选项卡的任何位置。但是，您不能在选项卡之间移动构件。

可以查看的控制面板构件取决于正在使用的设备类型、用户角色和当前域（在多域部署中）。请记住，因为并非所有用户角色都有权访问所有控制面板构件，查看权限较高的用户创建的控制面板的权限较低的用户可能无法使用控制面板上的所有构件。尽管未授权的构件仍将在控制面板上显示，但它们会被禁用。

过程

步骤 1 查看要添加构件的控制面板；请参阅查看仪表板，第 198 页。

步骤 2 点击要添加构件的选项卡。

步骤 3 点击 **Add Widgets**。您可以点击类别名称查看每个类别中的构件，也可以点击**所有类别 (All Categories)** 查看所有构件。

步骤 4 点击要添加的构件旁边的**添加 (Add)**。“添加构件”(Add Widgets) 页面会显示每种类型有多少个构件在选项卡上，包括您要添加的构件。

提示 要添加多个相同类型的构件（例如，您可能希望添加多个 RSS Feed 构件，或多个 Custom Analysis 构件），可再次点击 **Add**。

步骤 5 构件添加完毕后，点击**完成 (Done)** 返回到控制面板。

接下来的操作

- 如果添加的是“自定义分析”(Custom Analysis) 构件，请配置构件首选项；请参阅配置构件首选项，第 194 页。

配置构件首选项

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

每个构件都有一组可确定其行为的首选项。

过程

步骤 1 在您想要更改首选项的构件标题栏上，点击显示首选项图标 ( )。

步骤 2 根据需要进行更改。

步骤 3 在构件标题栏上，点击隐藏首选项图标 ( ) 隐藏首选项部分。

创建自定义控制面板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

提示 您无需创建新的控制面板，而是可以从其他设备中导出，然后将其导入到设备中。随后，您将可以编辑所导入的控制面板以满足自身需求。

过程

步骤 1 选择**概述 (Overview)** > **控制面板 (Dashboards)** > **管理 (Management)**。

步骤 2 点击 **Create Dashboard**。

步骤 3 修改自定义控制面板选项，如自定义控制面板选项，第 194 页中所述。

步骤 4 点击**保存 (Save)**。

自定义控制面板选项

下表介绍在创建或编辑自定义控制面板时可以使用的选项。

表 *30*：自定义控制面板选项

选项	说明
复制控制面板 (Copy Dashboard)	创建自定义控制面板时，您可以选择是否将其基于任何现有控制面板（无论是用户创建的还是系统定义的都如此）。此选项会创建预先存在的控制面板的副本，您可以修改该副本以满足需求。或者，可以通过选择**无 (None)** 创建空白的新控制面板。仅在创建新控制面板时，此选项才可用。 在多域部署中，您可以从祖先域复制任何非专用控制面板。
Name	自定义控制面板的唯一名称。
说明	自定义控制面板的简短说明。
选项卡更改频率 (Change Tabs Every)	指定控制面板循环使用其选项卡的频率（以分钟为单位）。除非您暂停控制面板或控制面板上只有一个选项卡，否则该设置会在您指定的时间间隔将视图转至下一个选项卡。要禁用选项卡循环，请输入 0 到 **Change Tabs Every** 字段中。
页面刷新频率 (Refresh Page Every)	指定当前控制面板选项卡应使用新数据进行刷新的频率（以分钟为单位）。该值必须高于 **Change Tabs Every** 设置。除非您暂停控制面板，否则该设置将在您指定的时间间隔刷新整个控制面板。要禁用定期页面刷新，请输入 0 到 **Refresh Page Every** 字段中。确定整个控制面板页面自动刷新的频率。 刷新整个控制面板可以让您查看自上一次控制面板更新以来，其他用户对共享控制面板所作的，或者您对另一台计算机上的专用控制面板所作的任何首选项或布局更改。例如，在控制面板始终显示的网络运营中心 (NOC) 中，频繁刷新可能非常有用。如果在本地计算机对控制面板的进行更改，则 NOC 中的控制面板会按照指定的间隔自动刷新，并且无需手动刷新。请注意，您不需要更新整个控制面板以查看数据更新；各个构件会根据其首选项进行更新。 **注释** 此设置与许多单个构件上的可用更新间隔分离；虽然刷新控制面板页面会重置单个构件上的更新间隔，但是构件将根据其各自的首选项进行更新，即使禁用**页面刷新间隔 (Refresh Page Every)** 设置也如此。
另存为专用 (Save As Private)	确定自定义控制面板是可由设备的所有用户查看和修改还是与您的用户帐户相关联并专门保留供自己使用。请记住，无论角色如何，具有控制面板访问权限的任何用户都可以修改共享控制面板。如果您希望确保只有您可以修改特定控制面板，请将其保存为专用控制面板。

自定义构件显示

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

您可以将构件最小化和最大化，以及在选项卡上重新排列构件。

过程

步骤 1 查看控制面板；请参阅查看仪表板，第 198 页。

步骤 2 自定义构件显示：

- 要在选项卡上重新排列构件，请点击要移动的构件的标题栏，然后将其拖到新位置。
  注释 不能在选项卡之间移动构件。如果您想要构件显示在不同的选项卡上，您必须将其从现有选项卡中删除，并将其添加到新的选项卡上。
- 要将控制面板上的构件最小化或最大化，请点击构件的标题栏中的最小化 ( ) 或最大化图标 ( )。
- 如要在选项卡上不再查看构件时删除该构件，请点击构件的标题栏中的关闭图标 ( )。

编辑控制面板选项

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

过程

步骤 1 查看要编辑的控制面板；请参阅查看仪表板，第 198 页。

步骤 2 点击要修改的控制面板旁边的编辑图标 ( )。

步骤 3 如自定义控制面板选项，第 194 页中所述更改选项。

步骤 4 点击**保存 (Save)**。

修改控制面板时间设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。当您更改时间范围时，可按时间限制构件自动更新以反映新的时间范围。

请注意，并非所有的构件都可受时间限制。例如，控制面板时间范围对设备信息构件无影响，该构件可提供包括设备名称、型号和当前版本的 Firepower 系统软件的信息。

请记住，对于Firepower系统的企业部署而言，将时间范围更改为长周期可能对“自定义分析”(Custom Analysis) 之类的构件无效，具体取决于新事件取代旧事件的频率。

您还可以暂停控制面板，这可以让您检查构件提供的数据，而无需更改和中断您的分析的显示。暂停控制面板具有以下影响：

- 各个构件停止更新，任何 **Update Every** 构件均如此。
- 控制面板选项卡停止循环，无论控制面板属性中的 **Cycle Tabs Every** 设置如何。
- 控制面板页面停止刷新，无论控制面板属性中的 **Refresh Page Every** 设置如何。
- 更改时间范围无效。

当您完成分析时，您可以取消控制面板暂停。恢复控制面板运行会使得页面上的所有相应的构件更新以反映当前时间范围。此外，控制面板选项卡会恢复循环，控制面板页面会根据您在控制面板属性中指定的设置进行刷新。

如果出现中断控制面板系统信息流的连接问题或其他问题，控制面板会自动暂停，并显示错误通知，直至问题解决为止。

注释 您的会话一般会在 1 小时（或其他配置的时间间隔）的非活动期后注销，无论控制面板是否暂停。如果您计划长时间被动监控控制面板，您可考虑使某些用户免于会话超时，或更改系统超时设置。

过程

步骤 1 查看要添加构件的控制面板；请参阅查看仪表板 ，第 198 页。

步骤 2 或者，要更改控制面板时间范围，请从**显示最后时间 (Show the Last)** 下拉列表中选择时间范围。

步骤 3 或者，根据时间范围控制，使用暂停 (⏸) 或播放图标 (▶) 暂停或中止暂停控制面板。

重命名控制面板选项卡

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

过程

步骤 1 查看要修改的控制面板；请参阅查看仪表板，第 198 页。

步骤 2 点击要重命名的选项卡标题。

步骤 3 键入选项卡的名称。

步骤 4 点击 **OK**。

查看仪表板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/维护人员

默认情况下，设备的主页会显示默认控制面板。如果您没有确定默认控制面板，主页会显示Dashboard Management 页面，您可以在此选择控制面板视图。

过程

可以随时执行以下操作之一：

- 要查看设备的默认控制面板，请选择**概述 (Overview)** > **控制面板 (Dashboards)**。
- 要查看特定控制面板，请选择**概述 (Overview)** > **控制面板 (Dashboards)**，然后从菜单中选择该控制面板。
- 要查看所有可用的控制面板，请选择**概述 (Overview)** > **控制面板 (Dashboards)** > **管理 (Management)**。然后，您可以选择单个控制面板旁边的查看图标 () 来查看该控制面板。

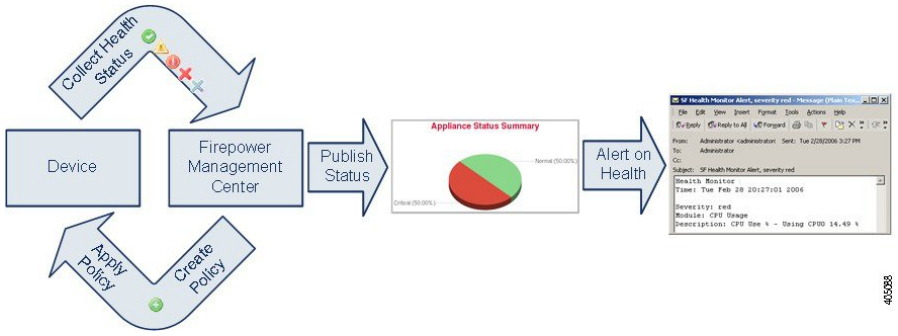
第 12 章

运行状况监控

以下主题介绍如何在 Firepower 系统中使用运行状况监控：

运行状况监控基础知识

Firepower 管理中心上的运行状况监控器跟踪各种运行状况指标，以确保 Firepower 系统中的硬件和软件正常工作。您可以使用运行状况监控器检查整个 Firepower 系统部署中关键功能的状态。



可以使用运行状况监控器创建一个测试集合（称为运行状况策略），并将该运行状况策略应用到一个或多个设备上。测试（称为运行状况模块）是用来测试您指定的标准的脚本。您可以通过启用或

禁用测试或者通过更改测试设置来修改运行状况策略，可以删除不再需要的运行状况策略。您还可以将来自所选设备的消息加入黑名单，从而抑制这些消息。

运行状况策略中的测试以所配置的时间间隔自动运行。您还可以按需运行所有测试或特定测试。运行状况监视器基于配置的测试条件收集运行状况事件。

注释 所有设备都通过“硬件警报”(Hardware Alarms) 运行状况模块自动报告其硬件状态。Firepower 管理中心还使用默认运行状况策略中配置的模块自动报告状态。某些运行状况模块（例如“设备测信号”[Appliance Heartbeat] 模块）在 Firepower 管理中心上运行并报告 Firepower 管理中心的受管设备的状态。除非将使用某些运行状况模块配置的运行状况策略应用到设备，否则这些模块不提供受管设备状态。

可以使用运行状况监控器访问特定设备（在多域部署中，则是特定域）的整个系统的运行状态信息。“运行状况监控器”(Health Monitor) 页面上的饼形图和状态表提供网络上所有设备（包括 Firepower 管理中心）的状态的可视摘要。单个设备运行状况监视器使您可以向下钻取到特定设备的运行状况详细信息。

完全可定制的事件视图使您可以快速轻松地分析运行状况监视器所收集的运行状况事件。这些事件视图使您可以搜索和查看事件数据，并访问可能与正调查的事件有关的其他信息。例如，如果要查看用一定百分比表示的 CPU 使用率的所有状况，您可以搜索 CPU 使用率模块并输入百分比值。

您还可以配置回应运行状况事件而作出的邮件、SNMP 或者系统日志警报。运行状况警报是指标准警报和运行状况级别之间的关联。例如，如果要确保设备不会因硬件过载出现故障，您可以设置邮件警报。然后，您可以创建运行状况警报，每当 CPU、磁盘或内存占用率达到您在该设备所应用的运行状况策略中配置的“警告”级别时，就可以触发该邮件警报。您可以设置警报阈值，以最小化您收到的重复警报的数量。

如果支持人员要求您为设备生成故障排除文件，您也可以执行此操作。

由于运行状况监控是管理活动，因此只有具有管理员用户角色权限的用户才可以访问系统运行状况数据。

运行状况模块

运行状况模块（有时也称为运行状况测试）是用来测试您在运行状况策略中指定的标准的脚本。下表中介绍可用的运行状况模块。

表 *31*：运行状况模块

模块	适用的设备	说明
面向终端的AMP状态	管理中心	如果 Firepower 管理中心在初始成功连接后无法连接到 AMP 云或思科 AMP 私有云 (AMPv)，或者如果 AMPv 无法连接 AMP 云，则该模块发出警报。如果您使用面向终端的 AMP 管理控制台撤销注册 AMP 云连接，该模块也发出警报。 该模块仅在Firepower 管理中心上运行。

模块	适用的设备	说明
面向 Firepower 的 AMP 状态	管理中心	如果发生以下情况，则该模块发出警报： • Firepower 管理中心无法联系 AMP 云、思科 AMP 私有云 (AMPv)、AMP Threat Grid 云、AMP Threat Grid 本地部署设备，或 AMPv 无法联系 AMP 云。 • 用于连接的加密密钥无效。 • 设备无法联系 AMP Threat Grid 云或 AMP Threat Grid 本地部署设备以提交进行动态分析的文件。 • 根据文件策略配置，在网络流量中检测到大量文件。 该模块仅在Firepower 管理中心上运行。 如果 Firepower 管理中心丢失与互联网的连接，系统最多可能需要 30 分钟才能生成一个面向 Firepower 的 AMP 状态的运行状况警报。
设备心跳	任意	该模块确定设备是否正监听设备心跳并基于设备心跳状态发出警报。 该模块仅在Firepower 管理中心上运行。
自动应用旁路状态	7000 和 8000 系列	该模块确定，由于设备在旁路阈值设置的秒数内不响应所以设备是否被绕过，以及发生旁路时该模块是否发出警报。
经典许可证监控	管理中心	该模块确定是否有足够的经典许可证用于控制、保护、URL 过滤、恶意软件和VPN。当堆栈中的设备与许可证集不匹配时，该模块也发出警报。基于为该模块自动配置的警告级别，该模块发出警报。您无法更改该模块的配置。 该模块仅在Firepower 管理中心上运行。
CPU 使用情况	任意	该模块检查设备上的CPU未过载，并且在CPU使用率超过为模块配置的百分比时发出警报。
卡重置	任意	该模块检查由于硬件故障而重新启动的网卡，并且在发生重置时发出警报。
磁盘状态	任意	该模块检测硬盘的性能和设备上的恶意软件存储包（如果已安装）。当硬盘和RAID控制器（如果安装）存在发生故障的危险时，或者，如果安装的其他安装硬盘驱动器不是恶意软件包时，该模块生成“警告”（黄色）运行状况警报。当无法检测到已安装恶意软件存储包时，该模块生成“警报”（红色）运行状况警报。

模块	适用的设备	说明
磁盘使用情况	任意	该模块将设备的硬盘驱动器和恶意软件存储包中的磁盘使用率与为该模块配置的限值进行对比，并在使用率超过为模块配置的百分比时发出警报。基于模块阈值，当系统删除过多的监控磁盘使用类别的文件，或者当这些类别以外的磁盘使用率达到过高级别时，该模块也发出警报。使用磁盘使用率运行状况模块监控设备上的 / 和 /volume 分区的磁盘使用率并跟踪耗尽频率。尽管磁盘使用率模块将 /boot 分区列为监控分区，但是分区的大小是静态的，因此该模块在引导分区中不发出警报。
FireSIGHT 主机限制	管理中心	该模块确定 Firepower 管理中心可以监控的主机数量是否即将达到限制，并基于为该模块配置的警告级别发出警报。有关详细信息，请参阅 Firepower 系统主机限制，第 1135 页。 该模块仅在Firepower 管理中心上运行。
硬件告警	7000 和 8000 系列	该模块确定物理受管设备上的硬件是否需要更换并基于硬件状态发出警报。该模块还报告硬件相关的后台守护程序的状态和高可用性部署中 7000 和 8000 系列设备的状态。
运行状况监视器流程	任意	该模块监控运行状况监视器本身的状态，并且如果Firepower 管理中心最后收到运行状况事件后的分钟数超过“警告”或“严重”限值，则发出警报。 该模块仅在Firepower 管理中心上运行。
内联链路不匹配告警	除 ASA FirePOWER 外的任何受管设备	该模块监控与内联集相关的端口，并且如果内联对的两个接口协商不同的速度，则发出警报。
入侵和文件事件率	任何受管设备	该模块将每秒钟入侵事件的数量与为该模块配置的限值进行对比。如果超过限值，则该模块发出警报。如果入侵和文件事件速率为零，则入侵进程可能已关闭或者受管设备可能没有发送事件。选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事件 (Events)**，检查是否正从该设备接收事件。 通常，网段的事件速率平均为每秒 20 个事件。对于具有本平均速率的网段，每秒事件（严重）数应设置为 50，每秒事件（警告）数应该设置 为 30。要确定系统的限值，请在设备的“统计信息”(Statistics) 页面（**系统 (System)** > **监控 (Monitoring)** > **统计信息 (Statistics)**）找到“事件/秒”(Events/Sec) 值，然后使用以下公式计算限值： • 每秒事件（严重）数 = Events/Sec * 2.5 • 每秒事件（警告）数 = Events/Sec * 1.5 您可以为每种限值设置的最大事件数是 999，“严重”限值必须高于“警告”限值。

模块	适用的设备	说明
接口状态	任意	此模块确定设备当前是否收集流量并根据物理接口和汇聚接口的流量状态发出警报。对于物理接口，信息包括接口名称、链路状态和带宽。对汇聚接口，信息包括接口名称、活动链路的数量和总汇聚带宽。 对于 ASA FirePOWER，标记为 DataPlaneInterfacex（其中 x 是一个数值）的接口是 ASA 内部接口（不是用户定义的），涉及系统中的数据包流。
链路状态传播	任何设备，NGIPSv和 ASA FirePOWER 除外	该模块确定成对的内联集中链路发生故障的时间，并且触发链路状态传播模式。 如果链路状态传播到该对，该模块的状态分类变更为“严重”，并且状态读作： `Module Link State Propagation: ethx_ethy is Triggered` 其中 `x` 和 `y` 为成对的接口编号。
本地恶意软件分析	任意	如果设备被配置为进行本地恶意软件分析但是从 AMP 云下载本地恶意软件分析引擎签名更新失败，则该模块发出警报。
内存使用率	任意	该模块将设备的内存使用率与为模块配置的限值进行对比，并在使用率超过为该模块配置的级别时发出警报。 对于内存超过 4 GB 的设备而言，基于一个公式来预设警报阈值，该公式计算在可能导致系统问题的可用内存中所占的比例。在内存超过 4 GB 的设备上，因为“警告”(Warning) 和“严重”(Critical) 阈值之间的时间间隔可能非常短，所以思科建议您将**警告阈值 % (Warning Threshold %)** 值手动设置为 `50`。这将进一步确保您及时收到设备的内存警报来解决问题。 复杂的访问控制策略和规则可控制重要资源并对性能产生不利影响。有些采用 FirePOWER 服务软件的低端 ASA 设备可能会生成间歇性内存使用率警告，因为这些设备的内存是按最大限度使用分配的。
电源	物理管理中心、7000 和 8000 系列	该模块确定设备的电源是否需要更换，并基于电源状态发出警报。 该模块在物理 Firepower 管理中心上运行。 该模块在 7000 和 8000 系列受管设备上运行。
进程状态	任意	该模块确定设备上的进程是否在进程管理器外部退出或终止。如果进程在进程管理器外部被故意退出，模块状态变更为“警告”，并且运行状况事件消息指示哪一个进程被退出，直到该模块再次运行、该进程重新启动为止。如果进程在进程管理器外部异常终止或者崩溃，模块状态变更为“严重”，并且运行状况事件消息指示被终止的进程，直到该模块再次运行、该进程重新启动为止。
重新配置检测	任何受管设备	如果设备重新配置失败，则该模块发出警报。

模块	适用的设备	说明
RRD 服务器进程	管理中心	该模块确定存储时序数据的轮询数据服务器是否正常运行。如果自上次RRD服务器更新后其重新启动，则该模块将发出警报；如果在RRD服务器重新启动后连续更新的次数达到模块配置中指定的次数，则该模块将输入“严重”或“警告”状态。 该模块仅在Firepower 管理中心上运行。
安全情报	管理中心	该模块在涉及安全情报过滤的各种情况下发出警报。如果安全情报正在使用中并且发生以下状况，该模块发出警报： • Firepower管理中心无法更新源，或者源数据损坏或不包含可识别的IP 地址。 • 受管设备在从Firepower管理中心接收更新的安全情报数据方面存在问题。 • 由于内存问题，受管设备无法加载Firepower管理中心为其提供的所有安全情报数据。 如果安全情报内存警告显示在运行状况监控器中，您可以重新部署受影响的设备的访问控制策略以增加分配给安全情报的内存。
时序数据监视器	管理中心	该模块跟踪已损坏文件在存储时序数据（例如关联事件计数）的目录中的存在情况，并且在文件标记为已损坏和已移除时发出警报。 该模块仅在Firepower 管理中心上运行。
时间同步状态	任意	该模块跟踪将 NTP 与 NTP 服务器上的时钟配合使用以获取时间的设备时钟的同步状态，并且在两个时钟的时间差超过十秒钟时发出警报。 该模块仅在Firepower 管理中心上运行。
URL 过滤监视器	管理中心s	URL过滤监控器模块跟踪Firepower管理中心及其受管设备与思科综合安全情报(CSI)之间的通信，系统从CSI获取经常访问的URL的威胁情报。如果 Firepower 管理中心无法成功与思科 CSI 通信或无法从中检索更新，则该模块发出警报。 如果 Firepower 管理中心无法将 URL 数据推送到受管设备，该模块也发出警报。
用户代理状态监视器	管理中心	当没有为连接到Firepower 管理中心的任何用户代理检测到心跳时，该模块发出警报。 该模块仅在Firepower 管理中心上运行。
VPN 状态	管理中心	当系统检测到 VPN 功能不起作用时，该模块发出警报。 该模块仅在Firepower 管理中心上运行。

配置运行状况监控

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

过程

步骤 1 为设备创建运行状况策略。
您可以为 Firepower 系统中的每种设备设定特定策略、仅为该设备执行适当的测试。

提示 如果要快速启用运行状况监控，而不定制监控行为，您可以应用出于该目的而提供的默认策略。

步骤 2 将运行状况策略应用到要跟踪运行状况的每台设备上。

步骤 3 或者，配置运行状况监视器警报。
您可以设置在运行状况级别达到特定运行状况模块的特定严重性级别时触发的邮件、系统日志或 SNMP 警报。

运行状况策略

运行状况策略包含为若干模块配置的运行状况测试标准。您可以控制根据每个设备要运行的运行状况模块、配置每个模块运行的测试中所用的具体限值。

当配置运行状况策略时，您决定是否为该策略启用每个运行状况模块。您可以选择用来控制每个已启用模块在每次访问进程的运行状况时报告的运行状况的标准。

您可以创建在系统中每个设备上应用的一个运行状况策略、定制您计划在特定设备上应用的每个运行状况策略，或者使用为您提供的默认运行状况策略。在多域部署中，祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

默认运行状况策略

Firepower管理中心上的运行状况监控器提供默认的运行状况策略，让您可以快速实现设备运行状况监控。在默认的运行状况策略中，运行平台上可用的大多数运行状况模块都可自动启用。您无法编辑默认的运行状况策略，但是，您可以基于其配置进行复制以创建自定义策略。默认的运行状况策略会自动应用于 Firepower 管理中心，但您必须将其应用于您要监控运行状况的所有受管设备。

创建运行状况策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

如果要定制用于设备的运行状况策略，您可以创建一个新策略。策略中的设置初始填充您选定为新策略基础的运行状况策略的设置。您可以按需启用或禁用策略内的模块并更改每个模块的警报标准。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **策略 (Policy)**。

步骤 2 点击 **Create Policy**。

步骤 3 从**复制策略 (Copy Policy)** 下拉列表中选择要用作新策略基础的现有策略。

步骤 4 输入策略的名称。

步骤 5 输入策略的说明。

步骤 6 选择**保存 (Save)** 以保存策略信息。

步骤 7 选择要使用的模块。

步骤 8 为**已启用 (Enabled)** 选项选择**开 (On)**，以允许使用该模块进行运行状况测试。

步骤 9 酌情设置**严重 (Critical)** 和**警告(Warning)** 标准。

步骤 10 配置模块的任何其他设置。对每个模块重复步骤 7-10。

步骤 11 此时，您有三种选择：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对此模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

接下来的操作

- 如应用运行状况策略，第 207 页中所述，将该运行状况策略应用到每台设备。此操作将应用更改并更新所有受影响策略的策略状态。

应用运行状况策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

当您将运行状况策略应用到设备时，您在策略中启用的所有模块的运行状况测试自动监控设备上的进程和硬件的运行状况。然后，运行状况测试继续以您在策略中配置的时间间隔运行，为设备收集运行状况数据并将该数据转发到Firepower 管理中心。

如果您在运行状况策略中启用一个模块，然后将该策略应用到不需要该运行状况测试的设备，则运行状况监视器报告该运行状况模块的状态为禁用。

如果您将启用所有模块的策略应用到设备中，它从该设备移除所有已应用的运行状况策略，以便不应用任何运行状况策略。

当您将不同的策略应用到已应用策略的设备时，请基于新应用的测试在显示新数据时使用一些延迟。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **策略 (Policy)**。

步骤 2 点击要应用的策略旁边的应用图标 ( )。

提示 Health Policy 列旁边的状态图标 ( ) 指示该设备的当前运行状况。System Policy 列旁边的状态图标 ( ) 指示Firepower 管理中心与设备之间的通信状态。请注意，您可以通过点击移除图标 来移除当前应用的策略。

步骤 3 选择要应用运行状况策略的设备。

步骤 4 点击**应用 (Apply)** 以将该策略应用到所选设备上。

接下来的操作

- 或者，监控任务状态；请参阅查看任务消息，第 239 页。

  只要成功应用该策略，设备监控即开始。

编辑运行状况策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。祖先域中的管理员可以将运行状况策略应用于后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **策略 (Policy)**。

步骤 2 点击要修改的策略旁边的编辑图标 ( )。

步骤 3 根据需要，编辑**策略名称 (Policy Name)** 或**策略说明 (Policy Description)** 字段。

步骤 4 点击要修改的运行状况模块。

步骤 5 修改设置，如运行状况模块，第 200 页中所述。

步骤 6 您会看到三个选项：

- 要保存对该模块的更改并返回到 Health Policy 页面，请点击 **Save Policy and Exit**。
- 要返回到 Health Policy 页面而不保存对该模块所做的任何设置，请点击 **Cancel**。
- 要临时保存对此模块的更改并切换到另一个模块的设置进行修改，请从页面左侧的列表中选择其他模块。如果完成后点击 **Save Policy and Exit**，将保存所做的所有更改；如果点击 **Cancel**，则丢弃所有更改。

接下来的操作

- 重新应用运行状况策略，如应用运行状况策略，第 207 页中所述。此操作将应用更改并更新所有受影响策略的策略状态。

删除运行状况策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

您可以删除不再需要的运行状况策略。如果您删除仍然应用于设备的策略，直到您应用不同的策略，该策略设置仍然有效。此外，如果您删除应用到设备的运行状况策略，在您禁用基础的相关警报响应之前，该设备仍在生效的任何运行状况监控警报仍然处于活动状态。

在多域部署中，只能删除在当前域中创建的运行状况策略。

提示 要停止设备的运行状况监控，请创建一个所有模块都禁用的运行状况策略并将其应用到设备。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **策略 (Policy)**。

步骤 2 点击要删除的策略旁边的删除图标 ( )。
系统将显示一则消息，指示删除是否成功。

运行状况监控器黑名单

在正常的网络维护过程中，您禁用设备或使其暂时不可用。因为这些停运是故意为之，您不希望这些设备的运行状态影响 Firepower 管理中心上的摘要运行状态。

您可以使用运行状况监视器黑名单功能禁用对设备或模块的运行状况监控状态报告。例如，如果您知道一个网段将不可用，因为到该网段上受管设备的连接失效，所以您可以临时禁用对该设备的运行状况监控，以禁止Firepower 管理中心上的运行状况显示警告或严重状态。

当您禁用运行状况监控状态时，仍会生成运行状况事件，但是它们处于禁用状态，不会影响运行状况监视器的运行状况。如果您从黑名单移除设备或模块，列入黑名单过程中生成的事件继续显示禁用的状态。

要在设备上临时禁用运行状况事件，请转到黑名单配置页面并将设备添加至黑名单。在设置生效后，系统在计算整体运行状况时，不再包含列入黑名单的设备。Health Monitor Appliance Status Summary 列出处于禁用状态的设备。

有时，只将设备上的单个运行状况监控模块列入黑名单可能更实用。例如，当在Firepower管理中心上达到主机限制时，可以将 FireSIGHT 主机限制状态消息列入黑名单。

请注意，在Health Monitor主页面，如果您通过点击该状态行上的箭头来展开以查看具有特定状态的设备列表，就可以区分被列入黑名单的设备。

在您展开被列入黑名单或部分被列入黑名单的设备的视图后，可以看见黑名单图标 ( ) 和注释。

注释 在Firepower 管理中心，运行状况监视器黑名单设置是本地配置设置。因此，如果您将设备列入黑名单，接着将其删除，然后使用Firepower 管理中心重新注册，黑名单设置保持不变。最近重新注册的设备仍旧被列入黑名单。

在多域部署中，祖先域中的管理员可以将后代域中的设备或运行状况模块列入黑名单。但是，后代域中的管理员可以覆盖祖先配置并清除其域中设备的黑名单。

将设备列入黑名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

您可以单独或按组、型号或关联运行状况策略将设备列入黑名单。

在黑名单设置生效后，设备在 Health Monitor Appliance Module Summary 和 Device Management 页面显示为禁用状态。设备的运行状况事件具有禁用的状态。

如果需要将单个设备的事件和运行状况设置为禁用，您可以将该设备列入黑名单。在黑名单设置生效后，该设备在“运行状况监控设备模块摘要”(Health Monitor Appliance Module Summary) 中显示为已禁用，并且该设备的运行状况事件的状态为已禁用。

在多域部署中，将祖先域中的设备列入黑名单会针对所有后代域将该设备列入黑名单。后代域可以覆盖此继承配置并清除黑名单。您只能在全局级别将 Firepower 管理中心列入黑名单。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **黑名单 (Blacklist)**。

步骤 2 使用右侧的下拉列表按设备组、型号或者策略对列表进行排序。

提示 Health Policy 列 ( ) 旁边的状态图标指示该设备的当前运行状况。System Policy 列 ( ) 旁边的状态图标指示Firepower 管理中心与设备之间的通信状态。

步骤 3 您有两种选择：

- 要将组、型号或策略类别中的所有设备列入黑名单，请选中类别的对应复选框，然后点击**将所选设备列入黑名单 (Blacklist Selected Devices)**。
- 要从组、型号或策略类别中的所有设备清除黑名单，请选中类别的对应复选框，然后点击**清除所选设备上的黑名单 (Clear Blacklist on Selected Devices)**。

将运行状况策略模块列入黑名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

您可以将设备上的单个运行状况策略模块列入黑名单。您可能想要执行此操作以禁止来自模块的事件将设备的状态变更为警告或严重。

在黑名单设置生效后，设备在 Blacklist 页面和 Appliance Health Monitor Module Status Summary（但是仅在 Appliance Status Summary 主页面的展开的视图中）上显示为 **Partially Blacklisted** 或 **All Modules Blacklisted**。

提示 确保您跟踪单独列入黑名单的模块，以便您可以在需要时重新激活它们。如果您意外地禁用模块，则可能漏掉所需的警告或严重消息。

在多域部署中，祖先域中的管理员可以将后代域中的运行状况模块列入黑名单。但是，后代域中的管理员可以覆盖此祖先配置，并清除在其域中应用的策略的黑名单。只能在全局级别将 Firepower 管理中心运行状况模块列入黑名单。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **黑名单 (Blacklist)**。

步骤 2 点击要修改的设备旁边的编辑图标 ( )。

步骤 3 选中要列入黑名单的运行状况策略模块旁边的复选框。某些模块仅适用于特定设备；有关详细信息，请参阅运行状况模块，第 200 页。

步骤 4 点击**保存 (Save)**。

运行状况监控器警报

您可以设置警报以在运行状况策略中的模块状态变更时，通过电子邮件、SNMP 或系统日志通知您。您可以将现有警报响应与运行状况事件级别相关联，以在特定级别的运行状况事件发生时触发和发出警报。

例如，如果您担心设备可能用尽硬盘空间，可以在剩余磁盘空间达到警告级别时自动向系统管理员发送一封电子邮件。如果硬盘驱动器继续加载，您可以在硬盘驱动器达到严重性级别时发送第二封电子邮件。

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

运行状况监控器警报信息

运行状况监控器生成的警报包含以下信息：

- 严重程度，指明警报的严重性级别。
- 模块，指定其测试结果触发警报的运行状况模块。
- 说明，包括触发警报的运行状况测试结果。

下表介绍了这些严重级别。

表 *32*：警报严重性

严重性	说明
Critical	运行状况测试结果符合触发“严重”警报状态的标准。
Warning	运行状况测试结果符合触发“警告”警报状态的标准。
正常状态	运行状况测试结果符合触发“正常”警报状态的标准。
Error	运行状况测试未运行。
已恢复	运行状况测试结果符合在“严重”或“警告”警报状态之后返回到正常警报状态的条件。

创建运行状况监控器警报

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

当您创建运行状况监视器警报时，您可以在严重性级别、运行状况模块和警报响应之间建立关联。您可以使用现有警报或特别配置新的警报以报告系统运行状况。当选定的模块发生严重性级别时，警报触发。

如果您以复制现有阈值的方式创建或更新阈值，将会收到冲突通知。当存在重复的阈值时，运行状况监视器使用生成最少警报的阈值并忽略其他阈值。该阈值的超时值必须介于 5 和 4,294,967,295 分钟之间。

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

开始之前

- 配置用于管理 Firepower 管理中心与 SNMP、系统日志或邮件服务器（用于发送运行状况警报）通信的警报响应；请参阅Firepower 管理中心警报响应，第 1371 页。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控器警报 (Monitor Alerts)**。

步骤 2 在**运行状况警报名称 (Health Alert Name)** 字段中输入运行状况警报的名称。

步骤 3 从**严重性 (Severity)** 列表中选择要用于触发警报的严重性级别。

步骤 4 从**模块 (Module)** 列表中选择要为其应用警报的运行状况策略模块。

步骤 5 从**警报 (Alert)** 列表中选择在达到指定的严重性级别时要触发的警报响应。

步骤 6 或者，在**阈值超时 (Threshold Timeout)** 字段中，输入在每个阈值期间结束和阈值计数重置之前应经过的分钟数。
即使策略运行时间间隔值小于阈值超时值，给定模块中报告的两个运行状况事件之间的间隔始终较大。例如，如果将阈值超时更改为 8 分钟，并且策略运行时间间隔为 5 分钟，则报告的事件之间的时间间隔为 10 (5 x 2) 分钟。

步骤 7 点击**保存 (Save)** 保存运行状况警报。

编辑运行状况监控器警报

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

您可以编辑现有运行状况监视器警报以更改与运行状况监控器警报相关的严重性级别、运行状况模块或警报响应。

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控器警报 (Monitor Alerts)**。

步骤 2 从**活动运行状况警报 (Active Health Alerts)** 列表中选择要修改的警报。

步骤 3 点击**加载 (Load)** 以加载所选警报的配置设置。

步骤 4 根据需要修改设置。

步骤 5 点击**保存 (Save)** 以保存已修改的运行状况警报。
系统将显示一条消息，指示是否已成功保存警报配置。

删除运行状况监控器警报

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在多域部署中，只能查看和修改在当前域中创建的运行状况监控器警报。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控器警报 (Monitor Alerts)**。

步骤 2 选择要删除的活动运行状况警报，然后点击**删除 (Delete)**。

接下来的操作

- 禁用或删除基础警报响应，以确保不会继续发出警报；请参阅Firepower 管理中心警报响应，第 1371 页。

使用运行状况监控器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

运行状况监控器为 Firepower 管理中心管理的所有设备以及 Firepower 管理中心提供已编译的运行状况。运行状况监控器由以下部分组成：

- 状态表 - 通过整体运行状态为此 Firepower 管理中心提供受管设备的计数。
- 饼形图 - 指示当前每个运行状态类别中的设备百分比。
- 设备列表 - 提供受管设备的运行状况详细信息。

在多域部署中，祖先域中的运行状况监控器显示所有后代域中的数据。在后代域中，它仅显示当前域中的数据。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控器 (Monitor)**。

步骤 2 在表的**状态 (Status)** 列或饼形图的适当部分中选择适当的状态，以列出具有该状态的设备。

提示 如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3 有以下选项可供选择：

- 查看设备运行状况监控器；请参阅查看设备运行状况监控器，第 215 页。
- 创建运行状况策略；请参阅创建运行状况策略，第 206 页。

• 创建运行状况监控器警报；请参阅创建运行状况监控器警报 ， 第 212 页。

运行状况监控器状态类别

可用状态类别按严重性在下表中列出。

表 33：运行状况指示灯

状态级别	状态图标	饼形图中的状态颜色	说明
Error		黑色	表示设备中的至少一个运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。请与您的技术支持代表联系以获得对运行状况监控模块的更新。
Critical		红色	表示对于设备中的至少一个运行状况模块而言，已超过严重限值，并且该问题尚未解决。
Warning		黄色	表示对于设备中的至少一个运行状况模块而言，已超过警告限值，并且该问题尚未解决。
正常状态		绿色	表示设备中的所有运行状况模块都在应用于该设备的运行状况策略中配置的限值内运行。
已恢复		绿色	表示设备中的所有运行状况模块（包括处于“严重”或“警告”状态的模块）都在应用于该设备的运行状况策略中配置的限值内运行。
禁用		蓝色	表示设备被禁用或列入黑名单，设备没有应用运行状况策略，或者设备当前无法访问。

查看设备运行状况监控器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

设备运行状况监控器提供设备的运行状态的详细视图。

在多域部署中，您可以查看后代域中的设备的运行状况。

提示 在会话处于不活动状态达到1小时（或配置的其他时间间隔）之后，会话通常注销。如果计划长时间被动监控运行状态，请考虑免除某些用户发生会话超时，或者更改系统超时设置。有关详细信息，请参阅用户帐户登录选项，第 64 页和配置会话超时，第 468 页。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控器 (Monitor)**。

步骤 2 展开设备列表。要显示具有特定状态的设备，请点击该状态行中的箭头。或者，在**设备状态摘要 (Appliance Status Summary)** 图形中，点击要查看的设备状态类别的颜色。

提示 如果表示状态级别的该行的箭头方向向下，则该状态的设备列表显示在下方的表中。如果箭头方向向右，则设备列表已隐藏。

步骤 3 在设备列表的 **Appliance** 列中，点击要查看详细信息的设备的名称。

步骤 4 或者，在**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的事件状态类别的颜色。警报详细信息列表切换显示内容以显示或隐藏事件。

运行设备的所有模块

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行所有运行状况模块测试以收集该设备的最新运行状况信息。

在多域部署中，可以运行当前域和任何后代域中的设备的运行状况模块测试。

过程

步骤 1 查看设备的运行状况监控器；请参阅查看设备运行状况监控器，第 215 页。

步骤 2 点击 **Run All Modules**。状态栏指示测试进程，然后 Health Monitor Appliance 页面刷新。

注释 当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

运行特定运行状况模块

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

在您创建运行状况策略时配置的策略运行时间间隔内，运行状况模块测试自动运行。但是，您也可以按需运行一个运行状况模块测试以收集该模块的最新运行状况信息。

在多域部署中，可以运行当前域和任何后代域中的设备的运行状况模块测试。

过程

步骤 1 查看设备的运行状况监控器；请参阅查看设备运行状况监控器，第 215 页。

步骤 2 在**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的运行状况警报状态类别的颜色。

步骤 3 在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Run**。
状态栏指示测试进程，然后 Health Monitor Appliance 页面刷新。

注释 当您手动运行运行状况模块时，第一次自动发生的刷新可能不会影响自动运行测试的数据。如果没有为您手动运行的模块更改该值，请等待几秒钟，然后点击设备名称来刷新该页面。您还可以等待页面再次自动刷新。

生成运行状况模块警报图形

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

您可以图表表示特定设备的特定运行状况测试的一段时间内的结果。

过程

步骤 1 查看设备的运行状况监控器；请参阅查看设备运行状况监控器，第 215 页。

步骤 2 在“运行状况监控设备”(Health Monitor Appliance) 页面的**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的运行状况警报状态类别的颜色。

步骤 3 在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Graph**。

提示 如果未显示事件，您可能需要调整时间范围。

用于故障排除的运行状况监控器报告

某些情况下，如果您的设备有问题，支持人员可能要求您生成故障排除文件以帮助诊断该问题。您可以选择下表中列出的任何选项以定制运行状况监控器报告的故障排除数据。

请注意，在所报告的数据方面，某些选项重叠，但是无论您选择什么选项，故障排除文件都不会包含冗余备份。

表 *34*：可选择的故障排除选项

该选项.....	报告.....
Snort Performance and Configuration	与设备上的 Snort 相关的数据和配置设置
Hardware Performance and Logs	与设备硬件性能相关的数据和日志
System Configuration, Policy, and Logs	与设备的当前系统配置相关的配置设置、数据和日志
Detection Configuration, Policy, and Logs	与对设备的检测相关的配置设置、数据和日志
Interface and Network Related Data	与设备的内联集和网络配置相关的配置设置、数据和日志
Discovery, Awareness, VDB Data, and Logs	与设备上的当前发现和感知配置相关的配置设置、数据和日志
Upgrade Data and Logs	与设备的前期升级相关的数据和日志
All Database Data	包含在故障排除报告中的所有数据库相关数据
All Log Data	设备数据库收集的所有日志
Network Map Information	当前网络拓扑数据

生成设备故障排除文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

可以生成可发送给支持人员的定制故障排除文件。

在多域部署中，您可以为后代域中的设备生成故障排除文件。

过程

步骤 1 查看设备的运行状况监控器；请参阅查看设备运行状况监控器，第 215 页。

步骤 2 点击 **Generate Troubleshooting Files**。

步骤 3 选择**所有数据 (All Data)** 以生成所有可能的故障排除数据或选中单个复选框以自定义报告。

步骤 4 点击 **OK**。

接下来的操作

- 或者，监控任务状态；请参阅查看任务消息，第 239 页。
- 按下载故障排除文件，第 219 页中所述下载故障排除文件。

下载故障排除文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

在多域部署中，您可以为后代域中的设备下载故障排除文件。

过程

步骤 1 在消息中心查看任务消息；请参阅查看任务消息，第 239 页。

步骤 2 找出对应所生成的故障排除文件的任务。

步骤 3 在设备生成故障排除文件并且任务状态变更为 `Completed` 之后，点击 **Click to retrieve generated files**。

步骤 4 按照浏览器的提示下载文件。

注释 对于受管设备，系统通过将设备名称置于文件名前面来重命名文件。

步骤 5 按照支持部门的指示将故障排除文件发送给思科。

运行状况事件视图

通过“运行状况事件视图”(Health Event View) 页面，您可以查看由运行状况监控器在 Firepower 管理中心日志运行状况事件中记录的运行状况事件。完全可自定义的事件视图使您可以快速轻松地分析运行状况监控器所收集的运行状况事件。可以搜索事件数据，以便轻松访问可能与正调查的事件

有关的其他信息。如果您了解每个运行状况模块测试的条件，就可以更有效地配置运行状况事件的警报。

可以在运行状况事件视图页面执行许多标准事件视图功能。

查看运行状况事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

“运行状况事件表视图”(Table View of Health Events) 页面提供指定设备上所有运行状况事件的列表。

当您在Firepower 管理中心中从 Health Monitor 页面访问运行状况事件时，您可以检索所有受管设备的所有运行状况事件。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

提示 您可以为该视图添加书签，使您可以返回到其中包含事件的运行状况事件表的运行状况事件工作流程页面。加入书签的视图检索您当前正查看的时间范围内的事件，但是如果需要，您可以稍后修改时间范围以使用较新的信息更新该表。

过程

选择**系统 (System)** > **运行状况 (Health)** > **事件 (Events)**。

提示 如果您使用的自定义工作流程不包括运行状况事件表视图，请点击 **(switch workflow)**。在 Select Workflow 页面上，点击 **Health Events**。

注释 如果未显示事件，您可能需要调整时间范围。

按模块和设备查看运行状况事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

过程

步骤 1 查看设备的运行状况监控器；请参阅查看设备运行状况监控器，第 215 页。

步骤 2 在**模块状态摘要 (Module Status Summary)** 图形中，点击要查看的事件状态类别的颜色。
警报详细信息列表切换显示内容以显示或隐藏事件。

步骤 3 在要查看其事件列表的警报的 **Alert Detail** 行，请点击 **Events**。
系统将显示“运行状况事件”(Health Events) 页面，其中包含以设备名称和指定运行状况警报模块名称为限制的查询的结果。如果未显示事件，您可能需要调整时间范围。

步骤 4 如果要查看指定设备的所有运行状况事件，请展开**搜索限制 (Search Constraints)**，然后点击**模块名称 (Module Name)** 限制将其删除。

查看运行状况事件表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **事件 (Events)**。

步骤 2 有以下选项可供选择：

- 书签 - 要将当前页面加入书签，以便可以快速返回到该页面，请点击**将此页面加入书签 (Bookmark This Page)**，提供书签的名称，然后点击**保存 (Save)**。
- 更改工作流程 - 要选择其他运行状况事件工作流程，请点击（**切换工作流程**）**([switch workflows])**。
- 删除事件 - 要删除运行状况事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)**。要删除当前受限制视图中的所有事件，请点击 **Delete All**，然后确认要删除所有事件。
- 生成报告 - 根据表视图中的数据生成报告 - 点击**报告设计器 (Report Designer)**。
- 修改 - 修改在“运行状况”(Health) 表视图中列出的事件的时间和日期范围。请注意，如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间段（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。
- 导航 - 浏览事件视图页面。
- 导航书签 - 要导航至书签管理页面，请点击任何事件视图中的**查看书签 (View Bookmarks)**。

- 导航其他 - 导航至其他事件表以查看关联事件。
- 排序 - 对显示的事件进行排序，更改事件表中显示的列，或者限制显示的事件
- 查看全部 - 要查看视图中所有事件的事件详细信息，请点击**查看全部 (View All)**。
- 查看详细信息 - 要查看与单个运行状况事件关联的详细信息，请点击事件左侧的向下箭头链接。
- 查看多个 - 要查看多个运行状况事件的事件详细信息，请选中与要查看其详细信息的事件对应的行旁边的复选框，然后点击**查看 (View)**。
- 查看状态 - 要查看特定状态的所有事件，请点击“状态”(Status) 列中的状态图标以获取具有该状态的事件。

7000 和 8000 系列设备的硬件警报详细信息

注释 8350 硬件平台有六个风扇，显示为 FAN2 到 FAN7。这是预期行为。如果您在 8350 平台上收到关于 FAN1 或一般风扇编号的硬件警报，可以忽略该警报。

表 *35*: 为 *7000* 和 *8000* 系列设备监控的条件

监控的条件	黄色或红色错误条件的原因
设备高可用性状态	如果高可用性对中的 7000 或 8000 系列设备彼此不再通信（例如，由于布线问题），硬件告警模块变为红色。
`ftwo` 守护程序状态	如果 `ftwo` 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
检测到的 NFE 卡	表示系统中检测到的 NFE 卡的数量。如果该值不匹配设备的预期 NFE 计数，硬件告警模块变为红色。
NFE 硬件状态	如果一个或多个 NFE 卡不进行通信，硬件告警模块变为红色，并且适用的卡显示在消息详细信息中。
NFE 心跳	如果系统检测不到 NFE 心跳，硬件告警模块变为红色，消息详细信息中包括对相关卡的参考。
NFE 内部链路状态	如果 NMSB 和 NFE 卡之间的链路断开，硬件告警模块变为红色，消息详细信息中包括对相关端口的参考。
NFE 消息守护程序	如果 NFE 消息守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序（以及 NFE 卡号 [如果适用]）的参考。

监控的条件	黄色或红色错误条件的原因
NFE 温度	如果 NFE 温度超过 97 摄氏度，硬件告警模块的运行状况变为黄色，消息详细信息中包括对 NFE 温度（以及 NFE 卡号 [如果适用]）的参考。 如果 NFE 温度超过 102 摄氏度，硬件告警模块的运行状况变为红色，消息详细信息中包括对 NFE 温度（以及 NFE 卡号 [如果适用]）的参考。
NFE 温度状态	表示给定的NFE卡的当前温度状态。硬件告警模块用绿色表示“正常”，用黄色表示“警告”，用红色表示“严重”（以及 NFE 卡号 [如果适用]）。
NFE TCAM 守护程序	如果 NFE TCAM 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序（以及NFE卡号[如果适用]）的参考。
nfm_ipfragd（主机碎片）守护程序	如果 nfm_ipfragd 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序（以及NFE卡号[如果适用]）的参考。
NFE 平台守护程序	如果NFE平台守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序（以及 NFE 卡号 [如果适用]）的参考。
NMSB 通信	如果媒体组件不存在或不进行通信，硬件告警模块的运行状况变为红色，消息详细信息包括对 NFE 温度（以及 NFE 卡号 [如果适用]）的引用。
psls 守护程序状态	如果 psls 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。
Rulesd（主机规则）守护程序	如果 Rulesd 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序（以及 NFE 卡号 [如果适用]）的参考。
scmd 守护程序状态	如果 scmd 守护程序断开，硬件告警模块的运行状况变为红色，消息详细信息中包括对守护程序的参考。

运行状况事件表

您选择在运行状况策略中启用的运行状况监视器模块运行各种测试，以确定设备运行状况。当运行状况满足您指定的标准时，生成一个运行状况事件。

下表介绍在运行状况事件表中可以查看和搜索的字段。

表 *36*: 运行状况事件字段

字段	说明
模块名称	指定生成要查看的运行状况事件的模块的名称。例如，要查看度量 CPU 性能的事件，请键入 `CPU`。搜索应检索适用的 CPU 使用率和 CPU 温度事件。
Test Name （仅限搜索）	生成事件的运行状况模块的名称。
Time （仅限搜索）	运行状况事件的时间戳。
说明	生成事件的运行状况模块的说明。例如，当无法执行进程时生成的运行状况事件被标记为 `Unable to Execute`。
值	生成事件的运行状况测试所获得的结果值（单位数量）。 例如，如果其正在监控的设备使用的 CPU 资源达到 80% 或更多时Firepower 管理中心生成运行状况事件，则该值可以是介于 80 到 100 之间的一个数字。
单位	结果的单位描述符。您可以使用星号 (*) 创建通配符搜索。 例如，如果其正在监控的设备使用的 CPU 资源达到 80% 或更多时Firepower 管理中心生成运行状况事件，则单位描述符为百分号 (%)。
状态	为设备报告的状态（严重、黄色、绿色或已禁用）。
域	对于受管设备报告的运行状况事件，即报告运行状况事件的设备的域。对于 Firepower 管理中心报告的运行状况事件，即为 `Global`。此字段只存在于多域部署中。
设备	报告运行状况事件的设备。

第 13 章

监控系统

以下主题介绍如何监控 Firepower 系统：

- 系统统计项，第 225 页
- 系统消息，第 234 页
- 管理系统消息，第 237 页

系统统计项

Firepower 系统 Web 界面中的“统计信息”(Statistics) 页面列出常规设备统计信息的当前状态，包括磁盘使用率和系统进程、数据相关器统计信息和入侵事件信息。

您同时查看有关 Firepower 管理中心和 7000 和 8000 系列设备的系统统计信息。

按设备划分的系统统计信息可用性

系统统计信息在 Web 界面中提供，如下所示：

统计信息类型	统计信息页面部分	管理中心	7000 和 8000 系列设备
主机统计信息	主机统计信息部分，第 226 页	是	是
系统状态和磁盘空间使用情况	磁盘使用率部分，第 226 页	是	是
系统进程状态	进程部分，第 226 页	是	是
Data Correlator 统计信息	SFDataCorrelator 进程统计信息部分，第 232 页	是	否
入侵事件统计信息	入侵事件信息部分，第 233 页	是	否

主机统计信息部分

下表介绍了 Statistics 页面列出的主机统计信息。

表 *37*: 主机统计信息

类别	说明
Time	系统当前时间。
正常运行时间	系统上次启动后持续的天数（如果适用）、小时数和分钟数。
内存使用率	正使用的系统内存的百分比。
Load Average	过去 1 分钟、5 分钟和 15 分钟内 CPU 队列的平均进程数。
磁盘使用情况	正使用的磁盘空间的百分比。点击箭头查看更详细的主机统计信息。
流程	系统中运行的进程摘要。

磁盘使用率部分

Statistics 页面的 Disk Usage 部分提供磁盘使用情况快览，可以按类别和分区状态进行查看。如果您在设备上安装了一个恶意软件存储包，您还可以查看分区状态。您可以随时监控此页面，确保系统进程和数据库有充足的磁盘空间可用。

提示 在Firepower 管理中心中，您也可以使用运行状况监控在磁盘空间较低的情形下监控磁盘使用情况和警报。

进程部分

在“统计信息”(Statistics) 页面的“进程”(Processes) 部分，可以查看一台设备上正在运行的进程。它为每个运行的进程提供常规进程信息和特定信息。您可以使用 Firepower 管理中心的 Web 界面查看任何受管设备的进程状态。

请注意，设备上运行有两个不同类型的进程：后台守护程序和可执行文件。后台守护程序始终运行，可执行文件在需要时运行。

进程状态字段

展开“统计信息”(Statistics) 页面的“进程”(Processes) 部分时，也可以查看以下内容：

Cpu(s)

列出以下 CPU 使用信息：

- 用户进程使用百分比
- 系统进程使用百分比
- 优先使用情况百分比（拥有负优先值进程的CPU使用情况，表示更高优先级）。优先值是指系统进程的计划优先级，范围为 -20（最高优先级）到 19（最低优先级）。
- 空闲使用百分比

Mem

列出以下内存使用信息：

- 内存中千字节总数
- 内存中已使用千字节总数
- 内存中空闲的千字节总数
- 内存中缓存的千字节总数

交换

列出以下交换使用信息：

- 交换空间中千字节总数
- 交换空间中已使用千字节总数
- 交换空间中空闲的千字节总数
- 交换空间中缓存的千字节总数

下表介绍了显示在“进程”(Processes) 部分中的各列。

表 *38*：进程列表列

列	说明
Pid	进程 ID 编号
用户名	运行进程的用户或组的名称
Pri	进程优先级
尼斯	*nice* 值是表示一个进程计划优先级的值。值范围为 -20（最高优先级）到 19（最低优先级）
Size	进程使用的内存大小（以千字节计，除非数值后是 m，即表示兆字节）

列	说明
Res	内存中常驻页面文件的数量（以千字节计，除非数值后是 m，即表示兆字节）
省/自治区	进程状态： • D - 进程处于不可中断休眠（通常 Input/Output） • N - 进程有一个正优先值 • R - 进程可运行（在运行队列中） • S - 进程处于休眠模式 • T - 进程被跟踪或停止 • W - 进程在分页 • X - 进程已废弃 • Z - 进程已失效 • < - 进程有一个负优先值
Time	进程运行的时间（格式为小时:分钟:秒）
Cpu	进程正在使用的 CPU 的百分比
命令	进程的可执行名称

系统后台守护程序

后台守护程序在设备上持续运行。他们确保服务可用，并在需要时产生进程。下表列出了 Process Status 页面可以看到的后台守护程序，并对其功能进行简要说明。

注释 下表并非一台设备上可运行的所有进程的详尽列表。

表 *39*: 系统后台守护程序

后台守护程序	说明
crond	管理计划命令的实施（cron 作业）
dhclient	管理动态主机 IP 地址
fpcollect	管理客户端和服务器指纹集合

后台守护程序	说明
httpd	管理 HTTP（Apache 网络服务器）进程
httpsd	管理 HTTPS（使用 SSL 的 Apache 网络服务器）服务，检查正在运行的 SSL 和有效的证书身份验证；在后台运行，为设备提供安全的网络接入
keventd	管理 Linux 内核事件通知消息
klogd	管理 Linux 内核消息监听和记录
kswapd	管理 Linux 内核交换内存
kupdated	管理 Linux 内核更新进程，执行磁盘同步
mysqld	管理数据库进程
ntpd	管理网络时间协议 (NTP) 进程
pm	管理所有 Firepower 系统进程，启动所需进程，重新启动所有意外发生故障的进程
reportd	管理报告
safe_mysqld	管理数据库安全模式操作；如果出现错误，重新启动数据库后台守护程序，并向文件中记录运行时间信息
SFDataCorrelator	管理数据传输
sfestreamer （仅限管理中心）	管理使用事件流转换器的第三方客户端应用的连接
sfmgr	使用到一台设备的 sftunnel 连接，为远程管理和配置该设备提供 RPC 服务
SFRemediateD （仅限管理中心）	管理补救响应
sftimeserviced （仅限管理中心）	将时间同步消息转发到受管设备
sfmbservice	使用到设备的 sftunnel 连接，为在远程设备上运行的 sfmb 消息代理进程提供接入服务。目前只有运行状况监控功能使用此程序，将运行状况事件和警报从受管设备发送到 Firepower 管理中心。
sftroughd	侦听进入套接字的连接，然后调用正确的可执行程序（通常是思科消息代理 sfmb）处理请求

后台守护程序	说明
sftunnel	为需要与远程设备通信的所有进程提供安全的通信通道
sshd	管理安全外壳 (SSH) 进程；在后台运行，为设备提供 SSH 接入
syslogd	管理系统日志 (syslog) 流程

可执行文件和系统实用程序

系统会有许多可执行文件，它们在其他进程或用户操作执行时开始运行。下表介绍了在Process Status页面可能会看到的可执行程序。

表 *40*：系统可执行程序和实用程序

可执行程序	说明
awk	执行用 `awk` 编程语言书写的程序的实用程序
bash	GNU Bourne-Again 外壳
cat	读取文件并将内容写入标准输出的实用程序
chown	更改用户和组文件权限的实用程序
chsh	更改默认登录外壳的实用程序
SFDataCorrelator （仅管理中心）	分析由系统创建的二进制文件，从而生成事件、连接数据和网络映射
cp	复制文件的实用程序
df	列出设备可用空间量的实用程序
echo	将内容写入标准输出的实用程序
egrep	按特定输入搜索文件和文件夹、支持标准 grep 不支持的正则表达式扩展集的实用程序
find	按特定输入循环搜索目录的实用程序
grep	按特定输入搜索文件和目录的实用程序
halt	停用服务器的实用程序
httpsdctl	处理安全 Apache 网络进程

可执行程序	说明
hwclock	允许访问硬件时钟的实用程序
ifconfig	表示网络配置可执行程序。确保 MAC 地址保持不变
iptables	根据 Access Configuration 页面所做的更改处理访问限制。
iptables-restore	处理 iptables 文件恢复
iptables-save	处理对 iptables 保存的更改
kill	可用来结束会话和进程的实用程序
killall	可用来结束所有会话和进程的实用程序
ksh	Korn Shell 的公共域版本
记录器	提供通过命令行访问系统日志后台守护程序方法的实用程序
md5sum	为指定文件打印校验和以及块数量的实用程序
mv	移动（重命名）文件的实用程序
myisamchk	指数据库表校验和修复
mysql	指数据库进程；可能出现多个实例
openssl	指创建身份验证证书
perl	指一个 perl 进程
ps	将进程信息写入标准输出的实用程序
sed	用来编辑一个或多个文本文件的实用程序
sfheartbeat	识别心跳广播，表示设备处于活动状态；心跳用来保持设备和Firepower管理中心之间的联络
sfmb	表示消息代理进程；处理Firepower 管理中心和设备之间的通信。
sh	Korn Shell 的公共域版本
shutdown	关闭设备的实用程序
睡眠	在指定秒数内暂停进程的实用程序

可执行程序	说明
smtpclient	启用邮件事件通知功能后，处理邮件传输的邮件客户端
snmptrap	将 SNMP 陷阱数据转发到启用 SNMP 通知功能后指定的 SNMP 陷阱服务器
snort	表示 Snort 正在运行
ssh	表示与设备连接的安全外壳 (SSH)
sudo	指 sudo 进程，其允许管理员以外的用户运行可执行程序
top	显示最大 CPU 进程信息的实用程序
touch	用来更改指定文件的访问和修改时间的实用程序
vim	用来编辑文本文件的实用程序
wc	执行指定文件行、字和字节计数的实用程序

SFDataCorrelator 进程统计信息部分

在Firepower管理中心上，可以查看有关当日数据相关器和网络发现进程的统计信息。当受管设备执行数据收集、解码和分析时，网络发现进程将数据与指纹和漏洞数据库相关联，然后由Firepower管理中心上运行的Data Correlator处理成二进制文件。数据相关器分析二进制文件的信息后生成事件，然后创建网络映射。

网络发现和 Data Correlator 中显示的统计信息为当日的平均值，使用每台设备从 12:00 AM 到 11:59 PM 之间搜集的统计信息。

下表介绍了 Data Correlator 进程显示的统计信息。

表 *41*：数据相关器进程统计信息

类别	说明
Events/Sec	Data Correlator 每秒钟接收和处理的发现事件的数量
Connections/Sec	Data Correlator 每秒钟接收和处理的连接的数量
CPU Usage - User (%)	当日用户进程占 CPU 时间的平均百分比
CPU Usage - System (%)	当日系统进程占 CPU 时间的平均百分比
VmSize (KB)	当日分配给 Data Correlator 的平均内存大小，单位为千字节

类别	说明
VmRSS (KB)	当日 Data Correlator 使用的平均内存使用量，单位为千字节

入侵事件信息部分

在 Firepower 管理中心和受管设备上，可以查看“统计信息”(Statistics) 页面上有关入侵事件的摘要信息。此信息包括上次入侵事件的日期和时间、过去一小时和昨天发生的事件总数，以及数据库的事件总数。

注释 Statistics 页面 Intrusion Event Information 部分的信息依据是受管设备上存储的入侵事件，而不是发送到Firepower管理中心的信息。如果受管设备无法在本地存储（或配置为不存储）入侵事件，则此页面上不会列出入侵事件信息。

下表介绍了 Statistics 页面 Intrusion Event Information 部分显示的统计信息。

表 *42*：入侵事件信息

统计	说明
Last Alert Was	上次事件发生的日期和时间
Total Events Last Hour	过去一个小时内发生的事件总数
Total Events Last Day	过去 24 小时内发生的事件总数
Total Events in Database	时间数据库中的事件总数

查看系统统计信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任意 威胁（用于入侵事件数据）	任意 保护（用于入侵事件数据）	任意	仅全局	管理员/维护人员

在 Firepower 管理中心上，Web 界面会显示该设备及其管理的任何设备的统计信息。在 7000 和 8000 系列设备上，系统仅显示该设备的统计信息。

过程

步骤 1 选择**系统 (System)** > **监控 (Monitoring)** > **统计信息 (Statistics)**。

步骤 2 或者，在 Firepower 管理中心上，从**选择设备 (Select Device[s])** 列表中选择设备，然后点击**选择设备 (Select Devices)**。

步骤 3 查看可用统计信息；请参阅按设备划分的系统统计信息可用性，第 225 页。

步骤 4 或者，在“磁盘使用率”(Disk Usage) 部分中，可以执行以下操作：

- 在 **By Category** 层叠图中将指针悬停在一个磁盘使用类别上以（按顺序）查看：

  该类别使用的可用磁盘空间百分比

  该磁盘的实际存储空间

  该类别的总可用磁盘空间

- 点击**按分区 (By Partion)** 旁边的向下箭头将其展开。如果安装有恶意软件存储包，则系统会显示 `/var/storage` 分区使用情况。

步骤 5 或者，点击**进程 (Processes)** 旁边的箭头以查看进程状态字段，第 226 页中所述的信息。

系统消息

当需要跟踪发生在 Firepower 系统中的问题时，请从消息中心开始调查。通过此功能，可以查看 Firepower 系统持续生成的有关系统活动和状态的消息。

要打开消息中心，请点击位于主菜单中“部署”(Deploy) 按钮正右侧的“系统状态”(System Status) 图标。根据系统状态，此图标可采用以下形式之一：

- - 指示系统上存在一个或多个错误和任意数量的警告。
- - 指示系统上存在一个或多个警告而没有错误。
- - 指示系统上不存在任何警告或错误。

如果随该图标显示数字，则其指示错误或警告消息的当前总数。

要关闭消息中心，请点击 Firepower 系统 Web 界面内其外部的任意位置。

除消息中心以外，Web 界面也会显示对您的活动和日常系统活动的立即响应中的弹出通知。某些弹出通知在五秒后自动消失，而其他通知则“粘滞”，意味着它们会显示直至您通过点击其消除图标 (×) 明确将其消除为止。点击通知列表顶部的**消除 (Dismiss)** 链接以一次性解除所有通知。

提示 将光标悬停在非粘滞弹出通知的上方会导致其粘滞。

系统根据用户的许可证、域和访问角色确定在弹出通知和消息中心内向其显示哪些消息。

消息类型

消息中心显示消息报告系统活动和状态，分为三个不同选项卡：

部署

此选项卡显示与系统中的每个设备的配置部署相关的当前状态，按域分组。Firepower 系统在此选项卡上报告以下部署状态值：

- 运行（旋转 ）- 该配置处于部署过程中。
- 成功 ( ) - 该配置已成功部署。
- 警告 ( ) - 警告部署状态利用警告系统状态图标 ( ) 为所显示的消息计数提供帮助。
- 失败 ( ) - 该配置未能部署；请参阅过时策略，第 263 页。失败的部署利用错误系统状态图标 ( ) 为所显示的消息计数提供帮助。

健康状况

此选项卡显示系统中每个设备的当前运行状况信息，按域分组。运行状况由运行状况模块生成，如运行状况监控基础知识，第 199 页中所述。Firepower 系统在此选项卡上报告以下运行状况状态值：

- 警告 ( ) - 表示对于设备中的运行状况模块而言，已超过警告限值，并且该问题尚未解决。“运行状况监控”(Health Monitor) 页面利用黄色三角形图标 ( ) 来指示这些状况。警告状态利用警告系统状态图标 ( ) 为所显示的消息计数提供帮助。
- 严重 ( ) - 表示对于设备中的运行状况模块而言，已超过严重限值，并且该问题尚未解决。“运行状况监控”(Health Monitor) 页面利用 图标来指示这些状况。严重状态利用错误系统状态图标 ( ) 为所显示的消息计数提供帮助。
- 错误 ( ) - 表示设备中的运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。“运行状况监控”(Health Monitor) 页面利用 图标来指示这些状况。错误状态利用错误系统状态图标 ( ) 为所显示的消息计数提供帮助。

可以点击“运行状况”(Health) 选项卡中的链接来查看有关“运行状况监控”(Health Monitor) 页面的详细信息。如果没有当前运行状况条件，“运行状况”(Health) 选项卡不显示消息。

任务

在 Firepower 系统中，可以执行可能需要一些时间来完成的特定任务（例如配置备份或更新安装）。此选项卡显示这些长时间运行任务的状态，并且可以包括由您或系统中的其他用户（如果您有适合的访问权限）发起的任务。此选项卡根据每条消息的最新更新时间，按时间倒序显示消息。某些任务状态消息包括有关所述任务的更详细信息的链接。Firepower 系统在此选项卡上报告以下任务状态值：

- 等待 ( ) - 表示等待另一个正在进行的任务完成后再运行的任务。此消息类型显示更新进度条。
- 运行（旋转 ）- 表示正在进行的任务。此消息类型显示更新进度条。
- 重试 ( ) - 表示自动重试的任务。请注意，并非所有的任务都可以重试。此消息类型显示更新进度条。
- 成功 ( ) - 表示已成功完成的任务。
- 失败 ( ) - 表示未成功完成的任务。失败的任务利用错误系统状态图标 ( ) 为所显示的消息计数提供帮助。
- 停止 ( ) - 表示由于系统更新而中断的任务。停止的任务不能恢复。

当新任务开始时，此选项卡中显示新消息。随着任务完成（状态成功、失败或停止），此选项卡继续以指示的最终状态显示消息，直至删除它们。思科建议您删除消息以减少“任务”(Tasks) 选项卡和消息数据库的混乱。

邮件管理

从“消息中心”(Message Center) 可以执行以下操作：

- 配置弹出通知行为（选择是否显示通知）。
- 显示系统数据库中的其他任务状态消息（如有任何尚未移除的此类消息）。
- 移除单个任务状态消息。（此操作会影响到可以查看已移除消息的所有用户。）
- 批量移除任务状态消息。（此操作会影响到可以查看已移除消息的所有用户。）

提示 思科建议您定期在“任务”(Task) 选项卡中移除积累的任务状态消息，使显示画面和数据库减少凌乱感。当数据库中的消息数接近 100,000 条时，系统会自动删除您已移除的任务状态消息。

管理系统消息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	部署：具有**将配置部署到设备 (Deploy Configuration to Devices)** 权限的管理员/自定义用户角色 运行状况：具有**运行状况 (Health)** 权限的管理员/自定义用户角色 其他人发起的任务：管理员/具有**查看其他用户的任务 (View Other Users' Tasks)** 权限的自定义用户角色 您已发起的任务：任意

过程

步骤 1 点击“系统状态”(System Status) 图标以显示消息中心。

步骤 2 有以下选项可供选择：

- 点击**部署 (Deployments)** 选项卡以查看与配置部署相关的消息。请参阅查看部署消息，第 238 页。
- 点击**运行状况 (Health)** 选项卡以查看与您的 Firepower 管理中心和在其中注册的设备相关的消息。请参阅查看运行状况消息，第 238 页。
- 点击“任务”(Tasks) 选项卡以查看或管理与长期运行任务相关的消息。请参阅查看任务消息，第 239 页或管理任务消息，第 240 页。
- 点击消息中心右上角的齿轮图标 () 以配置弹出式通知行为。请参阅配置通知行为，第 240 页。

查看部署消息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	具有**将配置部署到设备 (Deploy Configuration to Devices)** 权限的管理员/用户角色

过程

步骤 1 点击“系统状态”(System Status) 图标以显示消息中心。

步骤 2 点击“部署”(Deployments) 选项卡。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)** 以查看所有当前部署状态。
- 点击状态值以只查看具有该部署状态的消息。
- 将光标悬停在消息的已逝时间指标上（例如，**1m 5s**）可查看已逝时间，以及部署的开始和停止时间。

查看运行状况消息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	具有**运行状况 (Health)** 权限的管理员/用户角色

过程

步骤 1 点击“系统状态”(System Status) 图标以显示消息中心。

步骤 2 点击“运行状况”(Health) 选项卡。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)** 以查看所有当前运行状态。

- 点击状态值以只查看具有该状态的消息。
- 将光标悬停在消息的相对时间指标上（例如，**3 天前**）可查看该消息最新更新的时间。
- 要查看特殊信息的详细运行状态信息，请点击该消息。
- 要查看“运行状况监控器”(Health Monitor) 页面上的完整运行状态，请点击选项卡底部的**运行状况监控器 (Health Monitor)**。

查看任务消息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	其他人发起的任务：管理员/具有**查看其他用户的任务 (View Other Users' Tasks)** 权限的自定义用户角色 您已发起的任务：任意

过程

步骤 1 点击“系统状态”(System Status) 图标以显示消息中心。

步骤 2 点击“任务”(Tasks) 选项卡。

步骤 3 有以下选项可供选择：

- 点击**总计 (total)** 以查看所有当前任务状态。
- 点击状态值以只查看具有该状态的任务的消息。

  注释 已停止任务的消息仅显示在任务状态消息总列表中。您无法过滤已停止任务。
- 将光标悬停在消息的相对时间指标上（例如，**3 天前**）可查看该消息最新更新的时间。
- 点击消息中的任何链接，查看有关该任务的详细信息。
- 如果可显示更多任务状态消息，请点击消息列表底部的**获取更多消息 (Fetch more messages)** 以对其进行检索。

管理任务消息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	其他人发起的任务：管理员/具有**查看其他用户的任务 (View Other Users' Tasks)** 权限的自定义用户角色 您已发起的任务：任意

过程

步骤 1 点击“系统状态”(System Status) 图标以显示消息中心。

步骤 2 点击“任务”(Tasks) 选项卡。

步骤 3 有以下选项可供选择：

- 如果可显示更多任务状态消息，请点击消息列表底部的**获取更多消息 (Fetch more messages)** 以对其进行检索。
- 要移除一条已完成的任务的消息（状态为已停止、成功或失败），请点击该消息旁边的移除图标 (✖)。
- 要移除已完成的所有任务的全部消息（状态为已停止、成功或失败），请使用**总数 (total)** 过滤消息，然后点击**移除所有已完成的任务 (Remove all completed tasks)**。
- 要移除已成功完成的所有任务的全部消息，请使用**成功 (success)** 过滤消息，然后点击**移除所有成功的任务 (Remove all successful tasks)**。
- 要移除已失败的所有任务的全部消息，请使用**失败 (failure)** 过滤消息，然后点击**移除所有失败的任务 (Remove all failed tasks)**。

配置通知行为

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何环境

注释 此设置会影响所有弹出通知并在登录会话之间持久保留。

过程

步骤 1 点击“系统状态”(System Status) 图标以显示消息中心。

步骤 2 点击消息中心右上角的齿轮图标 ( )。

步骤 3 要启用或禁用弹出通知显示，请点击**显示通知 (Show notifications)** 滑块。

步骤 4 再次点击齿轮图标 ( ) 可隐藏滑块。

步骤 5 再次点击“系统状态”(System Status) 图标可关闭消息中心。

第 IV 部分

部署管理

第 14 章

域管理

以下主题介绍如何使用域管理多租户：

使用域的多租户简介

您可以通过 Firepower 系统实施使用域的多租户。域对受管设备、配置和事件的用户访问进行分段。您在一个顶级全球域下最多可以创建 50 个子域，分为两个或三个级别。

当您登录到 Firepower 管理中心时，将会登录到单个域，称为当前域。根据您的用户帐户，您或许可以切换到其他域。

除了您的用户角色施加的任何限制之外，您当前的域级别也可能会限制您修改各种 Firepower 系统配置的能力。系统会将大多数管理任务（例如系统软件更新）限制于全局域。

系统会限制对枝叶域（不含子域的域）的其他任务。例如，您必须将每个受管设备与一个枝叶域相关联，并从该枝叶域的情景执行设备管理任务。

提示

本指南中的每个任务主题具有一个**支持域 (Supported Domains)** 值，其表示您可以执行任务的域级别。

根据每个枝叶域的设备收集的发现数据，该枝叶域可构建自己的网络映射。受管设备报告的事件（连接、入侵、恶意软件等）还会与设备的枝叶域相关联。

一个域级别：全局

如果不配置多租户，则所有设备、配置和事件属于全局域，其在此情景下也是一个枝叶域。除了域管理之外，系统会隐藏特定域配置和分析选项，直到您添加子域。

两个域级别：全局和第二级

在两个级别的多域部署中，全局域只有直接的后代域。例如，托管安全运营商 (MSSP) 可以使用单一 Firepower 管理中心来管理多个客户的网络安全：

- MSSP 的管理员可以登录全局域来管理所有客户的部署。
- 每个客户的管理员都可以登录第二级已命名子域，以便只管理适用于其组织的设备、配置和事件。这些本地管理员无法查看或影响 MSSP 的其他客户的部署。

三个域级别：全局、第二级和第三级

在三个级别的多域部署中，全局域拥有多个子域，且至少其中一个子域又拥有其自己的子域。要扩展上述示例，请考虑这样一个场景，其中一位 MSSP 客户（已经限制在一个子域中）希望进一步对其部署进行分段。此客户希望单独管理两类设备：位于网络边缘的设备，以及位于内部的设备：

- 客户的管理员可以登录第二级子域来管理客户的整个配置。
- 客户边缘网络的管理员可以登录第三级（枝叶）域，以便只管理部署在网络边缘的设备，以及适用的配置和事件。同样，客户内部网络的管理员可以登录第三级域来管理内部设备、配置和事件。边缘和内部管理员无法查看彼此的部署。

域术语

本文档在介绍域和多域部署时使用以下术语：

全局域

在多域部署中，是指顶级域。如果不配置多租户，则所有设备、配置和事件都属于全局域。全局域中的管理员可以管理整个 Firepower 系统部署。

子域

第二或第三级域。

第二级域

全局域的子级。第二级域可以是枝叶域，也可以具有子域。

第三级域

第二级域的子级。第三级域始终是枝叶域。

枝叶域

没有子域的域。每台设备都必须属于枝叶域。

后代域

从层次结构中的当前域下传的域。

子域

域的直接后代。

祖先域

当前域从其下传的域。

父域

域的直接祖先。

同级域

具有相同父级的域。

当前域

您现在登录的域。在 Web 界面的右上角，系统在您的用户名之前显示当前域的名称。除非您的用户角色受限，否则可以编辑当前域中的配置。

域属性

要修改域的属性，您必须在该域的父域中具有管理员访问权限。

名称和描述

每个域在层次结构中必须拥有唯一的名称。说明是可选的。

父域

第二和第三级域有父域。在创建域后，无法更改该域的父级。

设备

仅枝叶域可包含设备。换句话说，域可以包含子域或设备，但不能同时包含两者。不能保存由非枝叶域直接控制设备的部署。

在域编辑器中，Web 界面根据可用和所选设备在域层次结构中的当前位置来显示它们。

主机限制

Firepower 管理中心可以监控并因而存储在网络映射中的主机数，具体取决于其型号。在多域部署中，枝叶域共享受监控主机的可用池，但拥有单独的网络映射。

要确保每个枝叶域都可以填充其网络映射，可以在每个子域级别设置主机限制。如果将域的主机限制设置为 0，则域在通用池中共享。

设置主机限制对每个域级别有着不同的影响：

- 枝叶 - 对于枝叶域，主机限制仅是对枝叶域可以监控的主机数量进行简单限制。
- 第二级 - 对于用于管理第三级枝叶域的第二级域，主机限制表示枝叶域可以监控的主机总数。枝叶域共享可用主机池。
- 全局 - 对于全局域，主机限制与 Firepower 管理中心可以监控的主机总数相等。您无法进行更改

子域的主机限制总和加起来可超过其父域的主机限制。例如，如果全局域主机限制为 150,000，则可以配置多个子域，每个子域的主机限制为 100,000。这些域中的任一个（但并非总共）可监控 100,000 台主机。

网络发现策略控制在您达到主机限制后检测到新主机时发生的情况；您可以丢弃新主机或替代非活动时间最长的主机。由于每个枝叶域具有各自的网络发现策略，因此在系统发现新主机时，每个枝叶域会监管各自的行为。

如果您降低某个域的主机限制，且其网络映射包含比新限制更多的主机，则系统会删除处于非活动状态时间最长的主机。

管理域

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

要修改域的属性，您必须在该域的父域中具有管理员访问权限。

过程

步骤 1 选择**系统 (System)** > **域 (Domains)**。

步骤 2 管理域：

- 添加 - 点击**添加域 (Add Domain)**，或者点击父域旁边的**添加子域 (Add Subdomain)** 图标；请参阅创建新域，第 249 页。
- 编辑 - 点击要修改的域旁边的编辑图标 ( )；请参阅域属性，第 247 页。

- 删除 - 点击要删除的空域旁边的删除图标 ( )，然后确认选择。通过编辑设备的目标域移动要删除的域中的设备。

步骤 3 当您完成对域结构以及与枝叶域相关的所有设备的更改时，请点击**保存 (Save)** 以实施更改。

步骤 4 如有提示，请进行其他更改：

- 如果将枝叶域更改为父域，请移动或删除旧网络映射；请参阅在域之间移动数据，第 250 页。
- 如果在域之间移动设备，并且必须分配新的策略和安全区域，请参阅在域之间移动设备，第 251 页。

接下来的操作

- 为任何新域配置用户角色和策略（访问控制、网络发现等等）。根据需要更新设备属性。
- 部署配置更改；请参阅部署配置更改，第 254 页。

创建新域

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	全局与第二级	管理

您在一个顶级全球域下最多可以创建 50 个子域，分为两个或三个级别。

实施域配置之前，必须将所有设备分配到枝叶域。将某个子域到枝叶域时，该域不再是枝叶域，您必须重新分配其设备。

过程

步骤 1 在全局或第二级域中，选择**系统 (System)** > **域 (Domains)**。

步骤 2 点击**添加域 (Add Domain)** 或点击父域旁边的**添加子域 (Add Subdomain)** 图标。

步骤 3 输入 **Name** 和 **Description**。

步骤 4 在**父域 (Parent Domain)** 中选择父域。

步骤 5 在**设备 (Devices)** 选项卡上，选择**可用设备 (Available Devices)** 以添加域，然后点击**添加到域 (Add to Domain)** 或拖放到**所选设备 (Selected Devices)** 列表中。

步骤 6 或者，点击**高级 (Advanced)** 选项卡以限制新域可以监控的主机数；请参阅域属性，第 247 页。

步骤 7 点击**保存 (Save)** 返回域管理页面。

如果任何设备被分配到非枝叶域，则系统会向您发出警告。点击**创建新域 (Create New Domain)**，为这些设备创建新域。如果计划将设备移至现有域，请点击**保持未分配 (Keep Unassigned)**。

步骤 8 当您完成对域结构以及与枝叶域相关的所有设备的更改时，请点击**保存 (Save)** 以实施更改。

步骤 9 如有提示，请进行其他更改：

- 如果将枝叶域更改为父域，请移动或删除旧网络映射；请参阅在域之间移动数据，第 250 页。
- 如果在域之间移动设备，并且必须分配新的策略和安全区域，请参阅在域之间移动设备，第 251 页。

接下来的操作

- 为任何新域配置用户角色和策略（访问控制、网络发现等等）。根据需要更新设备属性。
- 部署配置更改；请参阅部署配置更改，第 254 页。

在域之间移动数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

由于事件和网络映射与枝叶域关联，因此当您将枝叶域更改为父域时，您有两种选择：

- 将网络映射和关联事件移动到新枝叶域。
- 删除网络映射但保留事件。在这种情况下，事件仍与父域关联，直到系统根据需要或根据配置删除事件。或者，您可以手动删除旧事件。

开始之前

- 实施一种域配置（其中之前的枝叶域现在是父域）；请参阅管理域，第 248 页。

过程

步骤 1 对于现在是父域的每个前枝叶域，您有两种选择：

- 选择新的**枝叶域 (Leaf Domain)** 以继承**父域 (Parent Domain)** 的事件和网络映射。
- 选择**无 (None)** 以删除父域的网络映射，但保留旧事件。

步骤 2 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

在域之间移动设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	全局与第二级	管理

在域之间移动设备可能会影响应用于该设备的配置和策略。系统自动保存和更新其可以保存和更新的配置和策略，并删除不能保存和更新的配置和策略。

当移动设备时，系统可能会提示您选择以下新的必要配置：

- 访问控制策略 - 如果分配给移动设备的访问控制策略在新域中无效或不可访问，请选择新策略。每个设备都必须有一个分配的访问控制策略。
- 运行状况策略 - 如果应用于移动设备的运行状况策略在新域中不可访问，您可以选择新的运行状况策略。
- 安全区域 - 如果移动设备上的接口属于在新域中不可访问的安全区域，您可以选择新区域。

如果设备需要策略更新，但您不需要在区域间移动设备，则系统会显示一条消息，表明区域配置为最新配置。例如，如果设备的接口属于在公共祖先域中配置的安全区域，则您无需在将设备从一个子域移动到另一个子域时更新区域配置。

开始之前

- 实施您将设备从一个域移动到另一个域的域配置，且现在必须分配新策略和安全区域；请参阅管理域，第 248 页。

过程

步骤 1 在**移动设备 (Move Devices)** 对话框中，在**选择要配置的设备 (Select Device(s) to Configure)** 下，选中要配置的设备。
选中多个设备，以分配相同的运行状况和访问控制策略。

步骤 2 在**访问控制策略 (Access Control Policy)** 中选择访问控制策略以应用于设备，或选择**新建策略 (New Policy)** 来创建新策略。

步骤 3 在**运行状况策略 (Health Policy)** 中选择运行状况策略以应用于设备，或选择**无 (None)** 使该设备没有运行状况策略。

步骤 4 如果系统提示将接口分配到新区域，请为列出的每个接口选择**新建安全区域 (New Security Zone)**，或选择**无 (None)** 以在稍后对其进行分配。

步骤 5 配置完所有受影响设备后，点击**保存 (Save)** 以保存策略和区域分配。

步骤 6 点击**保存 (Save)** 以实施域配置。

接下来的操作

- 在受移动影响的移动设备上更新其他配置。
- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

第 15 章

策略管理

以下主题介绍如何在 Firepower 管理中心上管理各种策略：

策略部署

在配置部署后，无论何时对该配置进行更改，您都必须向受影响设备部署更改。您可以在消息中心查看部署状态。

部署会更新以下组件：

- 设备和接口配置
- 设备相关的策略：NAT。VPN 平台设置
- 访问控制策略以及相关策略：DNS、文件、身份、入侵、网络分析、SSL
- 网络发现策略
- 入侵规则更新
- 与其中任一元素相关联的配置和对象

您可以将系统配置为自动部署，方法如下：安排一个部署任务，或者将系统设置为在导入入侵规则更新时进行部署。如果允许入侵规则更新修改系统提供的基本策略以进行入侵和网络分析，则自动部署策略的方法尤其有用。入侵规则更新还可修改访问控制策略中高级预处理和性能选项的默认值。

在多域部署中，可以为您的用户帐户所属的任何域部署更改。

- 切换到祖先域，以便将更改同时部署到所有子域。

- 切换到枝叶域，以便仅将更改部署到该域。

部署配置更改

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/网络管理员/安全审批人

在配置部署后，并且只要更改该配置，就将更改部署到受影响设备。

注意 当部署时，资源需求可能会导致丢弃少量数据包而不进行检测。此外，部署某些配置要求 Snort 进程重新启动，这会中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。在 Firepower 7010、7020 和 7030 受管设备上，部署配置更改可能最多需要五分钟。为最大限度地减少不便之处，请在更改窗口内进行部署。

开始之前

- 复查部署配置更改的准则；请参阅部署配置更改准则，第 256 页。
- 确保所有受管设备都使用安全区域对象的相同修订版。如果已编辑安全区域对象：在已编辑要同步的全部设备上接口的区域设置前，不得将受管设备部署到任何设备。必须一次性将设备更改部署到所有受管设备。请参阅同步安全区域对象修订版本，第 389 页。

过程

步骤 1 在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。
“部署策略”(Deploy Policies) 对话框列出具有过期配置的设备。对话框顶部的**版本 (Version)** 指定上次进行配置更改的时间。设备表中的**当前版本 (Current Version)** 列指定上次将更改部署到每个设备的时间。

步骤 2 识别并选择要部署配置更改的设备。

- 排序 - 通过点击列标题对设备列表进行排序。
- 展开 - 点击加号图标 ( )，展开设备列表以查看要部署的配置更改。系统使用索引 ( ) 图标标记过期策略。
- 过滤 - 过滤设备列表。点击显示的任何列标题右上角的箭头，在**过滤器 (Filter)** 文本框中输入文本，然后按 Enter 键。

步骤 3 点击 **Deploy**（部署）。

步骤 4 如果系统识别出要部署的更改中的错误或警告，有以下选项可供选择：

- 继续 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 取消 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

接下来的操作

- 或者，监控部署状态；请参阅查看部署消息，第 238 页。
- 如果配置无法部署，请参阅部署配置更改准则，第 256 页以获取可能的解决方案。

强制部署设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员/安全审批人

可以将配置设置部署到设备，即使不进行通常会将该配置标记为过期的更改也如此。

注意 当部署时，资源需求可能会导致丢弃少量数据包而不进行检测。此外，部署某些配置要求 Snort 进程重新启动，这会中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。在 Firepower 7010、7020 和 7030 受管设备上，部署配置更改可能最多需要五分钟。为最大限度地减少不便之处，请在更改窗口内进行部署。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**

步骤 2 点击要强制部署的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 点击**常规 (General)** 部分标题旁边的编辑图标 ( )。

步骤 5 点击**强制部署 (Force Deploy)** 箭头 ( )。

步骤 6 或者，展开设备列表以查看要部署的配置设置。
系统使用索引 ( ) 图标标记过期策略。

步骤 7 点击 **Deploy**（部署）。

步骤 8 如果系统识别出要部署的配置设置中的错误或警告，您有以下选项：

- 点击**继续 (Proceed)** 以在不解决错误或警告状况的情况下继续部署。如果系统仅识别出面向部署的警告，则会启用此按钮；如果系统识别出部署中的错误，则会禁用此按钮。
- 点击**取消 (Cancel)** 以退出而不进行部署。解决错误和警告情况，并尝试重新部署该配置。

接下来的操作

- 或者，监控部署状态；请参阅查看部署消息，第 238 页。
- 如果配置无法部署，请参阅部署配置更改准则，第 256 页以获取可能的解决方案。

部署配置更改准则

部署对受管设备的配置更改时，请记住以下要点。

重要事项 为最大限度地减少不便之处，请在更改窗口内进行部署

部署结果

注意 当部署时，资源需求可能会导致丢弃少量数据包而不进行检测。此外，部署某些配置要求 Snort 进程重新启动，这会中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。在 Firepower 7010、7020 和 7030 受管设备上，部署配置更改可能最多需要五分钟。

- 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。
- 如果执行的是应用控制，但是禁用所需的检测器，则系统会在策略部署时自动启用系统提供的适当检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。
- 将更改部署到网络发现策略时，系统会删除并重新发现受监控网络中主机的网络映射中的 MAC 地址、TTL 和跳数信息。此外，受影响的受管设备还会放弃任何尚未发送到 Firepower 管理中心的发现数据。

故障排除

- 请勿将内联配置应用于被动部署的设备，反之亦然。
- 请勿超过设备的能力。

  复杂的访问控制策略和规则可控制重要资源并对性能产生不利影响。当部署访问控制策略时，系统会一起评估所有规则并创建供目标设备用于评估网络流量的扩展条件集。

如果超过目标设备所支持的访问控制规则或调用的入侵策略的最大数量，系统会显示警告。该最大数量取决于很多因素，包括设备上的策略复杂度、物理内存以及处理器数量。

- 验证设备是否是所配置的功能的正确型号，并在使用Firepower系统的正确许可证和最低版本。例如，不能以运行 Firepower 系统的不同版本的堆叠式 7000 或 8000 系列设备为目标。

自动部署

可以将系统配置为自动部署，如下所示：

- 在完成入侵规则更新后
- 使用预定任务

Snort® 在配置部署期间重新启动

利用**在策略应用期间检查流量 (Inspect traffic during policy apply)** 高级访问控制策略常规设置，您可以在部署配置更改时检查流量，除非部署的配置需要重启 Snort 进程，如下所示：

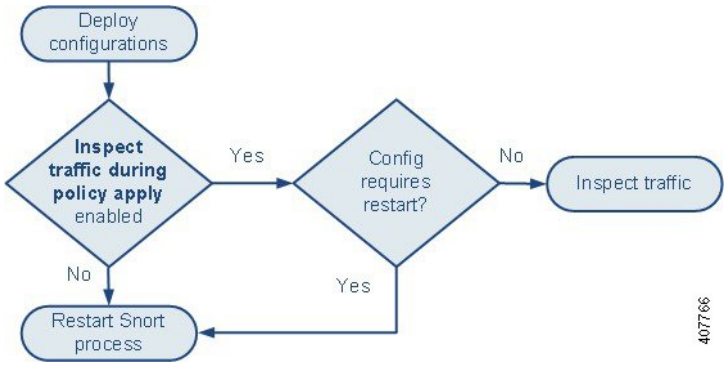
- 启用 - 某些配置可能需要重启 Snort 进程。

  当部署的配置不需要 Snort 重启时，系统最初使用当前部署的访问控制策略检查流量，并在部署期间切换到您正在部署的访问控制策略。

- 禁用 - Snort 进程在您部署时总是会重启。部署期间不会检查流量。

下图展示了当启用或禁用**在策略应用期间检查流量 (Inspect traffic during policy apply)** 时，Snort 如何重启。

注意 当部署时，资源需求可能会导致丢弃少量数据包而不进行检测。此外，部署某些配置要求 Snort 进程重新启动，这会中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。



Snort 重新启动影响流量的方式取决于受管设备的型号以及其如何处理流量。

表 *43*: 按照受管设备型号划分的重新启动流量影响

在此受管设备模型上…	配置为…	在重启过程中，流量会…
7000 和 8000 系列、NGIPSv、Firepower 威胁防御、Firepower 威胁防御虚拟	内联，**故障保护 (Failsafe)** 已启用或已禁用	不检查就通过（如果已禁用**故障保护 (Failsafe)**，并且 Snort 处于繁忙而非关闭状态，则一些数据包可能会丢弃）
	passive	不中断、不检查
	内联、分流模式	立即传出数据包，副本绕过 Snort
7000 和 8000 系列	路由式、交换式、透明	dropped
ASA FirePOWER	路由式或透明，且出故障时自动打开（**允许流量 [Permit Traffic]**）	不检查就通过
	路由式或透明，且出故障时自动关闭（**关闭流量 [Close Traffic]**）	dropped

注释 除了当 Snort 进程在重启时关闭这一情况下的流量处理外，在 Snort 进程繁忙时，流量也可不检查就通过或丢弃，具体取决于“故障保护”(Failsafe) 选项的配置。请参阅Firepower 系统上的内联集，第 396 页。

重新启动 Snort 进程的配置

当您部署配置更改时，以下任何配置或操作都会重新启动 Snort® 进程。

注意 当部署时，资源需求可能会导致丢弃少量数据包而不进行检测。此外，部署某些配置要求 Snort 进程重新启动，这会中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

访问控制策略

- 首次部署策略
- 在访问控制规则中的 URL 选项卡上添加或删除 URL 类别和信誉条件

- 通过以下方式可更改活动入侵策略的总数：将策略当前未使用的入侵策略与访问控制规则、默认操作或默认入侵策略关联；或者从其中任意一个中删除访问控制策略使用的最后一个入侵策略实例。
- 将第一个文件策略与访问控制规则关联，或从访问控制策略中删除所有文件策略。

访问控制策略高级设置

- 禁用“常规设置”(General Settings) 下的**在策略应用期间检查流量 (Inspect Traffic During Policy Apply)**
- 在“文件和恶意软件设置”(Files and Malware Settings) 下更改值
- 在“SSL 策略设置”(SSL Policy Settings) 下关联 SSL 策略，或者随后通过选择**无 (None)** 删除该策略
- 在“身份策略设置”(Identity Policy Settings) 下关联身份策略，或者随后通过选择**无 (None)** 删除该策略
- 在“检测增强功能设置”(Detection Enhancement Settings) 下启用或禁用自适应配置文件

安全情报

- 更改“安全情报”(Security Intelligence) 列表，但通过右键点击情景菜单上的**立即将 IP 列入白名单 (Whitelist IP Now)** 或**立即将 IP 列入黑名单 (Blacklist IP Now)** 进行更改除外
- 在访问控制策略中的“安全情报”(Security Intelligence) 选项卡上指定自定义 DNS 策略

SSL 策略

- 在 SSL 规则中的“类别”(Category) 选项卡上添加或删除 URL 类别和信誉条件

File Policy

- 启用或禁用存档文件检测
- 在文件规则中添加或删除文件类型或文件类别
- 将文件规则操作更改为**检测文件 (Detect Files)** 或**阻止恶意软件 (Block Malware)** 或从其进行更改
- 在文件规则中启用或禁用**存储文件 (Store files)**

身份策略 (Identity Policy)

- 添加或删除**主动身份验证 (Active Authentication)** 身份规则操作
- 当身份规则操作为**被动身份验证 (Passive Authentication)** 时，选择**领域和设置 (Realms & Settings)** 选项卡上的**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**

Network Analysis Policy

- 更改 IMAP、POP 或 SMTP 预处理器 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)** 的值

设备管理

- 路由 - 向 7000 或 8000 系列设备添加路由接口对或虚拟路由器
- VPN - 添加或删除 VPN（7000 或 8000 系列）
- MTU - 更改 7000 或 8000 系列或 NGIPSv 设备上非管理接口的最高 MTU 值
- 设备高可用性 - 更改 7000 或 8000 系列设备上的高可用性状态共享选项
- AAB - 激活 AAB

注释 仅当单个数据包使用过量的处理时间时，自动应用绕行 (AAB) 才会激活。

部署前更新 (Pre-Deployment Updates)

- 在导入包含新的或已更新的共享对象规则的入侵规则更新后部署
- 在安装漏洞数据库 (VDB) 更新后部署

系统更新 (System Updates)

安装不会重启系统并会包含二进制更改的系统更新或补丁需要重新启动 Snort。二进制更改可能包含对 Snort、预处理器、漏洞数据库 (VDB) 或共享对象规则的更改。请注意，在使用受管设备的情况下，不包括二进制更改的补丁有时可能需要重新启动 Snort。

策略比较

要查看策略更改是否符合您的组织的标准或优化系统性能，您可以检查两个策略之间的区别，或者已保存策略和正在运行策略之间的区别。

您可以比较以下策略类型：

- DNS
- 文件
- 健康状况
- Identity
- 入侵
- 网络分析

- SSL

比较视图以并排形式显示两个策略。会突出显示两个策略之间的差异：

- 蓝色表示突出显示的设置在两个策略中不同，并且差异以红色文本标注。
- 绿色表示突出显示的设置出现在一个策略中但未出现在另一个策略中。

比较策略

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任意	因功能而异	因功能而异

过程

步骤 1 访问要比较的策略的管理页面：

- DNS - **策略 (Policies)** > **访问控制 (Access Control)** > **DNS**
- 文件 - **策略 (Policies)** > **访问控制 (Access Control)** > **恶意软件和文件 (Malware & File)**
- 运行状况 - **系统 (System)** > **运行状况 (Health)** > **策略 (Policy)**
- 身份 - **策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**
- 入侵 - **策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**
- 网络分析 - **策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**

  注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**

步骤 2 点击 **Compare Policies**。

步骤 3 从 **Compare Against** 下拉列表中，选择要进行比较的类型：

- 要比较两个不同的策略，请选择 **Other Policy**。
- 要比较同一策略的两个版本，请选择 **Other Revision**。
- 要将其他策略与当前的有效策略进行比较，请选择**运行配置 (Running Configuration)**。

步骤 4 根据选择的比较类型，有以下选项可供选择：

- 如果要比较两个不同的策略，请从 **Policy A** 和 **Policy B** 下拉列表中选择要比较的策略。

- 如果与另一策略比较运行配置，请从 **Policy B** 下拉列表中选择另一个策略。

步骤 5 点击 **OK**。

步骤 6 查看比较结果：

- 比较查看器 - 要使用比较查看器逐一浏览策略差异，请点击标题栏上方的**上一个 (Previous)**或**下一个 (Next)**。
- 比较报告 - 要生成列出两个策略之间差异的 PDF 报告，请点击**比较报告 (Comparison Report)**。

策略报告

对于大多数策略，可以生成两种报告。有关单个策略的报告提供该策略的当前已保存配置的详细信息，而比较报告仅列出两个策略之间的区别。您可以为运行状况策略之外的所有策略类型生成单策略报告。

注释 入侵策略报告将基本策略中的设置与策略层的设置组合在一起，不区分源自基本策略或策略层的设置。

生成当前策略报告

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任意	因功能而异	因功能而异

过程

步骤 1 访问要为其生成报告的策略的管理页面：

- 访问控制 - **策略 (Policies)** > **访问控制 (Access Control)**
- DNS - **策略 (Policies)** > **访问控制 (Access Control)** > **DNS**
- 文件 - **策略 (Policies)** > **访问控制 (Access Control)** > **恶意软件和文件 (Malware & File)**
- 运行状况 - **系统 (System)** > **运行状况 (Health)** > **策略 (Policy)**
- 身份 - **策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**
- 入侵 - **策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**
- 7000 和 8000 系列设备的 NAT - **设备 (Devices)** > **NAT**

- 网络分析 - **策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**

  注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**

步骤 2　点击要生成报告的策略旁边的报告图标 ()。

过时策略

Firepower 系统使用红色状态文本标记过期策略，表明其需要策略更新的目标设备的数量。要清除此状态，必须将策略重新部署到设备。

要求策略重新部署的配置更改包括：

- 修改访问控制策略：对访问控制规则、默认操作、策略目标、安全情报过滤、高级选项（包括预处理）等等的任何更改。
- 修改访问控制策略调用的任何策略：SSL 策略、网络分析策略、入侵策略、文件策略、身份策略或 DNS 策略。
- 更改访问控制策略或其调用的策略中所使用的任何可重用对象或配置：

  网络、端口、VLAN 标记、URL 和地理位置对象。

  安全情报列表和源

  应用过滤器或检测器

  入侵策略变量集

  文件列表

  与解密相关的对象和安全区域

- 更新系统软件、入侵规则或漏洞数据库 (VDB)。

请记住，可以从 Web 界面中的多个位置更改其中某些配置。例如，可以使用对象管理器（**对象 (Objects)** > **对象管理 (Object Management)**）修改安全区域，但是修改设备配置（**设备 (Devices)** > **设备管理 (Device Management)**）中的接口类型还可更改区域并要求策略重新部署。

请注意，以下更新**不**要求策略重新部署：

- 使用上下文菜单自动对安全情报源进行更新和对安全情报全局黑名单或白名单进行添加
- 对 URL 过滤数据的自动更新
- 计划的地理位置数据库 (GeoDB) 更新

有限部署的性能注意事项

通过主机、应用和用户发现数据，系统可以创建完整、最新的网路配置文件。系统还可用作入侵检测和防御系统 (IPS)，分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。

将发现和 IPS 组合可提供网络活动情景并允许您利用许多功能，包括：

- 影响标志和危害指示，可以告诉您哪些主机易受特定漏洞、攻击或某种恶意软件的攻击
- 自适应配置文件和 Firepower 建议，允许您根据目标主机以不同方式检查流量
- 关联，允许您根据受影响主机以不同方式响应入侵（和其他事件）

但是，如果您的组织对仅执行 IPS 或仅执行发现感兴趣，则有一些配置可以优化系统的性能：

不带入侵防御的发现

通过发现功能，可以监控网络流量并确定网络上主机（包括网络设备）的数量和类型，以及这些主机上的操作系统、活动应用和开放式端口。您还可以配置受管设备以监控网络上的用户活动。可以使用发现数据执行流量量变分析，评估网络合规性和对策略违规作出响应。

在基本部署中（仅包含发现和简单、基于网络的访问控制），可以通过在配置设备的访问控制策略时遵循一些重要准则来提高该设备的性能。

注释 必须使用访问控制策略，即使其只是允许所有流量也如此。网络发现策略**只**能检查访问控制策略允许通过的流量。

首先，确保访问控制策略不要求复杂的处理并仅使用简单、基于网络的条件处理网络流量。必须实施以下**所有**准则；错误配置其中任何一个选项都会消除性能优势：

- 请**勿**使用安全情报功能。从策略的安全情报配置中移除任何已填充的全局白名单或黑名单。
- 请**勿**包含具有 Monitor 或 Interactive Block 操作的访问控制规则。仅使用 Allow、Trust 和 Block 规则。请记住，可以通过发现检查允许的流量，但无法检查受信任和受阻止的流量。
- 请**勿**包含具有应用、用户、URL，ISE 属性或基于地理位置的网络条件的访问控制规则。仅使用简单的基于网络的条件：区域、IP 地址、VLAN 标记和端口。
- 请**勿**包含执行文件、恶意软件或入侵检查的访问控制规则。换句话说，请勿将文件策略或入侵策略与任何访问控制规则相关联。
- 确保访问控制策略的默认入侵策略设置为**无活动规则 (No Rules Active)**。
- 选择 **Network Discovery Only** 作为策略的默认操作。请**勿**为执行入侵检查的策略选择默认操作。

与访问控制策略相结合，可以配置并部署网络发现策略，它指定系统为发现数据检查的网段、端口和区域，以及是否在网段、端口和区域上发现了主机、应用和用户。

不带发现的入侵防御

通过入侵检测和防御功能，可以分析入侵和漏洞的网络流量，或者丢弃有问题的数据包。如果要执行入侵检查，但不需要利用发现数据，可以通过禁用发现来提高设备的性能。

注释 如果执行的是应用、用户或 URL 控制，则**无法**禁用发现以获取性能优势。虽然可以防止系统存储发现数据，但是系统**必须**收集并检查该数据才能实施这些功能。

要禁用发现，请实施以下**所有**准则；错误配置任何准则都会消除性能优势：

- 在访问控制策略中，请**勿**包含具有基于应用、用户、URL、ISE 属性或地理位置的网络条件的规则，即使设备相应地获得许可也如此。仅使用简单的基于网络的条件：区域、IP 地址、VLAN 标记和端口。
- 从网络发现策略中删除所有规则。

部署访问控制策略和网络发现策略后，会在目标设备上停止新的发现。系统根据您在网络发现策略中指定的超时期逐渐删除网络映射中的信息。或者，可以立即清除所有发现数据。

第 16 章

规则管理：共同特征

以下主题介绍如何在 Firepower 管理中心上管理各种策略中的规则的共同特征：

规则简介

各种策略中的规则对网络流量实行精细控制。系统使用第一个匹配算法按您指定的顺序根据规则评估流量。

虽然这些规则可能包含在策略之间不一致的其他配置，但它们共享许多基本特征和配置机制，包括：

- 条件 - 规则条件指定每个规则处理的流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。
- 操作 - 规则的操作确定系统如何处理匹配流量。请注意，即使规则没有可供选择的**操作 (Action)** 列表，该规则仍然具有关联操作。例如，自定义网络分析规则使用网络分析策略作为其“操作”。
- 位置 - 规则的位置确定其评估顺序。当使用策略评估流量时，系统按您指定的顺序将流量与规则匹配。通常，系统根据第一个规则（其中所有规则的条件都与流量匹配）处理流量。（监控规则是例外，这些规则跟踪和记录流量，但不影响流量。）适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。
- 类别 - 要组织某些规则类型，您可以在每个父策略中创建自定义规则类别。

- 日志记录 - 对于许多规则，日志记录设置会监管系统是否以及如何记录规则处理的连接。某些规则（例如身份和网络分析规则）不包括日志记录设置，因为规则既不确定连接的最终处置情况，也不是专门设计为记录连接。
- 注释 - 对于某些规则类型，每次保存更改时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。

提示 许多策略编辑器中的右键点击菜单提供很多规则管理选项的快捷方式，包括编辑、删除、移动、启用和禁用。

具有共享特征的规则

本章记录以下规则和配置的许多常见方面。有关非共享配置的信息，请参阅：

- 访问控制规则 -访问控制规则， 第 625 页
- SSL 规则 -创建和修改 SSL 规则， 第 706 页
- DNS 规则 -创建和编辑 DNS 规则， 第 662 页
- 身份规则 -创建身份规则， 第 1244 页
- 网络分析规则 -配置网络分析规则， 第 995 页
- 智能应用绕行 (IAB) -智能应用绕行 (IAB)， 第 671 页
- 应用过滤器 -应用过滤器， 第 310 页

不具有共享特征的规则

未在本章中记录其配置的规则包括：

- 入侵规则 -使用规则调整入侵策略， 第 817 页
- 文件规则 -文件规则， 第 760 页
- 关联规则 -配置关联规则， 第 1281 页
- NAT 规则（典型）-7000 和 8000 系列设备的 NAT， 第 507 页
- 8000 系列快速路径规则 -配置 8000 系列快速路径规则， 第 381 页

规则条件类型

下表介绍本章中记录的通用规则条件，并列出使用这些规则条件的配置。

情况	流量控制方式	支持的规则/配置
安全区域条件，第 271 页	源和目标安全区域	访问控制规则 SSL 规则 DNS 规则 身份规则 网络分析规则
网络条件，第 272 页	源和目标 IP 地址，以及受支持情况下的地理位置	访问控制规则 SSL 规则 DNS 规则 身份规则 网络分析规则
VLAN 条件，第 273 页	VLAN 标记	访问控制规则 SSL 规则 DNS 规则 身份规则 网络分析规则
端口和 ICMP 代码条件，第 274 页	源和目标端口、协议及 ICMP 代码	访问控制规则 SSL 规则 身份规则
应用条件（应用控制），第 276 页	应用或应用特性（类型、风险、业务关联性、类别和标记）	访问控制规则 SSL 规则 身份规则 应用过滤器 智能应用绕行 (IAB)
URL 条件（URL 过滤），第 280 页	URL 以及受支持情况下的 URL 特征（类别和信誉）	访问控制规则 SSL 规则
用户、领域和 ISE 属性条件（用户控制），第 286 页	主机的已登录授权用户，或者该用户的领域、组或 ISE 属性	访问控制规则 SSL 规则（无 ISE 支持）

规则条件机制

规则条件指定每条规则处理的流量。可以为每条规则配置多个条件，流量必须匹配所有条件才能匹配规则。可用条件类型取决于规则类型。

在规则编辑器中，每个条件类型都有自己的选项卡。通过选择要匹配的流量特征来构建条件。一般来说，从左侧的一个或两个可用项目列表中选择条件，然后添加或将那些条件合并为右侧的一个或两个所选项目列表。例如，在访问控制规则的 URL 条件中，可以将 URL 类别和信誉条件组合在一起，以创建单个要阻止的网站组。

为了帮助您构建条件，您可以使用各种系统提供的配置和自定义配置（包括领域、ISE 属性以及各种类型的对象和对象组）来匹配流量。通常，可以手动指定规则条件。

源和目标条件

如果规则包含源和目标条件（区域、网络，端口），通常可以使用其中一个或两个条件作为限制。如果使用两个条件，匹配的流量必须源自其中一个指定源区域、网络或端口并从其中一个目标区域、网络或端口流出。

每个条件包含的项目

每个条件最多可以添加 50 个项目。对于带有源和目标条件的规则，每个规则可以使用最多 50 个条件。匹配任何所选项目的流量与条件匹配。

简单规则机制

在规则编辑器中，您一般有以下选择。有关构建条件的详细说明，请参阅每个条件类型的主题。

- 选择项目 - 点击项目或选中其复选框。通常您可以使用 Ctrl 或 Shift 键选择多个项目，或者右键点击以选择**全选 (Select All)**。
- 搜索 - 在搜索字段中输入条件。列表会随着键入的内容进行更新。系统会搜索项目名称，而对于对象和对象组，会搜索其值。点击重新加载 () 或清除 () 以清除搜索。
- 添加预定义项目 - 在选择一个或多个可用项目后，点击**添加 (Add)** 按钮或进行拖放。系统会阻止您添加无效项目：重复、无效组合等等。
- 添加手动项目 - 点击**已选定 (Selected)** 项目列表下的字段，输入有效值，然后点击**添加 (Add)**。添加端口时，也可以从下拉列表中选择协议。
- 创建对象 - 点击添加图标 () 以创建可在您正在构建的条件中立即使用的新的、可重复使用的对象，然后在对象管理器中进行管理。使用此方法即时添加应用过滤器时，无法保存包含另一个用户创建过滤器的过滤器。
- 删除 - 点击项目的删除图标 ()，或选择一个或多个项目并右键点击以选择**删除所选项 (Delete Selected)**。

安全区域条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（全都为内联、被动、交换、路由或ASA FirePOWER），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

具有安全区域条件的规则

以下规则支持安全区域条件：

- 访问控制
- SSL
- DNS（仅限源区域限制）
- Identity
- 网络分析

示例：使用安全区域的访问控制

假设在某个部署中，您希望主机对互联网具有不受限制的访问权限，但是仍然通过检测传入流量是否存在入侵和恶意软件来保护这些主机。

首先，创建两个安全区域：内部和外部。然后，将一个或多个设备上的接口对分配到这些区域，每个对中的一个接口位于内部区域，另一个接口位于外部区域。在内侧连接至网络的主机代表您的受保护资产。

注释 您不需要将所有内部（或外部）接口分组至单个区域。选择对您的部署和安全策略有意义的分组。

然后，配置访问控制规则，其中目标区域条件设置为“内部”(Internal)。此简单规则与从内部区域中的任何接口传出设备的流量相匹配。要检查匹配流量中是否存在入侵和恶意软件，请选择规则操作**允许 (Allow)**，然后将该规则与入侵和文件策略相关联。

网络条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

网络条件中的地理位置

某些规则可以使用源或目标的地理位置来匹配流量。如果规则类型支持地理位置，则可以混用网络条件和地理位置条件。要确保使用最新地理位置数据过滤流量，思科强烈建议定期更新地理位置数据库 (GeoDB)。

具有网络条件的规则

规则类型	支持地理位置限制？
访问控制	yes
SSL	yes
DNS（仅限源网络）	否
Identity	yes
网络分析	否

配置网络条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在规则编辑器中，点击**网络 (Networks)** 选项卡。

步骤 2 从**可用网络 (Available Networks)** 列表中查找并选择要添加的预定义网络。

如果规则支持地理位置，则可以在同一规则中混用网络和地理位置条件：

- 网络 - 点击**网络 (Networks)** 子选项卡以选择网络。
- 地理位置 - 点击**地理位置 (Geolocation)** 子选项卡以选择地理位置对象。

步骤 3 点击**添加到源 (Add to Source)**或**添加到目标 (Add to Destination)**，或者进行拖放。
DNS 规则仅支持源网络。

步骤 4 添加要手动指定的网络。输入源或目标 IP 地址或地址块，然后点击**添加 (Add)**。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

示例：访问控制规则中的网络条件

下图显示的网络条件与阻止源自您的内部网络并尝试访问位于朝鲜或 93.184.216.119 (example.com) 的连接的访问控制规则相对应。

在此示例中，称为专用网络的网络对象组（包括 IPv4 和 IPv6 专用网络网络对象，未显示）表示您的内部网络。此示例还手动指定了 example.com IP 地址，并使用系统提供的朝鲜地理定位对象代表朝鲜 IP 地址。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

VLAN 条件

VLAN 规则条件可控制 VLAN 标记的流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

具有 VLAN 条件的规则

以下规则类型支持 VLAN 条件：

- 访问控制
- SSL
- DNS
- Identity
- 网络分析

端口和 ICMP 代码条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据传输层协议控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 无端口 - 可以使用其他未使用端口的协议来控制流量。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

将非 TCP 流量与端口条件相匹配

虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。
- SSL 规则 - SSL 规则仅支持 TCP 端口条件。
- 身份规则 - 系统无法对非 TCP 流量执行主动身份验证。如果身份规则操作为“主动身份验证”(Active Authentication)，或者如果您选中**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)** 选项，请仅使用 TCP 端口限制。如果身份规则操作为“被动身份验证”(Passive Authentication) 或“无身份验证”(No Authentication)，则可以根据非 TCP 流量创建端口条件。

注意 添加或删除**主动身份验证 (Active Authentication)** 规则操作，或者在规则操作为**被动身份验证 (Passive Authentication)** 时选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

具有端口条件的规则

以下规则支持端口条件：

- 访问控制
- SSL（仅支持 TCP 流量）
- 身份（主动身份验证仅支持 TCP 流量）

配置端口条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在规则编辑器中，点击**端口 (Ports)** 选项卡。

步骤 2 从**可用端口 (Available Ports)** 列表中查找并选择要添加的预定义端口。

步骤 3 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**，或进行拖放操作。

步骤 4 添加要手动指定的任何源或目标端口：

- 源 - 选择**协议 (Protocol)**，输入**端口 (Port)**（0 到 65535），然后点击**添加 (Add)**。
- 目标（非 ICMP） - 选择或输入**协议 (Protocol)**。如果不想指定协议，或者如果选择 **TCP** 或 **UDP**，请输入单个**端口 (Port)**（0 到 65535）。点击 **Add**。

- 目标 (ICMP) - 从**协议 (Protocol)** 下拉列表中选择 **ICMP** 或 **IPv6-ICMP**，然后在显示的弹出窗口中选择**类型 (Type)** 和相关**代码 (Code)**。有关 ICMP 类型和代码的详细信息，请参阅互联网编号分配机构 (IANA) 网站。

步骤 5 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

应用条件（应用控制）

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

具有应用条件的配置

下表中的配置可帮助您执行应用控制。该表还显示如何根据配置限制应用控制。

配置	类型、风险、关联性、类别	标签	用户定义的过滤器
访问控制规则	是	是	是
SSL 规则	yes	否；通过 SSL 协议标记自动限制为已加密应用流量	否
身份规则（让应用免于进行主动身份验证）	yes	否；通过用户代理排除标记进行自动限制	否

配置	类型、风险、关联性、类别	标签	用户定义的过滤器
对象管理器中的用户定义应用过滤器	是	是	否；您无法嵌套用户定义的过滤器
智能应用绕行 (IAB)	是	是	是

配置应用条件和过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员/访问管理员/网络管理员

要构建应用条件或过滤器，请从可用应用列表中选择要控制其流量的应用。或者，可以按照建议使用过滤器限制可用应用。在相同条件下可以使用过滤器和单独指定的应用。

过程

步骤 1 调用规则或配置编辑器：

- 访问控制、SSL 规则条件 - 在规则编辑器中，点击**应用 (Applications)** 选项卡。
- 身份规则条件 - 在规则编辑器中，点击**领域和设置 (Realm & Settings)** 选项卡并启用主动身份验证；请参阅在身份规则中关联领域，第 1250 页。
- 应用过滤器 - 在对象管理器的“应用过滤器”(Application Filters) 页面上，添加或编辑应用过滤器。在**名称 (Name)** 中为过滤器提供唯一名称。
- 智能应用绕行 (IAB) - 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，编辑 IAB 设置，然后点击**可绕行的应用和过滤器 (Bypassable Applications and Filters)**。

注意 对于身份规则，添加或删除**主动身份验证 (Active Authentication)** 规则操作，或者在规则操作为**被动身份验证 (Passive Authentication)** 时选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

步骤 2 从**可用应用 (Available Applications)** 列表查找并选择要添加的应用。
要限制**可用应用 (Available Applications)** 中显示的应用，请选择一个或多个**应用过滤器 (Application Filters)** 或搜索单个应用。在限制可用应用后，可以添加**所有匹配过滤器的应用 (All apps matching the filter)**，或选择并添加单个应用。

提示 点击应用旁边的信息图标 () 以显示摘要信息和互联网搜索链接。解锁图标 () 标记系统只能在已解密流量中识别的应用。

选择过滤器（单一或组合）时，“可用应用”(Available Applications) 列表会更新为仅显示符合条件的应用。您可以选择系统提供的组合形式的过滤器，但不能选择用户定义的过滤器。

- 针对同一特征选择多个过滤器（风险、业务关联性等）- 应用流量必须仅匹配其中一个过滤器。例如，如果选择中风险和高风险过滤器，则“可用应用”(Available Applications) 列表会显示所有中风险和高风险应用。
- 针对不同应用特征选择过滤器 - 应用流量必须与两个过滤器类型匹配。例如，如果您选择高风险和低业务关联性过滤器，则“可用应用”(Available Applications) 列表仅显示满足这两个条件的应用。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

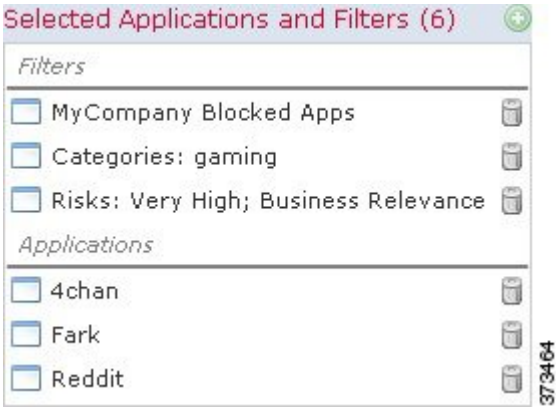
提示 在添加更多过滤器和应用之前，点击**清除过滤器 (Clear Filters)** 以清除当前选择。

Web 界面将添加到条件的过滤器列在单独添加的应用上方，并与之分开。

步骤 4 保存或继续编辑规则或配置。

示例：访问控制规则中的应用条件

下图显示用于阻止以下内容的访问控制规则的应用条件：MyCompany 的用户定义应用过滤器、具有高风险和低业务关联性的所有应用、游戏应用以及一些单独选定的应用。



接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *44*：应用特征

特征	描述	示例
Type	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	P2P 应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为高带宽和展示广告。

对应用控制的限制

自动启用应用检测器

如果没有为要检测的应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。

应用识别的速度

在执行以下操作之前，系统无法执行应用控制，包括智能应用绕行 (IAB)：

- 客户端和服务器之间建立受监控连接，并且
- 系统识别会话中的应用

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。

如果早期流量与所有其他条件都匹配，但是应用识别未完成，则系统允许数据包通过并建立连接（或完成 SSL 握手）。在系统完成其识别后，系统会将相应的操作应用于剩余会话流量。

对于访问控制，这些通过的数据包由访问控制策略的默认入侵策略（既不是默认操作入侵策略，也不是近乎匹配规则的入侵策略）检查。

加密和解密流量的应用控制

系统可识别和过滤已加密和解密的流量：

- 加密流量 - 系统可以检测使用 StartTLS（包括 SMTP、PoP、FTP、Telnet 和 IMAP）加密的应用流量。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示，或服务器证书的使用者可分辨名称值来识别某些加密应用。这些应用附以 `SSL Protocol` 标记；在 SSL 规则中，可以仅选择这些应用。只能在未加密或已解密的流量中检测到没有此标记的应用。
- 解密流量 - 系统还会将 `decrypted traffic` 标记分配给系统只能在解密流量中检测到（在加密或未加密流量中无法检测到）的应用。

将应用免于进行主动授权

在身份策略中，可以将某些应用免于主动授权，允许流量继续进行访问控制。这些应用附以 `User-Agent Exclusion` 标记。在身份规则中，仅可以选择这些应用。

处理无负载的应用流量数据包

在执行访问控制时，对于在用于识别出应用的连接中没有负载的数据包，系统会应用默认策略操作。

处理推荐应用流量

要处理由 Web 服务器所推荐的流量（如广告流量），请匹配被推荐应用（而非推荐应用）。

控制使用多个协议的应用流量 (Skype)

系统可以检测多个类型的 Skype 应用流量。要控制 Skype 流量，请从**应用过滤器 (Application Filters)** 列表中选择 **Skype** 标记，而非选择个别应用。这确保系统可以相同方式检测和控制所有 Skype 流量。

内容限制功能支持的搜索引擎

系统仅支持特定搜索引擎的安全搜索过滤。系统将 `safesearch supported` 标记从这些搜索引擎分配给应用流量。

URL 条件（URL 过滤）

URL 条件控制用户在您的网络中可访问的网站。此功能称为 *URL* 过滤。

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。
- 手动 URL 过滤 - 通过任意许可证，可以手动指定单个 URL、URL 组以及 URL 列表和源，以实现对网络流量的精细、自定义控制。

当阻止网络流量时，可以允许用户浏览器的默认行为，也可以显示通用的系统提供的或自定义的 *HTTP* 响应页面。交互式阻止为用户提供机会，通过点击忽略警告页面来绕过网站阻止。有关详细信息，请参阅HTTP 响应页面和交互式阻止，第 645 页。

具有 URL 条件的规则

下表列出了支持 URL 条件的规则，以及每个规则类型支持的过滤类型。

规则类型	支持 **Cat.** 和 **Rep.**过滤？	支持手动过滤？
访问控制	是	是
SSL	yes	否；使用可分辨名称条件

基于信誉的 URL 过滤

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，ebay.com 属于“拍卖”(Auctions) 类别，而 monster.com 属于“求职”(Job Search) 类别。URL 可以属于多个类别。
- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。范围可从“高风险”(High Risk)（第 1 级）到“知名”(Well known)（第 5 级）。

注释 要查看事件和应用详细信息中的 URL 类别和信誉信息，必须至少创建一个带 URL 条件的访问控制规则。您还必须启用与思科综合安全情报 (CSI) 的通信以获取最新的威胁情报。

注意 添加或删除访问控制或 SSL规则中的 URL 类别和信誉条件在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

基于信誉的 URL 过滤的优势

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，可以使用访问控制阻止“滥用药物”(Abused Drugs) 类别中的高风险 URL。

使用类别和信誉数据可简化策略创建和管理。此方法可保证系统按预期控制网络流量。由于思科会不断更新有关新 URL 的威胁情报以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁的站点或提供不良内容的站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下是一些系统如何适应的示例：

- 如果访问控制规则阻止所有博彩站点，当新的域名注册并分类为“博彩”(Gaming) 时，系统可以自动阻止这些站点。
- 如果某个访问控制规则阻止所有恶意软件站点，而某个博客页面受到恶意软件感染，系统可以将来自该博客的 URL 重新分类为恶意软件，并阻止该站点。
- 如果访问控制规则阻止高风险社交网站，但有人在其简档页面发布的链接中包含指向恶意负载的链接，则系统可以将该页面的信誉从“良性站点”(Benign Sites) 更改为“高风险”(High Risk)，并阻止该网站。

手动 URL 过滤

在访问控制规则和 QoS 规则中，您可以通过手动过滤各个 URL、URL 组或 URL 列表和源，补充或选择性地覆盖基于类别和信誉的 URL 过滤。您可以在没有特殊许可证的情况下执行此类型的 URL 过滤。SSL 规则不支持手动 URL 过滤；相反，使用可分辨名称条件。

例如，您可使用访问控制阻止不适合您的组织的网站类别。但是，如果该类别包含合适的网站，并且您要为其提供访问权限，则您可以为该站点创建手动的“允许”(Allow) 规则，然后将其置于该类别的“阻止”(Block) 规则之前。

手动过滤特定 URL 时，请仔细考虑可能受影响的其他流量。要确定网络流量是否与 URL 条件相匹配，系统执行简单的子字符串匹配。如果请求的 URL 与字符串的任何部分匹配，则认为该 URL 匹配。

例如，如果您允许到 example.com 的所有流量，用户可以浏览的 URL 将包括：

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

再例如，请考虑要明确阻止 ign.com（游戏站点）的情景。但是，子字符串匹配意味着阻止 ign.com 也会阻止 verisign.com，这可能并非您的意愿。

配置 URL 条件

智能许可证	经典许可证	支持的设备	支持的域	Access
URL 过滤 (cat/rep) 任意（手动）	URL 过滤 (cat/rep) 任意（手动）	任何环境	任何环境	管理员/访问管理员/网络管理员

构建 URL 条件时，选择要控制其流量的 URL 类别。或者，您可以使用信誉来限制这些 URL 类别。

在访问控制 规则中，也可以用预定义的 URL 对象、URL 列表和源过滤个别 URL，以及手动过滤每个规则的 URL。不能使用信誉限制这些 URL。SSL 规则不支持手动 URL 过滤；相反，使用可分辨名称条件。

注意 添加或删除访问控制或 SSL规则中的 URL 类别和信誉条件在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在规则编辑器中，点击 URL 条件的选项卡：

- 访问控制 - 点击 **URL** 选项卡。

- SSL - 点击**类别 (Category)** 选项卡。

步骤 2 查找并选择要控制的 URL：

- 类别 - 选择 URL 的 URL 类别，或者保持默认值**任意 (Any)**。在访问控制 规则中，点击**类别 (Category)** 子选项卡以选择类别。
- URL 对象、列表和源 - 选择预定义 URL 对象以及 URL 列表和源。在访问控制 规则中，点击 **URL** 子选项卡以选择 URL。

步骤 3 （可选）通过选择**信誉 (Reputation)** 来限制 URL 类别。
选择信誉级别也会将比您选择的级别更高或更低的其他信誉包括在内，具体取决于规则操作。如果更改规则操作，则系统会自动更改 URL 条件中的信誉级别。

- 如果规则允许或信任网络流量，则包括级别更低的信誉。例如，如果您将访问控制规则配置为允许良性站点（4 级），系统还会自动允许已知（5 级）站点。
- 如果规则对网络流量进行、解密、阻止或监控，则包括级别更高的信誉。例如，如果将访问控制规则配置为阻止可疑站点（2 级），则系统还会阻止高风险（1 级）站点。

步骤 4 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 5 （可选）在访问控制 规则中，通过输入 URL 并点击**添加 (Add)** 来添加任何要手动指定的 URL。
您可以输入 URL 或 IP 地址。此字段不支持通配符。

步骤 6 保存或继续编辑规则。

示例：访问控制规则中的 URL 条件

下图显示用于阻止以下内容的访问控制规则的URL条件：所有恶意软件站点、所有高风险站点以及所有非良性社交网站。它还会阻止 URL 对象表示的单个站点 example.com。

下表总结如何构建该条件。

受阻 URL	类别或 URL 对象	信誉
恶意软件站点，无论信誉如何	Malware Sites	任意
具有高风险（1 级）的任何 URL	任意	1 - High Risk

受阻 URL	类别或 URL 对象	信誉
风险大于良性（1 至 3 级）的社交网站	社交网络	3 - Benign sites with security risks
example.com	名为 example.com 的 URL 对象	none

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

过滤 HTTPS 流量

要过滤加密流量，系统会根据 SSL 握手期间传递的以下信息确定所请求的 URL：用于加密流量的公钥证书中的使用者公用名。

HTTP过滤考虑包括子域在内的整个主机名。不过，HTTP过滤会忽略主题公用名中的子域，因此在访问控制 策略中手动过滤 HTTPS URL 时请勿包含子域信息。例如，使用 example.com 而不是 www.example.com。

提示

在 SSL 策略中，可以通过定义可分辨名称 SSL 规则条件来处理和解密发送到特定 URL 的流量。证书的主题可分辨名称中的公用名属性包含站点的 URL。通过解密 HTTPS 流量，访问控制规则可以评估解密的会话，从而改进 URL 过滤。

按加密协议控制流量

在访问控制 策略中执行 URL 过滤时，系统会忽略加密协议（HTTP 与 HTTPS）。对于手动 URL 条件和基于信誉的 URL 条件均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- http://example.com/
- https://example.com/

要配置仅与HTTP或HTTPS流量匹配的规则，请向该规则添加应用条件。例如，可以通过构造两个访问控制规则（每个规则具有应用和URL条件）来允许对某个站点进行HTTP访问，同时禁止HTTP访问。

第一个规则允许 HTTPS 流量到达网站：

Action: Allow
Application: HTTPS
URL: example.com

第二个规则阻止对同一网站进行 HTTP 访问：

Action: Block

Application: HTTP
URL: example.com

对 URL 过滤的限制

URL 识别的速度

在满足以下情况之前，系统无法过滤 URL：

- 客户端与服务器之间建立受监控连接
- 系统识别会话中的 HTTP 或 HTTPS 应用
- 系统识别所请求的 URL（对于加密会话，则为 ClientHello 消息或服务器证书中的 URL）

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。

如果早期流量与所有其他规则条件都匹配，但是识别未完成，则系统允许数据包通过并建立连接（或完成 SSL 握手）。在系统完成其识别后，系统会将相应的规则操作应用于剩余会话流量。

对于访问控制，这些通过的数据包由访问控制策略的默认入侵策略（既不是默认操作入侵策略，也不是近乎匹配规则的入侵策略）检查。

具有未知类别或信誉的 URL

如果系统不知道 URL 的类别或信誉，则浏览到该网站与具有基于类别或信誉的 URL 条件的规则不匹配。在这种情况下，您将无法手动对该 URL 指定类别或信誉。

手动 URL 过滤

手动过滤特定 URL 时，请仔细考虑可能受影响的其他流量。要确定网络流量是否与 URL 条件相匹配，系统执行简单的子字符串匹配。如果请求的 URL 与字符串的任何部分匹配，则认为该 URL 匹配。

加密网络流量的 URL 过滤

对加密网络流量执行 URL 时，系统执行以下操作：

- 忽略加密协议；如果规则具有 URL 条件但不具有指定该协议的应用条件，则该规则将同时匹配 HTTPS 和 HTTP 流量
- 根据用于加密流量的公钥证书中的主题公用名与 HTTPS 流量相匹配，并且忽略主题公用名中的子域
- 对于被访问控制规则（或其他任何配置）阻止的已加密或已解密连接，系统不显示 HTTP 响应页面；请参阅 对 HTTP 响应页面的限制，第 645 页

在 URL 中搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，使用网络搜索来搜索 amazon.com 不会被阻止，但是，浏览 amazon.com 则会被阻止。

所选设备型号的内存限制

由于内存限制，某些设备型号以规模较小、精细程度较低的类别和信誉集执行URL过滤。例如，如果父 URL 的子站点具有不同的 URL 类别和信誉，有些设备可能会对所有子站点使用父 URL 的数据。具体举例而言，系统可能会使用 google.com 的类别和信誉来评估 mail.google.com。受影响设备包括 7100 系列和以下 ASA 型号：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X 和 ASA5525-X。对于虚拟设备，请参阅《《*Firepower* 系统虚拟安装指南》》以了解有关分配正确的内存量来执行基于类别和信誉的 URL 过滤的信息。

用户、领域和 ISE 属性条件（用户控制）

在指定用户登录或注销主机或使用 Microsoft Active Directory (AD) 或 LDAP 凭证进行身份验证时，身份源会对其进行监控。系统检测到新用户会话时，用户会话数据会保留在用户数据库中，直至出现以下其中一种情形：

- 某个 Firepower 管理中心用户从“用户”(Users) 表中手动删除用户会话。
- 某个身份源报告该用户会话的注销操作。
- 某个领域根据其**用户会话超时：通过身份验证的用户 (User Session Timeout: Authenticated Users)**、**用户会话超时：身份验证失败的用户 (User Session Timeout: Failed Authentication Users)** 或**用户会话超时：访客用户 (User Session Timeout: Guest Users)** 设置结束用户会话。

您可以使用存储在用户数据库中的授权用户数据执行用户控制。有关您的 Firepower 系统版本支持的身份源的详细信息，请参阅概述：用户身份源，第 1197 页。

与用户相关的规则条件根据与受监控主机相关联的已登录授权用户来匹配流量。

- 用户和领域条件 - 根据主机的已登录授权用户来匹配流量。您可以根据领域、个别用户或这些用户所属的组来控制流量。
- ISE 属性条件 - 如果已将 ISE 配置为身份源，则根据用户的已分配 ISE 安全组标记 (SGT)、终端配置文件或终端位置来匹配流量。

带用户相关条件的规则

规则类型	支持用户和领域条件？	支持 ISE 属性条件？
访问控制	是	是
SSL	是	否

用户控制必备条件

配置身份源/身份验证方法

配置要执行的身份验证类型的身份源。有关详细信息，请参阅概述：用户身份源，第 1197 页。

如果将用户代理或 ISE 设备配置为监控大量用户组，或者如果将大量用户映射到网络上的主机，则系统可能会由于Firepower管理中心用户限制而根据组丢弃用户映射。因此，具有领域、用户或用户组条件的规则可能无法按预期与流量匹配。

配置领域

配置要监控的每个 AD 或 LDAP 服务器（包括 ISE 或用户代理服务器）的领域，并执行用户下载。有关详细信息，请参阅创建领域，第 1235 页。

当配置领域时，请指定要监控其活动的用户和用户组。包含某个用户组即会自动包含该组的所有成员（包括任何辅助组的成员）。但是，如果要使用辅助组作为规则条件，则必须在领域配置中明确包含辅助组。

对于每个领域，可以启用用户数据自动下载，以刷新用户和用户组的授权数据。

创建身份策略

创建身份策略以将领域与身份验证方法相关联，并将该策略与访问控制相关联。有关详细信息，请参阅创建身份策略，第 1240 页。

在设备上执行用户控制的策略（访问控制、SSL）共享身份策略。该身份策略确定可以在影响这些设备上的流量的规则中使用的领域、用户和组。

配置用户和领域条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员/访问管理员/网络管理员

可以按领域或者按该领域内的用户和用户组限制规则。

开始之前

- 满足用户控制必备条件，如用户、领域和 ISE 属性条件（用户控制），第 286 页中所述。

过程

步骤 1 在规则编辑器中，点击**用户 (Users)** 选项卡。

步骤 2 从**可用领域 (Available Realms)** 中查找并选择要使用的领域。

步骤 3 （可选）通过从**可用用户 (Available Users)** 列表中选择用户和组，进一步限制规则。

步骤 4 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 5 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置 ISE 属性条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员/访问管理员/网络管理员

开始之前

- 满足用户控制必备条件，如用户、领域和 ISE 属性条件（用户控制），第 286 页中所述。

过程

步骤 1 在规则编辑器中，点击 **ISE 属性 (ISE Attributes)** 选项卡。

步骤 2 从**可用 ISE 会话属性 (Available ISE Session Attributes)** 列表中查找并选择要使用的 ISE 属性。

步骤 3 （可选）通过从**可用 ISE 元数据 (Available ISE Metadata)** 列表选择元数据进一步限制规则。或者，请保留默认值：**任意 (any)**。

步骤 4 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 5 （可选）利用“位置 IP”(Location IP) ISE 属性来限制规则。在**添加位置 IP 地址 (Add a Location IP Address)** 字段中输入 IP 地址，然后点击**添加 (Add)**。
系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 6 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

对用户控制进行故障排除

如果您发现意外的用户规则行为，请考虑调整规则、身份源或领域配置。有关其他相关故障排除信息，请参阅对用户身份源问题进行故障排除，第 1198 页和对领域和用户下载问题进行故障排除，第 1234 页。

针对领域、用户或用户组的规则与流量不匹配

如果将用户代理或 ISE 设备配置为监控大量用户组，或者如果将大量用户映射到网络上的主机，则系统可能会由于Firepower管理中心用户限制而丢弃用户记录。因此，具有用户条件的规则可能不会按预期与流量匹配。

针对用户组或用户组内的用户的规则不是按预期与流量匹配

如果配置具有用户组条件的规则，则 LDAP 或 Active Directory 服务器必须配置用户组。如果服务器以基本对象层次结构形式来组织用户，则系统无法执行用户组控制。

针对辅助组中的用户的规则不是按预期与流量匹配

如果配置具有用户组条件的规则，并且该条件包含或排除属于 Active Directory 服务器中辅助组的成员的用户，则服务器可能会限制其报告的用户数。

默认情况下，Active Directory 服务器会限制从辅助组报告的用户数量。必须自定义此限制，以便辅助组中的所有用户都报告给 Firepower 管理中心并适合在具有用户条件的规则中使用。

规则与首次发现的用户不匹配

在系统检测到先前未发现的用户的活动后，会从服务器检索其有关信息。直到系统成功检索此信息后，此用户发现的活动才**不**由匹配规则处理。相反，用户会话由其匹配的下一个规则（或适用时的策略默认操作）处理。

例如，这可能解释以下情形：

- 属于用户组成员的用户与具有用户组条件的规则不匹配。
- 当用于用户数据检索的服务器是 Active Directory 服务器时，由用户代理或 ISE 设备报告的用户与规则不匹配。

请注意，这可能会导致系统延迟显示事件视图和分析工具中的用户数据。

规则与所有 ISE 用户都不匹配

这是预期行为。可以对由 Active Directory 域控制器进行身份验证的 ISE 用户执行用户控制。不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。

搜索规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在许多策略中，您可以搜索所需的规则以及在匹配规则中您所感兴趣的规则。系统会将您输入的内容与规则名称和条件值（包括对象和对象组）匹配。

不能在“安全情报”(Security Intelligence) 或 URL 列表或源中搜索值。

过程

步骤 1 在策略编辑器中，点击**规则 (Rules)** 选项卡。

步骤 2 点击**搜索规则 (Search Rules)** 提示，输入完整或部分搜索字符串，然后按 Enter 键。
对于每个匹配规则，匹配值列将会突出显示。状态消息会显示当前的匹配项以及匹配项的总数量。

步骤 3 查找感兴趣的规则。
要在匹配规则之间导航，可以点击下一匹配项 ( ) 或上一匹配项 ( ) 图标。

接下来的操作

- 在开始新的搜索之前，请点击清除图标 ( ) 以清除搜索和任何高亮显示内容。

按设备过滤规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	因功能而异	任意	管理员/访问管理员/网络管理员

有些策略编辑器允许您按受影响设备过滤您的规则视图。

系统使用规则的接口限制来确定该规则是否影响设备。如果您按接口限制规则（安全区域条件），则该规则会影响接口所在的设备。无接口限制的规则会应用于任何接口，因此也会应用于每台设备。

过程

步骤 1 在策略编辑器中，点击**规则 (Rules)** 选项卡，然后点击**按设备过滤 (Filter by Device)**。

系统将会显示目标设备和设备组列表。

步骤 2 选中一个或多个复选框，以仅显示应用于这些设备或组的规则。或者，选中**全部 (All)** 复选框，以重置和显示所有的规则。

提示 将指针悬停在规则标准上方可查看其值。如果标准代表具有设备特定覆盖的对象，则系统会在您仅按该设备过滤规则列表时显示覆盖值。如果标准代表具有域特定覆盖的对象，则系统会在您按该域中的设备过滤规则列表时显示覆盖值。

步骤 3 点击 **OK**。

规则和其他策略警告

策略和规则编辑器使用图标来标记可能会对流量分析和流动有不利影响的配置。根据问题，系统可能会在您部署时向您发出警告或完全阻止您进行部署。

提示 将您的鼠标指针悬停在图标之上，即可读取警告、错误或信息文本。

表 *45*: 策略错误图标

图标	描述	示例
error	如果规则或配置具有错误，则更正错误之前无法部署，即使禁用任何受影响规则也如此。	在将没有URL过滤许可证的设备设为目标之前，执行基于类别和信誉的 URL 过滤的规则有效。此时，在规则旁边会显示错误图标，并且在编辑或删除规则、将策略重新设为目标或启用许可证之前，无法进行部署。
warning	可以部署显示规则或其他警告的策略。然而，标记有警告的不当配置将不起作用。 如果禁用存在警告的规则，警告图标将会消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。	已占用的规则或由于配置不当而无法与流量相匹配的规则不起作用。这包括使用空对象组的条件、与应用不匹配的应用过滤器、已排除的LDAP用户、无效端口等等。 但是，如果警告图标标记许可错误或型号不匹配，则在更正问题之前无法进行部署。
信息	信息图标传达有关可能影响流量流动的配置的有用信息。这些问题不会阻止您进行部署。	通过应用控制和 URL 过滤，系统可能会跳过根据某些规则来匹配连接的前几个数据包，直至系统识别该连接中的应用或网络流量为止。这样，就可建立连接，以便识别应用和 HTTP 请求。

规则性能准则

在Firepower系统中，各种策略中的规则对网络流量进行精细控制。对规则正确进行配置和排序对于构建有效的部署至关重要。尽管每个组织和部署都拥有唯一的策略和规则集，但是需要遵循几条通用准则，才可优化性能，同时满足您的需求。

如果执行资源密集型分析，则优化性能尤其重要。复杂的策略和规则可控制重要资源并对性能产生不利影响。当部署配置更改时，系统会将所有规则共同进行评估，并创建目标设备用于评估网络流量的扩展标准集。如果这些标准超过目标设备的资源（物理内存、处理器等），则您无法部署到该设备。

注释 始终应根据您的组织的需求对规则进行排序。将必须应用于所有流量的最优先规则靠近策略的顶部放置。但是，如果您没有对具备应用或URL条件的规则进行优先排序，则它们更有可能匹配流量。这是因为系统可能会跳过根据某些规则来匹配连接的前几个数据包，直至系统识别该连接中的应用或网络流量为止。这样，就可建立连接，以便识别应用和HTTP请求。

简化和集中规则准则

简化：不过度配置

如果一个条件足以匹配您想要处理的流量，请不要使用两个条件。

最小化单个规则条件。在规则条件中使用尽可能少的单独元素。例如，在网络条件中，使用IP地址块，而不是单独的IP地址。在端口条件中，使用端口范围。使用应用过滤器及URL类别和声誉来执行应用控制和URL过滤，使用LDAP用户组来执行用户控制。

将元素组合到对象中**不**会提高性能。例如，使用包含50个IP地址的网络对象，与逐一将这些IP地址纳入条件中相比，只能给您带来组织优势，而不是性能优势。

集中：更严格地限制资源密集型规则，尤其是按接口限制

尽可能使用规则条件以更严格定义资源密集型规则处理的流量。集中规则很重要的另一原因是，有着广泛条件的规则可能与许多不同类型的流量相匹配，并且可以抢占较为靠后、更为具体的规则。资源密集型规则的示例包括：

- 解密流量的SSL规则 - 不仅解密，而且进一步分析已解密流量，也都需要资源。缩小集中范围，并尽可能阻止或选择不解密加密流量。
- 调用深度检查的访问控制规则 - 入侵、文件和恶意软件检查需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更是如此。确保只在必要时调用深度检查。

为获得最大性能优势，请按接口限制规则。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

排序规则准则

规则抢占

当一条规则由于评估中排序靠前的规则首先匹配流量而永远无法匹配流量时，会出现规则抢占问题。规则的条件控制其是否会抢占其他规则。在以下示例中，第二条规则无法阻止管理员流量，因为第一条规则会允许该流量：

访问控制规则 1：允许管理员用户
访问控制规则 2：阻止管理员用户

任何类型的规则条件均可以取代后续规则。第一条 SSL 规则中的 VLAN 范围包含第二条规则中的 VLAN，因此第一条规则将抢占第二条规则：

规则 1：不解密 VLAN 22-33
SSL 规则 2：阻止 VLAN 27

在以下示例中，规则 1 匹配所有 VLAN，因为没有配置 VLAN，因此规则 1 会取代尝试匹配 VLAN 2 的规则 2：

访问控制规则 1：允许源网络 10.4.0.0/16
访问控制规则 2：允许源网络 10.4.0.0/16，VLAN 2

规则还会抢占所有已配置条件均相同的相同后续规则：

访问控制规则 1：允许 VLAN 1 URL www.example.com
访问控制规则 2：允许 VLAN 1 URL www.example.com

如有任何条件不同，则后续规则不会被抢占：

访问控制规则 1：允许 VLAN 1 URL www.example.com
访问控制规则 2：允许 VLAN 2 URL www.example.com

示例：对 SSL 规则进行排序以避免抢占

请考虑以下场景，其中受信任 CA（好 CA ）错误地将 CA 证书颁发给恶意实体（坏 CA），但是尚未撤销该证书。您希望使用 SSL 策略来阻止使用由不受信任 CA 颁发的证书加密的流量，但是以其他方式允许受信任 CA 的信任链中的流量。在上传 CA 证书和所有中间 CA 证书后，请配置包含如下排序规则的 SSL 策略：

SSL 规则 1：阻止颁发者 CN=www.badca.com
SSL 规则 2：不解密颁发者 CN=www.goodca.com

如果恢复规则，会首先与受良好 CA 信任的所有流量相匹配，包括受不良 CA 信任的流量。由于流量不曾与后续不良 CA 规则相匹配，因此可能会允许而非阻止恶意流量。

规则操作和规则顺序

规则操作确定系统如何处理匹配的流量。通过将不执行也不确保进一步流量处理的规则置于会执行并确保进一步流量处理的资源密集型规则之前来提高性能。然后，系统可以转移可能已另外检查的流量。

以下示例显示在规则集中无任何规则更重要且抢占不是问题的情况下，可能如何在各种策略中对规则进行排序。

最佳顺序：SSL 规则

不仅解密需要资源，进一步分析已解密的流量也同样需要资源。请将用于解密流量的 SSL 规则放在最后。

1. 监控 - 记录匹配连接但不对流量采取任何其他操作的规则。
2. 阻止、阻止并重置 - 阻止流量而不进一步检测的规则
3. 不解密 - 不解密加密流量，从而将加密会话传递到访问控制规则的规则。这些会话的负载不执行深度检查。
4. 解密 - 已知密钥 - 使用已知私钥解密传入流量的规则。
5. 解密 - 重新签名 - 通过对服务器证书重新签名来解密传出流量的规则。

最佳顺序：访问控制规则

入侵、文件和恶意软件检测需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更加如此。请将调用深度检查的访问控制规则放在最后。

1. 监控 - 记录匹配连接但不对流量采取任何其他操作的规则。
2. 信任、阻止、阻止并重置 - 处理流量而不进一步检测的规则。请注意，受信任的流量会受到身份策略实施的身份验证要求的制约。
3. 允许，交互式阻止（无深度检查）- 不进一步检测流量，但是允许发现的规则。请注意，允许的流量会受到身份策略实施的身份验证要求的制约。
4. 允许，交互式阻止（深度检查）- 与对禁止的文件、恶意软件和漏洞执行深度检查的文件或入侵策略关联的规则。

内容限制规则顺序

为了避免 SSL 和访问控制策略中出现规则抢占，请将管理 YouTube 限制的规则排在管理安全搜索限制的规则前面。

当您对访问控制规则启用安全搜索时，系统会将`搜索引擎 (search engine)`类别添加到**所选应用和过滤器 (Selected Applications and Filters)**。此应用类别包括 YouTube。因此，除非在评估优先级较高的规则中启用了 YouTube EDU，否则 YouTube 流量将与安全搜索规则进行匹配。

在评估顺序中，如果将具有`支持安全搜索 (safesearch supported)`过滤器的 SSL 规则排在具有特定 YouTube 应用条件的 SSL 规则前面，则会发生类似的规则抢占。

SSL 规则顺序

允许来自证书固定站点的流量

在建立 SSL 会话之前，证书固定强迫客户端的浏览器验证服务器的公钥证书与已用来将浏览器和服务器关联的证书相匹配。由于**解密 - 重新签名 (Decrypt - Resign)** 操作涉及在将服务器证书传递给客户端之前对其进行修改，如果浏览器已固定该证书，则会拒绝这些已修改的证书。

例如，如果客户端浏览器连接到 windowsupdate.microsoft.com（使用证书固定的站点），并且您配置 SSL 规则（用来将此流量与**解密 - 重新签名 [Decrypt - Resign]** 操作相匹配），则系统会对服务器证书重新签名，然后将其传递给客户端浏览器。因为这一修改的服务器证书不匹配 windowsupdate.microsoft.com 的浏览器的固定证书，客户端浏览器拒绝此连接。

如果要允许此流量，请配置一个 SSL 规则，将“不解密”(Do not decrypt) 操作与服务器证书公用名或可分辨名称相匹配。在 SSL 策略中，将此规则排在也与此流量匹配的所有**解密 - 重新签名 (Decrypt - Resign)** 规则之前。成功连接到网站后，您可以通过客户端的浏览器检索固定的证书。无论连接成功与否，您都可以从记录的连接事件查看证书。

避免入侵策略激增的准则

在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。

但是，目标设备支持的访问控制规则或入侵策略存在最大数量的限制。该最大数量取决于很多因素，包括设备上的策略复杂度、物理内存以及处理器数量。

如果超过了设备支持的最大数量，则您无法部署访问控制策略，且必须重新评估。您可能希望整合入侵策略或变量集，从而能够将单个入侵策略/变量集对与多个访问控制规则相关联。

第 17 章

可重用对象

以下主题介绍如何在 Firepower 系统中管理可重用对象：

可重用对象简介

为了提高灵活性和 Web 界面的易用性，Firepower 系统会使用命名对象，命名对象是将名称与值相关联的可重用配置。当您要使用该值时，可使用命名对象来替代。系统支持在 Web 界面中的不同位

置使用这些对象，包括许多策略和规则、事件搜索、报告、控制面板等等。系统提供许多代表常用配置的预定义对象。

使用对象管理器创建和管理对象。许多使用对象的配置也允许您根据需要即时创建对象。您也可以使用对象管理器进行以下操作：

- 将对象分组，以用一个配置引用多个对象；请参阅对象组，第 301 页。
- 覆盖所选设备或所选域（在多域部署中）的对象值；请参阅对象覆盖，第 303 页。

编辑在活动策略中使用的对象后，必须重新部署更改的配置，才能使更改生效。您无法删除活动策略正在使用的对象。

对象类型

下表列出了您可以在Firepower系统中创建的对象，并指示是否可以对每个对象类型进行分组或配置以允许覆盖。

对象类型	是否可分组？	是否允许覆盖？
网络	是	是
端口	是	是
安全区域	否	否
应用过滤器	否	否
VLAN 标记	是	是
URL	是	是
Geolocation	否	否
变量集	否	否
安全情报：网络、DNS 和 URL 列表和源	否	否
Sinkhole	否	否
文件列表	否	否
密码套件列表	否	否
可分辨名称	是	否

对象类型	是否可分组？	是否允许覆盖？
公钥基础设施 (PKI)： • 内部和受信任 CA • 内部和外部证书	是	否

对象和多租户

在多域部署中，您可以在全局域和后代域中创建对象，。系统会显示在当前域中创建的对象，您可以对其进行编辑。它还会显示在祖先域中创建的对象，但您无法对其进行编辑，除了安全区域。

注释 因为安全区域与在枝叶级别配置的设备接口绑定，后代域中的管理员可以查看并编辑在祖先域中创建的安全区域。子域用户可以在祖先区域中添加和删除接口，但无法删除或重命名区域。

对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

对于支持分组的对象，可以将当前域中的对象与从祖先域中继承的对象分到一组。

对象覆盖允许您定义某些类型对象的设备特定或域特定值，包括网络、端口、VLAN 标记和 URL。在多域部署中，可以为祖先域中的对象定义默认值，但允许后代域中的管理员为该对象添加覆盖值。

对象管理器

可以使用对象管理器创建和管理对象和对象组。

对象管理器每页显示 20 个对象或对象组。如果有超过 20 个任何类型的对象或对象组，请使用位于页面底部的导航链接查看其他页面。还可以转到特定页或点击刷新图标 ( ) 刷新视图。

默认情况下，页面会按名称的字母顺序列示对象和对象组。然而，也可以按显示的任何列对每种类型的对象或对象组进行排序。还可以按名称或值对页面上的对象进行过滤。

编辑对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从列表中选择对象类型；请参阅可重用对象简介，第 297 页。

步骤 3 点击要编辑的对象旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 根据需要修改对象设置。

步骤 5 如果编辑的是变量集，请管理变量集中的变量；请参阅管理变量，第 324 页。

步骤 6 对于可以配置为允许覆盖的对象：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖 (Allow Overrides)** 复选框；请参阅允许对象覆盖，第 304 页。只可以为属于当前域的对象更改此设置。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 305 页。

步骤 7 点击 **Save**。

步骤 8 如果编辑的是变量集，并且该变量集正在被一个访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

过滤对象或对象组

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域和祖先域中创建的对象，您可以对其进行过滤。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 在**过滤 (Filter)** 字段中输入过滤器条件。

页面会在您键入内容时进行更新，以显示匹配的项目。

可以使用以下通配符：

- 星号 [*] 匹配零或重复出现的一个字符。
- 脱字符 (^) 匹配字符串开头的内容。
- 美元符号 ($) 匹配字符串结尾的内容。

对象排序

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 点击列标题。要按相反方向排序，请再次点击标题。

对象组

将对象分组使得可以引用带有单个配置的多个对象。系统允许在网络界面中互用对象和对象组。例如，在任何要使用端口对象的地方，也可以使用端口对象组。

可以将网络、端口、VLAN 标记、URL 和 PKI 对象分组。

相同类型的对象和对象组不能具有相同的名称。在多域部署中，对象组的名称在域层次结构中必须是唯一的。请注意，系统可能会识别出与您在当前域中无法查看的对象组名称的冲突。

编辑策略中使用的对象组（例如，访问控制策略中使用的网络对象组）时，您必须重新部署已更改的配置以使更改生效。

删除组不会删除组中的对象，只会删除对象之间的相关性。此外，您也无法删除活动策略中正在使用的组。例如，无法删除用于已保存访问控制策略中的 VLAN 条件的 VLAN 标记组。

对可重用对象进行分组

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以将当前域中的对象与从祖先域中继承的对象分到一组。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 如果要分组的对象类型为**网络 (Network)**、**端口 (Port)**、**URL** 或 **VLAN 标记 (VLAN Tag)**：

a) 从对象类型列表中选择对象类型。

b) 从**添加（对象类型）(Add [Object Type])** 下拉列表中选择**添加组 (Add Group)**。

步骤 3 如果要分组的对象类型为**可分辨名称 (Distinguished Name)**：

a) 展开**可分辨名称 (Distinguished Name)** 节点。

b) 选择**对象组 (Object Groups)**。

c) 点击**添加可分辨名称 (Add Distinguished Name)**。

步骤 4 如果要分组的对象类型为 **PKI**：

a) 展开 **PKI** 节点。

b) 选择以下其中一个选项：

- **内部 CA 证书 (Internal CA Groups)**
- **受信任 CA 证书 (Trusted CA Groups)**
- **内部证书组 (Internal Cert Groups)**
- **外部证书组 (External Cert Groups)**

c) 点击**添加（对象类型）组 (Add [Object Type] Group)** 按钮。

步骤 5 在**名称 (Name)** 中输入唯一的名称。

步骤 6 从列表中选择一个或多个对象，然后点击**添加 (Add)**。
您还可以：

- 使用过滤器字段( )可搜索要包括的现有对象，在您键入时，该字段会更新以显示匹配项目。点击搜索字段上方的重新加载图标 ( )，或点击搜索字段中的清除图标 ( ) 以清除搜索字符串。

- 如果现有对象不符合您的需要，可点击添加图标 () 快速创建对象。

步骤 7 或者对于**网络 (Network)**、**端口 (Port)**、**URL** 和 **VLAN 标记 (VLAN Tag)** 组：

- 输入**说明 (Description)**。
- 选中**允许覆盖 (Allow Override)** 复选框，允许对此对象组进行覆盖；请参阅允许对象覆盖，第 304 页。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象组，请部署配置更改；请参阅部署配置更改，第 254 页。

对象覆盖

通过对象覆盖，您可以为对象定义一个备选值，系统将为您指定的设备使用该值。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，您可能想要拒绝 ICMP 流量传送到公司的不同部门，每个部门连接到不同的网络。可以通过定义带有特定规则（包括一个称为“部门网络”的网络对象）的访问控制策略来实现。通过允许覆盖此对象，即可在每个相关设备上创建覆盖，指定该设备所连接的实际网络。

在多域部署中，可以为祖先域中的对象定义默认值，并允许后代域中的管理员为该对象添加覆盖值。例如，托管安全运营商 (MSSP) 可以使用单一 Firepower 管理中心来管理多个客户的网络安全。MSSP 的管理员可以在全局域中定义在所有客户的部署中使用的对象。每个客户的管理员可以登录后代域，为其组织覆盖该对象。这些本地管理员无法查看或影响 MSSP 的其他客户的覆盖值。

您可以将对象覆盖的目标对准特定域。在这种情况下，除非已在设备级覆盖该值，否则系统会将对象覆盖值用于目标域中的所有设备。

在对象管理器中，可以选择可覆盖的对象并为该对象定义设备级或域级覆盖列表。

只能使用具有以下对象类型的对象覆盖：

- 网络
- 端口
- VLAN 标记
- URL

如果可以覆盖对象，则系统会在对象管理器中为该对象类型显示**覆盖 (Override)** 列。此列的可能值包括：

- 绿色勾选标记 - 表示可为对象创建覆盖且尚未添加任何覆盖
- 红色 X - 表示无法为对象创建覆盖
- 数字 - 表示已添加到该对象的覆盖计数（例如，“2”表示已添加两个覆盖）

管理对象覆盖

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中进行选择；请参阅可重用对象简介，第 297 页。

步骤 3 点击要编辑的对象旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 管理对象覆盖：

- 添加 - 添加对象覆盖；请参阅添加对象覆盖，第 305 页。
- 允许 - 允许对象覆盖；请参阅允许对象覆盖，第 304 页。
- 删除 - 在对象编辑器中，点击要删除的覆盖旁边的删除图标 ( )。
- 编辑 - 编辑对象覆盖；请参阅编辑对象覆盖，第 306 页。

允许对象覆盖

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在对象编辑器中，选中**允许覆盖 (Allow Overrides)**复选框。

步骤 2 点击**保存 (Save)**。

接下来的操作

- 添加对象覆盖值；请参阅添加对象覆盖 ， 第 305 页。

添加对象覆盖

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

开始之前

- 允许对象覆盖；请参阅允许对象覆盖 ， 第 304 页。

过程

步骤 1 在对象编辑器中，展开**覆盖 (Override)** 部分。

步骤 2 点击 **Add**。

步骤 3 在**目标 (Targets)** 选项卡中，选择**可用设备和域 (Available Devices and Domains)** 列表中的域或设备，然后点击**添加 (Add)**。

步骤 4 在“覆盖”(Override) 选项卡中，输入**名称 (Name)**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 输入覆盖值。

示例：
对于网络对象，请输入网络值。

步骤 7 点击 **Add**。

步骤 8 点击 **Save**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改 ， 第 254 页。

编辑对象覆盖

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

可以修改说明和现有覆盖的值，但不可以修改现有目标列表。相反，您必须添加一个具有新目标的新覆盖，该覆盖将代替现有覆盖。

过程

步骤 1 在对象编辑器中，展开**覆盖 (Override)** 部分。

步骤 2 点击要修改的覆盖旁边的编辑图标 ( )。

步骤 3 或者，修改**说明 (Description)**。

步骤 4 修改覆盖值。

步骤 5 点击**保存 (Save)** 保存覆盖。

步骤 6 点击**保存 (Save)** 保存对象。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

网络对象

网络对象代表可单独指定或作为地址块指定的一个或多个 IP 地址。您可以在系统 Web 界面中的各个位置使用网络对象和组，包括访问控制策略、网络变量、入侵规则、身份规则、网络发现规则、事件搜索、报告等等。

创建网络对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**网络 (Network)**。

步骤 3 从**添加网络 (Add Network)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 在**网络 (Network)** 字段中，输入 IP 地址或地址块以添加到对象中。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖 (Allow Overrides)** 复选框；请参阅允许对象覆盖，第 304 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 305 页。

步骤 8 点击 **Save**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

端口对象

端口对象以略有不同的方式代表不同协议：

TCP 和 UDP

代表传输层协议（协议号括在括号内，加上一个可选的关联端口或端口范围）的端口对象。例如：`TCP(6)/22`。

ICMP 和 ICMPv6 (IPv6-ICMP)

代表互联网层协议再加上可选类型和代码的端口对象。例如：`ICMP(1):3:3`。

您可以按类型和代码（如果适用）来限制 ICMP 或 IPV6-ICMP 端口对象。有关 ICMP 类型和代码的详细信息，请参阅：

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

其他

可以代表不使用端口的其他协议的端口对象。

Firepower 系统为已知端口提供默认端口对象。您无法修改或删除这些默认对象。除默认对象以外，还可以创建自定义端口对象。

可在系统 Web 界面中的不同位置使用端口对象和对象组，包括访问控制策略、身份规则、网络发现规则、端口变量和事件搜索。例如，如果您的组织使用的自定义客户端使用特定范围的端口并导致系统生成过多误导事件，可以配置网络发现策略来排除对这些端口的监控。

使用端口对象时，请遵循以下准则：

- 不能为访问控制规则中的源端口条件添加除 TCP 或 UDP 以外的任何协议。此外，在规则中设置源端口条件和目标端口条件时，不能混用传输协议。
- 如果要将不受支持的协议添加到用于源端口条件的端口对象组，则在部署配置时使用该协议的规则不会在受管设备上生效。
- 如果创建同时包含 TCP 和 UDP 端口的端口对象，然后将其添加为规则的源端口条件，则不能添加目标端口，反之亦然。

创建端口对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**端口 (Port)**。

步骤 3 从**添加端口 (Add Port)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。

步骤 5 选择**协议 (Protocol)**。

步骤 6 根据选择的协议，按**端口 (Port)** 进行限制，或者选择 ICMP **类型 (Type)** 和**代码 (Code)**。
可输入 1 到 65535 之间的端口。使用连字符指定端口范围。如果选择与**所有 (All)** 协议匹配，则必须使用**其他 (Other)** 下拉列表按端口限制对象。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖 (Allow Overrides)** 复选框；请参阅允许对象覆盖，第 304 页。

- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 305 页。

步骤 8 点击 **Save**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

安全区域

安全区域将网络分段，以帮助您管理和分类流量。安全区域只是对接口进行分组。这些组可以跨多个设备；您还可以在单个设备上配置多个区域。

安全区域中的所有接口都必须为同一类型：全都为内联、被动、交换、路由或ASA FirePOWER。创建安全区域后，不能更改其包含的接口类型。一个接口只能属于一个区域。

对象管理器的安全区域 (Security Zones) 页面列出受管设备上配置的区域。该页面还显示每个区域中的接口类型，并且您可以展开每个区域以查看每个区域包含哪些设备上的哪些接口。

型号特定备注和警告

在 7000 或 8000 系列设备的初始配置期间，系统会根据您为设备选择的检测模式创建安全区域。例如，系统在被动部署中创建被动区域，在内联部署中则创建外部区域和内部区域。将设备注册到 Firepower 管理中心时，这些安全区域会添加到管理中心。

如果修改 ASA FirePOWER 安全情景，从而在单情景模式与多情景模式之间进行切换，则系统会从其分配的安全区域中删除设备的所有接口。

区域和多租户

在多域部署中，您可以在任何级别创建安全区域。在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在此情况下，在对象管理器中查看祖先区域配置的子域用户只能看到其域中的接口。

除非受角色限制，否则子域用户可以查看和编辑祖先域中创建的区域。子域用户可以从这些区域添加和删除接口。但是，他们无法删除或重命名区域。您既不能查看也不能编辑后代域中创建的区域。

创建安全区域对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	安全区域：任意 接口组：Firepower 威胁防御	任意	管理员/访问管理员/网络管理员

提示 可以创建空的安全区域并随后向其添加接口。要添加接口，该接口必须具有名称。您还可以在**设备 (Devices)** > **设备管理 (Device Management)**中配置接口时创建安全区域。

开始之前

- 了解每种类型的安全区域的使用要求和限制。请参阅安全区域，第 309 页。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**安全区域 (Security Zones)**。

步骤 3 点击**添加安全区域 (Add Security Zone)**。

步骤 4 输入 **Name**。

步骤 5 选择**接口类型 (Interface Type)**。

步骤 6 从**设备 (Device)** > **接口 (Interfaces)** 下拉列表中，选择包含要添加的接口的设备。

步骤 7 选择一个或多个接口。

步骤 8 点击**添加 (Add)** 以添加所选接口（按设备分组）。

步骤 9 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

应用过滤器

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以在对象管理器中，以系统提供的过滤器的组合为基础或以应用的自定义组合为基础，创建并管理可重复使用的用户定义的应用过滤器。有关详细信息，请参阅应用条件（应用控制），第 276 页。

VLAN 标记对象

配置的每个 VLAN 标记对象代表一个 VLAN 标记或标记范围。

可以将VLAN标记对象进行分组。组表示多个对象；就此意思而言，在单个对象中使用一系列VLAN标记不被视为组。

可以在系统 Web 界面中的各种位置使用 VLAN 标记对象和组，包括规则和事件搜索。例如，可以编写仅适用于特定 VLAN 的访问控制规则。

创建 VLAN 标记对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 访问管理员 网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中，选择 **VLAN 标记 (VLAN Tag)**。

步骤 3 从**添加 VLAN 标记 (Add VLAN Tag)** 下拉列表中，选择**添加对象 (Add Object)**。

步骤 4 输入**名称 (Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 在 **VLAN 标记 (VLAN Tag)** 字段中输入值。使用连字符可指定 VLAN 标记范围。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖 (Allow Overrides)** 复选框；请参阅允许对象覆盖，第 304 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 305 页。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

URL 对象

配置的每个 URL 对象代表单个 URL 或 IP 地址。您可在系统 Web 界面中的不同位置使用 URL 对象和对象组，包括访问控制策略和事件搜索。例如，可以编写阻止特定网站的访问控制规则。

在创建 URL 对象时，特别是如果未将 SSL 检查配置解密或阻止已加密的流量，请记住以下要点：

- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公用密钥中的主题公用名创建该对象。此外，系统会忽略在主题公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。
- 当使用包括URL条件的访问控制规则匹配网络流量时，系统会忽略加密协议（HTTP和HTTPS）。换句话说，如果阻止网站，将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个

应用条件细化该规则。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 `example.com` 而不是 `http://example.com/`。

创建 URL 对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择 **URL**。

步骤 3 从**添加 URL (Add URL)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 输入 **URL** 或 IP 地址。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖 (Allow Overrides)** 复选框；请参阅允许对象覆盖，第 304 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 305 页。

步骤 8 点击 **Save**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

地理位置对象

配置的每个地理定位对象代表系统识别为受监控网络上流量的源或目标的一个或多个国家/地区或大洲。可在系统网络界面中的不同位置使用地理定位对象，包括访问控制策略、SSL 策略和事件搜索。例如，可编写阻止流向或来自某些国家/地区的流量的访问控制规则。

要确保使用最新信息来过滤网络流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

创建地理位置对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**地理位置 (Geolocation)**。

步骤 3 点击 **Add Geolocation**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 选中要包括到地理定位对象中的国家/地区和大洲的相应复选框。选中大洲会选中该大洲的所有国家/地区，以及 GeoDB 更新将来可能添加到该大洲下的所有国家/地区。取消选中大洲下的任意国家/地区会取消选中该大洲。您可以选择国家/地区和大洲的任意组合。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

变量集

变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以在入侵策略中使用变量表示规则禁止、自适应配置文件和动态规则状态中的 IP 地址。

提示 无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。

可以使用变量集对变量进行管理、自定义和分组。可以使用系统提供的默认变量集，也可以创建您自己的自定义变量集。可以在任何变量集中修改预定义默认变量，以及添加和修改用户定义的变量。

Firepower 系统提供的大多数共享对象规则和标准文本规则均使用预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

当变量更准确地反映网络环境时，规则更加有效。至少应修改默认变量集中的的默认变量。通过确保变量（例如 $HOME_NET）正确地定义网络且 $HTTP_SERVERS 包括网络上的所有网络服务器，从而优化处理和监控所有相关系统的可疑活动。

要使用变量，请将变量集链接到与访问控制规则相关的入侵策略或访问控制策略的默认操作。默认情况下，默认设置集链接到访问控制策略使用的所有入侵策略。

将一个变量添加到任意变量集会将其添加到所有变量集；也就是说，每个变量集都是系统中当前配置的所有变量的集合。在任何变量集中，都可以添加用户定义的变量以及自定义任何变量的值。

最初，Firepower 系统提供由预定义默认值组成的单个默认变量集。默认变量集中的每个变量最初设置为其默认值，对于预定义变量，该默认值是由Cisco Talos 安全情报和研究小组 (Talos) 设置并在规则更新中提供的值。

虽然可以将预定义默认变量保留为所配置的默认值，但思科建议您修改预定义变量的子集。

可以仅使用默认变量集中的变量，但在许多情况下，执行以下操作可得到最大益处：添加一个或多个自定义变量集；在不同变量集中配置不同的变量值；甚至添加新变量。

使用多个变量集时务必谨记，默认变量集中任何变量的当前值决定所有其他变量集中该变量的默认值。

如果选择“对象管理器”(Object Management) 页面上的**变量集 (Variable Sets)**，则对象管理器会列出默认变量集以及您创建的任何自定义变量集。

在全新安装的系统上，默认变量集仅由思科预定义的默认变量组成。

每个变量集都包括系统提供的默认变量以及从任何变量集添加的所有自定义变量。请注意，可以编辑默认变量集，但不能重命名或删除默认变量集。

在多域部署中，系统会为每个子域生成默认变量集。

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

入侵策略中的变量集

默认情况下，Firepower 系统会将默认变量集链接到访问控制策略中使用的所有入侵策略。部署使用入侵策略的访问控制策略时，入侵策略中已启用的入侵规则将使用已链接变量集中的变量值。

修改访问控制策略中的入侵策略所使用的自定义变量集时，系统会反映该策略的状态，在 Access Control 页面上将其状态显示为过时。必须重新部署该访问控制策略，才能使变量集的更改生效。修改默认变量集时，系统会将使用入侵策略的所有访问控制策略的状态显示为过时，因此，必须重新部署所有访问控制策略才能使更改生效。

变量

变量属于以下类别之一：

默认变量

Firepower 系统提供的变量。不能重命名或删除默认变量，也不能更改其默认值。但是，可以创建默认变量的自定义版本。

自定义变量

您创建的变量。这些变量可包括：

- 自定义的默认变量

  编辑默认变量的值时，系统会将该变量从 Default Variables 区域转移到 Customized Variables 区域。由于默认变量集中的变量值决定自定义变量集中变量的默认值，因此，自定义默认变量集中的默认变量会修改所有其他变量集中该变量的默认值。

- 用户定义的变量

  您可以添加和删除自己的变量，在不同变量集中自定义这些变量的值，以及将自定义变量重置为默认值。重置用户定义的变量时，该变量保留在 Customized Variables 区域。

  用户定义的变量可以是以下类型之一：

  网络变量指定网络流量中的主机的 IP 地址。

  端口变量指定网络流量中的 TCP 或 UDP 端口，包括这两种端口类型的值 `any`。

例如，如果您创建自定义标准文本规则，您可能还希望添加自己的用户定义的变量，以便更准确地反映流量或作为快捷方式简化规则创建过程。或者，如果创建只检查“隔离区”(DMZ) 中流量的规则，可以创建名为 `$DMZ` 的变量，其值列出已暴露的服务器 IP 地址。这样，在所有为该区域编写的所有规则中都可以使用 `$DMZ` 变量。

高级变量

Firepower 系统在特定情况下提供的变量。这些变量的部署非常有限。

预定义默认变量

默认情况下，Firepower 系统提供一个由预定义默认变量组成的默认变量集。Cisco Talos 安全情报和研究小组 (Talos) 使用规则更新来提供新的和已更新的入侵规则及其他入侵策略元素，包括默认变量。

由于系统提供的许多入侵规则使用预定义默认变量，因此应为这些变量设置适当的值。可以在任何或所有变量集中修改这些默认变量的值，具体取决于如何使用变量集识别网络流量。

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

下表介绍系统提供的变量并指示通常会修改哪些变量。要获得为网络定制自定义变量方面的帮助，请联系专业服务或支持部门。

表 *46*：系统提供的变量

变量名称	说明	是否需要修改？
$AIM_SERVERS	定义已知的 AOL Instant Messenger (AIM) 服务器，并用于基于聊天的规则和查找 AIM 漏洞攻击的规则。	不需要。
$DNS_SERVERS	定义域名服务 (DNS) 服务器。如果创建专门影响 DNS 服务器的规则，可以使用 $DNS_SERVERS 变量作为目标或源 IP 地址。	在当前规则集中不需要。
$EXTERNAL_NET	定义 Firepower 系统视为未受保护的网络，并在许多规则中用于定义外部网络。	需要；应该充分定义 $HOME_NET，然后避免将 $HOME_NET 作为 $EXTERNAL_NET 的值。
$FILE_DATA_PORTS	定义非加密端口，用于检测网络数据流中的文件的入侵规则。	不需要。
$FTP_PORTS	定义网络上 FTP 服务器的端口，用于 FTP 服务器漏洞攻击规则。	如果 FTP 服务器使用除默认端口以外的端口，需要修改（可以在网络界面中查看默认端口）。
$GTP_PORTS	定义数据包解码器用于提取 GTP（通用分组无线业务 [GPRS] 隧道协议）PDU 中的负载的数据信道端口。	不需要。
$HOME_NET	定义相关入侵策略监控的网络，用于许多定义内部网络的规则。	需要，以便包括内部网络的 IP 地址。
$HTTP_PORTS	定义网络上 FTP 服务器的端口，用于网络服务器漏洞攻击规则。	如果网络服务器使用除默认端口以外的端口，需要修改（可以在网络界面中查看默认端口）。
$HTTP_SERVERS	定义网络上的网络服务器。用于网络服务器漏洞攻击规则。	如果运行 HTTP 服务器，需要修改。
$ORACLE_PORTS	定义网络上的 Oracle 数据库服务器端口，用于扫描针对 Oracle 数据库的攻击的规则。	如果运行 Oracle 服务器，需要修改。
$SHELLCODE_PORTS	定义希望系统对其扫描外壳代码漏洞的端口，用于检测使用外壳代码的漏洞的规则。	不需要。
$SIP_PORTS	定义网络上 SIP 服务器的端口，用于 SIP 漏洞攻击规则。	不需要。
$SIP_SERVERS	定义网络上的 SIP 服务器，用于针对 SIP 的漏洞攻击的规则。	需要；如果运行 SIP 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SIP_SERVERS 的值。

变量名称	说明	是否需要修改？
$SMTP_SERVERS	定义网络上的 SMTP 服务器，用于解决针对邮件服务器的漏洞的规则。	如果运行 SMTP 服务器，需要修改。
$SNMP_SERVERS	定义网络上的 SNMP 服务器，用于扫描针对 SNMP 服务器的攻击的规则。	如果运行 SNMP 服务器，需要修改。
$SNORT_BPF	识别传统高级变量，仅在 V5.3.0 之前的 Firepower 系统软件版本（后来升级到 V5.3.0 或更高版本）中的系统上存在该变量时，才会显示该变量。	不需要，只能查看或删除此变量。删除此变量后不能对其进行编辑或恢复。
$SQL_SERVERS	定义网络上的数据库服务器，用于解决针对数据库的漏洞的规则。	如果运行 SQL 服务器，需要修改。
$SSH_PORTS	定义网络上 SSH 服务器的端口，用于 SSH 服务器漏洞规则。	如果 SSH 服务器使用除默认端口以外的端口，需要修改（可以在网络界面中查看默认端口）。
$SSH_SERVERS	定义网络上的 SSH 服务器，用于解决针对 SSH 的漏洞的规则。	需要修改；如果运行 SSH 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SSH_SERVERS 的值。
$TELNET_SERVERS	定义网络上的已知 Telnet 服务器，用于解决针对 Telnet 的漏洞的规则。	如果运行 Telnet 服务器，需要修改。
$USER_CONF	提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。 存在冲突或重复的 $USER_CONF 配置会导致系统停止。	不需要，除非功能描述中有指示或在支持人员的指导下进行。

网络变量

网络变量代表可在已在入侵策略、入侵策略规则抑制、动态规则状态和自适应配置文件中启用的入侵规则中使用的 IP 地址。网络变量与网络对象和网络对象组的不同之处在于，网络变量特定于入侵策略和入侵规则，但可以使用网络对象和网络对象组在系统网络界面中的不同位置（包括访问控制策略、网络变量、入侵规则、网络发现规则、事件搜索和报告等）来代表 IP 地址。

可在以下配置中使用网络变量来指定网络上主机的 IP 地址：

- 入侵规则 - 通过入侵规则**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 报头字段，您可以将数据包检测限于源自或发往特定 IP 地址的数据包。
- 抑制 - 在特定 IP 地址或某个范围的 IP 地址触发入侵规则或预处理器时，通过源或目标入侵规则抑制中的**网络 (Network)** 字段，您可以抑制入侵事件通知。

- 动态规则状态 - 通过源或目标动态规则状态中的**网络 (Network)** 字段，您可以检测在给定时间段内出现入侵规则或预处理器规则的过多匹配项的情况。
- 自适应配置文件 - 自适应配置文件**网络 (Networks)** 字段识别您希望在其中改进被动部署中的数据包分段和 TCP 流的重组的主机。

在本节中所述字段中使用变量时，链接至入侵策略的变量集决定使用该入侵策略的访问控制策略处理的网络流量中的变量值。

可以将以下网络配置的任意组合添加到变量：

- 从可用网络列表中选择的网络变量、网络对象和网络对象组的任意组合
- 从 New Variable 或 Edit Variable 页面添加的单个网络对象（这些对象随后可添加到变量以及其他现有和将来的变量）
- 文字的、单个 IP 地址或地址块

  可以通过逐个添加来列出多个文字 IP 地址和地址块。可以单独列出 IPv4 和 IPv6 地址以及地址块，或者列出它们的任意组合。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在任何变量中添加的包含网络的默认值是单词 `any`，它表示任意 IPv4 或 IPv6 地址。已排除网络的默认值为 `none`，它表示无网络。还可以使用文字值指定地址 `::`，以指示包含网络列表中的任何 IPv6 地址，或排除列表中没有 IPv6 地址。

将网络添加到排除列表会使指定的地址和地址块无效。也就是说，可以匹配除了被排除的 IP 地址或地址块以外的所有 IP 地址。

例如，排除文字地址 `192.168.1.1` 会指定除 192.168.1.1 以外的所有 IP 地址，排除 `2001:db8:ca2e::fa4c` 会指定除 2001:db8:ca2e::fa4c 以外的所有 IP 地址。

使用文字网络或可用网络可以排除任意的网络组合。例如，排除文字值 `192.168.1.1` 和 `192.168.1.5` 会包含除 192.168.1.1 或 192.168.1.5 以外的任何 IP 地址。也就是说，系统将此解释为“**既不是** 192.168.1.1 **也不是** 192.168.1.5”，这就会匹配除括号中列出的 IP 地址以外的所有 IP 地址。

添加或编辑网络变量时，请注意以下几点：

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无地址。例如，不能将具有值 `any` 的变量添加到排除网络列表。
- 网络变量为指定的入侵规则和入侵策略功能识别流量。请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。
- 排除值必须解析为包含值的子集。例如，不能包含地址块 192.168.5.0/24 并排除 192.168.6.0/24。

端口变量

端口变量代表可在入侵策略中启用的入侵规则的 **Source Port** 和 **Destination Port** 报头字段中使用的 TCP 和 UDP 端口。端口变量与端口对象和端口对象组的不同之处在于，端口变量特定于入侵规则。可以为除 TCP 和 UDP 以外的其他协议创建端口对象，还可以在系统网络界面中的不同位置使用端口对象，包括端口变量、访问控制策略、网络发现规则和事件搜索。

可以在入侵规则 **Source Port** 和 **Destination Port** 报头字段中使用端口变量来限制仅检查来自或发往特定 TCP 或 UDP 端口的数据包。

在这些字段中使用变量时，链接到与访问控制规则或策略相关的入侵策略的变量集决定部署访问控制策略的网络流量中这些变量的值。

可以将以下端口配置的任意组合添加到变量：

- 从可用端口列表中选择的端口变量和端口对象的任意组合

  请注意，可用端口列表不显示端口对象组，而且不能将这些对象组添加到变量。

- 从 New Variable 或 Edit Variable 页面添加的单个端口对象（这些对象随后可添加到变量以及其他现有和将来的变量）

  仅 TCP 和 UDP 端口（包括两种端口类型的值 `any`）是有效的变量值。如果使用新建或编辑变量页面添加不是有效变量值的有效端口对象，对象将被添加到系统，但不会显示在可用对象列表中。使用对象管理器编辑用于变量的端口对象时，只能将其值更改为有效的变量值。

- 单个文本端口值和端口范围

  必须使用破折号 (-) 隔开端口范围。带有冒号 (:) 的端口范围表示具有向后兼容性，但不能在创建的端口变量中使用冒号。

  可以通过逐个添加来列出多个文本端口值的任意组合。

添加或编辑端口变量时，请注意以下几点：

- 在任何变量中添加的包含端口的默认值是单词 `any`，它表示任意端口或端口范围。排除端口的默认值为 `none`，它表示无端口。

  提示 要创建一个值为 `any` 的变量，请在不添加具体值的情况下命名并保存该变量。

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无端口。例如，将具有值 `any` 的变量添加到排除端口列表时，无法保存变量集。
- 将端口添加到排除列表会使指定端口和端口范围失效。也就是说，可以匹配除了被排除的端口或端口范围以外的所有端口。
- 排除值必须解析为包含值的子集。例如，不能包含端口范围 10-50 并排除端口 60。

高级变量

高级变量让您能够配置通常无法通过网络界面配置的功能。Firepower 系统当前只提供两个高级变量，并且您只能编辑 USER_CONF 高级变量。

USER_CONF

USER_CONF 提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。

注意 请**勿**使用高级变量USER_CONF来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

编辑 USER_CONF 时，可以在单行中最多输入总共 4096 个字符；达到该限制后，行会自动换行。可以包含任意数量的有效说明或行，直至达到变量的最大字符长度限制（8192 个字符）或物理限制（例如磁盘空间）。在命令指令中，可以在任何完整参数之后使用反斜杠 (\) 续行符。

重置 USER_CONF 会将其清空。

SNORT_BPF

SNORT_BPF 是传统高级变量，仅当在 V5.3.0（后来升级到 V5.3.0 或更高版本）之前的 Firepower 系统软件版本中的系统上进行了配置时，才会显示该变量。只能查看或删除此变量。删除此变量后不能对其进行编辑或恢复。

借助此变量，可以在流量到达系统之前对流量应用 Berkeley 数据包过滤器 (BPF)。如果 SNORT_BPF 提供访问控制规则，应使用这些规则而不是此变量来强制执行过滤。此变量仅出现在系统升级之前存在的配置中。

变量重置

在变量集新建或编辑变量页面上，可以将变量重置为默认值。下表总结了重置变量的基本原则。

表 *47*: 变量重置值

要重置的变量类型	所属变量集类型	重置后的值
default	default	规则更新值
用户定义的变量	default	`any`
默认变量或用户定义的变量	custom	当前默认变量集值（已修改或未修改）

重置自定义变量集中的变量会将其重置为该变量在默认变量集中的当前值。

相反，重置或修改默认变量集中某个变量的值总是会更新所有自定义变量集中该变量的默认值。如果重置图标呈灰色显示，表示不能重置变量，这意味着该变量在该变量集中没有自定义值。除非自定义了自定义变量集中某个变量的值，否则对默认变量集中该变量的更改会更新与该变量集链接的任何入侵策略中使用的值。

注释 理想做法是修改默认变量集中的某个变量，以评估这些更改如何影响使用链接自定义变量集中的该变量的任何入侵策略，尤其是在尚未定制自定义变量集中的变量值时。

将指针悬停在变量集中的重置图标(↩)上可查看重置值。当自定义值和重置值相同时，这表示以下其中一种情况属实：

- 您在自定义或默认变量集中，而且在其中添加了值为 any 的变量
- 您在自定义变量集中，在其中添加了具有显式值的变量，并且选择了使用配置值作为默认值

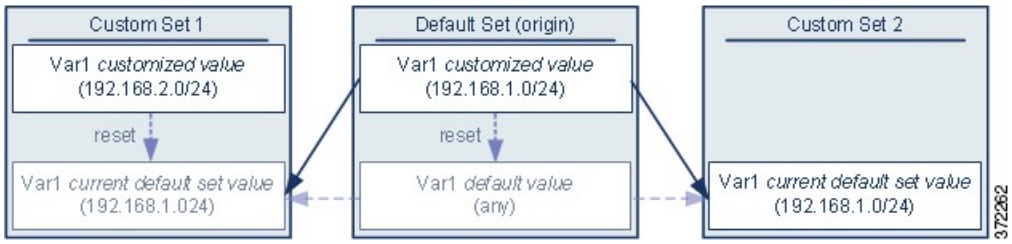
将变量添加到变量集

将变量添加到变量集会将其添加到所有其他变量集。添加自定义变量集中的变量时，必须选择是否使用配置值作为默认变量集中的自定义值：

- 如果**使用**配置的值（例如，192.168.0.0/16），变量添加到默认变量集时，将会使用配置值作为自定义值，且默认值为 any。由于默认变量集中的当前值决定在其他变量集中的默认值，因此，其他自定义变量集中的初始默认值为配置值（在本示例中为 192.168.0.0/16）。
- 如果**不使用**配置值，变量添加到默认变量集时，只会使用默认值 any，因此，其他自定义变量集中的初始默认值为 any。

示例：将用户定义变量添加到默认变量集

下图说明了将用户定义的变量 Var1（其值为 192.168.1.0/24）添加到默认变量集时发生的变量集交互。



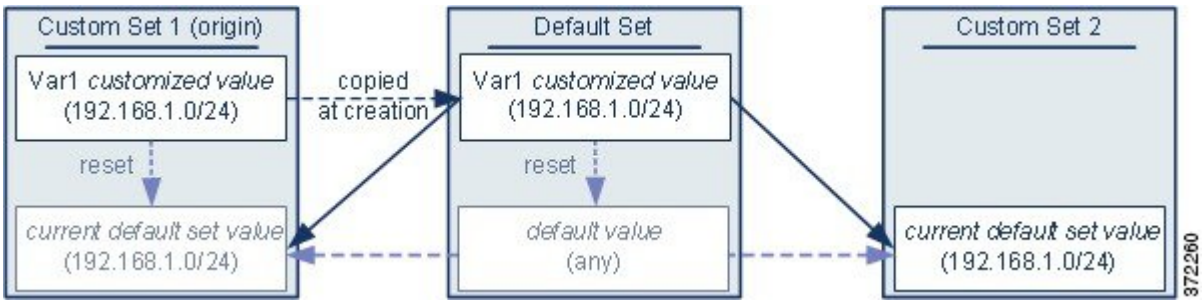
您可以在任何变量集中自定义 Var1 的值。在未自定义 Var1 的自定义变量集 2 中，此变量的值是 192.168.1.0/24。在自定义变量集 1 中，Var1 的自定义值 192.168.2.0/24 覆盖了默认值。重置默认变量集中某个用户定义的变量会将所有变量集中该变量的默认值重置为 any。

须注意的一点是，在本示例中，如果不更新自定义变量集 2 中的 Var1，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

请注意，虽然在本示例中未显示，但用户定义的变量和默认变量的变量集交互是相同的，唯一不同的是重置默认变量集中的默认变量会在当前规则更新中将其值重置为由思科配置的值。

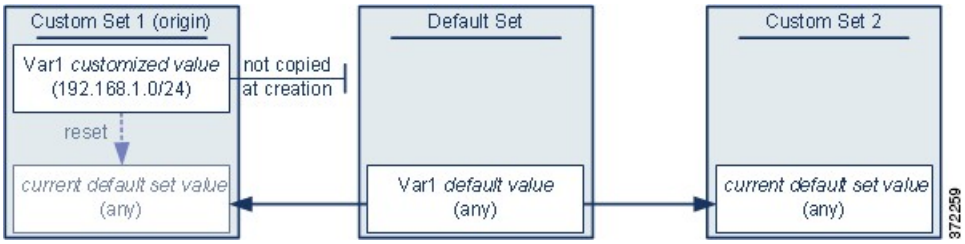
示例：将用户定义变量添加到自定义变量集

以下两个示例说明了将用户定义的变量添加到自定义变量集时变量集之间的交互。保存新变量时，系统会提示您选择是否将配置值用作其他变量集的默认值。在以下示例中，您选择**使用**配置值。



请注意，除了 Var1 来自自定义变量集 1 以外，本示例与以上将 Var1 添加到默认变量集的示例完全相同。将 Var1 的自定义值 192.168.1.0/24 添加到自定义变量集 1 会将该值复制到默认变量集，以作为默认值为 any 的自定义值。之后，Var1 值和交互就像之前将 Var1 添加到默认变量集一样。请记住，与前一个示例一样，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

在下一个示例中，像前一个示例一样，将 Var1（其值为 192.168.1.0/24）添加到自定义变量集 1，但选择**不使用** Var1 的配置值作为其他变量集中的默认值。



此方法会将 Var1（其默认值为 any）添加到所有变量集。添加 Var1 后，可以在任何变量集中自定义它的值。此方法的优点是，通过最初不在默认变量集中自定义 Var1，可以降低这样的风险：在默认变量集中自定义此变量的值时，无意中更改了尚未自定义 Var1 的变量集（例如，自定义变量集 2）中的当前值。

管理变量集

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 管理变量集：

- 添加 - 如果要添加自定义变量集，请点击**添加变量集 (Add Variable Set)**；请参阅创建变量集，第 323 页。
- 删除 - 如果要删除自定义变量集，请点击变量集旁边的删除图标 ( )，然后点击**是 (Yes)**。不能删除默认变量集或属于祖先域的变量集。

  注释 在删除的变量集中创建的变量不会被删除或以其他方式在其他集合中受影响。
- 编辑 - 如果要编辑变量集，请点击要修改的变量集旁边的编辑图标 ( )；请参阅编辑对象，第 299 页。
- 过滤 - 如果要按名称过滤变量集，请开始输入名称；当您键入时，页面会刷新以显示匹配的名称。如果要清除名称过滤，请点击过滤器字段中的清除图标 ( )。
- 管理变量 - 要管理变量集中包含的变量，请参阅管理变量，第 324 页。

创建变量集

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 点击**添加变量集 (Add Variable Set)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 管理变量集中的变量；请参阅管理变量，第 324 页。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

管理变量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**变量集 (Variable Set)**。

步骤 3 点击要编辑的变量集旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 管理变量：

- 显示 - 如果要显示变量的完整值，请将指针悬停在变量旁边的**值 (Value)** 列中的值上方。
- 添加 - 如果要添加变量，请点击**添加 (Add)**；请参阅添加变量，第 325 页。
- 删除 - 点击变量旁边的删除图标 ()。如果自添加变量后已保存变量集，请点击**是 (Yes)** 以确认是否要删除变量。

  不能删除以下变量：

  默认变量

  入侵规则或其他变量所使用的用户定义的变量

  属于祖先域的变量

- 编辑 - 点击要编辑的变量旁边的编辑图标 ()；请参阅编辑变量，第 326 页。

- 重置 - 如果要将已修改变量重置为其默认值，请点击已修改变量旁边的重置图标 ()。如果重置图标呈灰色显示，则表明以下情况之一成立：

  当前值已是默认值。

  配置属于祖先域。

  提示 将指针悬停在活动的重置图标上可显示默认值。

步骤 5 点击**保存 (Save)** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。
由于默认变量集中的当前值决定所有其他变量集中的默认值，因此，修改或重置默认变量集中的变量会更改未对该变量默认值进行自定义的那些变量集中的该变量当前值。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

添加变量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在变量集编辑器中，点击**添加 (Add)**。

步骤 2 在 **Name** 字段中为变量输入一个唯一名称。

步骤 3 从**类型 (Type)** 下拉列表中，选择**网络 (Network)** 或**端口 (Port)**。

步骤 4 为变量指定值：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示 如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符 (-) 隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。

- 如果要从包含或排除列表中删除项目，请点击该项目旁边的删除图标 ()。

注释　要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 5　点击 **Save** 保存变量。如果是添加自定义变量集中的新变量，有以下选项可供选择：

- 点击 **Yes** 添加使用配置值作为默认变量集中的自定义值（进而也是其他自定义变量集中的默认值）的变量。
- 点击**否 (No)** 将变量添加为默认变量集中的默认值 `any`（进而在其他自定义变量集中也使用此默认值）。

步骤 6　点击**保存 (Save)** 以保存变量集。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

编辑变量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以同时编辑自定义变量和默认变量。

无法更改现有变量中的**名称 (Name)** 或**类型 (Type)** 值。

过程

步骤 1　在变量集编辑器中，点击要修改的变量旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 2　修改变量：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示　如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符 (-) 隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的删除图标 。

注释 要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 3 点击 **Save** 保存变量。

步骤 4 点击**保存 (Save)** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

安全情报列表和源

安全情报列表和源（统称为安全情报对象）可帮助您配置安全情报。每个列表或源都是要将其加入黑名单（立即阻止）或白名单（允许通过以进行深入分析）的 IP 地址、URL 或域名的集合。

列表和源之间的主要差异如下：

- 列表 - 手动管理的静态集合。
- 源 - 通过 HTTP 或 HTTPS 按间隔更新的动态集合。

Lists

默认情况下，访问控制和 DNS 策略使用全局黑名单和白名单。**立即列入白名单 (Whitelist Now)** 和**立即列入黑名单 (Blacklist Now)** 操作允许您在无需重新部署的情况下构建和实施这些列表。请参阅立即列入黑名单 (Blacklist Now)、立即列入白名单 (Whitelist Now) 和全局列表 (Global Lists)，第 328 页。

您也可以配置自定义列表以增加和微调源和全局列表，但实施自定义列表需要重新部署。

源

思科提供对定期更新的用于根据最新威胁情报过滤网络流量的情报源的访问权限。您也可以使用第三方源。或者，利用自定义内部源，您可以在具有多个 Firepower 管理中心的大型部署中轻松维护企业级黑名单。系统更新源时，虽然更改可能需要几分钟时间才能完成传播，但您无需重新部署。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

注释 在下载自定义源时，系统不执行对等 SSL 证书验证，系统也不支持使用证书捆绑包或自签证书来验证远程对等设备。

格式化和已损坏源数据

源和列表源必须是大小不超过 500MB 的简单文本文件，其中每行一个 IP 地址、地址块、URL 或域名。每个源必须仅包含 IP 地址、URL 或域名。列表源文件必须使用 `.txt` 扩展名。

在 DNS 列表条目中，您可以为域标签指定星号 (`*`) 通配符。所有标签都与通配符匹配。例如，条目 `www.example.*` 与 `www.example.com` 和 `www.example.co` 均匹配。

如果在源文件中添加注释行，则其必须以井号 (`#`) 字符开头。如果上传具有注释的源文件，则系统会在上传期间删除注释。您下载的源文件包含不带注释的所有条目。

如果系统下载损坏的源或具有无法识别的条目的源，则系统会继续使用旧源数据（除非是第一次下载）。但是，如果系统可以识别即便源中的一个条目，也会使用其可识别的条目。

默认运行状况策略包括安全情报模块，该模块会在涉及安全情报过滤的一些情况中（包括系统无法更新源，或者源损坏或不包含可识别的条目）发出警报。

安全情报对象快速参考

对象类型	编辑功能	编辑后是否需要重新部署？
默认（但自定义填充）白名单和黑名单：全局、后代和特定域	使用上下文菜单添加条目。 使用对象管理器删除条目。	在添加条目之后需要。 在删除条目之后不需要。
自定义白名单和黑名单	使用对象管理器上传新列表和替代列表。	是
系统提供的情报源	使用对象管理器禁用或更改更新频率。	否
自定源	使用对象管理器进行全面修改。	否
Sinkhole	使用对象管理器进行全面修改。	是

立即列入黑名单 (Blacklist Now)、立即列入白名单 (Whitelist Now) 和全局列表 (Global Lists)

Firepower 管理中心上下文菜单（请参阅情景菜单，第 26 页）允许您通过安全情报将项目快速列入黑名单和白名单。例如，如果注意到入侵事件中的一组可路由 IP 地址涉及漏洞攻击尝试，可以立即将这些 IP 地址添加到黑名单。虽然更改可能需要几分钟时间才能完成传播，但您无需重新部署。

立即列入黑名单 (Blacklist Now) 和**立即列入白名单 (Whitelist Now)** 上下文菜单选项在 IP 地址、URL 和 DNS 请求热点上可用。通过上下文菜单列入黑名单或列入白名单可将所选项目添加到相应的默认全局列表。默认情况下，访问控制和 DNS 策略使用这些适用于所有安全区域的全局列表。您可以为每个策略选择不使用这些列表。

注释 这些选项仅适用于安全情报。安全情报无法将已使用快速路径的流量列入黑名单。同样，安全情报也不会自动将受信任或快速路径匹配流量列入白名单。有关详细信息，请参阅安全情报基础知识，第 651 页。

上下文菜单选项	目标项目	受影响的全局列表
立即列入黑名单 立即列入白名单	IP 地址	全局黑名单 全局白名单
立即将与 URL 的 HTTP/S 连接列入黑名单 立即将与 URL 的 HTTP/S 连接列入白名单	URL	URL 的全局黑名单 URL 的全局白名单
立即将与域的 HTTP/S 连接列入黑名单 立即将与域的 HTTP/S 连接列入白名单	整个域	URL 的全局黑名单 URL 的全局白名单
立即将对域的 DNS 请求列入黑名单 立即将对域的 DNS 请求列入白名单	整个域的 DNS 请求	DNS 的全局黑名单 DNS 的全局白名单

在多域部署中，可以选择要通过向域列表和全局列表添加项目来实施列入黑名单或白名单操作的 Firepower 系统域；请参阅安全情报列表和多租户，第 329 页。

由于将条目添加到安全情报列表会影响访问控制，因此必须具有以下其中一种权限或角色：

- 管理员访问权限
- 默认角色的组合：网络管理员或访问管理员，加上安全分析师和安全审批人
- 同时具有“修改访问控制策略”(Modify Access Control Policy) 和“将配置部署到设备”(Deploy Configuration to Devices) 权限的自定义角色

安全情报列表和多租户

在多域部署中，全局域拥有全局黑名单和白名单。只有全局管理员才可以在全局列表中添加或删除项目。因此，子域用户可以将网络、域名和 URL 列入白名单和黑名单，多租户则添加：

- 域列表 - 内容只适用于特定子域的白名单或黑名单。全局列表是全局域的域列表。
- 后代域列表 - 汇聚当前域的后代的域列表的白名单或黑名单。

域列表

除了能够访问（但不能编辑）全局列表之外，每个子域都具有自己的命名列表，命名列表的内容只应用于该子域。例如，名为 Company A 的子域拥有：

- 域黑名单 - Company A 与域白名单 - Company A
- DNS 的域黑名单 - Company A，DNS 的域白名单 - Company A
- URL 的域黑名单 - Company A，URL 的域白名单 - Company A

当前或以上域中的任何管理员都可以填充这些列表。您可以用情景菜单将当前及所有后代域中的项目列入白名单或黑名单。但只有关联域中的管理员可以删除域列表中的项目。

例如，全局管理员可以选择将全局域和 Company A 的域中的相同 IP 地址列入黑名单，但不能在 Company B 的域中将其列入黑名单。此操作会将 IP 地址添加到：

- 全局黑名单（只有全局管理员可以将其删除）
- 域黑名单 - Company A（只有 Company A 管理员可以将其删除）

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

后代域列表

后代域列表是汇聚当前域的后代的域列表的白名单或黑名单。枝叶域没有后代域列表。

后代域列表很有用，因为较高级别的域管理员可以执行通用安全情报设置，但仍允许子域用户将其自己部署中的项目列入黑名单和白名单。

例如，全局域具有以下后代域列表：

- 后代黑名单 - 全局，后代白名单 - 全局
- URL 的后代黑名单 - 全局，URL 的后代白名单 - 全局
- URL 的后代黑名单 - 全局，URL 的后代白名单 - 全局

注释 后代域列表不显示在对象管理器中，因为它们是象征性汇聚，不是手动填写列表。它们显示在您可以使用它们的位置：访问控制策略和 DNS 策略。

更改安全情报源的更新频率

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

虽然不能删除系统提供的源，但可以更改其更新频率（或禁用更新）。默认情况下，各个源每两小时更新一次。

在多域部署中，系统提供的源属于全局域，并且只能由该域中的管理员进行修改。您可以修改属于您的域的自定义源的更新频率。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择要更改其频率的源类型。

步骤 3 在要更新的源旁边，点击编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 编辑 **Update Frequency**。

步骤 5 点击**保存 (Save)**。

自定义安全情报源

自定义或第三方安全情报源允许您使用互联网上其他定期更新且信誉良好的白名单和黑名单来扩充系统提供的情报源。也可以设置内部源；如果要使用一个源列表来更新部署中的多个Firepower管理中心，这将会很有用。

注释 您无法在安全情报源中使用 `/0` 网络掩码将地址块添加到白名单或黑名单。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 `any`。

配置源时，可使用 URL 指定位置；但 URL 不能使用 Punycode 编码。默认情况下，系统按配置的间隔下载整个源，然后自动更新其受管设备。

您也可以将系统配置为使用 md5 校验和来确定是否下载更新的源。如果校验和自上次系统下载源以来没有更改，则系统无需重新下载该源。您可能希望将 md5 校验和用于内部源，尤其是那些很大的内部源。md5 校验和必须存储在仅带有该校验和的简单文本文件中。不支持注释。

手动更新安全情报源会更新所有源，包括情报源。

创建安全情报源

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择要添加的源类型。

步骤 3 点击适合您在上方所选源类型的选项：

- **添加网络列表和源**
- **添加 DNS 列表和源 (Add DNS Lists and Feeds)**
- **添加 URL 列表和源 (Add URL Lists and Feeds)**

步骤 4 为源输入**名称 (Name)**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**类型 (Type)** 下拉列表中选择**源 (Feed)**。

步骤 6 输入**源 URL (Feed URL)**。

步骤 7 或者，输入 **MD5 URL**。

步骤 8 选择**更新频率 (Update Frequency)**。

步骤 9 点击**保存 (Save)**。
除非已禁用源更新，否则系统会尝试下载并验证源。

手动更新安全情报源

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（安全情报）	保护（安全情报）	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择源类型。

步骤 3 点击**更新源 (Update Feeds)**，然后确认。

步骤 4 点击 **OK**。

Firepower管理中心下载和验证源更新后，会将任何更改通知其受管设备。您的部署开始使用更新的源过滤流量。

自定义安全情报列表

安全情报列表是手动上传到系统的IP地址和地址块、URL或域名的简单静态列表。如果要扩充和微调单个Firepower 管理中心的受管设备的源或其中一个全局列表，自定义列表很有用。

例如，如果信誉良好的源错误地阻止对重要资源的访问，但整体来说对组织有用，您即可创建仅包含分类不当的 IP 地址的自定义白名单，而不是从访问控制策略的黑名单中删除 IP 地址源对象。

注释 您不能通过在安全情报列表中使用 `/0` 网络掩码，将地址块列入白名单或黑名单。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 `any`。

有关列表条目格式，请注意以下事项：

- 地址块的网络掩码可以是 `0` 到 `32` 之间或 `0` 到 `128` 之间的整数（分别适用于 IPv4 和 IPv6）。
- 域名中的 Unicode 必须使用 punycode 格式进行编码，并且不区分大小写。
- 域名中的字符不区分大小写。
- URL 中的 Unicode 应使用百分比编码格式进行编码。
- URL 子目录中的字符区分大小写。
- 以井号 (`#`) 开头的列表条目被视为注释。

有关匹配的列表条目，请注意以下事项：

- 如果在 URL 或 DNS 列表中存在较高级别的域，则系统与子级别域匹配。例如，如果将 `example.com` 添加到 DNS 列表，则系统与 `www.example.com` 和 `test.example.com` 均匹配。
- 系统不对 DNS 或 URL 列表条目执行 DNS 查找（正向或反向）。例如，如果向 URL 列表中添加 `http://192.168.0.2`，并且其解析为 `http://www.example.com`，则系统仅与 `http://192.168.0.2` 匹配，而与 `http://www.example.com` 不匹配。
- 如果向 URL 列表中添加以正斜杠 (/) 字符结尾的 URL，则只有精确的 URL 才与该条目匹配。
- 如果向 URL 或 DNS 列表中添加不是以正斜杠结尾的 URL，则共享同一通用前缀的任何 URL 都与该条目匹配。例如，如果向URL列表中添加 `www.example.com`，则系统与 `www.example.com` 和 `www.example.com/example` 均匹配。

将新的安全情报列表上传到 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

要修改安全情报列表，必须更改源文件并上传新副本。不能使用 Web 界面来修改文件内容。如果您无法访问源文件，可以从系统下载副本。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择列表类型。

步骤 3 点击适合您在上方所选列表的选项：

- **添加网络列表和源**
- **添加 DNS 列表和源 (Add DNS Lists and Feeds)**
- **添加 URL 列表和源 (Add URL Lists and Feeds)**

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**类型 (Type)** 下拉列表中，选择**列表 (List)**。

步骤 6 点击 **Browse** 浏览至列表 `.txt` 文件，然后点击 **Upload**。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

更新安全情报列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开**安全情报 (Security Intelligence)** 节点，然后选择列表类型。

步骤 3 在要更新的列表旁边，点击编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如果需要列表副本进行编辑，请点击 **Download**，然后按照浏览器的提示将列表保存为文本文件。

步骤 5 根据需要对列表进行更改。

步骤 6 在 Security Intelligence 弹出窗口中，点击 **Browse** 浏览到修改后的列表，然后点击 **Upload**。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

Sinkhole 对象

Sinkhole 对象代表为 Sinkhole 中所有域名提供非可路由地址的 DNS 服务器或没有解析到服务器的 IP 地址。您可以在 DNS 策略规则中引用 Sinkhole 对象，以将匹配流量重定向到 Sinkhole。您必须为对象同时分配 IPv4 地址和 IPv6 地址。

创建 Sinkhole 对象

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择 **Sinkhole**。

步骤 3 点击**添加 Sinkhole (Add Sinkhole)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入 Sinkhole 的 **IPv4 地址 (IPv4 Address)**和 **IPv6 地址 (IPv6 Address)**。

步骤 6 您有以下选择：

- 如果要将流量重定向到 Sinkhole 服务器，请选择**记录与 Sinkhole 的连接 (Log Connections to Sinkhole)**。
- 如果要将流量重定向到非解析 IP 地址，请选择**阻止并记录与 Sinkhole 的连接 (Block and Log Connections to Sinkhole)**。

步骤 7 如果要将危害表现 (IoC) 类型分配给 Sinkhole，请从**类型 (Type)** 下拉列表中选择一种类型。

步骤 8 点击**保存 (Save)**。

文件列表

如果使用面向 Firepower 的 AMP，而 AMP 云错误地识别某个文件的处置情况，则您可以将该文件添加到文件列表，以便将来能够更好地检测该文件。这些文件使用 SHA-256 散列值进行指定。每个文件列表最多可以包含 10000 个唯一的 SHA-256 值。

文件列表有两种预定义类别：

干净的列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了干净处置情况。

自定义检测列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了恶意软件处置情况。

在多域部署中，将为每个域呈现一个干净的列表和自定义检测列表。在低层域中，您可以查看但无法修改祖先列表。

由于您手动指定这些列表中包含的文件的阻止行为，系统不会在 AMP 云中查询这些文件的处置情况。您必须配置文件策略中的规则（通过**恶意软件云查找 [Malware Cloud Lookup]** 或**阻止恶意软件 [Block Malware]** 操作）和匹配的文件类型才能计算文件的 SHA 值。

注意 请**勿**在干净的列表中包含恶意软件。干净的列表会覆盖 AMP 云和自定义检测列表。

文件列表的源文件

可通过上传包含 SHA-256 值和描述的列表的逗号分隔值 (CSV) 源文件将多个 SHA-256 值添加到文件列表。Firepower 管理中心会验证内容并使用有效 SHA-256 值填充文件列表。

源文件必须为具有 .csv 文件扩展名的简单文本文件。所有标题必须以井号 (#) 开头；标题将被视为注释，不会上传。每个条目都应包含一个 SHA-256 值，后跟说明并以 LF 或 CR+LF 换行字符结尾。系统将会忽略条目中的任何其他信息。

请注意以下几点：

- 从文件列表删除源文件也会从该文件列表删除所有相关的 SHA-256 哈希值。
- 如果成功上传源文件导致文件列表包含超过 10000 个不同的 SHA-256 值，则不能将多个文件上传到该文件列表。
- 上传时，系统会截去描述中超过 256 个字符的字符，仅保留前 256 个字符。如果描述包括逗号，必须使用转义字符 (\,)。如果未包含描述，将会改为使用源文件名。
- 所有非重复的 SHA-256 值都将被添加到文件列表。如果文件列表包含 SHA-256 值，并且上传了包括该值的源文件，新上传的值不会修改现有 SHA-256 值。查看与 SHA-256 值相关的捕获的文件、文件事件或恶意软件事件时，所有威胁名称或描述都来源于单个 SHA-256 值。
- 系统不会在源文件中上传无效的 SHA-256 值。
- 如果多个上传的源文件包括相同 SHA-256 值的条目，系统将使用最新的值。
- 如果源文件包括相同 SHA-256 值的多个条目，系统将使用最后一个。
- 不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。
- 与源文件相关的条目数是指不同的 SHA-256 值的数量。如果从文件列表删除某个源文件，文件列表包含的 SHA-256 条目总数将会减少等于该源文件中有效条目的数量。

将单个 SHA-256 值添加到文件列表

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	Firepower	任意	管理员/网络管理员/访问管理员

可以提交文件的 SHA-256 值以将其添加到文件列表。不能添加重复的 SHA-256 值。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

开始之前

- 在事件视图中右键点击某个文件或恶意软件事件，在情景菜单中选择**显示全文 (Show Full Text)**，然后复制完整的 SHA-256 值以粘贴到列表中。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉列表中选择 `Enter SHA Value`。

步骤 5 在 **Description** 字段中输入源文件的描述。

步骤 6 在 **SHA-256** 字段中输入或粘贴文件的完整值。系统不支持匹配部分值。

步骤 7 点击 **Add**。

步骤 8 点击 **Save**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将单个文件上传到文件列表

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任何环境	任何环境	管理员/访问管理员/网络管理员

如果要将文件副本添加到文件列表，可以将文件上传到Firepower管理中心进行分析；系统会计算文件的SHA-256值并将文件添加到列表。系统不对用于SHA-256计算的文件大小强制实施任何限制。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择**计算 SHA (Calculate SHA)**。

步骤 5 或者，在 **Description** 字段中输入文件的描述。如果不输入描述，在上传时文件名将被用作描述。

步骤 6 点击**浏览 (Browse)**，然后选择要上传的文件。

步骤 7 点击**计算并添加 SHA (Calculate and Add SHA)**。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将源文件上传到文件列表

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 点击 **File List**。

步骤 3 点击要从源文件向其添加值的文件列表旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择 `List of SHAs`。

步骤 5 或者，在 **Description** 字段中输入源文件的描述。如果不输入描述，系统将会使用文件名。

步骤 6 点击**浏览 (Browse)** 浏览到源文件，然后点击**上传并添加列表 (Upload and Add List)**。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

注释 在部署策略后，系统不再查询 AMP 云以查找列表中的文件。

编辑文件列表中的 SHA-256 值

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任何环境	任何环境	管理员/访问管理员/网络管理员

可以编辑或删除文件列表中的各个 SHA-256 值。请注意，不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 点击 **File List**。

步骤 3 点击要修改文件的干净列表或自定义检测列表旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 您可以执行以下操作：

- 点击要更改的 SHA-256 值旁边的编辑图标 ( )，并根据需要修改 **SHA-256** 或**说明 (Description)** 值。
- 点击要删除的 SHA-256 值旁边的删除图标 ( )。

步骤 5 点击**保存 (Save)** 以更新列表中的文件条目。

步骤 6 点击**保存 (Save)** 以保存文件列表。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

从文件列表下载源文件

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任何环境	任何环境	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要下载源文件的干净列表或自定义检测列表旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 点击要下载的源文件旁边的视图图标 ( )。

步骤 5 点击 **Download SHA List** 并按照提示保存源文件。

步骤 6 点击 **Close**。

密码套件列表

密码套件列表是由多个密码套件组成的对象。每个预定义密码套件值代表用于协商 SSL 或 TLS 加密会话的一个密码套件。可以在 SSL 规则中使用密码套件和密码套件列表根据协商 SSL 会话的客户端和服务器是否使用该加密套件来控制加密流量。如果将密码套件列表添加到 SSL 规则，使用该列表中的任何密码套件协商的 SSL 会话都匹配该规则。

注释 虽然密码套件和密码套件列表在网络界面中可使用的位置相同，但不能添加、修改或删除密码套件。

创建密码套件列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 从对象类型列表中选择**密码套件列表 (Cipher Suite List)**。

步骤 3 点击 **Add Cipher Suites**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从**可用密码 (Available Ciphers)** 列表中选择一个或多个密码套件。

步骤 6 点击 **Add**。

步骤 7 或者，点击**所选密码 (Selected Ciphers)** 列表中要删除的任何密码套件旁边的删除图标 ( )。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

可分辨名称对象

每个可分辨名称对象代表所列出的公共密钥的使用者或颁发者的可分辨名称。您可在 SSL 规则中使用可分辨名称对象和对象组根据协商 SSL 会话的客户端和服务器是否使用将该可分辨名称作为使用者或颁发者的服务器证书来控制加密流量。

可分辨名称对象包含公用名属性 (**CN**)。如果添加不带“CN=”的公用名称，系统会在名称前面加上“CN=”，再保存对象。

还可以添加带有下表中列出的每个属性（用逗号隔开）的一个可分辨名称。

表 *48*: 可分辨名称属性

属性	说明	允许的值
选	国家/地区代码	两个字母字符

属性	说明	允许的值
CN	Common Name	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
O	Organization	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
OU	组织单位	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格

可以定义一个或多个星号 (*) 作为属性中的通配符。在公用名属性中，可以为每个域名标签定义一个或多个星号。通配符仅在该标签中匹配，不过，可以使用通配符定义多个标签。请参阅下表中的示例。

表 *49*：公用名属性通配符示例

属性	匹配	不匹配
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

创建可分辨名称对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开**可分辨名称 (Distinguished Name)** 节点，然后选择**单个对象 (Individual Objects)**。

步骤 3 点击 **Add Distinguished Name**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **DN** 字段中，输入可分辨名称或公用名的值。您有以下选择：

- 如果添加可分辨名称，则可包括可分辨名称对象，第342页中列出的每个属性（以逗号隔开）。
- 如果添加公用名，则可包括多个标签和通配符。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

PKI 对象

PKI 对象代表支持您的部署所需的公钥证书和配对的私钥。内部和可信 CA 对象包括证书颁发机构 (CA) 证书；内部 CA 对象还包括与证书配对的私有密钥。内部和外部证书对象包括服务器证书；内部证书对象还包括与证书配对的私有密钥。

如果使用可信证书颁发机构对象和内部证书对象来配置 ISE，则可与 ISE 建立连接以用作身份源。

如果使用内部证书对象来配置强制网络门户，在连接到用户的 Web 浏览器时，系统可验证强制网络门户设备的身份。

如果使用可信证书颁发机构对象来配置领域，则可配置与 LDAP 或 AD 服务器的安全连接。

如果在 SSL 规则中使用 PKI 对象，可以匹配使用以下证书加密的流量：

- 外部证书对象中的证书

- 由可信 CA 对象中的 CA 签名的证书或在 CA 的信任链中的证书

如果在 SSL 规则中使用 PKI 对象，可以解密：

- 传出流量（通过对带有内部 CA 对象的服务器证书进行重签）
- 传入流量（使用内部证书对象中的已知私有密钥）

可以手动输入证书和密钥信息，上传包含这些信息的文件，在某些情况下，还可以生成新的 CA 证书和私有密钥。

在对象管理器中查看 PKI 对象列表时，系统会将证书的使用者可分辨名称显示为对象值。将指针悬停在该值上可查看证书使用者的完整可分辨名称。要查看其他证书的详细信息，请编辑 PKI 对象。

注释 Firepower 管理中心和受管设备在保存存储在内部 CA 对象和内部证书对象中的所有私有密钥之前，会使用随机生成的密钥对它们进行加密。如果上传受密码保护的私有密钥，设备会使用用户提供的密码对该密钥进行解密，然后用随机生成的密钥对其重新加密，再进行保存。

内部证书颁发机构对象

配置的每个内部证书颁发机构 (CA) 对象代表组织控制的 CA 的 CA 公共密钥证书。此类对象由对象名称、CA 证书和配对私有密钥组成。您可以在 SSL 规则中使用内部 CA 对象和组通过使用内部 CA 对服务器证书进行重新签名来解密传出加密流量。

注释 如果在 **Decrypt - Resign** SSL 规则中引用内部 CA 对象，且该规则与加密会话相匹配，在协商 SSL 握手时，用户的浏览器可能会警告证书不可信。要避免此问题，请将内部 CA 对象证书添加到可信根证书的客户端或域列表。

可以通过以下方式创建内部 CA 对象：

- 导入现有基于 RSA 或基于椭圆曲线的 CA 证书和私有密钥
- 生成新的基于 RSA 的自签 CA 证书和私有密钥
- 生成未签名的基于 RSA 的 CA 证书和私有密钥。使用内部 CA 对象之前，必须向另一个 CA 提交证书签名请求 (CSR) 以对证书进行签名。

创建包含签名证书的内部 CA 对象后，可以下载 CA 证书和私有密钥。系统使用用户提供的密码对下载的证书和私有密钥进行加密。

无论是系统生成还是用户创建的内部 CA 对象名称，您都只能修改其名称，但不能修改其他对象属性。

不能删除正在使用的内部 CA 对象。此外，在编辑用于 SSL 策略的内部 CA 对象后，相关联的访问控制策略已过时。必须重新部署访问控制策略才能使更改生效。

CA 证书和私钥导入

可以通过导入 X.509 v3 RSA 证书和私有密钥来配置内部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果私有密钥文件受密码保护，您可以提供解密密码。如果证书和密钥采用PEM格式编码，还可以复制并粘贴信息。

只能上传包括适当的证书或密钥信息并且相互配对的文件。系统在保存对象之前会验证文件对。

注释 如果配置具有 **Decrypt - Resign** 操作的规则，除了任何配置的规则条件之外，该规则还根据引用的内部 CA 证书的加密算法类型匹配流量。例如，必须上传一个基于椭圆曲线的 CA 证书，以解密用基于椭圆曲线的算法进行加密的出站流量。

导入 CA 证书和私钥

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击 **Import CA**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

生成新的 CA 证书和私钥

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

可以通过提供识别信息生成基于 RSA 的自签 CA 证书和私有密钥来配置内部 CA 对象。

生成的 CA 证书有效期为十年。有效期起始日期为生成一周之前。

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击 **Generate CA**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入标识属性。

步骤 6 点击 **Generate self-signed CA**。

新签名证书

可以通过从 CA 获取签名证书来配置内部 CA 对象。这包括两个步骤：

- 提供识别信息以配置内部 CA 对象。这会生成未签名证书和配对私有密钥，并创建向您指定的 CA 发出的证书签名请求 (CSR)。
- 在 CA 颁发签名证书后，请上传证书到内部 CA 对象，用以替换未签名证书。

仅当内部 CA 对象包含签名证书时，才能在 SSL 规则中引用该对象。

创建未签名的 CA 证书和 CSR

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击 **Generate CA**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 输入标识属性。

步骤 6 点击 **Generate CSR**（生成 CSR）。

步骤 7 复制 CSR 以将其提交到 CA。

步骤 8 点击 **OK**。

接下来的操作

- 必须上传由 CA 颁发的签名证书，如 中所述 上传为响应 CSR 而颁发的签名证书，第 348 页

上传为响应 CSR 而颁发的签名证书

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

上传之后，签名证书可在 SSL 规则中引用。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击包含等待 CSR 的未签名证书的 CA 对象旁边的编辑图标 ( )。

步骤 4 点击 **Install Certificate**。

步骤 5 点击**浏览 (Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果上传的文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击**保存 (Save)** 以将签名证书上传到 CA 对象。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

CA 证书和私钥下载

可以通过下载包含内部CA对象中的证书和密钥信息的文件来备份或传输CA证书和配对私有密钥。

注意 系统始终将下载的密钥信息存储在安全的位置。

系统在保存密钥信息之前，会使用随机生成的密钥对存储在内部 CA 对象中的私有密钥进行加密。如果从内部 CA 下载证书和私有密钥，系统在创建包含证书和私有密钥信息的文件之前，会首先对这些信息进行解密。然后，您必须提供系统用于加密下载文件的密码。

注意 作为系统备份一部分下载的私有密钥将被解密，然后存储在未加密的备份文件中。

下载 CA 证书和私钥

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

可以同时为当前域和祖先域下载 CA 证书。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 在要下载其证书和私钥的内部 CA 对象旁边，点击编辑图标 ( )。

在多域部署中，点击查看图标 ( )，为祖先域中的对象下载证书和私钥。

步骤 4 点击**下载**。

步骤 5 在**密码 (Password)** 和**确认密码 (Confirm Password)** 字段中输入加密密码。

步骤 6 点击 **OK**。

受信任证书颁发机构对象

配置的每个受信任证书颁发机构 (CA) 对象代表属于受信任 CA 的 CA 公钥证书。此类对象由对象名称和 CA 公共密钥证书组成。您可以在以下位置使用外部 CA 对象和组：

- SSL 策略，用于控制使用由受信任 CA 或信任链中的任何 CA 签名的证书加密的流量。
- 领域配置，用于建立与 LDAP 或 AD 服务器的安全连接。
- ISE 集成配置，用于连接到 ISE。为 **pxGrid 服务器 CA (pxGrid Server CA)** 和 **MNT 服务器 CA (MNT Server CA)** 对象选择受信任证书颁发机构对象。

创建可信 CA 对象后，可以修改名称和添加证书撤销列表 (CRL)，但不能更改其他对象属性。可添加到对象的 CRL 数量没有限制。要修改已上传到对象的 CRL，必须删除并重新创建该对象。

注释 当在 ISE 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

不能删除正在使用的可信 CA 对象。此外，在编辑正在使用的受信任 CA 对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

受信任的 CA 对象

您可以通过上传 X.509 v3 CA 证书来配置外部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书采用PEM格式编码，还可以复制并粘贴信息。

仅当文件包含适当的证书信息时，才可以上传 CA 证书；系统在保存对象之前会对证书进行验证。

添加受信任 CA 对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击 **Add Trusted CAs**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 点击**浏览 (Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

受信任 CA 对象中的证书撤销列表

可以将 CRL 上传到可信 CA 对象。如果在 SSL 策略中引用上传的可信 CA 对象，可以根据颁发会话加密证书的 CA 随后是否会撤销证书来控制加密流量。可以上传采用下列其中一种受支持格式编码的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

添加CRL后，可以查看已撤销证书的列表。要修改已上传到对象的CRL，必须删除并重新创建该对象。

只能上传包含适当CRL的文件。可添加到可信CA对象的CRL数量没有限制。但是，每次上传CRL之后，必须先保存对象再添加另一个 CRL。

注释 当在 ISE 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

向受信任 CA 对象添加证书撤销列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的对象，您可以对其进行编辑。系统还会显示在祖先域中创建的对象，在大多数情况下您不可以对其进行编辑。要查看和编辑在后代域中的对象，请切换至该域。

注释 当在 ISE 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击可信 CA 对象旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击 **Add CRL** 上传 DER 或 PEM 编码的 CRL 文件。

步骤 5 点击 **OK**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

外部证书对象

配置的每个外部证书对象代表一个不属于组织的服务器公共密钥证书。此类对象由对象名称和证书组成。可以在 SSL 规则中使用外部证书对象和对象组来控制使用服务器证书加密的流量。例如，您可以上传您信任的自签服务器证书，但不能使用可信 CA 证书进行验证。

您可以通过上传 X.509 v3 服务器证书来配置外部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可区别编码规则 (DER)

- 隐私增强电子邮件 (PEM)

仅当文件包含适当的服务器证书信息时，才可以上传文件；系统在保存对象之前会对文件进行验证。如果证书采用 PEM 格式编码，还可以复制并粘贴信息。

添加外部证书对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**外部证书 (External Certs)**。

步骤 3 点击 **Add External Cert**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 254 页。

内部证书对象

配置的每个内部证书对象代表一个属于组织的服务器公共密钥证书。此类对象由对象名称、公共密钥证书和配对私有密钥组成。您可以在以下位置使用内部证书对象和组：

- SSL 规则，用于通过已知私钥解密传入到您的组织其中一台服务器的流量。
- ISE 集成配置，用于连接到 ISE。为 **MC 服务器证书 (MC Server Certificate)** 字段选择内部证书对象。
- 强制网络门户配置，用于在连接到用户的 Web 浏览器时对强制网络门户设备的身份进行身份验证。为**服务器证书 (Server Certificate)** 字段选择内部证书对象。

可以通过上传基于 X.509 v3 RSA 或基于椭圆曲线的服务器证书和配对的私有密钥来配置内部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可区别编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书和密钥采用PEM格式编码，还可以复制并粘贴信息。

只能上传包括适当的证书或密钥信息并且相互配对的文件。系统在保存对象之前会验证文件对。

创建内部证书对象后，可以修改其名称，但不能更改其他对象属性。

不能删除正在使用的内部证书对象。此外，在编辑正在使用的内部证书对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

添加内部证书对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**对象 (Objects)** > **对象管理 (Object Management)**。

步骤 2 展开 **PKI** 节点，然后选择**内部证书 (Internal Certs)**。

步骤 3 点击 **Add Internal Cert**。

步骤 4 输入 **Name**。
在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的私有密钥文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 8 点击**保存 (Save)**。

第 V 部分

设备管理基础

第 18 章

Firepower 管理中心基础知识

以下主题介绍 Firepower 管理中心基础知识：

Firepower 管理中心

可以使用 Firepower 管理中心管理组成 Firepower 系统的全套设备。管理设备时，会在Firepower 管理中心和设备之间设置双向、SSL 加密的通信信道。Firepower 管理中心使用此通道向设备发送有关要如何分析和管理流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到Firepower 管理中心。

设备管理

Firepower管理中心是Firepower系统中的关键组件。您可以使用Firepower管理中心管理组成Firepower系统的完整范围的设备，以及汇聚、分析和应对这些设备在网络中检测到的威胁。

通过使用Firepower 管理中心管理设备，可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向受管设备推送运行状况策略并从Firepower 管理中心监控其运行状态

Firepower管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用Firepower 管理中心管理设备行为的几乎每个方面。

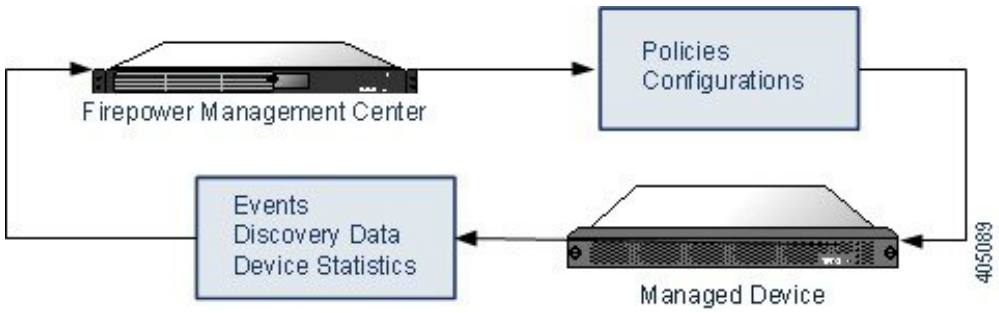
Firepower 管理中心可以管理哪些内容？

可以使用 Firepower 管理中心作为 Firepower 系统部署中的中央管理点来管理以下设备：

- 7000 和 8000 系列设备
- ASA FirePOWER模块
- NGIPSv设备

管理设备时，信息通过 SSL 加密的安全 TCP 隧道在Firepower 管理中心和该设备之间传输。

下图列出了在Firepower管理中心及其受管设备之间传输的内容。请注意，设备间发送的事件和策略的类型基于设备类型。



除策略和事件以外的其他功能

除将策略部署到设备和从其接收事件以外，还可以在Firepower管理中心上执行其他设备相关任务。

备份设备

您**不能**创建或恢复 NGIPSv 设备或 ASA FirePOWER 模块的备份文件。

当您从设备本身执行物理受管设备的备份时，**只**会备份设备配置。要备份配置数据和（可选的）统一文件，请使用管理Firepower 管理中心执行设备备份。

要备份事件数据，请对管理Firepower 管理中心执行备份。

更新设备

思科会不定期发布 Firepower 系统更新，包括：

- 入侵规则更新，其中可能包含新的和已更新的入侵规则
- 漏洞数据库更新
- 地理定位更新
- 软件补丁和更新

可以使用Firepower 管理中心在其管理的设备上安装更新。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及在流量通过路由器传递时重新分配源或目标 IP 地址。使用 NAT 的典型应用支持专用网络上的多个主机使用单个公共 IP 地址访问公共网络。

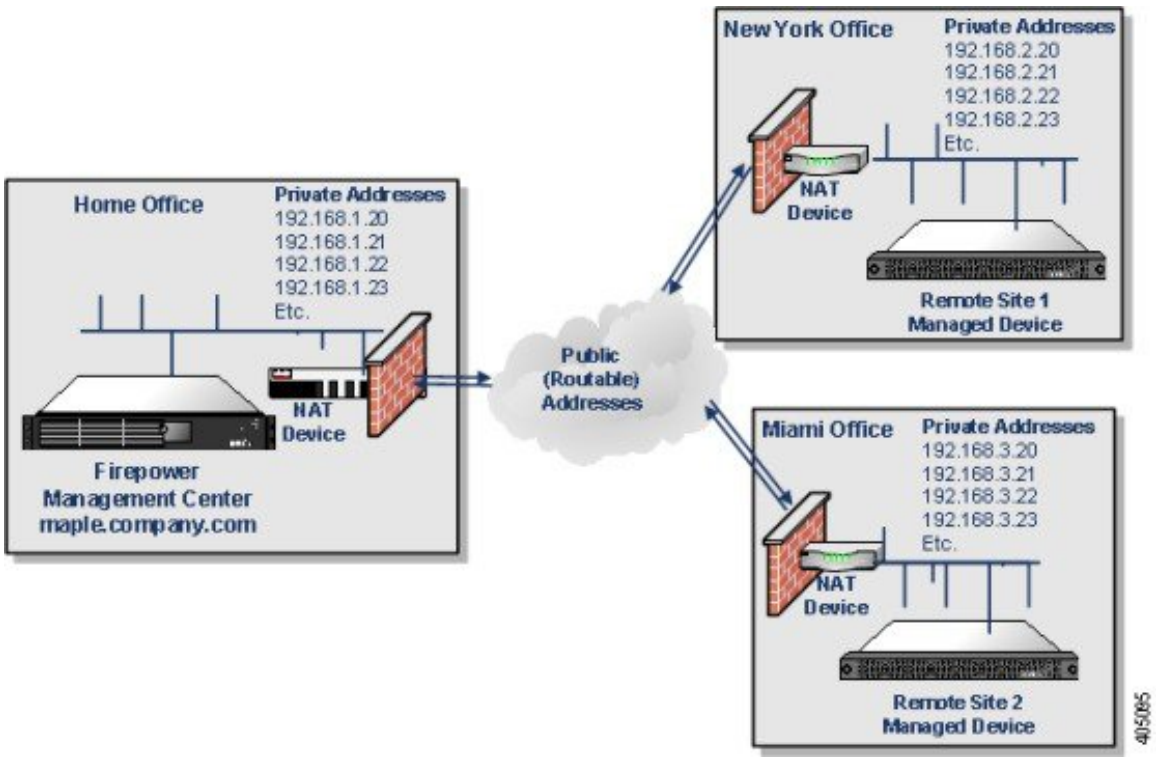
将设备添加到Firepower管理中心时，会在设备之间建立通信。建立通信所需的信息取决于环境是否使用 NAT：

- 在不使用 NAT 的环境中，需要注册密钥以及两台设备的 IP 地址或完全限定域名。
- 在使用 NAT 的环境中，需要注册密钥和唯一 NAT ID。

注释 NAT ID **必须**在用于将设备注册到Firepower 管理中心的所有 NAT ID 中唯一。

请注意，使用非默认管理接口连接Firepower管理中心和受管设备并且这些设备由NAT设备分隔时，必须配置两个流量信道使用同一管理接口。

下图显示在 NAT 环境中管理两台设备的Firepower 管理中心。添加这两台设备时可以使用同一注册密钥，因为注册密钥不必唯一。但是，将设备添加到Firepower管理中心时，**必须**使用唯一NAT ID。



第 19 章

设备管理基础知识

以下主题介绍如何在 Firepower 系统中管理设备：

设备管理页面

“设备管理”(Device Management) 页面提供可用于管理注册设备、7000 和 8000 系列设备高可用性对和设备组的一系列信息和选项。该页面显示Firepower 管理中心上当前注册的所有设备的列表。

您可以使用**排序方式 (sort-by)** 下拉列表按以下类别对设备列表进行排序：组、许可证类型、型号或访问控制策略。在多域部署中，还可以按域排序，它是该部署中的默认显示类别。设备必须属于枝叶域。

您可以展开和折叠任何设备类别中的设备列表。默认情况下，设备列表已展开。

有关设备列表的详细信息，请参阅下表。

表 *50*：设备列表字段

字段	说明
Name	用于 Firepower 管理中心中的设备的显示名称。名称左侧的状态图标指示其当前运行状况状态。

字段	说明
Group	受管设备分配到的组。
型号	受管设备的型号。
许可证类型	在受管设备上启用的许可证。
访问控制策略	指向当前部署的访问控制策略的链接。如果系统将访问控制策略身份为过期，则其会在链接旁边显示警告图标 ()。

远程管理配置

在可以管理 Firepower 系统设备之前，必须在设备和 Firepower 管理中心之间设置双向、SSL 加密的通信通道。设备使用信道共享配置和事件信息。

注释 本文档说明如何在将设备注册至 FMC 之前，使用其本地 Web 界面配置 7000 或 8000 系列设备的远程管理。有关为其他型号配置远程管理的信息，请参阅相应的快速入门指南。

要启用两台设备之间的通信，必须提供设备相互识别的方法。在允许通信时Firepower系统使用三个条件：

- 尝试建立通信时所使用的设备的主机名或 IP 地址。

  在 NAT 环境中，即使另一设备没有可路由地址，在配置远程管理或添加受管设备时也必须提供主机名或 IP 地址。

- 长度多达 37 个字符的用于识别连接的自生成字母数字注册密钥。
- 可帮助 Firepower 系统在 NAT 环境中建立通信的可选唯一字母数字 NAT ID。

  该 NAT ID **必须**在用于注册受管设备的所有 NAT ID 中唯一。

将设备添加到 Firepower 管理中心

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/网络管理员

使用Firepower管理中心管理设备之前，必须确保在该设备上正确配置网络设置。这通常在安装过程中完成。

请注意，如果注册了Firepower 管理中心和一个使用 IPv4 的设备并要将其转换为 IPv6，则必须删除并重新注册该设备。

注册 7000 和 8000 系列设备高可用性对或设备堆栈时，虽然可以选择许可证，但在设备注册时无法应用这些许可证。这可确保高可用性对或堆栈运行正确的许可证，以防止因许可证不匹配而进入降级状态。注册后，可以在“设备管理”(Device Management) 页面的通用属性（7000 和 8000 系列高可用性对）或堆栈属性（堆栈）中评估许可证。

提示

要修改设备的详细配置，请点击设备旁边的编辑图标()。有关详细信息，请参阅设备配置设置，第 365 页和配置传感接口，第 385 页。

在多域部署中，可以从任何域添加设备，但必须将设备分配到叶域。添加设备后，必须切换到叶域配置设备。

开始之前

- 将设备配置为由Firepower 管理中心管理。有关 7000 和 8000 系列设备，请参阅在受管设备上配置远程管理，第 378 页。有关为其他型号配置远程管理的信息，请参阅相应的快速入门指南。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加设备 (Add Device)**。

步骤 3 在**主机 (Host)** 字段中，输入要添加的设备的 IP 地址或主机名。

- 设备的主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。
- 在 NAT 环境中，如果在将设备配置为由 Firepower 管理中心管理时已经指定 Firepower 管理中心的 IP 地址或主机名，则可能无需指定设备的 IP 地址或主机名。有关详细信息，请参阅NAT 环境，第 359 页。

注意 如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

步骤 4 在**显示名称 (Display Name)** 字段中，输入要在 Firepower 管理中心中显示的设备名称。

步骤 5 在**注册密钥 (Registration Key)** 字段中，输入将设备配置为由 Firepower 管理中心管理时所使用的同一注册密钥。

步骤 6 在多域部署中，将设备分配到叶**域 (Domain)**。
如果当前域是叶域，设备会自动添加到当前域。

步骤 7 或者，也可将设备添加到设备**组 (Group)**。

步骤 8 选择初始**访问控制策略 (Access Control Policy)** 以部署到设备，或创建一个新策略。

注释 如果设备与所选策略不兼容，在注册时部署会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。请在解决导致失败的问题后，手动将配置部署到设备。

步骤 9 选择要应用到设备的许可证。
对于传统设备，请注意：

- 控制、恶意软件和 URL 过滤许可证需要保护许可证。
- 不能在 NGIPSv 设备或 ASA FirePOWER 模块上启用 VPN 许可证。
- 虽然可在 NGIPSv 设备或 ASA FirePOWER 模块上启用控制许可证，但这些设备不支持 8000 系列快速路径规则、交换、路由、堆叠或设备高可用性。
- 不能更改高可用性对中的 7000 和 8000 系列设备上的许可证设置。
- 对于堆叠设备，可以在设备编辑器的 Stack 页面上启用或禁用堆栈的许可证。有关详细信息，请参阅Firepower 系统许可，第 103 页。

步骤 10 如果在将设备配置为由Firepower 管理中心管理时使用 NAT ID 识别设备，请展开 **Advanced** 部分并在 **Unique NAT ID** 字段中输入同一 NAT ID。

步骤 11 要允许设备将数据包传输到 Firepower 管理中心，请选中**传输数据包 (Transfer Packets)** 复选框。默认情况下，此选项已启用。如果将其禁用，则完全禁止将数据包传输到 Firepower 管理中心。

步骤 12 点击**注册 (Register)** 将设备添加到 Firepower 管理中心。
Firepower 管理中心可能需要长达两分钟来验证设备的心跳并建立通信。

从 Firepower 管理中心删除设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/网络管理员

如果不希望再管理设备，可以将其从Firepower 管理中心中删除。删除设备：

- 会切断 Firepower 管理中心和设备之间的所有通信。
- 从“设备管理”(Device Management) 页面删除设备。
- 如果通过平台设置策略将设备配置为通过 NTP 从 Firepower 管理中心接收时间，则将设备返回本地时间管理。

要在以后管理设备，请将其重新添加到 Firepower 管理中心。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要删除的设备旁，点击删除图标 ( )。

步骤 3 确认要删除设备。

设备配置设置

设备编辑器的 Device 页面显示详细设备配置和信息。通过该页面，还可以对设备配置的某些部分进行更改，例如启用和禁用许可证、关闭并重新启动设备、修改管理以及配置高级选项。

常规设备设置

设备 (Device) 选项卡的“常规”(General) 部分显示下表所述的设置。

表 *51*：“常规”*(General)* 部分表字段

字段	说明
Name	Firepower 管理中心上的设备的显示名称。
Transfer Packets	受管设备是否将数据包数据随事件一起发送到 Firepower 管理中心。
强制部署	强制部署设备上的所有策略和设备配置更新。

设备许可证设置

设备 (Device) 选项卡的“许可证”(License) 部分显示为设备启用的许可证。

设备系统设置

Device 选项卡的 System 部分显示只读系统信息表，如下表中所述。

表 *52*：系统部分表字段

字段	说明
型号	受管设备的型号名称和编号。
序列	受管设备的机箱的序列号。
Time	设备的当前系统时间。
版本	受管设备上当前安装的软件版本。
策略	指向当前部署到受管设备的平台设置策略的链接。

也可以关闭或重新启动设备。

设备运行状况设置

设备 (Device) 选项卡上的“运行状况”(Health) 部分显示下表所述信息。

表 *53*: 运行状况部分表字段

字段	说明
状态	一个代表设备当前运行状况的图标。点击该图标将显示设备的“运行状况监控器”(Health Monitor)。
策略	一个指向当前部署在设备上的运行状况策略的只读版本的链接。
Blacklist	一个指向“运行状况黑名单”(Health Blacklist) 页面的链接，您可以在该页面上启用和禁用运行状况黑名单模块。

设备管理设置

设备 (Device) 选项卡的“管理”(Management) 部分显示下表中描述的字段。

表 *54*: “管理” *(Section Table Fields)* 部分表字段

字段	说明
Host	设备的 IP 地址或主机名。主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称（即，主机名）。
状态	指示 Firepower 管理中心与受管设备之间的通信通道的状态的图标。您可以将鼠标悬停在状态图标上，查看上次 Firepower 管理中心联系设备的时间。

查看设备信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/网络管理员

在多域部署中，祖先域可以查看后代域中所有设备的相关信息。您必须处于枝叶域才可编辑设备。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要查看的设备旁边的编辑图标 ( )。

在多域部署中，如果您正处于祖先域中，则可点击查看图标 ( ) 以只读模式查看后代域中的设备。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 可以查看以下信息：

- 常规 - 显示设备的常规设置；请参阅常规设备设置，第 365 页。
- 许可证 - 显示设备的许可证信息；请参阅设备许可证设置，第 365 页。
- 系统 - 显示有关设备的系统信息；请参阅设备系统设置，第 365 页。
- 运行状况 - 显示设备的当前运行状况的相关信息；请参阅设备运行状况设置，第 366 页。
- 管理 - 显示 Firepower 管理中心和设备之间的通信通道的相关信息；请参阅设备管理设置，第 366 页。
- 高级 - 显示有关高级功能配置的信息；请参阅高级设备设置，第 380 页。

编辑设备管理设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员

注释 有时，如果您通过其他方法编辑设备的主机名或 IP 地址（例如使用设备的 LCD 面板或 CLI），可能需要使用以下操作步骤手动更新管理Firepower 管理中心上的主机名或 IP 地址。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改管理选项的设备旁边，点击编辑图标 ( )。

在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡。

提示 对于堆叠设备，修改设备编辑器的“设备”(Device) 页面上单个设备的管理选项。

步骤 4 您可以执行以下操作：

- 禁用远程管理 - 点击**管理 (Management)** 部分的滑块以启用或禁用设备的管理。禁用管理会阻止 Firepower 管理中心和设备之间的连接，但是**不**会从 Firepower 管理中心删除设备。如果不想再管理设备，请参阅从 Firepower 管理中心删除设备，第 364 页。
- 编辑管理主机 - 点击**管理 (Management)** 部分的编辑图标 ( )，修改**主机 (Host)** 字段中的名称或 IP 地址，然后点击**保存 (Save)**。您可以使用此设置指定管理主机名和重新生成虚拟 IP 地址。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

编辑常规设备设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击 **Device**。

步骤 4 在**常规 (General)** 部分中，点击编辑图标 ( )。

步骤 5 输入受管设备的**名称 (Name)**。

提示 对于堆叠设备，编辑设备编辑器的 Stack 页面上堆栈的分配的设备名称。可以编辑设备编辑器的 Devices 页面上单个设备的分配的设备名称。

步骤 6 更改**传输数据包 (Transfer Packets)** 设置：

- 选中该复选框以使数据包数据能够随事件一起存储在 Firepower 管理中心上。
- 清除该复选框以防止受管设备随事件发送数据包数据。

步骤 7 点击**强制部署 (Force Deploy)** 以强制将当前策略和设备配置部署到设备。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

启用和禁用设备许可证

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员

如果在Firepower 管理中心上有可用的许可证，则可以启用设备上的许可证。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要启用或禁用许可证的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡。

提示 对于堆叠设备，可以在设备编辑器的 Stack 页面上启用或禁用堆栈的许可证。

步骤 4 在**许可证 (License)** 部分中，点击编辑图标 ( )。

步骤 5 选中或取消选中要为受管设备启用或禁用的许可证旁边的复选框。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

管理系统关闭

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 ASA FirePOWER	仅限枝叶	管理员/网络管理员

注释 不能使用 Firepower 系统用户界面关闭或重新启动 ASA FirePOWER。有关如何关闭各自设备的详细信息，请参阅 ASA 文档。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要重新启动的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡。
提示 对于堆叠设备，关闭或重新启动设备编辑器的 Devices 页面上的单个设备。

步骤 4 要关闭设备，请点击**系统 (System)** 部分的关闭设备图标 ( )。

步骤 5 出现提示时，确认是否要关闭设备。

步骤 6 要重新启动设备，请点击重新启动设备图标 ( )。

步骤 7 出现提示时，确认是否要重新启动设备。

接口表视图

接口表视图位于硬件视图的下方，并且列出设备上的所有可用接口。该表包含可用来查看所有已配置的接口的可扩展式导航树。您可以点击接口旁的箭头图标以收起或展开接口，从而隐藏或查看其子部件。接口表视图还提供有关每个接口的汇总信息，如下表所述。

典型设备接口

请注意，仅 8000 系列设备会显示 MAC Address 列和 IP Address 列。有关详细信息，请参阅下表。

表 55：典型设备接口表视图字段

字段	说明
Name	每个接口类型都用指示其类型和链路状态（如适用）的唯一图标表示。您可以在工具提示中将指针悬停在名称或图标上面以查看接口类型、速度和双工模式（如果适用）。接口图标，第 383 页对接口图标进行了说明。 这些图标使用标记规则指示接口的当前链接状态，其可能是以下三种状态之一： • 错误 () • 故障 () • 不可用 () 逻辑接口具有与其父物理接口相同的链路状态。ASA FirePOWER 模块不显示链路状态。请注意，禁用的接口以半透明的图标表示。 在图标右侧显示的接口名称是自动生成的，但混合接口和 ASA FirePOWER 接口除外，那是用户定义的。请注意，对于 ASA FirePOWER 接口，系统仅显示已启用、已命名和具有链路的接口。 物理接口显示物理接口的名称。逻辑接口显示物理接口和分配的 VLAN 标记的名称。 ASA FirePOWER 接口显示安全上下文的名称和接口的名称（如果有多个安全上下文）。如果只有一个安全上下文，则系统仅显示接口的名称。
安全区域	已分配接口的安全区域。要添加或编辑安全区域，请点击编辑图标 ()。
Used by	已分配接口的内联集、虚拟交换机或虚拟路由器。ASA FirePOWER 模块不显示“使用者”(Used by) 列。
MAC Address	为交换式和路由式功能启用接口时，所显示的该接口的 MAC 地址。 对于 NGIPSv 设备，会显示 MAC 地址，以便可以将设备上配置的网络适配器与“接口”(Interfaces) 页面上显示的接口匹配。ASA FirePOWER 模块不显示 MAC 地址。
IP 地址	分配给接口的 IP 地址。将指针悬停在 IP 地址上方以查看其处于活动还是非活动状态。非活动 IP 地址会灰显。ASA FirePOWER 模块不显示 IP 地址。

设备组管理

Firepower 管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。可以展开和折叠组中的设备列表。默认情况下，列表以折叠状态显示。

在多域部署中，您可以只在枝叶域内创建设备组。当您为多租户配置Firepower管理中心时，现有设备组会被删除；您可以在枝叶域级别重新添加这些组。

添加设备组

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员

可以使用设备组轻松分配策略，并在多台设备上安装更新。

如果将堆栈或高可用性对中的主设备添加到某个组，则系统会将两台设备均添加到该组中。如果对设备取消堆叠或取消高可用性，则两台设备均会保留在该组中。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。

步骤 3 输入 **Name**。

步骤 4 在**可用设备 (Available Devices)** 下，选择一台或多台要添加到设备组的设备。点击的同时使用 Ctrl 或 Shift 选择多台设备。

步骤 5 点击**添加 (Add)** 将所选设备包含在设备组中。

步骤 6 点击**确定 (OK)** 以添加组。

编辑设备组

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/网络管理员

可以更改驻留在任何设备组中的设备集。必须先从设备的当前组中移除该设备，然后才能将其添加到新组。

将设备移至新组不会将其策略更改为先前分配到组的策略。必须为新设备分配组策略。

如果将堆栈或设备高可用性对中的主设备添加到某个组，则系统会将两台设备均添加到该组中。如果对设备取消堆叠或取消高可用性，则两台设备均会保留在该组中。

在多域部署中，只可以在创建设备组的域中编辑它们。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑的设备组旁边，点击编辑图标 ( )。

步骤 3 或者，在**名称 (Name)** 字段中，输入组的新名称。

步骤 4 在**可用设备 (Available Devices)** 下，选择一台或多台要添加到设备组的设备。点击的同时使用 Ctrl 或 Shift 选择多台设备。

步骤 5 点击**添加 (Add)** 将所选设备包含在设备组中。

步骤 6 或者，要将设备从设备组中删除，请点击要删除的设备旁边的删除图标 ( )。

步骤 7 点击**确定 (OK)** 以保存对设备组的更改。

第 VI 部分

配置基础知识

第 20 章

典型设备管理基础知识

以下主题介绍如何在 Firepower 系统中管理典型设备（7000 和 8000 系列设备、具备 FirePOWER 服务的 ASA 和 NGIPSv）：

远程管理配置

在可以管理 Firepower 系统设备之前，必须在设备和 Firepower 管理中心之间设置双向、SSL 加密的通信通道。设备使用信道共享配置和事件信息。

注释 本文档说明如何在将设备注册至 FMC 之前，使用其本地 Web 界面配置 7000 或 8000 系列设备的远程管理。有关为其他型号配置远程管理的信息，请参阅相应的快速入门指南。

要启用两台设备之间的通信，必须提供设备相互识别的方法。在允许通信时 Firepower 系统使用三个条件：

- 尝试建立通信时所使用的设备的主机名或 IP 地址。

  在 NAT 环境中，即使另一设备没有可路由地址，在配置远程管理或添加受管设备时也必须提供主机名或 IP 地址。

- 长度多达 37 个字符的用于识别连接的自生成字母数字注册密钥。
- 可帮助 Firepower 系统在 NAT 环境中建立通信的可选唯一字母数字 NAT ID。

  该 NAT ID **必须**在用于注册受管设备的所有 NAT ID 中唯一。

在受管设备上配置远程管理

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	不适用	管理员/网络管理员

过程

步骤 1 在要管理的设备的 Web 界面上，选择**配置 (Configuration)** > **ASA FirePOWER 配置 (ASA FirePOWER Configuration)** > **集成 (Integration)** > **远程管理 (Remote Management)**。

步骤 2 如果**远程管理 (Remote Management)** 选项卡尚未显示，请点击该选项卡。

步骤 3 点击 **Add Manager**。

步骤 4 在**管理主机 (Management Host)** 字段中，为要用于管理此设备的 Firepower 管理中心输入以下之一：

- IP 地址
- 完全限定域名或名称，通过本地 DNS 解析为有效的 IP 地址（即，主机名）。

注意　如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

在 NAT 环境中，如果计划在添加受管设备时指定 IP 地址或主机名，则无需在此处进行指定。在此情况下，Firepower 系统使用随后将提供的 NAT ID 来识别受管设备的 Web 界面上的远程管理器。

步骤 5 在**注册密钥 (Registration Key)** 字段中，输入要用于设置设备之间的通信的注册密钥。

步骤 6 对于 NAT 环境，请在**唯一 NAT ID (Unique NAT ID)** 字段中，输入要用于设置设备之间的通信的**唯一**字母数字 NAT ID。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 等待直至设备确认其可以相互通信并且显示“注册待定”(Pending Registration) 状态。
- 将此设备添加到 Firepower 管理中心；请参阅将设备添加到 Firepower 管理中心，第 362 页。

在受管设备上编辑远程管理

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	不适用	管理员/网络管理员

在编辑远程管理器时，请注意：

- **主机 (Host)** 字段指定完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称（即主机名）。
- **名称 (Name)** 字段指定管理设备的显示名称，该名称仅在 Firepower 系统环境内使用。输入另一个显示名称不会更改管理设备的主机名。

过程

步骤 1 在设备的 Web 界面上，选择**系统 (System)** > **集成 (Integration)**。

步骤 2 如果**远程管理 (Remote Management)** 选项卡尚未显示，请点击该选项卡。

步骤 3 您可以执行以下操作：

- 禁用远程管理 - 点击管理器旁边的滑块以进行启用或禁用。禁用管理会阻止 Firepower 管理中心和设备之间的连接，但是不会从 Firepower 管理中心删除设备。如果不想再管理设备，请参阅从 Firepower 管理中心删除设备，第 364 页。
- 编辑管理器信息 - 点击要修改的管理器旁边的编辑图标 ( )，修改**名称 (Name)** 和**主机 (Host)** 字段，然后点击**保存 (Save)**。

更改管理端口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列 管理中心	仅全局	管理员/网络管理员

设备使用双向、SSL 加密的通信通道（默认情况下在端口 8305 上）进行通信。

尽管思科强烈建议保持默认设置，但如果管理端口与网络上的其他通信冲突，则可以选择不同的端口。通常，在 Firepower 系统安装期间对管理端口进行更改。

注意 如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。

过程

步骤 1 选择系统 **(System)** > 配置 **(Configuration)**。

步骤 2 点击 **Management Interfaces**。

步骤 3 在共享设置 **(Shared Settings)** 部分，输入要在远程管理端口 **(Remote Management Port)** 字段中使用的端口号。

步骤 4 点击保存 **(Save)**。

接下来的操作

- 对部署中必须与此设备进行通信的每台设备重复此过程。

高级设备设置

设备 (Device) 选项卡的“高级”(Advanced) 部分显示高级配置设置表，如下所述。可以使用 Advanced 部分编辑其中任何设置。

表 ***56***：“高级”***(Advanced)*** 部分表字段

字段	说明	支持的设备
Application Bypass	设备上 Automatic Application Bypass 的状态。	7000 和 8000 系列、NGIPSv、ASA FirePOWER
Bypass Threshold	Automatic Application Bypass 阈值（以毫秒为单位）。	7000 和 8000 系列、NGIPSv、ASA FirePOWER
检查本地路由器流量	设备是否检查在路由式接口上接收的以其本身为目标的流量，如 ICMP、DHCP 和 OSPF 流量。	7000 和 8000 系列
快速路径规则	设备上已创建的 8000 系列快速路径规则数。	8000 系列

自动应用旁路

自动应用旁路 (AAB) 功能限制通过接口处理数据包所允许的时间，并在超过时间的情况下允许数据包绕开检测。该功能适用于任何部署；但在内联部署中最有价值。

通过网络的数据包延迟容限来平衡数据包处理时延。如果 Snort 中出现故障或设备配置不当导致流量处理时间超过指定阈值，则 AAB 会导致 Snort 在发生故障后的 10 分钟内重新启动，并生成故障排除数据，您可以分析这些数据以调查处理时间过长的原因。

在版本 6.0 和更高版本中，AAB 选项的默认行为根据设备而异，如下所示：

- 7000 和 8000 系列、NGIPSv：关闭
- ASA FirePOWER：关闭

如果您从低于 5.3 的版本升级，则会保留现有设置。如果选择该选项，则可以更改旁路阈值。默认设置为 3000 毫秒 (ms)。有效范围为 250 ms 到 60,000 ms。

通常，在超过延迟阈值后使用入侵策略中的 Rule Latency Thresholding 通过快速路径传送数据包。Rule Latency Thresholding 不关闭引擎或生成故障排除数据。

注意 只有在花费过量时间处理单个数据包时，才会激活 AAB。AAB 激活 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

如果绕过了检测，则设备会生成运行状况监控警报。

配置 8000 系列快速路径规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	8000 系列	仅限枝叶	管理员/网络管理员

作为早期流量处理形式，8000 系列快速路径规则可以直接通过 8000 系列设备发送流量，无需进一步检查或记录。（在被动部署中，8000 系列快速路径规则只是停止分析。）每个 8000 系列快速路径规则应用于特定安全区域或内联接口集。由于8000系列快速路径规则在硬件级别运作，因此只能使用以下简单、外部报头标准对流量进行快速路径传递：

- 发起方和响应方 IP 地址或地址块
- 协议，以及对于 TCP 和 UDP 而言的发起方和响应方端口
- VLAN ID

默认情况下，8000 系列快速路径规则会影响从指定发起方到指定响应方的连接。要通过快速路径传递符合规则标准的所有连接（无论哪个主机是发起方和哪个主机是响应方），可以使规则为双向。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要配置规则的 8000 系列设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡（或对应于堆叠设备的**堆栈 [Stack]** 选项卡），然后点击“高级”(Advanced) 部分中的编辑图标 ( )。

步骤 4 点击**新建 IPv4 规则 (New IPv4 Rule)** 或**新建 IPv6 规则 (New IPv6 Rule)**。

步骤 5 从**域 (Domain)** 下拉列表中，选择内联集或被动安全区域。

步骤 6 配置要通过快速路径传递的流量。流量必须符合所有条件才能通过快速路径传递。

- “发起方”(Initiator) 和“响应方”(Responder)（必要） - 输入发起方和响应方的 IP 地址或地址块。
- “协议”(Protocol) - 选择协议或选择**全部 (All)**。
- “发起方端口”(Initiator Port) 和“响应方端口”(Responder Port) - 对于 TCP 和 UDP 流量，请输入发起方和响应方端口。将字段保留为空白或输入 Any 以匹配所有 TCP 或 UDP 流量。可以输入端口的逗号分隔列表，但是不能输入端口范围。
- VLAN - 输入 VLAN ID。将字段保留为空白或输入 Any 以匹配所有流量（无论 VLAN 标记如何）。

步骤 7 （可选）使规则为**双向 (Bidirectional)**。

步骤 8 点击**保存 (Save)**，然后再次点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改， 第 254 页。

编辑高级设备设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	因功能而异	仅限枝叶	管理员 网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑高级设备设置的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡（或对应于堆叠设备的**堆栈 [Stack]** 选项卡），然后点击“高级”(Advanced) 部分中的编辑图标 ( )。

步骤 4 配置高级设备设置：

- 自动应用绕行 (AAB) - 选中**自动应用绕行 (Automatic Application Bypass)**，然后在**绕行阈值 (Bypass Threshold)** 中输入范围在 250 毫秒到 60,000 毫秒内的绕行阈值。
- 本地路由器流量检查 - 当 7000 或 8000 系列设备部署为路由器时，选中**检查本地路由器流量 (Inspect Local Router Traffic)** 以检查异常流量。
- 8000 系列快速路径规则 - 点击**新建 IPv4 规则 (New IPv4 Rule)** 或**新建 IPv6 规则 (New IPv6 Rule)**，或者点击现有规则旁边的编辑图标 ( )。请参阅配置 8000 系列快速路径规则，第 381 页。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

接口配置设置

设备编辑器的“接口”(Interfaces) 页面显示详细接口配置和信息。该页面由物理硬件视图和接口表视图组成，通过其可以深入了解详细配置信息。可以从此页面添加和编辑接口。

物理硬件视图

“接口”(Interfaces) 页面的顶部以图形显示 7000 或 8000 系列设备的物理硬件视图。

使用物理硬件视图可：

- 查看网络模块的类型、部件号和序列号
- 在接口表视图中选择接口
- 打开接口编辑器
- 查看接口的名称、接口的类型、接口是否具有链路、接口的速度设置，以及接口当前是否处于旁路模式
- 查看有关错误或警告的详细信息

接口图标

表 *57*：接口图标类型和说明

图标	接口类型	有关详细信息，请参阅.....
	物理 - 未经配置的物理接口。	配置物理交换接口，第 528 页 或配置物理路由接口，第 539 页

图标	接口类型	有关详细信息，请参阅.....
	被动-配置用于分析被动部署中的流量的感应接口。	配置被动接口，第 392 页
	内联-配置用于处理内联部署中的流量的感应接口。	配置内联接口，第 395 页
	交换 - 配置用于交换第 2 层部署中的流量的接口。	交换接口配置，第 527 页
	路由 - 配置用于路由第 3 层部署中的流量的接口。	路由接口，第 538 页
	汇聚 - 配置为单个逻辑链路的多个物理接口。	汇聚接口，第 569 页
	汇聚交换 - 配置为第 2 层部署中单个逻辑链路的多个物理接口。	添加汇聚交换接口，第 574 页
	汇聚路由 - 配置为第 3 层部署中单个逻辑链路的多个物理接口。	添加汇聚路由接口，第 576 页
	混合 - 配置用于桥接虚拟路由器和虚拟交换机之间流量的逻辑接口。	逻辑混合接口，第 583 页
	ASA FirePOWER - 在安装了 ASA FirePOWER 模块的 ASA 设备上配置的接口。	管理思科 ASA FirePOWER 接口，第 388 页

使用物理硬件视图

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要管理的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 使用图形界面执行以下操作：

- 选择 - 如果要选择接口，请点击接口图标。系统会突出显示接口表中的相关条目。
- 编辑 - 如果要打开接口编辑器，请双击接口图标。
- 查看错误或警告信息 - 如果要查看有关错误或警告的详细信息，请将光标悬停在网络模块上的受影响端口上方。
- 查看接口信息 - 如果要查看接口的名称、接口类型、接口是否有链路、接口的速度设置以及接口当前是否处于绕行模式，请将光标悬停在接口上方。
- 查看网络模块信息 - 如果要查看网络模块的类型、部件号和序列号，请将光标悬停在网络模块左下角的黑色圆圈上方。

配置传感接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	传统	仅限枝叶	管理员/网络管理员

根据 Firepower 系统部署，可以从设备编辑器的“接口”(Interfaces) 页面配置受管设备的传感接口。请注意，受管设备上最多只能配置 1024 个接口。

注释 在 SPAN 端口模式下部署 ASA FirePOWER 时，Firepower 管理中心不显示 ASA 接口。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要配置接口的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击要配置的接口旁边的编辑图标 ( )。

步骤 4 使用接口编辑器配置传感接口：

- 高可用性链路 - 如果要在设备高可用性对每个成员上配置的用作设备之间冗余通信通道的接口（又称为高可用性链路接口），请点击**高可用性链路 (HA Link)**，然后如配置高可用性链路接口，第 386 页中所述继续操作。
- 内联 - 如果要配置用于处理内联部署中的流量的接口，请点击**内联 (Inline)**，然后如配置内联接口，第 395 页中所述继续操作。
- 被动 - 如果要配置用于分析被动部署中的流量的接口，请点击**被动 (Passive)**，然后如配置被动接口，第 392 页中所述继续操作。
- 路由 - 如果要配置用于路由第 3 层部署中的流量的接口，请点击**路由 (Routed)**，然后如路由接口，第 538 页中所述继续操作。
- 交换 - 如果要配置用于交换第 2 层部署中的流量的接口，请点击**交换 (Switched)**，然后如交换接口配置，第 527 页中所述继续操作。

步骤 5 点击**保存 (Save)** 保存更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置高可用性链路接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

在建立 7000 或 8000 系列设备高可用性对之后，可以将物理接口配置为高可用性 (HA) 链路接口。此链路充当用于在配对设备之间共享运行状况信息的冗余通信通道。在一台设备上配置高可用性链路接口时，在第二台设备上会自动配置接口。必须在同一广播域中配置两个高可用性链路。

动态 NAT 依靠动态分配 IP 地址和端口来映射到其他 IP 地址和端口。如果没有高可用性链路，则这些映射在故障切换中会丢失，导致所有已转换的连接失败，因为它们通过高可用对中的当前主用设备进行路由。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要配置高可用性链路接口的高可用对成员设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要配置为高可用性链路接口的接口旁边，点击编辑图标 ( )。

步骤 4 点击**高可用性链路 (HA Link)**

步骤 5 选中**已启用 (Enabled)** 复选框。

注释 如清除此复选框，则将禁用并强制性断开该接口。

步骤 6 从**模式 (Mode)** 下拉列表中，选择一个选项以指定链路模式，或者选择**自动协商 (Autonegotiation)** 以指定将接口配置为自动协商速度和双工设置。

步骤 7 从 **MDI/MDIX** 下拉列表中，选择一个选项以指定接口是配置用于 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。

注释 通常，MDI/MDIX 设置为 **Auto-MDIX**，它会自动处理 MDI 和 MDIX 之间的切换以获取链路。

步骤 8 在 **MTU** 字段中输入最大传输单位 (MTU)。MTU 的设置范围可能根据 Firepower 系统设备型号和接口类型而异。有关详细信息，请参阅7000 和 8000 系列设备与 NGIPSv 的 MTU 范围，第 389 页。

步骤 9 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

禁用接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列 NGIPSv	仅限枝叶	管理员/网络管理员

可以通过将接口类型设置为 **None** 禁用接口。已禁用的接口在接口列表中会灰显。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要禁用接口的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要禁用的接口旁边，点击编辑图标 ( )。

步骤 4 点击 **None**。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

管理思科 ASA FirePOWER 接口

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	ASA FirePOWER	仅限枝叶	管理员/网络管理员

编辑 ASA FirePOWER 接口时，从 Firepower 管理中心只能配置接口的安全区域。

可使用特定于 ASA 的软件和 CLI 全面配置 ASA FirePOWER 接口。如果编辑 ASA FirePOWER 并从多情景模式切换至单情景模式（或反之），ASA FirePOWER 会重命名其所有接口。必须重新配置所有 Firepower 系统的安全区域、关联规则和相关配置，才能使用更新的 ASA FirePOWER 接口名称。有关 ASA FirePOWER 接口配置的详细信息，请参阅 ASA 文档。

注释 既不能更改 ASA FirePOWER 接口的类型，也不能从 Firepower Firepower 管理中心禁用接口。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑接口的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 如果尚未显示**接口 (Interfaces)** 选项卡，请点击该选项卡。

步骤 4 在要编辑的接口旁边，点击编辑图标 ( )。

步骤 5 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域，或选择**新建 (New)** 添加新的安全区域。

步骤 6 点击**保存 (Save)** 配置安全区域。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

7000 和 8000 系列设备与 NGIPSv 的 MTU 范围

当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

注释 系统会从已配置的 MTU 值中删除 18 个字节。请勿将 IPv4 MTU 设置为低于 594 或将 IPv6 MTU 设置为低于 1298。

典型设备型号	MTU 范围
7000 和 8000 系列	576 到 9234（管理接口） 576 到 10172（内联集、被动接口） 576 到 9922（所有其他）
NGIPSv	576 到 9018（所有接口和内联集）

同步安全区域对象修订版本

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	7000 和 8000 系列 NGIPSv	仅限枝叶	管理员/网络管理员

更新安全区域对象时，系统会保存新修订版本的对象。因此，如果同一安全区域中的受管设备具有接口中配置的安全区域对象的不同修订版本，则可以记录看似重复的连接。

如果发现重复的连接报告，则可以更新所有受管设备以使用同一修订版本的对象。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要更新安全区域选择的设备旁边，请点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 对于记录重复连接事件的每个接口，请将**安全区域 (Security Zone)** 更改为其他区域，点击**保存 (Save)**，然后将其重新更改为所需区域，并再次点击**保存 (Save)**。

步骤 4 为记录重复事件的每台设备重复第 2 步到第 3 步。在继续之前，必须编辑所有设备。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

注意 在已编辑要同步的全部设备上接口的区域设置前，不得将受管设备部署到任何设备。必须一次性将设备更改部署到所有受管设备。

第 21 章

IPS 设备部署和配置

以下主题介绍如何在 IPS 部署中配置设备：

IPS 设备部署和配置简介

您可以被动或内联 IPS 部署方式配置设备。在被动部署中，您可以在网络流量的带外部署系统。在内联部署中，您可以将两个端口绑定在一起，从而在网段上透明配置系统。

被动 IPS 部署

在被动 IPS 部署中，Firepower 系统使用交换机 SPAN 或镜像端口监控网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。这可以提供网络内系统可视性，无需网络流量。如果在被动部署中进行配置，系统无法采取某些措施（例如，流量阻断和整形）。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

注释 出站流量包括流控制数据包。因此，设备上的被动接口可能根据您的配置显示出站流量并生成事件；这是预期行为。

Firepower 系统上的被动接口

您可以将受管设备的一个或多个物理端口配置为被动接口。

启用被动接口来监控流量时，需要指定模式和 MDI/MDIX 设置，该设置仅适用于铜接口。8000 系列设备上的接口不支持半双工选项。

出于安全考虑，当禁用某个被动接口后，用户不能再访问该接口。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

配置被动接口

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	因功能而异	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要配置被动接口的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击要配置为被动接口的接口旁边的编辑图标 ( )。

步骤 4 点击**被动 (Passive)**。

步骤 5 如果要将被动接口与安全区域相关联，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象， 第 309 页。

步骤 6 选中**已启用 (Enabled)** 复选框。
如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 7 仅限 7000 和 8000 系列：从**模式 (Mode)** 下拉列表中，指定链路模式，或者选择**自动协商 (Autonegotiation)** 以指定将接口配置为自动协商速度和双工设置。
模式设置仅适用于铜缆接口。

8000 系列设备上的接口不支持半双工选项。

步骤 8 仅限 7000 和 8000 系列：从 **MDI/MDIX** 下拉列表中，指定接口是配置为 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。
MDI/MDIX 设置仅适用于铜缆接口。

默认情况下，MDI/MDIX 设置为 **Auto-MDIX**，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 9 在 **MTU** 字段中输入最大传输单位 (MTU)。
MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意　当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 10　点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

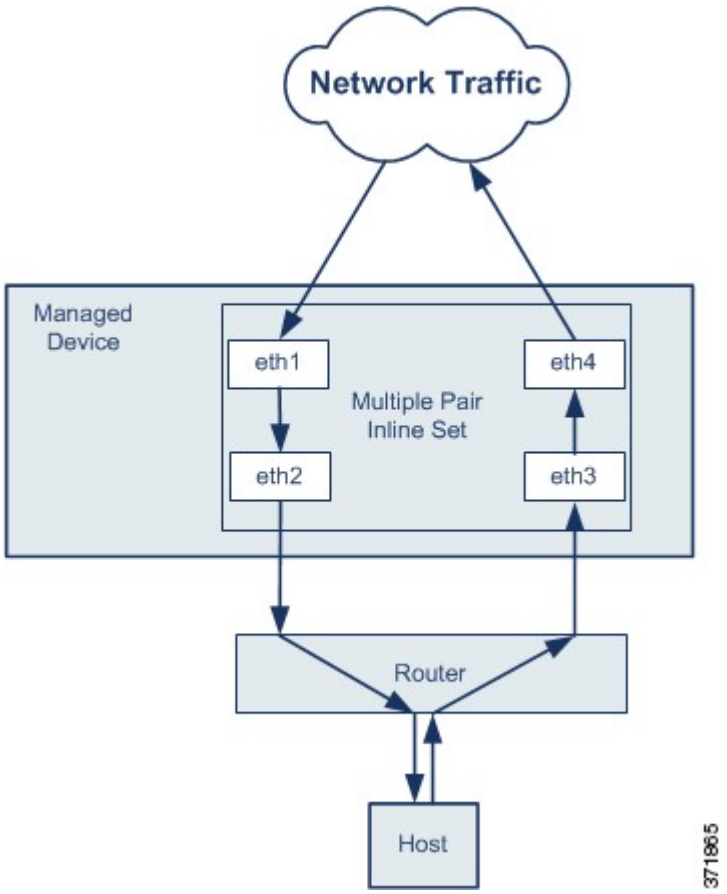
内联 IPS 部署

在内联 IPS 部署中，通过将两个端口绑定在一起在网段上透明地配置 Firepower 系统。这使系统可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

注释　为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向受管设备部署相关配置。

您可以将受管设备上的接口配置为在您网络上的主机和外部主机之间通过不同的内联接口对路由流量，具体取决于设备流量是入站流量还是出站流量。这是异步路由配置。如果您部署异步路由，但一个内联集只包含一个接口对，设备可能无法正确分析网络流量，因为它可能只发现一半的流量。作为同一流量的一部分，将多个内联接口对添加到同一内联接口集允许系统识别入站和出站流量。也可以通过将接口对包括在同一安全区域中来实现此目的。

当系统从通过异步路由配置的流量生成连接事件时，事件可能识别来自同一内联接口对的入口接口和出口接口。例如，下图中的配置会生成一个连接事件，将 **eth3** 识别为入口接口，并将 **eth2** 识别为出口接口。在此配置中，这是预期行为。



注释 如果将多个接口对分配到单个内联接口集，但在流量重复时遇到问题，请重新配置以帮助系统唯一识别数据包。例如，您可以重新指定接口对以分隔内联集或修改您的安全区域。

对于有内联集的设备，在设备重新启动后，自动设置软件网桥传输数据包。如果设备正在重新启动，没有任何软件网桥在运行。如果在内联集中开启旁路模式，在设备重新启动时将变为硬件旁路模式。在这种情况下，当系统出现故障并恢复运行时，可能由于设备链路的重新协商丢失了几秒钟的数据包。但是，当 Snort 重新启动时，系统会传递流量。

Firepower 系统中的内联接口

您可以将受管设备的一个或多个物理端口配置为内联接口。在一对内联接口处理内联部署中的流量之前，必须将这对内联接口分配给内联集。

注意：

- 如果将内联对中的接口设置为不同的速度或者接口协商为不同的速度，系统将向您发出警告。
- 如果将接口配置为内联接口，网络模块中的相邻端口也自动成为内联接口来完成组对。
- 要在 NGIPSv 设备上配置内联接口，必须使用相邻接口创建内联对。

配置内联接口

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	因功能而异	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要配置接口的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击要配置的接口旁边的编辑图标 ( )。

步骤 4 点击**内联 (Inline)**。

步骤 5 如果要将内联接口与安全区域相关联，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象，第 309 页。

步骤 6 从**内联集 (Inline Set)** 下拉列表中选择现有内联集，或选择**新建 (New)** 以添加新的内联集。

注释 如果添加新的内联集，则必须在设置内联接口后进行配置；请参阅添加内联集，第 397 页。

步骤 7 选中**已启用 (Enabled)** 复选框。
如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8 仅限 7000 和 8000 系列：从**模式 (Mode)** 下拉列表中，指定链路模式，或者选择**自动协商 (Autonegotiation)** 以指定将接口配置为自动协商速度和双工设置。
模式设置仅适用于铜缆接口。

8000 系列设备上的接口不支持半双工选项。

步骤 9 仅限 7000 和 8000 系列：从 **MDI/MDIX** 下拉列表中，指定接口是配置为 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。
MDI/MDIX 设置仅适用于铜缆接口。

默认情况下，MDI/MDIX 设置为 **Auto-MDIX**，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

Firepower 系统上的内联集

在内嵌部署使用内联接口之前，必须配置内联集和分配内联接口对。内联集是设备上的一个或多个内联接口对的集合；一个内联接口对每次只能属于一个内联集。

Device Management 页面的 **Inline Sets** 选项卡显示设备中配置的所有内联集的列表。

您可以从 Device Management 页面的 **Inline Sets** 选项卡添加内联集，或者可以在配置内联接口时添加内联集。

只能将内联接口对分配给内联集。如果在受管设备上配置内联接口前要创建内联集，您可以创建一个空内联集，然后向其中添加接口。输入内联集的名称时，可以使用字母数字字符和空格。

Name

内联集名称。

接口

分配给内联集的所有内联接口对的列表。通过 Interfaces 选项卡禁用接口对中的任一接口时，该接口对不可用。

MTU

内联集的最大传输单位。MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

故障保护

允许流量绕过检测并继续通过设备。受管设备在内部流量缓冲区已满的情况下监控这些缓冲区和旁路检测。

旁路模式

仅限 Firepower 7000 或 8000 系列：配置的内联集绕行模式。此设置可以确定在接口出现故障时内联接口中的中继如何做出响应。绕行模式允许流量继续通过接口。非绕行模式则会阻止流量。

注意 在旁路模式下，重新启动设备时可能会丢失一些数据包。不能为高可用性对中的 7000 或 8000 系列设备上的内联集、NGIPSv 设备上的内联集、8000 系列设备上的非绕行 NetMod 或为 Firepower 7115 或 7125 设备上的 SFP 模块配置绕行模式。

查看内联集

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要在其中查看内联集的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**内联集 (Inline Sets)** 选项卡。

添加内联集

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	因功能而异	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要添加内联集的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**内联集 (Inline Sets)** 选项卡。

步骤 4 点击 **Add Inline Set**。

步骤 5 输入 **Name**。

步骤 6 在**接口 (Interfaces)** 旁边，选择一个或多个内联接口对，然后点击添加所选项图标 ( )。要将所有接口对添加到内联集中，请点击添加所有图标 ( )。

提示 要从内联集中删除内联接口，请选择一个或多个内联接口对，然后点击删除所选项图标 ( )。要从内联集删除所有接口对，请点击删除所有图标 ( )。通过 **Interfaces** 选项卡禁用接口对中的任一接口也可以删除该接口对。

步骤 7 在 **MTU** 字段中输入最大传输单位 (MTU)。
MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意　当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 8　如果您要指定允许流量绕过检测并继续通过设备，请选择**故障安全 (Failsafe)**。
受管设备在内部流量缓冲区已满的情况下监控这些缓冲区和旁路检测。

步骤 9　仅限 7000 和 8000 系列：指定绕行模式：

- 点击**绕行 (Bypass)** 以允许流量继续通过接口。
- 点击**非绕行 (Non-Bypass)** 以阻止流量。

注释　不能为高可用性对中的 7000 或 8000 系列设备上的内联集、NGIPSv 设备上的内联集、8000 系列设备上的非绕行 NetMod 或为 Firepower 7115 或 7125 设备上的 SFP 模块配置绕行模式。

步骤 10　或者，配置高级设置；请参阅高级内联集选项，第 398 页。

步骤 11　点击 **OK**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

高级内联集选项

在配置内联集时有多个高级选项可供考虑。

分流模式

当您创建内联或带有失效开放接口集的内联时，分流模式在 7000 和 8000 系列设备上可用。

在分路模式下，设备部署内联，但是包级流不通过设备，而是每个数据包副本发送到设备，并且网络流量不会受到干扰。由于您使用的是数据包副本而不是数据包本身，设置为丢弃的规则和使用替换关键字的规则不会影响包数据流。但是，这些类型的规则在触发时会生成入侵事件，而且入侵事件表视图显示了触发数据包会在内联部署中被丢弃。

在已部署内联的设备上使用分路模式有很多优点。例如，您可以设置设备和网络之间的布线，就像设备是内联，并分析设备生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效性的丢弃规则。准备部署设备内联时，您可以禁用分路模式，并开始丢弃可疑流量，而无需重新配置设备和网络之间的走线。

请注意，您不能在同一内联集中启用此选项和严格 TCP 执行选项。

传播链路状态

链路状态传播是旁路模式下配置的内联集的一个特性，因两对内联集都要设置跟踪状态。链路状态传播适用于铜和光纤可配置旁路接口。

在内联集的一个接口断开时，链路状态传播自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，备用接口也自动恢复运行。换句话说，如果一个接口的链路状态更改，设备感知该更改并更新其他接口的链路状态以与其匹配。请注意，设备需要至多 4 秒传播链路状态更改。

在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

请注意，只有 7000 和 8000 系列设备才支持链路状态传播。

您不能禁用高可用性对中的 7000 和 8000 系列设备上配置的内联集的链路状态传播。

透明内联模式

Transparent Inline Mode 选项允许设备作为“线内凸点”，这意味着不管是源地址还是目的地址，设备都将转发其看见的所有网络流量。请注意，您不能在 7000 和 8000 系列设备上禁用此选项。

严格 TCP 实施

为最大程度地提高 TCP 安全性，您可以启用严格执行，从而阻止未完成三次握手的连接。严格执行功能也阻止：

- 三次握手尚未完成的连接的非 SYN TCP 数据包
- TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
- TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

请注意，只有 7000 和 8000 系列设备才支持此选项。此外，您不能在同一内联集中启用此选项和分路模式。

配置高级内联集选项

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	因功能而异	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要在其中编辑内联集的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**内联集 (Inline Sets)** 选项卡。

步骤 4 点击要编辑的内联集旁边的编辑图标 ( )。

步骤 5 点击 **Advanced** 选项卡。

步骤 6 配置选项，如高级内联集选项 ， 第 398 页中所述。

步骤 7 点击 **OK**。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

删除内联集

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任意	仅限枝叶	管理员/网络管理员

删除一个内联集时，分配给该集的任何内联接口都可包含在另一个集合中。接口没有删除。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要删除内联集的设备旁的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**内联集 (Inline Sets)** 选项卡。

步骤 4 点击要删除的内联集旁的编辑图标 ( )。

步骤 5 出现提示时，确认您要删除内联集。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

第 VII 部分

高可用性和可扩展性

第 22 章

7000 和 8000 系列设备高可用性

以下主题介绍如何在 Firepower 系统中为 Firepower 7000 系列和 8000 系列设备配置高可用性：

设备高可用性

通过 7000 和 8000 系列设备高可用性，您可以在两个对等设备或两个对等设备堆栈之间建立网络功能和配置数据的冗余。

可以通过将两个对等设备或两个对等设备堆栈配置为高可用性对，作为用于策略应用、系统更新和注册的单个逻辑系统来实现配置冗余。系统自动同步其他配置数据。

高可用性要求

设备或设备堆栈主成员必须为同一型号并具有相同的铜接口和光纤接口，然后才能配置 7000 和 8000 系列设备高可用性对。设备或设备堆栈还必须均运行的是相同软件并具有相同许可证。除已安装的恶意软件存储包以外，设备堆栈必须具有相同的硬件配置。例如，可以将一个 Firepower 8290 与另一个 8290 配对。在任一堆栈中，可能没有任何设备、有一台设备或所有设备都具有恶意软件存储包。如果 NAT 策略以设备为目标，则两个对等体均必须具有相同的 NAT 策略。将设备配对后，不能更改单个配对设备的许可证选项，但是可以更改整个高可用性对的许可证。

注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件仅可从思科购买，而且仅限用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*Firepower* 系统恶意软件存储包指南》。

高可用性故障切换和维护模式

通过 7000 和 8000 系列设备高可用性，系统可以手动或自动进行故障切换。通过使其中一个配对设备或堆栈进入维护模式，可以手动触发故障切换。

在主用设备或堆栈的运行状况受损之后、系统更新期间或具有管理员权限的用户关闭设备之后，会发生自动故障转移。在主用设备或设备堆栈经历 NMSB 故障、NFE 故障、硬件故障、固件故障、重要流程故障、磁盘已满条件或两个堆叠设备之间链路故障之后，也会发生自动故障转移。如果备份设备或堆栈的运行状况同样受损，则系统不进行故障转移并会进入降级状态。其中一台设备或设备堆栈处于维护模式中时，系统也不进行故障转移。请注意，将堆叠电缆与活动堆栈断开连接会使该堆栈进入维护模式。关闭活动堆栈中的辅助设备也会使该堆栈进入维护模式。

注释 如果高可用性对的活动成员进入维护模式并且活动角色故障切换至另一配对成员，当原活动配对成员恢复正常运行时，它不会自动恢复活动角色。

部署策略和更新

部署策略时，将策略部署到设备高可用性对而不是单个设备或堆栈。如果策略失败，则系统不会将其部署到设备或堆栈。策略首先部署到主用设备或堆栈，然后部署到备份，以便高可用性对始终有一个对等体处理网络流量。

高可用性对中的设备将作为单个实体而不是单个设备或堆栈接收更新。更新开始时，系统先将其部署到备份设备或堆栈，随后进入维护模式，直到所有必要的进程均重新启动，并且设备再次开始处理流量。然后，系统以同样的方式将更新部署到主用设备或堆栈。

在不使用设备高可用性的情况下实现冗余

大多数情况下，可以使用思科冗余协议 (SFRP) 在不使用 7000 或 8000 系列设备高可用性的情况下实现第 3 层冗余。SFRP 允许设备充当指定 IP 地址的冗余网关。通过网络冗余，可配置两台设备或堆栈以提供相同的网络连接，从而确保网络上其他主机的连接。

根据 Firepower 系统部署（被动、内联、路由式或交换式），可确定如何配置设备高可用性。也可以一次性以多个角色部署系统。在四种部署类型中，仅被动部署要求您使用高可用性来配置设备或堆栈以提供冗余。您可以在具有或没有设备高可用性的情况下为其他部署类型建立网络冗余。以下各节简要概述各部署类型中的高可用性。

被动部署冗余

被动接口通常连接到中央交换机上的分接头端口，这使其能够分析流经交换机的所有流量。如果多台设备连接到同一分接器，则系统从每台设备生成事件。在高可用性对中进行配置后，设备充当主用或备用设备，这使系统即使在发生故障的情况下也能分析流量，同时还可防止事件重复。

内联部署冗余

由于内联集无法控制通过其传递的数据包的路由，因此其在部署中必须始终处于活动状态。因此，冗余需要依靠外部系统才能正确路由流量。您可以在具有或没有 7000 或 8000 系列设备高可用性的情况下配置冗余内联集。

要部署冗余内联集，可配置网络拓扑，以便其仅允许流量通过其中一个内联集传递，同时防止循环路由。如果其中一个内联集失败，则周围的网络基础设施会检测与网关地址的连接是否丢失，并将路由调整为通过冗余集发送流量。

路由式部署冗余

IP 网络中的主机必须使用众所周知的网关地址将流量发送到不同网络。在路由式部署中建立冗余要求路由式接口共享网关地址，以便仅一个接口在任何指定时间处理该地址的流量。为此，必须在虚拟路由器上保留相等数量的IP地址。一个接口通告地址。如果该接口发生故障，则备份接口开始通告地址。

在不是高可用性对成员的设备中，通过配置多个路由接口之间共享的网关 IP 地址来使用 SFRP 建立冗余。您可以在具有或没有 7000 或 8000 系列设备高可用性的情况下配置 SFRP，也可以使用动态路由协议（例如 OSPF 和 RIP）建立冗余。

交换机式部署冗余

使用生成树协议(STP)（其中一项高级虚拟交换机设置）在交换式部署中建立冗余。STP是一种管理桥接网络拓扑的协议。它专门用于允许冗余链路为交换机式接口提供自动备份而不配置备份链路。交换机式部署中的设备依靠 STP 管理冗余接口之间的流量。连接到同一广播网络的两台设备根据 STP 计算的拓扑接收流量。

注释 思科强烈建议在配置计划在 7000 或 8000 系列设备高可用性对中部署的虚拟交换机时启用 STP。

高可用性和多租户

在多域部署中，您只能建立 7000 或 8000 系列设备高可用性或枝叶域内的设备堆栈。

设备高可用性配置

建立 7000 或 8000 系列设备高可用性时，请将其中一个设备或堆栈指定为主用，将另一个设备或堆栈指定为备用。系统会将合并的配置应用于配对设备。如果存在冲突，则系统应用已指定为活动的设备或堆栈中的配置。

将设备配对后，不能更改单个配对设备的许可证选项，但是可以更改整个高可用性对的许可证。如果有需要在交换接口或路由接口上设置的接口属性，则系统会建立高可用性对，但是将其设置为待处理状态。配置必要的属性后，系统会完善高可用性对并将其设置为正常状态。

建立高可用性对之后，系统在“设备管理”(Device Management) 页面上将对等设备或堆栈视为单个设备。设备高可用性对在设备列表中显示高可用性图标( )。所进行的任何配置更改都会在配对设备之间同步。“设备管理”(Device Management) 页面显示高可用性中的哪个设备或堆栈为主用（在手动或自动故障切换后会发生更改）。

从Firepower管理中心中删除设备高可用性对的注册会从两个设备或堆栈中均删除注册。请按照处理单个受管设备的方式从 Firepower 管理中心中删除设备高可用性对。

然后，可以在其他Firepower管理中心上注册高可用性对。要从高可用性对注册单一设备，请将远程管理添加到该对中的主用设备，然后将该设备添加到Firepower管理中心，从而添加整个对。要在高可用性对中注册堆叠设备，请将远程管理添加到任一堆栈的主设备，然后将该设备添加到Firepower管理中心，从而添加整个对。

在建立设备高可用性对之后，可以配置高可用性链路接口。

建立设备高可用性

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列 Firepower 威胁防御 Firepower 威胁防御虚拟	任意	管理员/网络管理员

建立设备高可用性对时，请将其中一个设备或堆栈指定为主用，将另一个设备或堆栈指定为备用。系统会将合并的配置应用于配对设备。如果存在冲突，则系统应用已指定为活动的设备或堆栈中的配置。

在多域部署中，高可用性对中的设备必须属于同一个域。

开始之前

- 要建立 7000 和 8000 系列高可用性，请执行以下操作：

  确认在堆栈中的各设备或各主设备上有已配置的接口。

  确认在高可用性对中包含的各设备或设备堆栈主成员为同一型号并具有相同的铜缆接口或光纤接口。

  确认设备或设备堆栈均具有正常运行状态，运行同一软件，并具有相同许可证。有关详细信息，请参阅使用运行状况监控器，第 214 页。特别是，设备不能具有会导致其进入维护模式并触发故障转移的硬件故障。

  确认在高可用性对中没有不匹配的设备和堆栈。必须将具有相同硬件配置的单一设备与单一设备或设备堆栈与设备堆栈进行配对，但存在恶意软件存储包时除外。例如，可以将一个 Firepower 8290 与另一个 8290 配对。任一堆栈中无任何设备、有一个设备或所有设备可能具有已安装的恶意软件存储包。有关恶意软件存储包的详细信息，请参阅《*Firepower* 系统恶意软件存储包指南》。

  注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅**限用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*Firepower* 系统恶意软件存储包指南》。

  确认两个对等体均具有相同的 NAT 策略（如果 NAT 策略以设备为目标）。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加高可用性 (Add High Availability)**。

步骤 3 输入 **Name**。

步骤 4 对于 7000 和 8000 系列设备：

a) 选择高可用性对的**主用 (Active)** 设备或堆栈。

b) 为高可用性对选择**备用 (Backup)** 设备或堆栈。

步骤 5 对于 7000 和 8000 系列设备，点击**添加 (Add)** 以添加高可用性对或完成进一步配置步骤。由于此过程会同步系统数据，因此需要花费几分钟时间。

编辑设备高可用性

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

建立 7000 或 8000 系列设备高可用性对后，对设备配置进行的大多数更改还会更改整个高可用性对的配置。

通过将指针悬停在“常规”(General) 部分中的状态图标上方，可以查看高可用性对的状态。还可以查看哪台设备或堆栈是对中的活动对等体和备份对等体。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑配置的设备高可用性对旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 按照更改单一设备配置的方式，使用“高可用性”(High Availability) 页面上的各部分对高可用性对配置进行更改。

配置高可用性对中的单个设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

建立 7000 或 8000 系列设备高可用性对后，仍可以为高可用性对内的每台设备配置某些属性。可以完全按照更改单台设备的方式对成对设备进行更改。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑配置的设备高可用性对旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Devices) 选项卡**。

步骤 4 从**所选设备 (Selected Device)** 下拉列表中，选择要修改的设备。

步骤 5 按照更改单台设备的方式，使用“设别”(Devices) 页面上的各部分对单个成对设备进行更改。

配置高可用性对中的单个设备堆栈

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	Firepower 8140、8200 系列、8300 系列	仅限枝叶	管理员/网络管理员

将堆叠式8000系列设备配置为高可用性对后，系统会限制可编辑的堆栈属性。可以编辑成对堆栈中的堆栈的名称。此外，可以编辑堆栈的网络配置，如配置高可用性对中设备上的接口，第 409 页中所述。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑配置的设备高可用性对旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**堆栈 (Stacks)** 选项卡。

步骤 4 从**所选设备 (Selected Device)** 下拉列表中，选择要修改的堆栈。

步骤 5 在 **General** 部分旁边，点击编辑图标 ( )。

步骤 6 输入 **Name**。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置高可用性对中设备上的接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可以在 7000 或 8000 系列设备高可用性对中的一台设备上配置接口。但是，还必须在高可用性对中的对等设备上配置等效接口。对于成对堆栈，请在堆栈的主设备上配置相同接口。配置虚拟路由器时，请选择要在其中配置路由器的堆栈。

成对设备的“接口”(Interfaces) 页面包含在单个设备上找到的硬件和接口视图。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要配置接口的设备高可用性对旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**接口**选项卡。

步骤 4 从**所选设备 (Selected Device)** 下拉列表中，选择要修改的设备。

步骤 5 按照在单个设备上进行配置的方式配置接口。

切换设备高可用性对中的主用对等体

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	任意	管理员/网络管理员

建立 7000 或 8000 系列设备高可用性对后，可以手动切换主用和备用对等设备或堆栈。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要更改主用对等体的设备高可用性对旁边，点击“切换主用对等体”图标 ( )。

步骤 3 您可以执行以下操作：

- 点击**是 (Yes)** 将使备用设备立即变成高可用性对中的主用设备。
- 点击 **No** 将取消并返回到 Device Management 页面。

将高可用性对中的设备置于维护模式

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	任意	管理员/网络管理员

在建立 7000 或 8000 系列设备高可用性对后，可以通过将其中一个成对设备或堆栈置于维护模式以对该设备执行维护来手动触发故障切换。在维护模式中，系统以管理方式中断除管理接口以外的所有接口。维护完成后，可以重新启用设备以恢复正常运行。

注释 不应同时将高可用性对中的两个成员均置于维护模式。这样会阻止该对检测流量。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要置于维护模式的成对设备旁边，点击切换维护模式图标 ( )。

步骤 3 点击**是 (Yes)** 确认维护模式。

接下来的操作

- 当维护完成时，再次点击切换维护模式图标 ( ) 以使设备退出维护模式。

更换高可用性对中的堆栈中的设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	Firepower 8140、8200 系列、8300 系列	任意	管理员/网络管理员

将属于高可用性对成员的堆栈置于维护模式后，可以将该堆栈中的辅助设备更换为其他设备。只能选择当前未堆叠或成对的设备。新设备必须遵循建立设备堆栈的相同准则。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要使其进入维护模式的堆栈成员旁边，点击切换维护模式图标 ()。

步骤 3 点击**是 (Yes)** 确认维护模式。

步骤 4 点击替换设备图标 ()。

步骤 5 从下拉列表中选择**更换设备 (Replacement Device)**。

步骤 6 点击**更换 (Replace)** 更换设备。

步骤 7 再次点击切换维护模式图标 () 使堆栈立即退出维护模式。

注释 无需重新部署设备配置。

设备高可用性状态共享

高可用性对中的设备或堆栈可通过设备高可用性状态共享来同步尽可能多的状态，以便在设备或堆栈发生故障的情况下，其他对等体可以接管而不中断流量。如果不进行状态共享，则以下功能可能无法正常执行故障转移：

- 严格 TCP 实施
- 单向访问控制规则
- 阻止持久性

不过请注意，启用状态共享会降低系统性能。

必须在高可用性对中的两台设备或主堆叠设备上配置并启用高可用性链路接口，然后才能配置高可用性状态共享。Firepower 82xx 系列和 83xx 系列设备需要 10G 高可用性链路，而其他型号的设备需要 1G 高可用性链路。

必须禁用状态共享，然后才可修改高可用性链路接口。

注释 如果配对设备进行故障切换，则系统会终止主用设备上所有现有 SSL 加密的会话。即使建立高可用性状态共享，也必须在备份设备上重新协商这些会话。如果建立 SSL 会话的服务器支持会话重复使用，并且备份设备没有 SSL 会话 ID，则其无法重新协商会话。

严格 TCP 实施

对域启用严格 TCP 实施时，系统会丢弃 TCP 会话中顺序混乱的所有数据包。例如，系统丢弃在未建立的连接上收到的非 SYN 数据包。通过状态共享，高可用性对中的设备在故障切换后允许 TCP 会话继续，而不必重新建立连接，即使启用了严格 TCP 执行也如此。可以在内联集、虚拟路由器和虚拟交换机上启用严格 TCP 实施。

单向访问控制规则

如果配置了单向访问控制规则，则系统在故障转移后重新评估连接代答时，网络流量可能会与不同于预期的访问控制规则匹配。例如，请考虑是否有包含以下两种访问控制规则的策略：

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

在未进行状态共享的情况下，如果从 192.168.1.1 到 192.168.2.1 的允许连接在故障切换后仍处于活动状态，并且下一个数据包被视为响应数据包，则系统拒绝连接。在进行状态共享的情况下，中途代答会与现有连接匹配并继续允许代答。

阻止持久性

虽然根据访问控制规则或其他因素在第一个数据包上阻止了许多连接，但在一些情况下系统会允许通过一定数量的数据包，然后再确定是否应阻止连接。通过状态共享，系统也会立即阻止对等设备或堆栈上的连接。

为高可用性对建立状态共享时，可以配置以下选项：

启用

点击该复选框以启用状态共享。清除该复选框以禁用状态共享。

Minimum Flow Lifetime

指定系统为会话发送任何同步消息之前该会话经过的最短时间（以毫秒为单位）。可以使用从 0 到 65535 的任何整数。系统不同步未达到最低流量生命周期的任何会话，并且，仅当连接接收到数据包时系统才会同步。

Minimum Sync.Interval

指定会话的更新消息间隔的最短时间（以毫秒为单位）。可以使用从 0 到 65535 的任何整数。最小同步间隔防止在连接达到最小生命周期后以超过配置值的频率发送指定连接的同步消息。

Maximum HTTP URL Length

指定系统在配对设备之间同步的 URL 的最大字符数。可以使用从 0 到 225 的任何整数。

建立设备高可用性状态共享

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

高可用性对中的 7000 或 8000 系列设备或堆栈可通过设备高可用性状态共享同步尽可能多的状态，以便在设备或堆栈发生故障的情况下，对等点可以接管而不中断流量。

注释 思科建议使用默认值，除非您的部署有充分的理由更改这些值。减小值会提高成对的对等点的就绪程度，而增大值会改善性能。

注意 修改高可用性状态共享选项将在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 为设备高可用性对中的每台设备配置高可用性链路接口。有关详细信息，请参阅配置高可用性链路接口，第 386 页。

步骤 2 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 在要编辑的设备高可用性对旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 4 在**状态共享 (State Sharing)** 部分，点击编辑图标 ( )。

步骤 5 配置状态共享，如本节中先前所述。

步骤 6 点击 **OK**，保存更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

用于故障排除的设备高可用性状态共享统计信息

以下各节介绍您可以查看的每台设备的统计信息，以及如何使用这些信息来对 7000 和 8000 系列设备高可用性对的状态共享配置进行故障排除。

Messages Received (Unicast)

“接收的消息数”(Messages received) 是从成对的对等体接收的高可用性同步消息的数量。

该值应该接近对等体发送的消息数。在活动使用期间，值可能不匹配，但应该接近。如果流量停止，则值应该变得稳定，并且接收的消息会与发送的消息匹配。

要进行故障排除，应该同时查看接收的消息数和发送的消息数，比较增加率，并确保值接近。每个对等体上的发送值应该以与反对等体上的接收值大致相同的速率递增。

如果接收的消息数停止递增或递增速度慢于对等体发送消息的速度，请与技术支持部门联系。

Packets Received

系统将多个消息批处理为单一数据包，以便减少开销。Packets Received 计数器显示这些数据包以及设备已接收的其他控制数据包的总数。

该值应该接近对等设备发送的数据包数。在活动使用期间，值可能不匹配，但应该接近。由于接收的消息数应该接近并以与对等体发送的消息数相同的速率递增，因此接收的数据包数应具有相同行为。

要进行故障排除，应该同时查看接收的数据包数和发送的消息数，比较增加率，并确保值以相同速率增加。如果成对的对等体上的发送值在递增，则设备上的接收值也应以相同速率增加。

如果接收的数据包数停止递增或递增速度慢于对等体发送消息的速度，请与技术支持部门联系。

Total Bytes Received

Total bytes received 是组成对等体接收的数据包的字节数。

该值应该接近其他对等体发送的字节数。在活动使用期间，值可能不匹配，但应该接近。

要进行故障排除，应该同时查看接收的总字节数和发送的消息数，比较增加率，并确保值以相同速率增加。如果成对的对等体上的发送值在递增，则设备上的接收值也应以相同速率增加。

如果接收的字节数停止递增或递增速度慢于对等体发送消息的速度，请与技术支持部门联系。

Protocol Bytes Received

Protocol bytes received 是接收的协议开销的字节数，其中包括除会话状态同步消息的负载以外的所有内容。

该值应该接近对等体发送的字节数。在活动使用期间，值可能不匹配，但应该接近。

要进行故障排除，应该查看接收的总字节数以发现在与协议数据比较时共享的实际状态数据量。如果协议数据在所发送数据中占较大的百分比，则可以调整最小同步间隔。

如果接收的协议字节数以类似于接收的总字节数的速率递增，请与技术支持部门联系。根据接收的总字节数，接收的协议字节数应该最小。

Messages Sent

“已发送消息数”(Messages Sent) 是从成对的对等体接收的高可用性同步消息的数量。

此数据在与接收的消息数比较的过程中有用。在活动使用期间，值可能不匹配，但应该接近。

要进行故障排除，应该同时查看接收的消息数和发送的消息数，比较增加率，并确保值接近。

如果发送的消息数以类似于接收的总字节数的速率递增，请与技术支持部门联系。

已发送字节数

“已发送字节数”(Bytes Sent) 是组成发送到对等体的集群同步消息的发送的总字节数。

此数据在与接收的消息数比较的过程中有用。在活动使用期间，值可能不匹配，但应该接近。在对等体上接收的字节数应该接近，但是不大于该值。

如果接收的总字节数不是以与发送的字节数大致相同的速率递增，请与技术支持部门联系。

Tx Errors

“发送错误”(Tx Errors) 是系统为要发送到成对的对等体的消息分配空间时遇到的内存分配失败数。

该值在两个对等体上均应该始终为零。如果此数字不为零，或者如果数字稳定增大（表示系统遇到无法分配内存错误），请与技术支持部门联系。

Tx Overruns

Tx overruns 是系统尝试将消息放入传输队列并失败的次数。

该值在两个对等体上均应该始终为零。值不为零或稳定增大时，表示系统通过高可用性链路共享着太多无法足够快速地发送的数据。

如果高可用性链路 MTU 先前设置为低于默认值（9918 或 9922），则应该将其增大。可以更改最小流量生命周期和最小同步间隔设置，以减少通过高可用性链路共享的数据量，从而防止数字递增。

如果该值仍然存在或持续增大，请与技术支持部门联系。

Recent Logs

系统日志显示最新的高可用性同步消息。日志不应显示任何 ERROR 或 WARN 消息。它应保持在对等体之间可比较，如连接的插槽数相同。

但是，所显示的数据在某些实例中可能相反，例如，一个对等体报告它从另一个对等体收到连接并引用不同的 IP 地址。日志提供高可用性状态共享连接和连接内任何错误的全面视图。

如果日志显示 ERROR 或 WARN 消息或并未显示为纯参考性的任何消息，请与技术支持部门联系。

查看设备高可用性状态共享统计信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

启用状态共享后，可以在“高可用性”(High Availability) 页面的“状态共享”(State Sharing) 部分中查看有关配置的以下信息：

- 使用的高可用性链路接口及其当前链路状态
- 用于排除问题的详细同步统计信息

状态共享统计信息主要是发送和接收的高可用性同步流量的不同方面的计数器，以及一些其他错误计数器。此外，还可以查看高可用性对中每台设备的最新系统日志。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑的设备高可用性对旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在 **State Sharing** 部分中，点击查看统计图标 ( )。

步骤 4 如果高可用性对由设备堆栈组成，请在**设备 (Device)** 中选择要查看的设备。

步骤 5 您可以执行以下操作：

- 点击**刷新 (Refresh)** 以更新统计信息。
- 点击**查看 (View)** 以查看高可用性对中每台设备的最新数据日志。

在高可用性对中分隔设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	任意	管理员/网络管理员

中断 7000 或 8000 系列设备高可用性对时，主用设备或堆栈保留完整部署功能。除非选择保持接口配置处于活动状态，在此情况下备份设备或堆栈会恢复正常操作，否则备份设备或堆栈会丢失其接口配置并故障转移到主用设备或堆栈。中断高可用性对始终会移除备份设备上被动接口的配置。中断高可用性对后，维护模式中的任何设备都会恢复正常操作。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要中断的高可用性对旁边，点击中断高可用性对图标 ( )。

步骤 3 或者，选中复选框以移除备份设备或堆栈上的接口配置。这意味着会以管理方式断开除管理接口以外的所有接口。

步骤 4 点击 **Yes**。系统分隔设备高可用性对。

第 23 章

8000 系列设备堆叠

以下主题介绍如何在 Firepower 系统中使用 Firepower 8000 系列设备堆叠：

设备堆栈

可以通过在堆叠配置中使用设备来增加网段检查的流量。对于每个堆叠配置，堆栈中的所有设备都必须具有相同硬件。但是，无任何设备、某些设备或所有设备可能具有已安装的恶意软件存储包。根据以下堆叠配置，设备还必须来自同一设备子系列：

Firepower 8140、8200 系列、8300 系列设备支持堆叠配置。

对于 81xx 系列：

- 两台 Firepower 8140

对于 82xx 系列：

- 最多四台 Firepower 8250
- 一台 Firepower 8260（一台主设备和一台辅助设备）
- 一台 Firepower 8270（一台具有 40G 容量的主设备和两台辅助设备）
- 一台 Firepower 8290（一台具有 40G 容量的主设备和三台辅助设备）

对于 83xx 系列：

- 最多四台 Firepower 8350
- 最多四台 AMP8350
- 一台 Firepower 8360（一台具有 40G 容量的主设备和一台辅助设备）
- AMP8360（一台具有 40G 容量的主设备和一台辅助设备）

- 一台 Firepower 8370（一台具有 40G 容量的主设备和两台辅助设备）
- AMP8370（一台具有 40G 容量的主设备和两台辅助设备）
- 一台 Firepower 8390（一台具有 40G 容量的主设备和三台辅助设备）
- AMP8390（一台具有 40G 容量的主要设备和三台辅助设备）

有关堆叠配置的详细信息，请参阅《《*Firepower* 系统安装指南》》。有关恶意软件存储包的详细信息，请参阅《《*Firepower* 系统恶意软件存储包指南》》。

注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件仅可从思科购买，而且仅限用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*Firepower* 系统恶意软件存储包指南》。

建立堆栈配置时，要将每个堆叠设备的资源集成到单个统一的共享配置中。

将一台设备指定为主设备，在该设备上配置整个堆栈的接口。将其他设备指定为辅助设备。辅助设备当前不得感知任何流量，并且不得在任何接口上具有链路。

请以与配置单台设备相同的方式将主设备连接到要分析的网段。按照在《《*Firepower* 系统安装指南》》中提供的堆叠设备布线说明将辅助设备连接到主设备。

堆叠配置中的所有设备都必须具有相同硬件，运行同一软件版本，并具有相同许可证。如果 NAT 策略以设备为目标，则主设备和辅助设备均必须具有同一 NAT 策略。您必须从 Firepower 管理中心将更新部署到整个堆栈。如果更新在堆栈中的一个或多台设备上失败，则堆栈进入混合版本状态。您不能在混合版本状态下将策略部署到堆栈或更新堆栈。要纠正此状态，可以中断堆栈或移除具有不同版本的单个设备，更新单个设备，然后重新建立堆叠配置。在堆叠设备后，可以立即仅更改整个堆栈的许可证。

建立堆叠配置后，设备如同单个共享配置。如果主设备发生故障，则无任何流量传递到辅助设备。系统会生成指示堆叠心跳在辅助设备上发生故障的运行状况警报。

如果堆栈中的辅助设备发生故障，已启用可配置旁路的内联集会进入主要设备的旁路模式。对于所有其他配置，系统会继续将均衡流量加载到发生故障的辅助设备。无论是哪一种情况，系统都会生成指示链路丢失的运行状况警报。

可以在部署中按照使用单台设备的方式使用设备堆栈，但会存在几个异常。如果您的高可用性对中有 7000 或 8000 系列设备，则不能堆叠设备高可用性对或高可用性对中的设备，也不能在设备堆栈上配置 NAT。

注释 如果使用 eStreamer 将事件数据从堆叠设备传输到外部客户端应用，请从每台设备收集数据并确保以相同方式配置每台设备。eStreamer 设置在堆叠设备之间未自动同步。

在多域部署中，只可以堆叠属于同一个域的设备。

设备堆栈配置

可以通过堆叠两个 Firepower 8140 设备、最多四个 8250、一个 8260、一个 8270、一个 8290、最多四个 8350、一个 8360、一个 8370 或一个 8390 并在单个共享配置中使用其组合资源来增加在网段上检测到的流量。如果您的高可用性对中有 7000 或 8000 系列设备，则不能堆叠设备高可用性对或高可用性对中的设备，但是可以将两个设备堆栈配置成一个高可用性对。

建立设备堆栈后，系统在 Device Management 页面上将多台设备视为单台设备。设备堆栈在设备列表中显示堆栈图标 ( )。

从Firepower管理中心中移除设备堆栈的注册会从两种设备中都移除注册。请按照删除单个受管设备的方式从Firepower 管理中心中删除堆叠设备；然后，可以在其他Firepower 管理中心上注册堆栈。只需在新的Firepower 管理中心上注册其中一个堆叠设备即可显示整个堆栈。

建立设备堆栈后，除非中断并重新建立堆栈，否则无法更改哪些设备是主或辅助。但是，可以：

- 将辅助设备添加到由两个或三个 Firepower 8250、一个 8260 或一个 8270 组成的现有堆栈（在一个堆栈中限制最多有四个 8250）
- 将辅助设备添加到由两个或三个 Firepower 8350、一个 8360 或一个 8370 组成的现有堆栈（在一个堆栈中限制最多有四个 8350）

对于其他设备，堆栈中的主设备必须具有其他已布线设备的必要的堆叠网络模块。例如，如果 Firepower 8260 中的主设备仅有单个堆叠 NetMod，则无法向此堆栈中添加其他辅助设备。请以最初建立堆叠设备配置的相同方式将辅助设备添加到现有堆栈。

建立设备堆栈

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	FirePOWER 8140、8200 系列、8300 系列	任意	管理员/网络管理员

堆栈中的所有设备都必须为同一硬件型号（例如，Firepower 8140 和另一台 8140）。可以在 82xx 系列和 83xx 系列中堆叠总共四台设备（一台主设备和最多三台辅助设备）。

在多域部署中，堆栈中的所有设备都必须属于同一域。

开始之前

- 确定哪台设备将作为主设备。
- 确认指定主/辅助设备关系之前，是否已对设备进行正确布线。有关布线的信息，请参阅《*Firepower* 系统安装指南》。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加堆栈 (Add Stack)**。

步骤 3 从**主要 (Primary)** 下拉列表中，选择已为主要操作布线的设备。

注释 如果选择未作为主设备进行布线的设备，则无法执行后面的一系列步骤。

步骤 4 输入 **Name**。

步骤 5 点击**添加 (Add)** 以选择要包含在堆栈中的设备。

步骤 6 从**主设备上的插槽 (Slot on Primary Device)** 下拉列表中，选择将主设备连接到辅助设备的堆叠网络模块。

步骤 7 从**辅助设备 (Secondary Device)** 下拉列表中，选择已为辅助操作布线的设备。

步骤 8 从**辅助设备上的插槽 (Slot on Secondary Device)** 下拉列表中，选择将辅助设备连接到主设备的堆叠网络模块。

步骤 9 点击 **Add**。

步骤 10 如果是将辅助设备添加到由多台 Firepower 8250、一台 8260、一台 8270 组成的现有堆栈或由多台 8350、一台 8360 或一台 8370 组成的现有堆栈，请重复步骤 5 到步骤 9。

步骤 11 点击**堆栈 (Stack)** 以建立设备堆栈或添加辅助设备。请注意，由于此过程会同步系统数据，因此需要花费几分钟时间。

编辑设备堆栈

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	8140、8200 系列、8300 系列	仅限枝叶	管理员/网络管理员

建立设备堆栈后，对设备配置进行的大多数更改还会更改整个堆栈的配置。在设备编辑器的 Stack 页面上，可以按照与在单台设备的 Device 页面上相同的方式对堆栈配置进行更改。

可以更改堆栈的显示名称，启用和禁用许可证，查看系统和运行状况策略，并配置高级设置。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑配置的堆叠设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 按照更改单一设备配置的方式，使用 Stack 页面上的各部分对堆叠配置进行更改。

配置堆栈中的单台设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	Firepower 8140、8200 系列、8300 系列	仅限枝叶	管理员/网络管理员

建立设备堆栈后，仍可以仅配置堆栈内一台设备的部分属性。可以按照更改单台设备的方式对堆栈中配置的设备进行更改。可以更改设备的显示名称，查看系统设置，关闭或重新启动设备，查看运行状况信息，以及编辑设备管理设置。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑配置的堆叠设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 从**所选设备 (Selected Device)** 下拉列表中，选择要修改的设备。

步骤 5 按照更改单台设备的方式，使用 Devices 页面上的各部分对单个堆叠设备进行更改。

在堆叠设备上配置接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	Firepower 8140、8200 系列、8300 系列	仅限枝叶	管理员/网络管理员

除管理接口以外，可以在堆栈中主设备的“接口”(Interfaces) 页面上配置堆叠设备接口。可以选择堆栈中的任何设备来配置管理接口。

Firepower 堆叠设备的“接口”(Interfaces) 页面包含在单个设备上找到的硬件和接口视图。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在主堆叠设备旁边，点击编辑图标 ()。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**接口**选项卡。

步骤 4 从**所选设备 (Selected Device)** 下拉列表中，选择要修改的设备。

步骤 5 按照在单个设备上进行配置的方式配置接口；请参阅配置传感接口，第 385 页。

分隔堆叠设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	FirePOWER 8140、8200 系列、8300 系列	任意	管理员/网络管理员

如果不再需要对设备使用堆叠配置，则可以中断堆栈并分隔设备。

注释 如果堆叠设备发生故障，或者如果堆叠的成员设备之间通信失败，则您无法使用 Firepower 管理中心 Web 界面分隔堆叠设备。在这种情况下，请使用辅助 CLI 命令 `configure stacking disable` 分别从每个设备中删除堆栈配置。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要中断的设备堆栈旁边，点击中断堆栈图标 ()。

提示 要从由三个或更多 Firepower 8250 设备组成的堆栈中移除辅助设备而不中断堆栈，请点击“从堆栈中移除”图标()。移除辅助设备会导致短暂中断流量检查、流量或链路状态，因为系统会重新配置堆栈以在没有额外设备的情况下运行。

步骤 3 点击**是 (Yes)** 以分隔设备堆栈。

第 VIII 部分

设备平台设置

第 24 章

系统配置

以下主题介绍如何在 Firepower 管理中心和受管设备上配置系统配置：

系统配置简介

系统配置设置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER、NGIPSv）：

- 对于 Firepower 管理中心，这些配置设置是“本地”系统配置的一部分。请注意，Firepower 管理中心上的系统配置特定于单个系统，并且对管理中心的系统配置的更改仅影响该系统。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。创建共享策略，以配置可能在整个部署中类似的适合于受管设备的系统配置设置的子集。

提示 对于 7000 和 8000 系列设备，可以从本地 Web 界面执行有限的系统配置任务，例如控制台配置和远程管理。这些不是使用平台设置策略应用于 7000 或 8000 系列设备的相同配置。

导航 Firepower 管理中心系统配置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

系统配置可识别 Firepower 管理中心的基本设置。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 使用导航面板选择要更改的配置；有关详细信息，请参阅表 58：系统配置设置 ， 第 427 页。

系统配置设置

下表介绍了适用于 Firepower 管理中心的系统配置设置。对于 7000 和 8000 系列设备，该表可确定从设备的本地 Web 界面配置的设置以及使用从 Firepower 管理中心部署的平台设置策略配置的设置。

表 *58*：系统配置设置

设置	说明	也可从以下设置进行配置：	
		平台设置	**7000** 和 **8000** 系列
信息	查看有关设备的当前信息并编辑显示名称；请参阅设备信息，第 429 页。	否	yes
HTTPS 证书	需要时从受信任机构请求 HTTPS 服务器证书，然后将证书上传到系统；请参阅自定义 HTTPS 证书，第 430 页。	否	yes
外部数据库访问 (External Database Access)	启用对数据库的外部只读访问权限，并提供客户端驱动程序供下载；请参阅外部数据库访问设置，第 434 页。	否	否
数据库	指定 Firepower 管理中心可存储的各类事件的最大数量；请参阅数据库事件限制，第 435 页。	否	否
管理接口	更改选项，如设备的 IP 地址、主机名和代理设置；请参阅管理接口配置，第 437 页。	否	yes
Process	关闭、重新启动、或重启与 Firepower 系统相关的进程；请参阅系统关闭和重新启动，第 444 页。	否	yes
Remote Storage Device	配置用于备份和报告的远程存储；请参阅远程存储管理，第 446 页。	否	否
Change Reconciliation	将系统配置为发送过去 24 小时内出现的系统变化的详细报告；请参阅 Change Reconciliation，第 450 页。	否	yes
访问控制首选项 (Access Control Preferences)	将系统配置为在用户添加或修改访问控制策略时提示他们添加注释；请参阅策略更改注释，第 451 页。	否	否
访问列表 (Access List)	控制可以访问特定端口上的系统的计算机；请参阅访问列表，第 453 页。	是	否
审核日志	将系统配置为将审核日志发送到外部主机；请参阅审核日志，第 454 页。	是	否
控制面板	启用控制面板上的“自定义分析”(Custom Analysis) 构件；请参阅Dashboard Settings（控制面板设置），第 456 页。	否	否
DNS 缓存 (DNS Cache)	将系统配置为自动解析事件查看页面上的 IP 地址；请参阅DNS 缓存，第 457 页。	否	否

设置	说明	也可从以下设置进行配置：	
		平台设置	**7000** 和 **8000** 系列
电子邮件通知	配置邮件主机，选择加密方法，并为基于邮件的通知和报告提供身份验证凭证；请参阅邮件通知，第 457 页。	否	否
外部身份验证	为其帐户经过外部身份验证的所有用户设置默认用户角色；请参阅 外部身份验证设置，第 488 页	是	否
入侵策略首选项 (Intrusion Policy Preferences)	将系统配置为在用户修改入侵策略时提示他们添加注释；请参阅策略更改注释，第 451 页。	否	否
语言	为 Web 界面指定不同的语言；请参阅选择语言，第 459 页。	是	否
登录标识	创建在用户登录时显示的自定义登录横幅；请参阅登录横幅，第 460 页。	是	否
网络分析策略首选项 (Network Analysis Policy Preferences)	将系统配置为在用户修改网络分析策略时提示他们添加注释；请参阅策略更改注释，第 451 页。	否	否
SNMP	启用简单网络管理协议 (SNMP) 轮询；请参阅SNMP 轮询，第 461 页。	是	否
STIG 合规性 (STIG Compliance)	确保符合美国国防部规定的特定要求；请参阅STIG 合规性，第 463 页。	是	否
Time	查看当前时间设置，如果当前系统配置中的时间同步设置设定为**在本地配置中手动设置 (Manually in Local Configuration)**，则更改时间；请参阅时间与时间同步，第 464 页。	否	yes
时间同步	更改系统上的时间同步；请参阅时间与时间同步，第 464 页。	是	否
Shell 超时 (Shell Timeout)	配置用户的登录会话由于不活动超时之前的空闲时间量（以分钟为单位）；请参阅会话超时，第 468 页。	是	否
漏洞映射 (Vulnerability Mapping)	将漏洞映射到该地址接收或从该地址发送的任何应用协议流量的主机 IP 地址；请参阅漏洞映射，第 469 页。	否	否
Console Configuration	配置通过 VGA 或串行端口，或通过无人值守管理 (LOM) 进行的控制台访问；请参阅远程控制台访问管理，第 470 页。	否	有限

设置	说明	也可从以下设置进行配置：	
		平台设置	7000 和 8000 系列
VMware 工具	启用并使用 Firepower 管理中心虚拟机上的 VMware 工具；请参阅VMware 工具和虚拟系统，第 477 页。	n/a	n/a

设备信息

Web 界面的“信息”(Information) 页面包含下表中列出的信息。除非另有说明，否则所有字段都为只读。

字段	说明
Name	您为设备指定的名称。请注意，此名称仅在 Firepower 系统环境中使用。尽管您可以使用主机名作为设备的名称，但在此字段中输入其他名称不会更改主机名。
产品型号	设备的型号名称。
Serial Number	设备的序列号。
Software Version	设备上当前安装的软件版本。
Prohibit Packet Transfer to the Firepower 管理中心	指定受管设备是否随事件发送数据包数据，允许数据存储在 Firepower 管理中心。7000 和 8000 系列设备的本地 Web 界面上提供此设置。
操作系统	当前在设备上运行的操作系统。
Operating System Version	当前设备上运行的操作系统的版本。
IPv4 地址	默认 (`eth0`) 管理接口的 IPv4 地址。如果 IPv4 管理处于禁用状态，此字段会予以指出。
IPv6 地址	默认 (`eth0`) 管理接口的 IPv6 地址。如果 IPv6 管理处于禁用状态，此字段会予以指出。
Current Policies	当前部署的系统级策略。如果策略自上一次部署以来已更新，则策略的名称以斜体显示。

字段	说明
型号编号	存储在内部闪存驱动器上的设备特定型号。此编号可能对于故障排除非常重要。

查看和修改系统信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

Firepower 管理中心 Web 界面或 7000 和 8000 系列本地 Web 界面上的信息页面提供有关系统的信息，包括只读信息，例如产品名称和型号。该页面还提供了更改系统的显示名称以及为 7000 和 8000 系列设备禁止数据包传输的选项。

注释 在低带宽部署（不关心触发入侵策略违规的数据包的具体内容）中，禁止数据包传输是个好主意。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 或者，更改系统信息设置：

- 名称 - 要更改显示名称，请在**名称 (Name)** 字段中输入名称。
- 禁止数据包传输 - 要防止将数据包发送到 Firepower 管理中心，请选中**禁止将数据包传输到管理中心 (Prohibit Packet Transfer to the Management Center)** 复选框。此选项只可以从 7000 或 8000 系列设备的本地 Web 界面访问。

步骤 3 点击**保存 (Save)**。

自定义 HTTPS 证书

通过安全套接字层 (SSL) 证书，Firepower 管理中心和 7000 和 8000 系列设备可以在系统和 Web 浏览器之间建立加密通道。所有 Firepower 设备都随附默认证书，但其不是由任何全球知名的证书颁发机构 (CA) 所信任的 CA 生成。因此，请考虑将其替换为由全球知名或内部信任的 CA 签名的自定义证书。

您可以根据系统信息和您提供的识别信息生成证书请求。如果安装有受浏览器信任的内部证书颁发机构 (CA)，则可以使用证书请求对证书进行自签名。您还可以将生成的请求发送到证书颁发机构以请求服务器证书。获得证书颁发机构 (CA) 的签名证书后，您可以导入该证书。

您可以使用客户端浏览器证书检查功能来限制对 Firepower 系统 Web 服务器的访问。启用用户证书时，网络服务器会检查用户的浏览器客户端是否选择了有效的用户证书。所选的用户证书必须由生成服务器证书的同一个可信证书颁发机构生成。浏览器无法在以下任何情况下加载 Web 界面：

- 用户在浏览器中选择的证书无效。
- 用户在浏览器中选择的证书不是由签署服务器证书的证书颁发机构生成。
- 用户在浏览器中选择的证书不是由设备上的证书链中的证书颁发机构生成。

您还可以加载服务器的证书撤销列表 (CRL)。CRL 列出证书颁发机构已撤销的任何证书，因此，Web 服务器可以验证客户端浏览器证书是否有效。如果用户选择在 CRL 中列为已撤销证书的证书，浏览器将无法加载 Web 界面。

查看当前服务器证书

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

只能查看已登录到的设备的服务器证书。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **HTTPS Certificate**。

生成和提交证书签名请求

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	任意	传统	仅全局	管理

当使用此程序通过本地配置“HTTPS 证书”(HTTPS Certificate) 页面生成证书请求时，只能为单个系统生成证书。同样，如果安装不是由全球知名或内部受信任的 CA 签名的证书，则在连接到设备时会接收到安全警告。

为证书请求生成的密钥采用 Base-64 编码的 PEM 格式。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 点击 **Generate New CSR**。

步骤 4 在**国家/地区名称（两字母代码）(Country Name [two-letter code])** 字段中输入国家/地区代码。

步骤 5 在**省/自治区/直辖市 (State or Province)** 字段中输入省/自治区/直辖市的邮编缩写。

步骤 6 输入**地区或城市 (Locality or City)**。

步骤 7 在**组织 (Organization)** 中输入组织名称。

步骤 8 在**组织单位（部门）(Organizational Unit [Department])** 中输入组织单位（部门）名称。

步骤 9 在**公用名 (Common Name)** 字段中输入要为其请求证书的服务器的完全限定域名。

注释 必须准确输入服务器的完全限定域名，因为它将显示在**公用名 (Common Name)** 字段的证书中。如果公用名称与 DNS 主机名不匹配，那么当连接至设备时，您将接收到警告。

步骤 10 点击**生成 (Generate)**。

步骤 11 打开一个文本编辑器。

步骤 12 复制证书请求中的整个文本块（包括 `BEGIN CERTIFICATE REQUEST` 和 `END CERTIFICATE REQUEST` 行），然后将其粘贴到一个空白文本文件中。

步骤 13 将该文件另存为 *servername*`.csr`，其中，*servername* 是计划使用证书的服务器的名称。

步骤 14 点击**保存 (Save)**。

接下来的操作

- 上传签名的服务器证书；请参阅上传服务器证书，第 432 页。

服务器证书上传

如果生成证书的签署机构要求您信任一个中间CA，那么您还必须提供一个证书链（有时称为证书路径）。如果您需要用户证书，这些证书必须由其中间机构包括在证书链中的证书颁发机构生成。

上传服务器证书

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

如果生成证书的签署机构要求您信任一个中间CA，那么您还必须提供一个证书链（有时称为证书路径）。如果您需要用户证书，这些证书必须由其中间机构包括在证书链中的证书颁发机构生成。

开始之前

- 生成证书签名请求；请参阅生成和提交证书签名请求，第 431 页。
- 将 CSR 文件上传至您想要向其请求证书的证书颁发机构，或者使用 CSR 来创建自签证书。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 点击 **Import HTTPS Certificate**。

步骤 4 在文本编辑器中打开服务器证书，复制整个文本块（包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行），然后将其粘贴到**服务器证书 (Server Certificate)** 字段中。

步骤 5 如果要上传私钥，请打开私有密钥文件，复制整个文本块（包括 `BEGIN RSA PRIVATE KEY` 和 `END RSA PRIVATE KEY` 行），然后将其粘贴到**私钥 (Private Key)** 字段中。

步骤 6 打开您需要提供的每一个中间证书，复制整个文本块，然后将其复制到 **Certificate Chain** 字段中。

步骤 7 点击**保存 (Save)**。

需要有效的用户证书

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

系统支持上传采用可区别编码规则 (DER) 格式的 CRL。对一台服务器只能上传一个 CRL。

要确保撤销证书列表是最新的，您可以创建计划任务来更新CRL。界面中会列出CRL的最新更新。

注释 要启用用户证书以便访问网络界面，浏览器中**必须**存在有效的用户证书（或者您的读卡器中已插入 CAC）。

开始之前

- 使用服务器证书所用的同一证书颁发机构来生成用户证书。
- 上传证书的中间证书；请参阅服务器证书上传，第 432 页。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **HTTPS Certificate**。

步骤 3 选择**启用用户证书 (Enable User Certificates)**。如有提示，请从下拉列表中选择相应的证书。

步骤 4 如果要检索 CRL，请选择**启用 CRL 获取 (Enable Fetching of CRL)**。

步骤 5 输入现有 CRL 文件的有效 URL，然后点击**刷新 CRL (Refresh CRL)**。所提供的 URL 的当前 CRL 会加载到服务器。

注释 启用 CRL 获取功能会创建计划任务来定期更新 CRL。编辑任务以设置更新的频率。

步骤 6 验证您是否拥有由创建服务器证书的同一证书颁发机构生成的有效用户证书。

注意 如果保存包含已启用用户证书的配置，但浏览器证书存储中无有效用户证书，则会禁用对设备的所有 Web 服务器访问。请确保在保存设置之前已安装有效证书。

步骤 7 点击**保存 (Save)**。

外部数据库访问设置

您可以将Firepower管理中心配置为允许第三方客户端对其数据库进行只读访问。这样，您可以通过以下任何方式使用 SQL 来查询数据库：

- 行业标准报告工具（例如，Actuate BIRT、JasperSoft iReport 或 Crystal Reports）
- 其他任何支持 JDBC SSL 连接的报告应用（包括自定义应用）
- 思科提供的命令行 Java 应用，名为 RunQuery，可以交互方式运行或用于获取单一查询的以逗号分隔的结果

使用Firepower管理中心的系统配置启用数据库访问，并创建允许选定主机查询数据库的访问列表。请注意，该访问列表不用于控制设备访问。

您也可以下载包含以下工具的软件包：

- RunQuery（这是思科提供的数据库查询工具）
- InstallCert（可以用于从要访问的Firepower 管理中心检索和接受 SSL 证书的工具）
- 连接到数据库时必须使用的 JDBC 驱动程序

有关使用下载包中的工具来配置数据库访问的信息，请参阅《《*Firepower* 系统数据库访问指南》》。

启用对数据库的外部访问

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击**外部数据库访问 (External Database Access)**。

步骤 3 选中**允许外部数据库访问 (Allow External Database Access)** 复选框。

步骤 4 在**服务器主机名 (Server Hostname)** 字段中输入相应的值。根据第三方应用要求，此值可以是 Firepower 管理中心的完全限定域名 (FQDN)、IPv4 地址或 IPv6 地址。

步骤 5 点击 **Client JDBC Driver** 旁边的 **Download** 并按照浏览器提示下载 `client.zip` 软件包。

步骤 6 要为一个或多个 IP 地址添加数据库访问权限，请点击 **Add Hosts**。此时，**Access List** 字段中将会显示 **IP Address** 字段。

步骤 7 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 8 点击 **Add**。

步骤 9 点击 **Save**。

提示 如果要恢复为上次保存的数据库设置，请点击**刷新 (Refresh)**。

数据库事件限制

您可以指定 Firepower 管理中心可存储的各类事件的最大数量。为提高性能，应将事件数量限制设置为您通常处理的事件数量。对于某些事件类型，可以禁用存储功能。

系统自动删除设备数据库中的入侵事件、发现事件、审核记录、安全情报数据或 URL 过滤数据。您可以配置系统以在删除事件时生成自动邮件通知。您也可以手动删除发现和用户数据库以删除所选发现数据；并且可以清除 Firepower 管理中心数据块中的发现和连接数据。

配置数据库事件限制

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

开始之前

- 如果要在从 Firepower 管理中心的数据库中修剪事件时收到邮件通知，则必须配置邮件服务器；请参阅配置邮件中继主机和通知地址，第 458 页。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 选择**数据库 (Database)**。

步骤 3 对于每个数据库，请输入要存储的记录的数量。
有关每个数据库可维护的记录的数量，请参阅数据库事件限制，第 436 页。

步骤 4 或者，在**数据修剪通知地址 (Data Pruning Notification Address)** 字段中，输入要接收修剪通知的邮箱地址。

步骤 5 点击**保存 (Save)**。

数据库事件限制

下表列出可在 Firepower 管理中心上存储的每种事件类型记录的最小和最大数量。

表 *59*: 数据库事件限制

事件类型	上限	下限
入侵事件	1000 万（管理中心虚拟） 2000 万 (MC750) 3000 万 (MC1500) 6000 万 (MC2000) 1.5 亿 (MC3500) 3 亿 (MC4000)	10,000
发现事件	1000 万 2000 万（MC2000 和 MC4000）	0（禁用存储）
连接事件 安全情报事件	4900 万（管理中心虚拟） 5000 万 (MC750) 1 亿 (MC1500) 3 亿 (MC2000) 5 亿 (MC3500) 10 亿 (MC4000) 连接事件和安全情报事件共用数量限制。配置的最大数量总和不能超过此限制。	0（禁用存储）

事件类型	上限	下限
连接摘要（汇聚连接事件）	1000 万（管理中心虚拟） 5000 万 (MC750) 1 亿 (MC1500) 3 亿 (MC2000) 5 亿 (MC3500) 10 亿 (MC4000)	0（禁用存储）
关联事件和合规白名单事件	100 万个 200 万（MC2000 和 MC4000）	一个
恶意事件	1000 万 2000 万（MC2000 和 MC4000）	10,000
文件事件	1000 万 2000 万（MC2000 和 MC4000）	0（禁用存储）
运行状况事件	100 万个	0（禁用存储）
审核记录	100,000	一个
补救状态事件	1000 万	一个
白名单违例历史记录	30 天的违例历史记录	1 天的历史记录
用户活动（用户事件）	1000 万	一个
用户登录（用户历史记录）	1000 万	一个
入侵规则更新导入日志记录	100 万个	一个

管理接口配置

首次设置设备时，应配置设备的网络设置，以便其可在内部受保护的网络中通信。在设置后，可以更改这些网络设置并配置其他设置，例如代理。可以更改设置以改进性能，启用不同功能，或者修改部署中的网络配置。

对于 Firepower 管理中心与 7000 和 8000 系列设备，可以将设备的 Web 界面用于：

- 启用流量通道并配置其他管理接口以提高性能。

- 查看或编辑到默认管理接口的路由，或查看路由统计信息，或创建到其他网络的新路由以管理和隔离 Firepower 管理中心和不同网络上设备之间的流量。
- 指定最多三个 DNS 服务器以及设备的主机名和域。
- 更改管理端口。
- 配置代理服务器的使用，您可以通过 HTTP 摘要对代理服务器进行身份验证。
- 允许用户使用 LCD 面板更改网络设置。

管理接口

管理接口提供Firepower管理中心与其管理的设备之间的通信方式。在设备之间维持良好的流量控制是部署成功的关键。

在7000和8000系列设备以及物理和虚拟Firepower管理中心上，您可以更改默认配置，以在Firepower管理中心和/或设备上启用管理接口，从而将设备之间的流量归入两个单独的流量通道。管理流量信道传送所有内部流量（例如特定于设备和系统管理的设备内部流量），事件流量信道传送所有事件流量（例如网络事件）。当您要将流量拆分为两个信道时，请在两个设备之间创建两个连接点，以提高吞吐量，从而提高性能。您还可以启用多个管理接口，每个管理接口拥有一个唯一IP地址（IPv4或IPv6）和主机名，从而分离和管理流量信道，同时仍可提供更大的吞吐量。

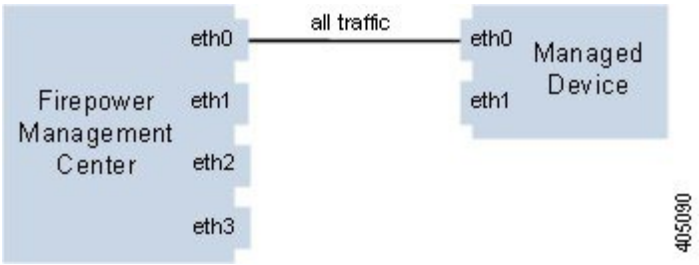
利用多个管理接口，您还可以只使用一个Firepower管理中心隔离和管理来自不同网络的流量。使用管理接口向目标网络添加静态路由，并将设备注册到单独的管理接口，以确保来自一个网络的流量与另一个网络上的流量隔离。可以在同一接口上发送两个流量信道，或者，如果有足够的附加管理接口，则既可以隔离网络流量，又可以将每个管理接口配置为仅传送一个流量信道。

管理接口通常位于设备背面。有关详细信息，请参阅《*Firepower*系统安装指南》中的“识别管理接口”。

单一管理接口

当您向Firepower 管理中心注册您的设备时，会建立一个传送Firepower 管理中心上的管理接口和设备上的管理接口之间所有流量的通信信道。

下图显示默认的单一通信信道。一个接口传送包含管理和事件流量的通信信道。



多个管理接口

您可以启用并配置多个管理接口，每个接口使用唯一的 IP 地址（IPv4 或 IPv6）和（可选的）主机名，通过将每个流量信道发送至不同的管理接口提高流量吞吐量。配置具有较小容量的接口以承载较轻的管理流量负载，配置较高容量的接口以承载较繁重的事件流量负载。您可以注册设备以分离管理接口，并为同一接口配置两个通信信道，或者使用一个专用管理接口传送由Firepower管理中心管理的所有设备的事件流量信道。

您还可以从您的Firepower管理中心上的特定管理接口创建通向不同网络上的设备的路由。当您向非默认管理接口注册不同网络上的设备时，该设备上的流量会与向默认 (`eth0`) 管理接口注册的设备上的流量隔离。

非默认管理接口的许多功能与默认管理接口相同，但以下情况除外：

- 只能在默认 (`eth0`) 管理接口上配置 DHCP。其他（`eth1` 等）接口需要唯一的静态 IP 地址和主机名。
- 当您使用一个非默认的管理接口来连接Firepower管理中心和受管设备，且这些设备被一台 NAT 设备隔开时，您必须配置两条流量信道使用同一个管理接口。
- 只能在默认管理接口上使用无人值守管理。
- 在 70xx 系列中，可以将流量分开到两个通道中并配置这些通道，以将流量发送到 Firepower 管理中心上的一个或多个管理接口。但是，由于 70xx 系列仅包含一个管理接口，因此设备仅在一个管理接口上接收从 Firepower 管理中心发送的流量。

流量通道

在一个管理接口上使用两个流量信道时，会在Firepower管理中心和受管设备之间创建两个连接。一个信道传送管理流量，一个信道传送事件流量，这两种流量在同一接口上单独进行传送。

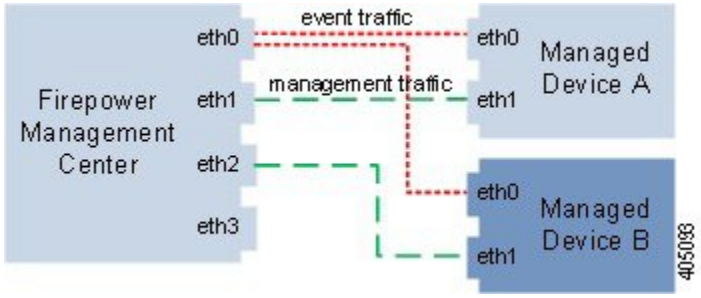
以下示例显示同一接口上有两个独立流量信道的通信信道。

使用多个管理接口时，可以在两个管理接口上划分流量信道，进而可以通过添加两个接口的容量来增加流量，从而进一步提高性能。一个接口传送管理流量信道，另一个接口传送事件流量信道。如果任一接口发生故障，则所有流量重新路由到活动接口，并且连接得以维持。

下图显示了两个管理接口上的管理流量信道和事件流量信道。

可以使用专用管理接口仅传送来自多台设备的事件流量。在此配置中，每台设备分别注册到不同管理接口上以传送管理流量信道，并且Firepower管理中心上的一个管理接口传送来自所有设备的所有事件流量信道。如果任一接口发生故障，流量重新路由到活动接口，并且连接得以维持。请注意，由于所有设备的事件流量都在同一接口上传送，因此未在网络之间隔离流量。

下图显示了使用不同管理通道流量接口的两台设备共用相同的事件流量信道专用接口。



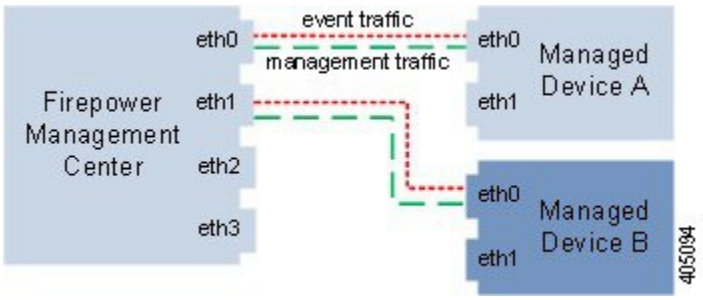
网络路由

您可以从Firepower管理中心上的特定管理接口创建通向不同网络的路由。当您从该网络向Firepower管理中心上指定的管理接口注册设备时，您将在Firepower管理中心和其他网络上的设备之间提供一个隔离连接。将两个流量信道配置为使用相同的管理接口，以确保来自该设备的流量与其他网络上的设备流量保持隔离。由于路由接口与Firepower管理中心上的所有其他接口隔离，因此，如果路由管理接口发生故障，连接会丢失。

提示 思科建议您在使用除默认 (`eth0`) 管理接口之外的任何管理接口注册 Firepower 管理中心及其设备时使用静态 IP 地址。只有默认的管理接口上才支持 DHCP。

安装Firepower 管理中心后，使用网络界面配置多个管理接口。

下图显示通过为所有流量使用独立管理接口隔离网络流量的两台设备。您可以添加更多管理接口，为每台设备配置独立的管理和事件流量信道接口。



管理接口配置选项

接口

Firepower 系统为 IPv4 和 IPv6 管理环境提供了双堆栈实施。可以选择这两个协议或其中之一，如果不想使用，也可以禁用协议（如果有）。

对于每个管理协议，必须指定默认 (`eth0`) 管理接口的 IP 地址、子网掩码或前缀长度和默认网关。可以手动设置这些设置，或者将设备配置为会从本地 DHCP 服务器或 IPv6 路由器检索这些设置。请注意，必须手动配置您所启用的每个附加管理接口（`eth1` 等）。

可以对管理接口配置以下选项：

- **已启用 (Enabled)** - 启用管理接口。在启用并保存另一管理接口之前，请**勿**禁用默认管理接口。
- **通道 (Channels)** - 启用接口上的 **管理流量 (Management Traffic)** 和**事件流量 (Event Traffic)** 通道。

  可以启用流量通道（管理流量和/或事件流量），以便在管理接口的通信通道中创建不同的连接。此外，还可以在多个管理接口上建立流量信道，从而合并两个接口的吞吐量以进一步提高性能。

- **模式 (Mode)** - 可更改默认“自动协商”或指定链路模式。请注意，您对“自动协商”作出的所有更改将被千兆接口忽略。

  请注意，向 Firepower 管理中心注册 8000 系列受管设备时，必须在连接两端自动协商或在两端设置相同的静态速度，以确保稳定的网络链路。8000 系列受管设备不支持半双工网络链路，也不支持两端的速度或双工配置存在差异的连接。

- **MTU** - 可更改默认设置。MTU 的设置范围可能因型号和接口类型而异。

注释 不同于其他接口，当您部署配置更改时，在该管理接口更改最大传输单位 (MTU) 不会中断设备上的流量。

表 *60*：按设备列出的管理接口 *MTU* 范围

设备型号	MTU 范围
NGIPSv	576 - 9018
7000 和 8000 系列默认 (eth0)	576 - 9234
7000 和 8000 系列非默认（eth1 等）	1518 - 9018

由于系统会自动从配置的 MTU 值修剪掉 18 字节，因此任何低于 1298 的值均不符合最小 IPv6 MTU 设置 1280，任何低于 594 的值均不符合最小 IPv4 MTU 设置 576。例如，系统会自动将配置值 576 调整为 558。

- **MDI/MDIX** - 允许更改默认的**自动 MDIX (Auto-MDIX)** 设置。
- **IPv4 配置 (IPv4 Configuration)** - 允许配置选择**静态 (Static)**、**DHCP** 或**已禁用 (Disabled)**。

  选择 **Static** 可输入 IPv4 管理 IP 地址和子网掩码。

  选择 **DHCP** 可从 DHCP 服务器检索网络设置（仅 eth0）。

  选择 **Disabled** 将会禁用协议。请**勿**同时禁用 IPv4 和 IPv6。

- **IPv6 配置 (IPv6 Configuration)** - 允许配置**静态 (Static)**、**DHCP**、**已分配路由器 (Router Assigned)** 或**已禁用 (Disabled)**。

  选择 **Static** 可输入 IPv4 管理 IP 地址和子网掩码。

  选择 **DHCP** 可从 DHCP 服务器检索网络设置（仅 eth0）。

  选择 **Router Assigned** 可从本地 IPv6 路由器检索网络设置。

  选择 **Disabled** 将会禁用协议。请**勿**同时禁用 IPv4 和 IPv6。

路由

点击编辑图标()可查看或编辑到默认管理接口的路由，点击查看图标()可查看路由统计信息。

可以创建到其他网络的新路由。点击添加图标()以显示一个弹出窗口，可以在该窗口中输入目标网络 IP 地址、子网掩码或前缀长度、接口和网关。例如，在 Firepower 管理中心上，可以创建到其他网络上设备的路由，以使一个 Firepower 管理中心能够管理和隔离来自其他网络上设备的流量。您可以在特定管理接口上配置以下设置来创建通向某个网络的路由：

- **目标 (Destination)** - 要创建路由的网络的目标地址。
- **网络掩码 (Netmask)** 或**前缀长度 (Prefix Length)** - 网络的网络掩码 (IPv4) 或前缀长度 (IPv6)。
- **接口 (Interface)** - 设备上分配给新路由的管理接口。
- **网关 (Gateway)** - 新网络的网关。

共享设置

系统设备使用双向、SSL 加密的通信通道（默认情况下在端口 8305 上）进行通信。思科强烈建议保留默认设置。但如果管理端口与网络上的其他通信冲突，则可以选择其他端口。

注意 如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。

LCD 面板

可以使用 7000 或 8000 系列设备上的 LCD 面板来编辑设备的 IP 地址。确认所做的所有更改均在管理 Firepower 管理中心上反映。在某些情况下，可能还需要在 Firepower 管理中心上手动更新数据。

注意 允许使用 LCD 面板进行重新配置可能带来安全风险。要使用 LCD 面板配置网络设置，只需进行物理访问，而不需要进行身份验证。

代理

所有 Firepower 系统设备都配置为通过 443/tcp (HTTPS) 端口和 80/tcp (HTTP) 端口直接连接到互联网。设备支持使用代理服务器（可以通过 HTTP 摘要对代理服务器进行身份验证）。

注意 使用 NT LAN Manager (NTLM) 身份验证的代理无法与 AMP 云或思科　综合安全情报 (CSI) 通信。

编辑管理接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

注释 必须使用命令行工具修改NGIPSv设备的网络和代理设置。有关详细信息，请参阅《*Cisco Firepower NGIPSv for VMware* 快速入门指南》。

使用 Firepower 管理中心的 Web 界面来修改管理中心上的默认管理接口的默认设置，以便更改管理接口设置及配置其他网络设置（例如，代理）。在 7000 和 8000 系列设备（物理和虚拟 Firepower 管理中心）上，还可以启用和配置流量通道和其他管理接口。您对自动协商值做出的所有更改将被千兆接口忽略。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 选择**管理接口 (Management Interfaces)**。

步骤 3 如果要修改接口，在**接口 (Interfaces)** 下，点击要配置的接口旁边的**编辑 (Edit)**，并修改选项，如管理接口配置选项，第 441 页中所述。

步骤 4 如果要修改路由，在**路由 (Routes)** 下修改选项，如管理接口配置选项，第 441 页中所述。

步骤 5 如果要修改共享设置，必须在**共享设置 (Shared Settings)** 下修改选项，如管理接口配置选项，第 441 页中所述。请注意，如果在上一步骤中选择了 **DHCP**，将无法手动指定这些共享设置。

注意 思科**强烈**建议保留默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，必须更改部署中需要相互通信的**所有**设备的该端口。

步骤 6 在7000 和 8000 系列 设备的 LCD 面板下，选中**允许重新配置网络设置 (Allow reconfiguration of network settings)** 复选框，以允许使用设备的 LCD 面板来更改网络设置。

注意 允许使用 LCD 面板进行重新配置可能带来安全风险。要使用 LCD 面板配置网络设置，只需进行物理访问，而不需要进行身份验证。网络界面会提醒您，启用此选项是潜在的安全问题。

步骤 7 如果要使用代理，在**代理 (Proxy)** 下执行以下操作：

a) 选中**已启用 (Enabled)** 复选框。

b) 在 **HTTP 代理 (HTTP Proxy)** 字段中，输入代理服务器的 IP 地址或完全限定域名。

c) 在**端口 (Port)** 字段中，输入端口号。

d) 或者，通过选择**使用代理身份验证 (Use Proxy Authentication)** 来提供身份验证凭证，然后提供**用户名 (User Name)** 和**密码 (Password)**。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 如果要在系统日志中反映设备的新主机名，请重新启动设备。在重启之前，名称不会反映出来。

系统关闭和重新启动

使用 Firepower 系统的 Web 界面来控制设备上的进程的关闭和重新启动。通过关闭设备，可让系统做好准备，在不丢失配置数据的情况下安全断电和重新启动。

有多种方法可以控制 Firepower 管理中心上的进程。您可以：

- 关闭系统 - 启动 Firepower 系统的正常关闭。
- 重新启动系统 - 有条不紊地关闭并重新启动系统。
- 重新启动控制台 - 重新启动通信、数据库和 HTTP 服务器进程。这通常在故障排除过程中使用。

这些选项也可用于 7000 和 8000 系列受管设备。您还可以重新启动这些设备上的 Snort 进程。

注意 重新启动 Snort 进程会暂时中断流量检查。流量在此中断期间丢弃还是通过而无需进检查取决于受管设备的型号及其处理流量的方式。

注意 请**勿**使用电源按钮关闭设备；这样做可能导致数据丢失。通过 Web 界面完全关闭设备。

对于 Firepower 虚拟受管设备，VMware 等虚拟基础设施通常会提供可配置的电源选项，用于定义虚拟机关闭、重新启动或暂停的方式。请查阅您的虚拟平台的文档以确定如何设置这些选项。

注释 对于在 VMware 上运行的 Firepower 虚拟受管设备，自定义电源选项是 VMware 工具的一部分，因此必须在虚拟机上安装 VMware 工具才能配置正常关闭。

关闭并重新启动系统

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 选择**进程 (Process)**。

步骤 3 要关闭设备，请执行以下操作：

- 管理中心 - 点击**关闭管理中心 (Shutdown Management Center)** 旁边的**运行命令 (Run Command)**。
- 受管设备 - 点击**关闭设备 (Shutdown Appliance)** 旁边的**运行命令 (Run Command)**。

步骤 4 要重新引导设备，请执行以下操作：

- 管理中心 - 点击**重新引导管理中心 (Reboot Management Center)** 旁边的**运行命令 (Run Command)**。
- 受管设备 - 点击**重新引导设备 (Reboot Appliance)** 旁边的**运行命令 (Run Command)**。

注释 重新引导 Firepower 管理中心或受管设备时，此操作会注销设备，并且系统会执行可能需要 1 小时才能完成的数据库检查。

步骤 5 要重新启动设备，请执行以下操作：

- 管理中心 - 点击**重新启动管理中心 (Restart Management Center)** 旁边的**运行命令 (Run Command)**。
- 受管设备 - 点击**重新启动设备控制台 (Restart Appliance Console)** 旁边的**运行命令 (Run Command)**。

注释 重新启动 Firepower 管理中心可能导致已删除的主机重新显示在网络映射中。

步骤 6 要重新启动受管设备上的 Snort 进程，请点击**重新启动 Snort (Restart Snort)** 旁边的**运行命令 (Run Command)**。

注释 此命令仅在 7000 和 8000 系列设备的本地 Web 界面中可用。

注意 临时重新启动 Snort 进程会中断流量。流量在此中断期间丢弃还是通过而无需进检查取决于受管设备的型号及其处理流量的方式。

远程存储管理

在 Firepower 管理中心上，您可以将本地或远程存储的以下系统用于备份和报告：

- 网络文件系统 (NFS)
- 服务器消息块 (SMB)/通用互联网文件系统 (CIFS)
- 安全外壳 (SSH)

注释 系统仅支持服务器消息块协议的第一版用于备份和远程存储。

不能将备份发送到一个远程系统而将报告发送到另一个，但是，可以选择这二者之一发送到远程系统，并将另一个存储在 Firepower 管理中心。

提示 在配置并选择远程存储之后，**只有**在**未**增加连接数据库限制的情况下，才可以切换回本地存储。

配置本地存储

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 选择**远程存储设备 (Remote Storage Device)**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择**本地（无远程存储）(Local [No Remote Storage])**。

步骤 4 点击**保存 (Save)**。

为远程存储配置 NFS

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

开始之前

- 确保外部远程存储系统可正常工作且能够从管理中心进行访问。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **NFS**。

步骤 4 添加连接信息：

- 在 **Host** 字段中输入存储系统的 IPv4 地址或主机名。
- 在 **Directory** 字段中输入存储区域的路径。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 450 页。

步骤 6 在**系统使用 (System Usage)** 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。
- 然后，在 **Disk Space Threshold** 中输入要备份远程存储的磁盘空间阈值。默认值为 90%。

步骤 7 要测试设置，请点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

为远程存储配置 SMB

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

开始之前

- 确保外部远程存储系统可正常工作且能够从管理中心进行访问。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **SMB**。

步骤 4 添加连接信息：

- 在 **Host** 字段中输入存储系统的 IPv4 地址或主机名。
- 在 **Share** 字段中输入存储区域共享。请注意，系统只能识别顶级共享，不能识别完整文件路径。要将指定的共享目录用作远程备份目标，必须在 Windows 系统上共享该目录。
- 或者，在 **Domain** 字段中输入远程存储系统的域名。
- 在 **Username** 字段中输入存储系统的用户名，在 **Password** 字段中输入该用户的密码。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 450 页。

步骤 6 在**系统使用 (System Usage)** 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。

步骤 7 要测试设置，请点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

为远程存储配置 SSH

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

注意 如果已在设备上启用 STIG 合规性，那么将无法对该设备使用 SSH 进行远程存储。

开始之前

- 确保外部远程存储系统可正常工作且能够从Firepower 管理中心进行访问。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **Remote Storage Device**。

步骤 3 从**存储类型 (Storage Type)** 下拉列表中选择 **SSH**。

步骤 4 添加连接信息：

- 在**主机 (Host)** 字段中输入存储系统的 IP 地址或主机名。
- 在 **Directory** 字段中输入存储区域的路径。
- 在 **Username** 字段中输入存储系统的用户名，在 **Password** 字段中输入该用户的密码。要将网络域指定为连接用户名的一部分，请在用户名前面加上域后跟正斜杠 (/)。
- 要使用 SSH 密钥，请将 **SSH Public Key** 字段中的内容复制到 authorized_keys 文件中。

步骤 5 或者，选中**使用高级选项 (Use Advanced Options)** 复选框并输入任何所需命令行选项；请参阅远程存储管理高级选项，第 450 页。

步骤 6 在“系统使用”(System Usage) 下：

- 选择**用于备份 (Use for Backups)** 以将备份存储在指定主机上。
- 选择**用于报告 (Use for Reports)** 以将报告存储在指定主机上。

步骤 7 如果要测试设置，必须点击**测试 (Test)**。

步骤 8 点击**保存 (Save)**。

远程存储管理高级选项

如果选择网络文件系统 (NFS) 协议、服务器消息阻止 (SMB) 协议或 SSH 以使用安全复制 (SCP) 来存储报告和备份，您可以选择**使用高级选项 (Use Advanced Options)** 复选框，以使用其中一个安装二进制选项，如 NFS、SMB 或 SSH 安装人员页面所记录。

如果选择 SMB 时，可以在**命令行选项 (Command Line Options)** 字段中使用以下格式进入安全模式：

`sec=`*`mode`*
其中，`mode` 是要用于远程存储的安全模式。

表 *61*：*SMB* 安全模式设置

模式	说明
[无]	尝试连接为 NULL 用户（无名称）。
`krb5`	使用 Kerberos V5 验证。
`krb5i`	使用 Kerberos 身份验证和数据包签名。
`ntlm`	使用 NTLM 密码散列。（默认设置）
`ntlmi`	使用带签名的 NTLM 密码散列（如果 `/proc/fs/cifs/PacketSigningEnabled` 已启用或服务器需要签名，则可能使用默认设置）。
`ntlmv2`	使用 NTLMv2 密码散列。
`ntlmv2i`	使用带数据包签名的 NTLMv2 密码散列。

Change Reconciliation

要监控用户进行的更改并确保它们符合您的组织的首选标准，可以将系统配置为通过邮件发送有关过去 24 小时内进行的更改的详细报告。每当用户保存对系统的配置更改，就会生成更改快照。更改调节报告将汇总这些快照的信息以提供最新系统更改的清晰摘要。

以下示例图表显示示例更改调节报告的“用户”部分，并且列出每个配置更改前和更改后的值。如果用户多次更改同一配置，报告会按时间顺序列出每次不同更改的摘要，最近的更改最先列出。

可以查看过去 24 小时内所做的更改。

配置更改调节

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	仅全局	管理

开始之前

- 配置邮件服务器，以接收过去 24 小时对系统进行的更改的报告邮件；有关详细信息，请参阅配置邮件中继主机和通知地址，第 458 页。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **Change Reconciliation**。

步骤 3 选中 **Enable** 复选框。

步骤 4 从**运行时间 (Time to Run)** 下拉列表中选择您希望系统每天发出更改调节报告的具体时间。

步骤 5 在**邮件收件人 (Email to)** 字段中输入邮箱地址。

提示 添加邮箱地址后，点击**重新发送上一报告 (Resend Last Report)** 以向收件人发送另一个最新更改调节报告的副本。

步骤 6 如果要包含策略更改，请选中**包含策略配置 (Include Policy Configuration)** 复选框。

步骤 7 如果要包含过去 24 小时进行的所有更改，请选中**显示完整更改历史记录 (Show Full Change History)** 复选框。

步骤 8 点击**保存 (Save)**。

更改调节选项

包括策略配置 (Include Policy Configuration) 选项用于控制系统是否在更改调节报告中包括策略更改记录。这包括对访问控制策略、入侵策略、系统策略、运行状况策略和网络发现策略的更改。如果未选择该选项，报告将不会显示对任何策略的更改。此选项仅在 Firepower 管理中心上可用。

显示完整更改历史记录 (Show Full Change History) 选项用于控制系统是否在更改调节报告中包括过去 24 小时内发生的所有更改的记录。如果未选择该选项，报告仅包括每个类别的更改的整合视图。

策略更改注释

当用户修改访问控制、入侵或网络分析策略时，可以配置 Firepower 系统以使用注释功能跟踪多个与策略相关的更改。

在启用策略更改注释的情况下，管理员可以快速评估修改部署中的关键策略的原因。或者，可以将对入侵策略和网络分析策略的更改写入到审核日志中。

配置跟踪策略更改的注释

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

可以将Firepower系统配置为在用户修改访问控制策略、入侵策略或网络分析策略时提示他们添加注释。可以使用注释来跟踪用户更改策略的原因。如果对策略更改启用了注释功能，则可以将注释设置为可选或必填项。每次保存对策略所作的新更改时，系统都会提示用户输入注释。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。
系统配置选项显示在左侧导航面板中。

步骤 2 为以下各项配置策略注释首选项：

- 点击**访问控制首选项 (Access Control Preferences)** 为访问控制策略配置注释首选项。
- 点击**入侵策略首选项 (Intrusion Policy Preferences)** 为入侵策略配置注释首选项。
- 点击**网络分析策略首选项 (Network Analysis Policy Preferences)** 为网络分析策略配置注释首选项。

步骤 3 每个策略类型有以下选项：

- **已禁用 (Disabled)** - 禁用更改注释。
- **可选 (Optional)** - 让用户可以根据需要在注释中描述其更改。
- **必需 (Required)** - 要求用户在保存之前在注释中描述其更改。

步骤 4 对于入侵或网络分析策略注释，还可以：

- 选中**将入侵策略中的更改写入审核日志 (Write changes in Intrusion Policy to audit log)** 以将所有入侵策略更改写入审核日志。
- 选中**将网络分析策略中的更改写入审核日志 (Write changes in Network Analysis Policy to audit log)** 以将所有网络分析策略更改写入审核日志。

步骤 5 点击**保存 (Save)**。

访问列表

在 Firepower 管理中心和典型受管设备上，可以使用访问列表限制 IP 地址和端口对系统的访问。默认情况下，可为任何 IP 地址启用以下端口：

- 443 (HTTPS) - 用于 Web 界面访问。
- 22 (SSH) - 用于命令行访问。

也可以在端口 161 上添加轮询 SNMP 信息的访问权限。

注意 默认情况下，访问**不**受限制。要在更安全的环境中操作，请考虑为特定 IP 地址添加访问权限，然后删除默认的 `any` 选项。

配置系统的访问列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

请注意，此访问列表不会控制外部数据库访问。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**访问列表 (Access List)**。

步骤 3 或者，要删除某一当前设置，请点击删除图标 ( )。

注意 对于您目前用来连接到设备接口的 IP 地址，如果您删除了它的访问权限，而且无“`IP=any port=443`”这一条目，那么当您部署该策略时，您将失去对系统的访问权限。

步骤 4 要添加对一个或多个 IP 地址的访问权限，请点击**添加规则 (Add Rules)**。

步骤 5 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 6 选择 **SSH**、**HTTPS**、**SNMP** 或其组合，以指定要为这些 IP 地址启用哪些端口。

步骤 7 点击 **Add**。

步骤 8 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

审核日志

Firepower 管理中心和典型受管设备记录用户活动的只读审核信息。在管理中心和 7000 和 8000 系列 Web 界面上，审核日志显示在标准事件视图中。在此事件视图中，您可以根据审核视图中的任何项目查看、排序和过滤审核日志消息。您可以轻松删除和报告审核信息，也可以查看用户所做更改的详细报告。

您可以配置 Firepower 管理中心和典型受管设备以将审核日志消息发送到系统日志。为此，您可指定系统日志服务器，以及与消息相关联的严重性、设施和可选标记。标记与审核日志消息一同显示在系统日志中。设备指明创建消息的子系统，严重性界定消息的严重性。系统日志消息不包含设施和严重性；这些值告知接收系统日志消息的系统如何对这些消息进行分类。

您也可以配置 Firepower 管理中心和典型受管设备以将审核日志消息传输到 HTTP 服务器。

审核日志的流式传输设置是不同配置的一部分，具体取决于设备的类型：

- 对于 Firepower 管理中心，传输审核日志是系统配置的一部分。
- 对于典型受管设备，审核日志的流式传输设置是 Firepower 管理中心平台设置策略的一部分。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

配置外部流式传输的审核日志

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

以下是输出结构的示例：

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

其中，本地日期、时间和主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如：

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page
View
```

开始之前

- 确保外部主机可正常工作，且可以通过发送审核日志的系统进行访问。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**审核日志 (Audit Log)**。

步骤 3 从**将审核日志发送到系统日志 (Send Audit Log to Syslog)** 下拉菜单中选择**已启用 (Enabled)**。

步骤 4 在 **Host** 字段中，使用 IP 地址或完全限定的主机名称指定审核信息的目标主机。默认端口 (514) 已被使用。

注意 对于您配置用于接收审核日志的计算机，如果未将其设置为可接收远程消息，主机将不会接受审核日志。

步骤 5 选择系统日志**消息来源 (Facility)**。

步骤 6 选择**严重性 (Severity)**。

步骤 7 或者，也可在**标记（可选）(Tag [optional])** 字段中插入参考标记。

步骤 8 要将定期审核日志更新发送到外部 HTTP 服务器，请从**将审核日志发送到 HTTP 服务器 (Send Audit Log to HTTP Server)** 下拉列表中选择**已启用 (Enabled)**。

步骤 9 在 **URL to Post Audit** 字段中，指定要用于发送审核信息的 URL。必须输入与将会监听下列 HTTP POST 变量的监听程序相对应的 URL：

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`

- result
- time
- tag（如果已如上所述进行了定义）

注意　要允许发送加密的信息，您必须使用HTTPS URL。请注意，将审核信息发送到外部URL可能会影响系统性能。

步骤 10　点击保存 (Save)。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

Dashboard Settings（控制面板设置）

控制面板通过使用构件提供当前系统状态的概要视图；构件是一些独立的小组件，可提供有关Firepower 系统不同方面的信息。Firepower 系统配置了数个预定义控制面板构件。

您可以配置 Firepower 管理中心，以便在控制面板上启用“自定义分析”(Custom Analysis) 构件。

启用控制面板的自定义分析构件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

使用“自定义分析”(Custom Analysis) 控制面板构件，根据灵活的用户可配置查询创建事件的直观表示。

过程

步骤 1　选择系统 (System) > 配置 (Configuration)。

步骤 2　点击控制面板 (Dashboard)。

步骤 3　选中启用自定义分析构件 (Enable Custom Analysis Widgets) 复选框以允许用户将“自定义分析”(Custom Analysis) 构件添加到控制面板。

步骤 4　点击保存 (Save)。

DNS 缓存

可以将系统配置为在事件视图页面上自动解析 IP 地址。还可以为设备执行的 DNS 缓存配置基本属性。配置 DNS 缓存让您可以识别之前解析过的 IP 地址，而无需执行额外查找。这样，启用 IP 地址解析后，可以减少网络上的流量并加快事件页面的显示速度。

配置 DNS 缓存属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

DNS 解析缓存是针对整个系统的设置，它允许对以前解析过的 DNS 查找进行缓存。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **DNS 缓存 (DNS Cache)**。

步骤 3 从 **DNS 解析缓存 (DNS Resolution Caching)** 下拉列表中，选择以下选项之一：

- **已启用 (Enabled)** - 启用缓存。
- **已禁用 (Disabled)** - 禁用缓存。

步骤 4 在 **DNS 缓存超时（以分钟为单位）(DNS Cache Timeout [in minutes])** 字段中，输入 DNS 条目在因无活动而被删除前在内存中缓存的分钟数。
默认设置为 300 分钟（5 小时）。

步骤 5 点击**保存 (Save)**。

邮件通知

如果要执行以下操作，请配置邮件主机：

- 通过邮件发送基于事件的报告
- 通过邮件发送有关预定任务的报告
- 通过邮件发送更改调节报告
- 通过邮件发送数据删除通知
- 将邮件用于发现事件、影响标志、关联事件警报，入侵事件警报和运行状况事件警报

配置邮件通知时，可以为系统与邮件中继主机之间的通信选择加密方法，并可根据需要为邮件服务器提供身份验证凭证。配置后，可以测试连接。

配置邮件中继主机和通知地址

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **Email Notification**。

步骤 3 在**邮件中继主机 (Mail Relay Host)** 字段中，输入要使用的邮件服务器的主机名或 IP 地址。输入的邮件主机**必须**允许从设备进行访问。

步骤 4 在**端口号 (Port Number)** 字段，请输入邮件服务器上使用的端口号。
典型的端口包括：

- 25，使用加密时
- 465，使用 SSLv3 时
- 587，使用 TLS 时

步骤 5 在**加密方法 (Encryption Method)** 中选择一种加密方法。

- **TLS** - 使用传输层安全加密通信。
- **SSLv3** - 使用安全套接字层加密通信。
- **无 (None)** - 允许未加密的通信。

注释 设备和邮件服务器之间的加密通信不要求进行证书验证。

步骤 6 在**源地址 (From Address)** 字段，输入要将其用作设备发送消息的源邮箱地址的有效邮箱地址。

步骤 7 或者，要在连接到邮件服务器时提供用户名和密码，请选择**使用身份验证 (Use Authentication)**。在 **Username** 名字段中输入用户名。在 **Password** 字段中输入密码。

步骤 8 要使用已配置的邮件服务器发送测试邮件，请点击 **Test Mail Server Settings**。
系统会在按钮旁边显示一条消息，以指明测试是否成功。

步骤 9 点击**保存 (Save)**。

选择语言

可以使用 Language 页面为网络界面指定不同的语言。

指定另一种语言

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	任意	管理

此配置适用于或 Firepower 管理中心或 7000 和 8000 系列受管设备。

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于 7000 和 8000 系列受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注意 在该页面上指定的语言将用于每个用户登录到设备时所用的网络界面。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **Language**。

步骤 3 选择要使用的语言。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

登录横幅

可以使用“登录横幅”(Login Banner) 页面为安全设备或共享策略指定会话、登录或自定义消息横幅。

在横幅文本中可以使用空格，但不能使用制表符。可以为横幅指定多个文本行。如果文本包括空行，则系统会在横幅中将此文本显示为回车 (CR)。只能使用 ASCII 字符，包括换行（按 Enter 键），换行计为两个字符。

通过 Telnet 或 SSH 访问安全设备时，如果没有足够的系统内存可用于处理横幅消息，或如果在尝试显示横幅消息时发生 TCP 写入错误，则会话将关闭。

添加自定义登录横幅

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

可以创建自定义登录横幅，当用户通过 SSH 或 Web 界面登录时，该横幅会向用户显示。

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 选择**登录横幅 (Login Banner)**。

步骤 3 在**自定义登录横幅 (Custom Login Banner)** 字段中，输入要使用的登录横幅。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

SNMP 轮询

您可以为 Firepower 管理中心和典型受管设备启用简单网络管理协议 (SNMP) 轮询功能。此功能支持使用 SNMP 协议第 1 版、第 2 版和第 3 版。

此功能允许访问：

- 标准管理信息库 (MIB)，包括联系人、管理、位置、服务信息、IP 寻址和路由信息以及传输协议使用统计信息等系统详细信息。
- 7000 和 8000 系列受管设备的其他 MIB，包括通过物理接口、逻辑接口、虚拟接口、ARP、NDP、虚拟网桥和虚拟路由器的流量的统计信息。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

请注意，启用系统策略 SNMP 功能不会导致系统发送 SNMP 陷阱；这样做只会使 MIB 中的信息可供网络管理系统轮询。

配置 SNMP 轮询

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注释 必须为计划用于轮询系统的任何计算机添加 SNMP 访问权限。请注意，SNMP MIB 包含可用于攻击您的部署的信息。思科建议将 SNMP 访问权限的访问列表限于将用于轮询 MIB 的特定主机。思科还建议使用 SNMPv3，并使用强密码进行网络管理访问。

SNMPv3 仅支持只读用户和使用 AES128 加密。

开始之前

- 为计划用于轮询系统的每台计算机添加 SNMP 访问权限，如配置系统的访问列表，第 453 页中所述。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **SNMP**。

步骤 3 从 **SNMP 版本 (SNMP Version)** 下拉列表中，选择要使用的 SNMP 版本。

步骤 4 有以下选项可供选择：

- 如果选择了**版本 1 (Version1)** 或**版本 2 (Version 2)**，请在**社区字符串 (Community String)** 字段中输入 SNMP 社区名称。转至步骤 13。

  注释 SNMPv2 仅支持只读社区。

- 如果选择了**版本 3 (Version 3)**，请点击**添加用户 (Add User)** 显示用户定义页面。

  注释 SNMPv3 仅支持只读用户和使用 AES128 加密。

步骤 5 输入**用户名 (Username)**。

步骤 6 从**身份验证协议 (Authentication Protocol)** 下拉列表中选择要用于身份验证的协议。

步骤 7 在**身份验证密码 (Authentication Password)** 字段中输入使用 SNMP 服务器进行身份验证时所需的密码。

步骤 8 在**验证密码 (Verify Password)** 字段中重新输入身份验证密码。

步骤 9 从**隐私协议 (Privacy Protocol)** 列表中选择要使用的隐私协议，或者选择**无 (None)** 以不使用隐私协议。

步骤 10 在**隐私密码 (Privacy Password)** 字段中输入 SNMP 服务器需要的 SNMP 隐私密钥。

步骤 11 在**验证密码 (Verify Password)** 字段中重新输入隐私密码。

步骤 12 点击 **Add**。

步骤 13 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

STIG 合规性

美国联邦政府内部的组织有时需要遵守《安全技术实施指南》(STIG)中规定的一系列安全检查要求。Firepower 系统支持遵守美国国防部规定的 STIG 要求。

如果在部署中的任一设备上启用了 STIG 合规性，则必须在所有设备上都将其启用。不符合 STIG 规定的受管设备无法注册到符合 STIG 规定的Firepower 管理中心，同样，符合 STIG 规定的设备无法注册到不合规的Firepower 管理中心。

启用 STIG 合规性不能保证严格遵守所有适用的 STIG 规定。

启用 STIG 合规性时，本地外壳访问帐户的密码复杂性和保留规则会发生更改。此外，在 STIG 合规性模式下，无法使用 SSH 远程存储。

注意 需在支持人员的协助下才能禁用此设置。此外，此设置可能会显著影响系统性能。除为了满足美国国防部的安全要求外，思科不建议启用 STIG 合规性。

启用 STIG 合规性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注意 如果在部署中的任一设备上启用了 STIG 合规性，则必须在所有设备上都将其启用。需在支持人员的协助下才能禁用此设置。此外，此设置可能会显著影响系统性能。除为了满足美国国防部的安全要求外，思科不建议启用 STIG 合规性。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。

- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **STIG Compliance**。

注释 设备在您启用 STIG 合规性时会重启。Firepower 管理中心在您保存系统配置时重启；受管设备在您部署配置更改时重启。

步骤 3 如果要永久在设备上启用 STIG 合规性，请选择**启用 STIG 合规性 (Enable STIG Compliance)**。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。
- 如果设备从版本 5.2.0 之前的版本进行了更新，则启用 STIG 合规性会重新生成设备证书。在整个部署中启用 STIG 合规性，请将受管设备重新注册到 Firepower 管理中心。

时间与时间同步

可以使用**时间 (Time)** 页面从 Firepower 管理中心或 7000 或 8000 系列设备的本地 Web 界面查看当前时间和时间源。还可以使用 Firepower 管理中心作为其受管设备的网络时间协议 (NTP) 服务器。可以使用**时间同步 (Time Synchronization)** 页面管理时间同步。可通过以下方式之一来同步时间：

- 手动
- 使用一个或多个 NTP 服务器（其中一个可以是Firepower 管理中心）

请注意，在设备的大多数页面上，时间设置是以您在 Time Zone 页面（默认为美国/纽约时区）上设置的本地时间显示的，但在设备自身上存储时用的是 UTC 时间。此外，当前时间以 UTC 显示在 Time Synchronization 页面的顶部（本地时间显示在 Manual 时钟设置选项中，如果此选项已启用）。

可以使用外部时间服务器来同步设备。如果指定远程 NTP 服务器，则设备必须可通过网络访问该服务器。请勿指定不受信任的 NTP 服务器。与 NTP 服务器之间的连接不使用已配置的代理设置。也可以使用 Firepower 管理中心作为 NTP 服务器。

思科建议您将设备同步到物理 NTP 服务器。请勿将受管设备与虚拟 Firepower 管理中心同步。

注释 同步时间后，请确保Firepower管理中心和受管设备上的时间相匹配。否则，当受管设备与Firepower管理中心通信时，可能会发生意外的后果。

手动时间规范

如果 Firepower 管理中心的时间同步设置为**在本地配置中手动设置 (Manually in Local Configuration)**，则可以手动设置系统的时间。

- 如果计划让 Firepower 管理中心使用 NTP 提供时间，则应在将 Firepower 管理中心配置为使用 NTP 提供时间**之前**手动更改时间。
- 将 Firepower 管理中心配置为 NTP 服务器**之后**，如果需要手动更改时间，则需要先禁用 NTP 选项，手动更改时间，然后重新启用 NTP 选项。

当系统根据 NTP 同步其时间时，您可以从 Firepower 管理中心的 Web 界面以及从 7000 和 8000 系列设备的本地 Web 界面查看 NTP 状态，该状态会提供有以下信息：

表 *62*: *NTP* 状态

列	说明
NTP Server	已配置的 NTP 服务器的 IP 地址和名称。
状态	NTP 服务器时间同步的状态。 • **Being Used** 表示设备已与 NTP 服务器同步。 • **Available** 表示 NTP 服务器可供使用，但时间尚未同步。 • **Not Available** 表示 NTP 服务器在您的配置中，但 NTP 后台守护程序无法使用该服务器。 • **Pending** 表示 NTP 服务器是新的或 NTP 后台守护程序最近重新启动过。随着时间的推移，此选项的值应更改为 **Being Used**、**Available** 或 **Not Available**。 • **Unknown** 表示 NTP 服务器的状态未知。
Offset	设备时间与已配置的NTP服务器上时间所相差的毫秒数。负值表示设备时间晚于 NTP 服务器，正值表示设备时间早于 NFP 服务器。
上次更新	自上次与 NTP 服务器同步以来过去的秒数。NTP 后台守护程序会根据若干条件自动调整同步时间。例如，如果显示更长的更新时间（例如 300 秒），表示时间相对稳定，这样，NTP 后台守护程序将会确定不需要使用更小的更新增量。

手动设置时间

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	任意	管理

可以使用**时间 (Time)** 页面从 Firepower 管理中心或 7000 和 8000 系列设备的本地 Web 界面查看当前时间和时间源。

注释 要使 Firepower 管理中心使用 NTP 提供时间，请在将管理中心配置为使用 NTP 提供时间之前手动更改时间。

过程

步骤 1 选择系统 (System) > 配置 (Configuration)。

步骤 2 点击 Time Synchronization。

步骤 3 如果通过 NTP 提供时间 (Serve Time via NTP) 处于已启用 (Enabled) 状态，请选择已禁用 (Disabled)。

步骤 4 点击保存 (Save)。

步骤 5 选择在本地配置中手动设置 (Manually in Local Configuration)。

步骤 6 点击保存 (Save)。

步骤 7 点击 Time。

步骤 8 使用设置时间 (Set Time) 下拉列表设置时间。

步骤 9 点击 Apply。

接下来的操作

- 要使 Firepower 管理中心使用 NTP 提供时间，请继续操作，如 中所述 从 Firepower 管理中心提供时间，第 466 页

从 Firepower 管理中心提供时间

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心	仅全局	管理

注释 如果将管理中心配置为使用 NTP 提供时间，然后又将其禁用，受管设备上的 NTP 服务仍会尝试与管理中心同步时间。必须更新并重新部署任何适用的平台设置策略，以建立新的时间源。

开始之前

- 手动更改时间；请参阅手动设置时间，第 465 页。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **Time Synchronization**。

步骤 3 从**通过 NTP 提供时间 (Serve Time via NTP)** 下拉列表中选择**已启用 (Enabled)**。

步骤 4 对于受管设备上的**设置我的时钟 (Set My Clock)** 选项，您有以下选择来指定同步时间的方式：

- 选择**在本地配置中手动设置 (Manually in Local Configuration)** 以通过 NTP 从 Firepower 管理中心接收时间。有关详细信息，请参阅手动设置时间，第 465 页。
- 选择**通过 NTP 从其他服务器接收 (Via NTP from)** 以通过 NTP 从其他服务器接收时间。在文本框中，输入 NTP 服务器的 IP 地址的逗号分隔列表，或者如果启用了 DNS，则输入完全限定的主机名和域名。

注意 如果设备已重新启动，并且 DHCP 服务器设置了不同于您在这里指定的记录的 NTP 服务器记录，则会使用 DHCP 提供的 NTP 服务器。为避免这种情况，请将 DHCP 服务器配置为会设置相同的 NTP 服务器。

步骤 5 点击**保存 (Save)**。

注释 管理中心与其受管设备进行同步可能需要几分钟时间。

同步时间

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。

- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **Time Synchronization**。

步骤 3 要指定受管设备上的时间同步方式，您有以下选择：

- 选择**通过 NTP 从管理中心接收 (Via NTP from Management Center)** 以通过 NTP 从管理中心接收时间。有关详细信息，请参阅从 Firepower 管理中心提供时间，第 466 页。
- 选择**通过 NTP 从其他服务器接收 (Via NTP from)** 以通过 NTP 从其他服务器接收时间。在文本框中，输入 NTP 服务器的 IP 地址的逗号分隔列表，或者如果启用了 DNS，则输入完全限定的主机名和域名。

步骤 4 点击**保存 (Save)**。

注释 受管设备与已配置的 NTP 服务器进行同步可能需要几分钟时间。此外，如果是将受管设备与配置为 NTP 服务器的管理中心进行同步，并且管理中心本身配置为使用 NTP 服务器，则时间同步可能需要一些时间。这是因为，管理中心必须首先与其配置的 NTP 服务器同步，然后才能为受管设备提供时间。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。
- 确认管理中心和受管设备上的时间匹配。

会话超时

Firepower 系统 Web 界面或辅助命令行界面的自动登录会话可能意味着安全风险。可以配置用户的登录会话因无活动而超时之前允许经过的空闲时间，以分钟为单位。也可以为外壳（命令行）会话设置类似的超时时间。

在部署中，可能有一些用户打算被动、安全、长时间地监控网络界面。可以通过某一用户配置选项来使用户免受网络界面会话超时的影响。具有“管理员”(Administrator) 角色的用户拥有对菜单选项的完整访问权限，这些访问权限受损会构成额外风险，因此他们不能获得会话超时豁免。

配置会话超时

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

如果必须限制对系统的外壳访问，则通过其他选项，您可以在辅助命令行界面中永久禁用 `expert` 命令。在设备上禁用 expert 模式可阻止所有用户（即使是有 Configuration 外壳访问权限的用户）进入外壳的专家模式。当用户在辅助命令行界面中进入专家模式后，该用户可以运行适用于外壳的任何 Linux 命令。不在专家模式时，命令行用户只能运行由辅助命令行界面提供的命令。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**外壳超时 (Shell Timeout)**。

步骤 3 有以下选项可供选择：

- 要配置 Web 界面的会话超时，请在**浏览器会话超时（分钟）(Browser Session Timeout [Minutes])** 字段中输入分钟数默认值为 `60`；最大值为 `1440`（24 小时）。有关如何使用户免受会话超时影响的信息，请参阅用户帐户登录选项，第 64 页。
- 要配置命令行界面的会话超时，请在**外壳超时（分钟）(Shell Timeout [Minutes])** 字段中输入分钟数。默认值为 `0`；最大值为 `1440`（24 小时）。
- 要在辅助命令行界面中永久禁用 `expert` 命令，请选中**永久禁用专家访问 (Permanently Disable Expert Access)** 复选框。

注意 在将已禁用专家模式的策略部署到设备后，无法通过 Web 界面或辅助命令行界面恢复访问专家模式的能力。要恢复专家模式功能，必须联系支持人员。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

漏洞映射

当服务器在发现事件数据库中拥有应用 ID 且流量的数据包报头包含供应商和版本时，Firepower 系统会针对从主机 IP 地址收到或发送的所有应用协议流量自动将漏洞映射到该地址。

对于在数据包中不包含供应商或版本信息的服务器，可以将系统配置为是否针对这些无供应商和版本信息的服务器将漏洞与服务器流量关联。

例如，在某一主机提供的 SMTP 流量中，其报头不含供应商或版本号。如果在系统配置的“漏洞映射”(Vulnerability Mapping) 页面上启用 SMTP 服务器，然后将该配置保存到管理检测到流量的设备的 Firepower 管理中心，则所有与 SMTP 服务器关联的漏洞都将被添加到该主机的主机配置文件。

尽管检测器会收集服务器信息并将其添加到主机配置文件中，但应用协议检测器不会用于漏洞映射，因为您无法为自定义的应用协议检测器指定供应商或版本，同时也无法为漏洞映射选择服务器。

映射服务器漏洞

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	保护	管理中心	仅全局	管理

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 选择**漏洞映射 (Vulnerability Mapping)**。

步骤 3 有以下选项可供选择：

- 要阻止服务器的漏洞被映射到接收不含供应商或版本信息的应用协议流量的主机上，请为相应服务器清除此复选框。
- 要使服务器的漏洞映射到接收不含供应商或版本信息的应用协议流量的主机上，请选中该服务器对应的复选框。

提示 可以使用**已启用 (Enabled)** 旁边的复选框一次性选中或清除所有复选框。

步骤 4 点击**保存 (Save)**。

远程控制台访问管理

您可以通过物理设备上的 VGA 端口（默认端口）或串行端口使用 Linux 系统控制台在受支持系统上进行远程访问。请选择最适合您的组织的思科部署的物理布局的选项。

您可以通过 LAN 上串行 (SOL) 连接在默认 (`eth0`) 管理接口上使用无人值守管理 (LOM) 来远程监控或管理 Firepower 系统，而无需登录系统的管理接口。在带外管理连接上使用命令行界面可以执行有限的任务，例如查看机箱序列号或监控诸如风扇速度和温度之类的状况。

您必须对系统和要管理系统的用户均启用 LOM。在启用系统和用户后，使用第三方智能平台管理接口 (IPMI) 实用程序访问和管理系统。

配置系统上的远程控制台设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意（NGIPSv 和 ASA FirePOWER 除外）	仅全局	具有 LOM 访问权限的管理员

开始之前

- 禁用与设备管理接口连接的所有第三方交换设备上的生成树协议 (STP)。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击**控制台配置 (Console Configuration)**。

步骤 3 选择远程控制台访问选项：

- 选择 **VGA** 将会使用设备的 VGA 端口。
- 选择**物理串行端口 (Physical Serial Port)** 将会使用设备的串行端口，或在 Firepower 管理中心、Firepower 7050 或 8000 系列设备上使用 LOM/SOL 功能。
- 选择**无人值守管理 (Lights-Out Management)** 将会在 7000 系列设备（Firepower 7050 除外）上使用 LOM/SOL 功能。在这些设备上，不能同时使用 SOL 和常规串行连接。

注释 如果在 70xx 系列设备（Firepower 7050 除外）上将远程控制台从**物理串行端口 (Physical Serial Port)** 更改为**无人值守管理 (Lights-Out Management)**，或者从**无人值守管理 (Lights-Out Management)** 更改为**物理串行端口 (Physical Serial Port)**，则必须重新启动设备两次才会出现预期的启动提示符。

步骤 4 要通过 SOL 配置 LOM，请输入必要的 IPv4 设置：

- 选择系统的地址**配置 (Configuration)**（**DHCP** 或**手动 [Manual]**）
- 输入要用于 LOM 的 **IP 地址 (IP Address)**。

  注释 LOM IP 地址必须不同于系统的管理接口 IP 地址。

- 输入系统的**网络掩码 (Netmask)**。
- 输入系统的**默认网关 (Default Gateway)**。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 如果配置了无人值守管理，请启用无人值守管理用户；请参阅无人值守管理用户访问配置，第 472 页。

无人值守管理用户访问配置

必须将“无人值守管理”权限明确授予将会使用此功能的用户。LOM 用户还有如下限制：

- 必须为用户指定管理员角色。
- 用户名最多可包含 16 个字母数字字符。不支持将短划线和更长的用户名用作 LOM 用户名。
- 密码最多可以包含 20 个字母数字字符，但在 71xx 系列设备上设置时除外。如果在 Firepower 7110、7115、7120 或 7125 设备上启用 LOM，则密码最多可以包含 16 个字母数字字符。对于 LOM 用户，不支持长度大于 20 或 16 个字符的密码。用户的 LOM 密码不得与该用户的系统密码相同。思科建议您为设备使用最大支持长度、不是基于字典的复杂密码，并且每三个月修改一次密码。
- 物理 Firepower 管理中心和 8000 系列设备最多可以有 13 个 LOM 用户。8000 系列设备最多可以有 8 个 LOM 用户。

请注意，如果在一个具有 LOM 权限的角色已登录时取消激活然后再重新激活该角色，或者在用户登录会话期间从备份恢复该用户或用户角色，那么该用户必须重新登录到网络界面才能重新获得对 IPMItool 命令的访问权限。

启用无人值守管理用户访问

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意（NGIPSv 和 ASA FirePOWER 除外）	仅全局	具有 LOM 访问权限的管理员

使用每个系统的本地 Web 界面逐个系统配置 LOM 和 LOM 用户。不能在受管设备上使用 Firepower 管理中心配置 LOM。同样，因为用户独立于每个设备受管理，因此，在Firepower 管理中心上启用或创建 LOM 用户不会将此功能转移到受管设备上的用户。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击**控制台配置 (Console Configuration)**。

步骤 3 点击**无人值守管理 (Lights Out Management)**。

步骤 4 有以下选项可供选择：

- 要向现有用户授予 LOM 用户访问权限，请点击列表中用户名旁边的编辑图标 ( )。
- 要向新用户授予 LOM 用户访问权限，请点击 **Create User**。

步骤 5 在 **User Configuration** 下，启用管理员角色。

步骤 6 选中**允许无人值守管理访问 (Allow Lights-Out Management Access)** 复选框。

步骤 7 点击**保存 (Save)**。

LAN 上串行连接配置

使用计算机上的第三方 IPMI 实用程序可通过 LAN 上串行与设备建立连接。如果您的计算机使用类似 Linux 的环境或 Mac 环境，请使用 IPMItool；对于 Windows 环境，请使用 IPMIutil。

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

Linux

IPMItool 是许多发行版的标准配置，可立即使用。

Mac

必须在 Mac 上安装 IPMItool。首先，请确认 Mac 上安装了 Apple 的 XCode 开发者工具，确保安装了用于命令行开发的可选组件（较新版本的 UNIX 开发和系统工具或较旧版本的 Command Line Support）。然后您可以安装 macports 和 IPMItool。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows 的 ISE 安全评估代理

必须在 Windows 上编译 IPMIutil。如果无法访问编译器，可以使用 IPMIutil 自身来编译。请使用您常用的搜索引擎搜索更多信息，以下网站也可能对您帮助：：

```
http://ipmiutil.sourceforge.net/
```

了解 IPMI 实用程序命令

用于 IPMI 实用程序的命令由若干段组成，如以下 IPMItool 示例：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

其中：

- `ipmitool` 调用实用程序
- `-I lanplus` 启用会话加密

- -H IP_address 表示要访问的设备的 IP 地址
- -U user_name 是授权用户的名称
- - command 是要发出的命令的名称

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 Windows，以上命令如下所示：

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

使用此命令可连接到设备的命令行，就像您本人在设备旁边一样。系统会提示您输入密码。

使用 IPMItool 配置 LAN 上串行

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意（NGIPSv 和 ASA FirePOWER 除外）	任意	具有 LOM 访问权限的管理员

过程

使用 IPMItool，输入以下命令，并在提示时输入密码：

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

使用 IPMIutil 配置 LAN 上串行

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意（NGIPSv 和 ASA FirePOWER 除外）	任意	具有 LOM 访问权限的管理员

过程

使用 IPMIutil，输入以下命令，如果出现提示则输入密码：

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

无人值守管理概述

通过无人值守管理 (LOM)，您可以在默认 (eth0) 管理接口上利用 SOL 连接执行有限的系列操作，而无需登录设备。可以使用命令创建 SOL 连接，然后使用其中一个 LOM 命令。命令执行完成后，连接将终止。请注意，并非所有电源控制命令在 70xx 系列设备上都有效。

注释 这样，当主机启动时，Firepower 71xx、Firepower 82xx 或 Firepower 83xx 设备的基板管理控制器 (BMC) 只有通过 1Gbps 的链路速度才能访问。设备断电时，BMC 只有在 10Mbps 和 100Mbps 的速度下才能建立以太网链路。因此，如果使用 LOM 远程启动设备，只能使用 10 Mbps 和 100 Mbps 的链路速度将设备连接至网络。

注意 在极少数情况下，如果您的计算机与系统的管理接口位于不同子网，而系统配置为使用 DHCP，则尝试访问 LOM 功能可能失败。如果发生这种情况，可以禁用然后在系统上重新启用 LOM，或者使用与系统位于同一子网的计算机来 ping 设备的管理接口。这样应该就可以使用 LOM。

注意 思科了解智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 固有的漏洞。在系统上启用无人值守管理 (LOM) 会暴露该漏洞。为了降低这种漏洞，请将您的系统部署在只有受信任用户才可以访问的安全管理网络上，并且使用最大支持长度、不是基于字典的复杂密码并且每三个月修改一次密码。为防止暴露此漏洞，请勿启用 LOM。

如果所有访问系统的尝试均失败，则可以使用 LOM 远程重新启动系统。请注意，如果在 SOL 连接处于活动状态时重新启动系统，LOM 会话可能会断开连接或超时。

注意 请**勿**重新启动系统，除非它不响应任何其他重新启动操作。远程重新启动系统不能正常重新启动系统，而且可能会丢失数据。

表 *63*：无人值守管理命令

IPMItool	IPMIutil	说明
（不适用）	`-V 4`	启用 IPMI 会话的管理员权限
`-I lanplus`	`-J 3`	启用 IPMI 会话加密
`-H`	`-N`	表示远程设备的 IP 地址
`-U`	`-U`	表示已获授权 LOM 帐户的用户名
`sol activate`	`sol -a`	开始 SOL 会话

IPMItool	IPMIutil	说明
`sol deactivate`	`sol -d`	结束 SOL 会话
`chassis power cycle`	`power -c`	重新启动设备（在 70xx 系列设备上无效）
`chassis power on`	`power -u`	打开设备电源
`chassis power off`	`power -d`	关闭设备电源（在 70xx 系列设备上无效）
`sdr`	`sensor`	显示设备信息，例如风扇速度和温度

例如，显示设备信息列表的 IPMItool 命令是：

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

注释 思科建议使用 IPMItool V1.8.12 或更高版本。

对于 IPMIutil 实用程序，以上命令如下：

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

使用 IPMItool 配置无人值守管理

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意（NGIPSv 和 ASA FirePOWER 除外）	任意	具有 LOM 访问权限的管理员

过程

为 IPMItool 输入以下命令以及密码（如果提示）：

```
ipmitool -I lanplus -H IP_address -U user_name command
```

使用 IPMIutil 配置无人值守管理

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意（NGIPSv 和 ASA FirePOWER 除外）	任意	具有 LOM 访问权限的管理员

过程

为 IPMIutil 输入以下命令以及密码（如果提示）：

```
ipmiutil -J 3 -H IP_address -U username command
```

VMware 工具和虚拟系统

VMware 工具是专为虚拟机而设计的一套性能增强实用工具。通过这些实用工具，您可以充分利用 VMware 产品方便的功能。系统支持在 VMware 上运行的 Firepower 系统虚拟设备上的以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

也可以在所有受支持的 ESXi 版本上启用 VMware 工具。有关受支持的版本列表，请参阅《《*Cisco Firepower NGIPSv for VMware* 快速入门指南》》。有关 VMware 工具全部功能的信息，请参阅 VMware 网站 (http://www.vmware.com/)。

在面向 VMWare 的 Firepower 管理中心上启用 VMware 工具

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	NGIPSv	仅全局	管理

由于 NGIPSv 没有 Web 界面，您必须在 NGIPSv 上使用命令行界面来启用 VMware 工具；请参阅《《*Cisco Firepower NGIPSv for VMware* 快速入门指南》》。

过程

步骤 1 选择**系统 (System)** > **配置 (Configuration)**。

步骤 2 点击 **VMware 工具 (VMware Tools)**.

步骤 3 点击**启用 VMware 工具 (Enable VMware Tools)**。

步骤 4 点击**保存 (Save)**。

第 25 章

受管设备的平台设置策略

以下主题介绍平台设置策略以及如何将这些策略部署到受管设备：

平台设置简介

平台设置策略是用于定义受管设备的可能类似于您的部署中其他受管设备的方面（例如时间设置和外部身份验证）的共享功能集或参数集。

通过共享策略，可以同时配置多个受管设备，从而在部署中提供一致性并精简管理工作。对平台设置策略的任何更改都会影响已应用该策略的所有受管设备。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

例如，您的组织的安全策略可能会要求您的设备在用户登录时显示“无授权使用”(No Unauthorized Use) 消息。通过平台设置，您可以在平台设置策略中设置一次登录横幅。

在Firepower管理中心上具有多个平台设置策略也有好处。例如，如果您具有在不同情况下使用的不同邮件中继主机，或者如果要测试不同的访问列表，则可以创建多个平台设置策略并在其之间切换，而非编辑单个策略。

管理平台设置策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

使用“平台设置”(Platform Settings) 页面（**设备 (Devices)** > **平台设置 (Platform Settings)**）管理平台设置策略。此页面指示每个策略的设备类型。“状态”(Status) 列显示策略的设备目标。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**。

步骤 2 管理平台设置策略：

- 创建 - 要创建新的平台设置策略，请点击**新建策略 (New Policy)**；请参阅创建平台设置策略，第 480 页。
- 复制 - 要复制平台设置策略，请点击复制图标 ( )。
- 编辑 - 要修改现有平台设置策略中的设置，请点击编辑图标 ( )。
- 删除 - 要删除未在使用的策略，请点击删除图标 ( )，然后确认选择。

  注意 不应删除上一次部署于任何目标设备的策略，即使该策略已过时。在完全删除该策略之前，最好是将其他策略部署到这些目标。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

创建平台设置策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

创建新的平台设置策略时，必须至少选择设备类型：典型受管设备。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**。

步骤 2 点击 **New Policy**。

步骤 3 从下拉列表中选择设备类型。

- 选择 **Firepower 设置 (Firepower Settings)** 为典型托管设备创建共享策略。

步骤 4 为新策略输入**名称 (Name)** 和**说明 (Description)**（可选）。

步骤 5 或者，选择要应用策略的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。可以在**搜索 (Search)** 字段中输入搜索字符串以缩小设备列表。

步骤 6 点击**保存 (Save)**。
系统创建策略，并打开以进行编辑。

步骤 7 根据设备平台类型配置平台设置：

- 有关 Firepower 设置，请参阅Firepower 平台设置简介，第 483 页。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

设置平台设置策略的目标设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

在创建新策略的同时可以添加目标设备，也可以稍后将它们添加到策略中，如以下操作步骤中所述。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**。

步骤 2 点击要编辑的平台设置策略旁边的编辑图标 ( )。

步骤 3 点击**策略分配 (Policy Assignment)**。

步骤 4 选择要添加到策略中的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。可以在**搜索 (Search)** 字段中输入搜索字符串以缩小设备列表。

步骤 5 点击**保存 (Save)** 以保存目标设备设置。

步骤 6 再次点击**保存 (Save)** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 26 章

FirePOWER 平台设置

以下主题介绍 FirePOWER 平台设置以及如何在设备上配置这些设置：

Firepower 平台设置简介

Firepower 典型受管设备的平台设置配置可能要在多个设备之间共享其值的一系列无关功能。在此情况下，是指 7000 和 8000 系列、ASA FirePOWER 模块和 NGIPSv 设备。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

配置 Firepower 平台设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	传统	任意	管理

要配置平台设置，可以编辑现有平台设置策略或创建新策略。如果编辑的平台设置策略当前已部署到某一设备，请在保存更改后重新部署该策略。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**。
系统将显示“平台设置”(Platform Settings) 页面，其中包含现有策略的列表。

步骤 2 创建新策略或编辑现有策略。

- 要创建新策略，请参阅创建平台设置策略，第 480 页。
- 要编辑现有策略，请点击要编辑的策略旁边的编辑图标 ()。

系统将显示 Edit Policy 页面。可以更改策略名称和策略描述。有关配置平台设置策略各方面的详细信息，请参阅以下其中一个部分：

- 配置系统的访问列表，第 453 页
- 配置外部流式传输的审核日志，第 454 页
- 启用外部身份验证，第 489 页
- 指定另一种语言，第 459 页
- 添加自定义登录横幅，第 460 页
- 配置会话超时，第 468 页
- 配置 SNMP 轮询，第 461 页
- 启用 STIG 合规性，第 463 页
- 从 Firepower 管理中心提供时间，第 466 页

步骤 3 （可选）点击**策略分配 (Policy Assignment)** 以在**可用设备 (Available Devices)** 中选择要在其上部署策略的可用设备。点击**添加到策略 (Add to Policy)** 或拖放以添加所选设备。
可以在**搜索 (Search)** 字段中输入搜索字符串以缩小设备列表。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

访问列表

在 Firepower 管理中心和典型受管设备上，可以使用访问列表限制 IP 地址和端口对系统的访问。默认情况下，可为任何 IP 地址启用以下端口：

- 443 (HTTPS) - 用于 Web 界面访问。
- 22 (SSH) - 用于命令行访问。

也可以在端口 161 上添加轮询 SNMP 信息的访问权限。

注意 默认情况下，访问**不**受限制。要在更安全的环境中操作，请考虑为特定 IP 地址添加访问权限，然后删除默认的 `any` 选项。

配置系统的访问列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

请注意，此访问列表不会控制外部数据库访问。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**访问列表 (Access List)**。

步骤 3 或者，要删除某一当前设置，请点击删除图标 ( )。

注意 对于您目前用来连接到设备接口的 IP 地址，如果您删除了它的访问权限，而且无“`IP=any port=443`”这一条目，那么当您部署该策略时，您将失去对系统的访问权限。

步骤 4 要添加对一个或多个 IP 地址的访问权限，请点击**添加规则 (Add Rules)**。

步骤 5 在 **IP 地址 (IP Address)** 字段中，输入 IP 地址或地址范围或 `any`。

步骤 6 选择 **SSH**、**HTTPS**、**SNMP** 或其组合，以指定要为这些 IP 地址启用哪些端口。

步骤 7 点击 **Add**。

步骤 8 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

审核日志

Firepower 管理中心和典型受管设备记录用户活动的只读审核信息。在管理中心和 7000 和 8000 系列 Web 界面上，审核日志显示在标准事件视图中。在此事件视图中，您可以根据审核视图中的任何项目查看、排序和过滤审核日志消息。您可以轻松删除和报告审核信息，也可以查看用户所做更改的详细报告。

您可以配置 Firepower 管理中心和典型受管设备以将审核日志消息发送到系统日志。为此，您可指定系统日志服务器，以及与消息相关联的严重性、设施和可选标记。标记与审核日志消息一同显示在系统日志中。设备指明创建消息的子系统，严重性界定消息的严重性。系统日志消息不包含设施和严重性；这些值告知接收系统日志消息的系统如何对这些消息进行分类。

您也可以配置 Firepower 管理中心和典型受管设备以将审核日志消息传输到 HTTP 服务器。

审核日志的流式传输设置是不同配置的一部分，具体取决于设备的类型：

- 对于 Firepower 管理中心，传输审核日志是系统配置的一部分。
- 对于典型受管设备，审核日志的流式传输设置是 Firepower 管理中心平台设置策略的一部分。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

配置外部流式传输的审核日志

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

以下是输出结构的示例：

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

其中，本地日期、时间和主机名称位于括号内的可选标记之前，发送设备名称在审核日志消息之前。

例如：

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page
View
```

开始之前

- 确保外部主机可正常工作，且可以通过发送审核日志的系统进行访问。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**审核日志 (Audit Log)**。

步骤 3 从**将审核日志发送到系统日志 (Send Audit Log to Syslog)** 下拉菜单中选择**已启用 (Enabled)**。

步骤 4 在 **Host** 字段中，使用 IP 地址或完全限定的主机名称指定审核信息的目标主机。默认端口 (514) 已被使用。

注意 对于您配置用于接收审核日志的计算机，如果未将其设置为可接收远程消息，主机将不会接受审核日志。

步骤 5 选择系统日志**消息来源 (Facility)**。

步骤 6 选择**严重性 (Severity)**。

步骤 7 或者，也可在**标记（可选）(Tag [optional])** 字段中插入参考标记。

步骤 8 要将定期审核日志更新发送到外部 HTTP 服务器，请从**将审核日志发送到 HTTP 服务器 (Send Audit Log to HTTP Server)** 下拉列表中选择**已启用 (Enabled)**。

步骤 9 在 **URL to Post Audit** 字段中，指定要用于发送审核信息的 URL。必须输入与将会监听下列 HTTP POST 变量的监听程序相对应的 URL：

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`

- `result`
- `time`
- `tag`（如果已如上所述进行了定义）

注意 要允许发送加密的信息，您必须使用HTTPS URL。请注意，将审核信息发送到外部URL可能会影响系统性能。

步骤 10 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

外部身份验证设置

如果创建引用外部身份验证服务器的身份验证对象，则可以启用外部身份验证，以使登录受管设备的用户对该服务器进行身份验证，而非使用本地数据库。

当启用外部身份验证时，系统会在LDAP或RADIUS服务器上对照用户验证用户凭证。此外，如果用户启用了本地的内部身份验证，并且在内部数据库中未找到用户凭证，则系统将会检查外部服务器以查找一组匹配的凭证。如果用户在多个系统上有相同的用户名，则其所有密码在所有服务器上都可使用。但请注意，如果在可用的外部身份验证服务器上进行身份验证失败，则系统不会恢复为检查本地数据库。

启用外部身份验证时，对于采用外部身份验证的所有用户，都可为其设置默认的用户角色。您可以选择多个角色，但它们必须可以组合在一起。例如，如果启用外部身份验证以仅检索贵公司的“网络安全”组中的用户，则可将默认用户角色设置为包含安全分析师这一角色，以便用户可以访问收集到的事件数据，同时您无需进行任何额外的用户配置。但是，如果外部身份验证不仅检索该安全组，还检索其他人员的记录，则您可能希望不选择默认角色。

如果未选择访问角色，用户可以登录但无法访问任何功能。在用户尝试登录后，其帐户会在用户管理页面（**系统 (System)** > **用户 (Users)**）上列出，可以在该页面上编辑帐户设置以授予其他权限。

提示 如果将系统配置为使用一个用户角色并应用策略，随后修改策略以使用不同的默认用户角色，则在修改帐户之前创建的任何用户帐户都会保留第一个用户角色，直至修改帐户或者删除并重新创建帐户为止。

如果要指定可以对LDAP服务器进行身份验证以执行外壳访问或执行CAC身份验证和授权的用户组，则必须为每个用户创建单独的身份验证对象并分别启用这些对象。

如果采用内部身份验证的用户尝试登录，则系统首先检查该用户是否存在于本地用户数据库中。如果该用户存在，则系统会对照本地数据库检查用户名和密码。如果找到匹配项，用户可成功登录。如果登录失败，并且外部身份验证已启用，则系统会按照配置中显示的身份验证顺序，对照各个外部身份验证服务器来检查用户。如果用户名和密码与来自外部服务器的结果相匹配，则系统会将用户更改为具有该身份验证对象的默认权限的外部用户。

如果外部用户尝试登录，则系统会对照外部身份验证服务器检查用户名和密码。如果找到匹配项，用户可成功登录。如果登录失败，则用户登录尝试会被拒绝。外部用户无法参照本地数据库中的用户列表进行身份验证。如果用户是新的外部用户，则本地数据库中会创建一个外部用户帐户，该帐户具有来自外部身份验证对象的默认权限。

启用外部身份验证

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心，典型	任意	管理

开始之前

- 配置外部身份验证对象，如外部身份验证，第 69 页中所述。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 从**状态 (Status)** 下拉列表中，选择**已启用 (Enabled)**。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中，选择用户角色以确定要授予进行了外部身份验证的用户的默认权限。

步骤 5 如果要用外部服务器对外壳访问帐户进行身份验证，请从**外壳身份验证 (Shell Authentication)** 下拉列表中选择**已启用 (Enabled)**。

步骤 6 如果要启用 CAC 身份验证和授权，请从 **CAC 身份验证 (CAC Authentication)** 下拉列表中选择可用的 CAC 身份验证对象。有关配置 CAC 身份验证和授权的信息，请参阅CAC 身份验证，第 71 页。

步骤 7 要启用预配置的身份验证对象，请选中相应对象旁边的复选框。您**必须**指定至少一个身份验证对象才能启用外部身份验证。
如果启用了外壳身份验证，则**必须**指定某个配置为允许外壳访问的身份验证对象。

在同一系统配置中，必须使用不同的身份验证对象来管理外壳访问和 CAC 身份验证；请参阅CAC 身份验证，第 71 页和LDAP 外壳访问字段，第 87 页。

步骤 8 或者，可以使用向上和向下箭头来更改出现身份验证请求时访问身份验证服务器的顺序。
外壳访问用户**只能**参照其身份验证对象在配置文件中排在第一位的服务器进行身份验证。

步骤 9 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

选择语言

可以使用 Language 页面为网络界面指定不同的语言。

指定另一种语言

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 7000 和 8000 系列	任意	管理

此配置适用于或 Firepower 管理中心或 7000 和 8000 系列受管设备。

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于 7000 和 8000 系列受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注意 在该页面上指定的语言将用于每个用户登录到设备时所用的网络界面。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **Language**。

步骤 3 选择要使用的语言。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

登录横幅

可以使用“登录横幅”(Login Banner) 页面为安全设备或共享策略指定会话、登录或自定义消息横幅。

在横幅文本中可以使用空格，但不能使用制表符。可以为横幅指定多个文本行。如果文本包括空行，则系统会在横幅中将此文本显示为回车 (CR)。只能使用 ASCII 字符，包括换行（按 Enter 键），换行计为两个字符。

通过 Telnet 或 SSH 访问安全设备时，如果没有足够的系统内存可用于处理横幅消息，或如果在尝试显示横幅消息时发生 TCP 写入错误，则会话将关闭。

添加自定义登录横幅

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

可以创建自定义登录横幅，当用户通过 SSH 或 Web 界面登录时，该横幅会向用户显示。

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 选择**登录横幅 (Login Banner)**。

步骤 3 在**自定义登录横幅 (Custom Login Banner)** 字段中，输入要使用的登录横幅。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

会话超时

Firepower 系统 Web 界面或辅助命令行界面的自动登录会话可能意味着安全风险。可以配置用户的登录会话因无活动而超时之前允许经过的空闲时间，以分钟为单位。也可以为外壳（命令行）会话设置类似的超时时间。

在部署中，可能有一些用户打算被动、安全、长时间地监控网络界面。可以通过某一用户配置选项来使用户免受网络界面会话超时的影响。具有“管理员”(Administrator) 角色的用户拥有对菜单选项的完整访问权限，这些访问权限受损会构成额外风险，因此他们不能获得会话超时豁免。

配置会话超时

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

如果必须限制对系统的外壳访问，则通过其他选项，您可以在辅助命令行界面中永久禁用 `expert` 命令。在设备上禁用 expert 模式可阻止所有用户（即使是有 Configuration 外壳访问权限的用户）进入外壳的专家模式。当用户在辅助命令行界面中进入专家模式后，该用户可以运行适用于外壳的任何 Linux 命令。不在专家模式时，命令行用户只能运行由辅助命令行界面提供的命令。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击**外壳超时 (Shell Timeout)**。

步骤 3 有以下选项可供选择：

- 要配置 Web 界面的会话超时，请在**浏览器会话超时（分钟）(Browser Session Timeout [Minutes])** 字段中输入分钟数默认值为 `60`；最大值为 `1440`（24 小时）。有关如何使用户免受会话超时影响的信息，请参阅用户帐户登录选项，第 64 页。

- 要配置命令行界面的会话超时，请在**外壳超时（分钟）(Shell Timeout [Minutes])** 字段中输入分钟数。默认值为 `0`；最大值为 `1440`（24 小时）。
- 要在辅助命令行界面中永久禁用 `expert` 命令，请选中**永久禁用专家访问 (Permanently Disable Expert Access)** 复选框。

注意 在将已禁用专家模式的策略部署到设备后，无法通过 Web 界面或辅助命令行界面恢复访问专家模式的能力。要恢复专家模式功能，必须联系支持人员。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

SNMP 轮询

您可以为 Firepower 管理中心和典型受管设备启用简单网络管理协议 (SNMP) 轮询功能。此功能支持使用 SNMP 协议第 1 版、第 2 版和第 3 版。

此功能允许访问：

- 标准管理信息库 (MIB)，包括联系人、管理、位置、服务信息、IP 寻址和路由信息以及传输协议使用统计信息等系统详细信息。
- 7000 和 8000 系列受管设备的其他 MIB，包括通过物理接口、逻辑接口、虚拟接口、ARP、NDP、虚拟网桥和虚拟路由器的流量的统计信息。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

请注意，启用系统策略 SNMP 功能不会导致系统发送 SNMP 陷阱；这样做只会使 MIB 中的信息可供网络管理系统轮询。

配置 SNMP 轮询

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注释 必须为计划用于轮询系统的任何计算机添加 SNMP 访问权限。请注意，SNMP MIB 包含可用于攻击您的部署的信息。思科建议将 SNMP 访问权限的访问列表限于将用于轮询 MIB 的特定主机。思科还建议使用 SNMPv3，并使用强密码进行网络管理访问。

SNMPv3 仅支持只读用户和使用 AES128 加密。

开始之前

- 为计划用于轮询系统的每台计算机添加 SNMP 访问权限，如配置系统的访问列表，第 453 页中所述。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **SNMP**。

步骤 3 从 **SNMP 版本 (SNMP Version)** 下拉列表中，选择要使用的 SNMP 版本。

步骤 4 有以下选项可供选择：

- 如果选择了**版本 1 (Version1)** 或**版本 2 (Version 2)**，请在**社区字符串 (Community String)** 字段中输入 SNMP 社区名称。转至步骤 13。

  注释 SNMPv2 仅支持只读社区。

- 如果选择了**版本 3 (Version 3)**，请点击**添加用户 (Add User)** 显示用户定义页面。

注释　SNMPv3 仅支持只读用户和使用 AES128 加密。

步骤 5　输入**用户名 (Username)**。

步骤 6　从**身份验证协议 (Authentication Protocol)** 下拉列表中选择要用于身份验证的协议。

步骤 7　在**身份验证密码 (Authentication Password)** 字段中输入使用 SNMP 服务器进行身份验证时所需的密码。

步骤 8　在**验证密码 (Verify Password)** 字段中重新输入身份验证密码。

步骤 9　从**隐私协议 (Privacy Protocol)** 列表中选择要使用的隐私协议，或者选择**无 (None)** 以不使用隐私协议。

步骤 10　在**隐私密码 (Privacy Password)** 字段中输入 SNMP 服务器需要的 SNMP 隐私密钥。

步骤 11　在**验证密码 (Verify Password)** 字段中重新输入隐私密码。

步骤 12　点击 **Add**。

步骤 13　点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

STIG 合规性

美国联邦政府内部的组织有时需要遵守《安全技术实施指南》(STIG)中规定的一系列安全检查要求。Firepower 系统支持遵守美国国防部规定的 STIG 要求。

如果在部署中的任一设备上启用了 STIG 合规性，则必须在所有设备上都将其启用。不符合 STIG 规定的受管设备无法注册到符合 STIG 规定的Firepower 管理中心，同样，符合 STIG 规定的设备无法注册到不合规的Firepower 管理中心。

启用 STIG 合规性不能保证严格遵守所有适用的 STIG 规定。

启用 STIG 合规性时，本地外壳访问帐户的密码复杂性和保留规则会发生更改。此外，在 STIG 合规性模式下，无法使用 SSH 远程存储。

⚠ 注意　需在支持人员的协助下才能禁用此设置。此外，此设置可能会显著影响系统性能。除为了满足美国国防部的安全要求外，思科不建议启用 STIG 合规性。

启用 STIG 合规性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注意 如果在部署中的任一设备上启用了 STIG 合规性，则必须在所有设备上都将其启用。需在支持人员的协助下才能禁用此设置。此外，此设置可能会显著影响系统性能。除为了满足美国国防部的安全要求外，思科不建议启用 STIG 合规性。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。
- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **STIG Compliance**。

注释 设备在您启用 STIG 合规性时会重启。Firepower 管理中心在您保存系统配置时重启；受管设备在您部署配置更改时重启。

步骤 3 如果要永久在设备上启用 STIG 合规性，请选择**启用 STIG 合规性 (Enable STIG Compliance)**。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。
- 如果设备从版本 5.2.0 之前的版本进行了更新，则启用 STIG 合规性会重新生成设备证书。在整个部署中启用 STIG 合规性，请将受管设备重新注册到 Firepower 管理中心。

时间与时间同步

可以使用**时间 (Time)** 页面从 Firepower 管理中心或 7000 或 8000 系列设备的本地 Web 界面查看当前时间和时间源。还可以使用Firepower管理中心作为其受管设备的网络时间协议(NTP)服务器。可以使用**时间同步 (Time Synchronization)** 页面管理时间同步。可通过以下方式之一来同步时间：

- 手动
- 使用一个或多个 NTP 服务器（其中一个可以是Firepower 管理中心）

请注意，在设备的大多数页面上，时间设置是以您在 Time Zone 页面（默认为美国/纽约时区）上设置的本地时间显示的，但在设备自身上存储时用的是 UTC 时间。此外，当前时间以 UTC 显示在Time Synchronization页面的顶部（本地时间显示在Manual时钟设置选项中，如果此选项已启用）。

可以使用外部时间服务器来同步设备。如果指定远程NTP服务器，则设备必须可通过网络访问该服务器。请勿指定不受信任的 NTP 服务器。与 NTP 服务器之间的连接不使用已配置的代理设置。也可以使用 Firepower 管理中心作为 NTP 服务器。

思科建议您将设备同步到物理 NTP 服务器。请勿将受管设备与虚拟 Firepower 管理中心同步。

注释 同步时间后，请确保Firepower管理中心和受管设备上的时间相匹配。否则，当受管设备与Firepower管理中心通信时，可能会发生意外的后果。

同步时间

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	管理中心 传统	任意	管理

此配置适用于 Firepower 管理中心或典型受管设备（7000 和 8000 系列、ASA FirePOWER 和 NGIPSv）：

- 对于 Firepower 管理中心，此配置是系统配置的一部分。
- 对于典型受管设备，将 Firepower 管理中心中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

过程

步骤 1 根据配置的是 Firepower 管理中心还是典型受管设备，执行以下操作：

- 管理中心 - 选择**系统 (System)** > **配置 (Configuration)**。

- 受管设备 - 选择**设备 (Devices)** > **平台设置 (Platform Settings)**并创建或编辑 Firepower 策略。

步骤 2 点击 **Time Synchronization**。

步骤 3 要指定受管设备上的时间同步方式，您有以下选择：

- 选择**通过 NTP 从管理中心接收 (Via NTP from Management Center)** 以通过 NTP 从管理中心接收时间。有关详细信息，请参阅从 Firepower 管理中心提供时间，第 466 页。
- 选择**通过 NTP 从其他服务器接收 (Via NTP from)** 以通过 NTP 从其他服务器接收时间。在文本框中，输入 NTP 服务器的 IP 地址的逗号分隔列表，或者如果启用了 DNS，则输入完全限定的主机名和域名。

步骤 4 点击**保存 (Save)**。

注释 受管设备与已配置的 NTP 服务器进行同步可能需要几分钟时间。此外，如果是将受管设备与配置为 NTP 服务器的管理中心进行同步，并且管理中心本身配置为使用 NTP 服务器，则时间同步可能需要一些时间。这是因为，管理中心必须首先与其配置的 NTP 服务器同步，然后才能为受管设备提供时间。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。
- 确认管理中心和受管设备上的时间匹配。

第 IX 部分

网络地址转换 (NAT)

第 27 章

NAT 策略管理

以下主题介绍如何为 Firepower 系统管理 NAT 策略：

管理 NAT 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

祖先域中的管理员可以将NAT策略设为针对后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。如果NAT策略针对不同后代域中的设备，则后代域中的管理员可以查看有关仅属于其域的目标设备的信息。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 管理 NAT 策略：

- 复制 - 点击要复制的策略旁边的复制图标 ( )；请参阅复制 NAT 策略， 第 505 页。

- 创建 - 点击**新建策略 (New Policy)**；请参阅创建 NAT 策略 ， 第 502 页。
- 删除 - 点击要删除的策略旁边的删除图标 ( )，然后点击**确定 (OK)**。当系统提示是否继续时，还会告知您是否有其他用户在策略中有未保存的更改。

  注意 将 NAT 策略部署于受管设备后，就不能从设备删除策略。相反，如果要删除受管设备上已出现的 NAT 规则，则必须部署不带任何规则的 NAT 策略。您也不能删除上一次部署于任何目标设备的策略，即使该策略已过时。要完全删除该策略，必须向目标部署其他策略。

- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改 ， 第 254 页。
- 编辑 - 点击编辑图标 ( )；请参阅配置 NAT 策略 ， 第 503 页。
- 报告 - 点击报告图标 ( )；请参阅生成当前策略报告 ， 第 262 页。

创建 NAT 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

创建新的NAT策略时，必须至少为其提供一个唯一的名称。虽然在创建策略过程中不需要识别策略目标，但必须执行这个步骤后才能部署策略。如果将不带有规则的NAT策略应用于某台设备，系统会从该设备删除所有 NAT 规则。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

祖先域中的管理员可以将NAT策略设为针对后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。如果NAT策略针对不同后代域中的设备，则后代域中的管理员可以查看有关仅属于其域的目标设备的信息。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 从**新策略 (New Policy)** 下拉列表中选择 **Firepower NAT**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。
在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 选择要部署策略的设备：

- 从**可用设备 (Available Devices)** 列表中选择一个设备，然后点击**添加到策略 (Add to Policy)**。
- 点击**可用设备 (Available Devices)** 列表中的设备并将其拖移到**所选设备 (Selected Devices)** 列表。
- 点击设备旁边的删除图标 ( )，从**所选设备 (Selected Devices)** 列表中删除设备。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置 NAT 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

祖先域中的管理员可以将NAT策略设为针对后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。如果NAT策略针对不同后代域中的设备，则后代域中的管理员可以查看有关仅属于其域的目标设备的信息。

如果将某个接口的类型更改为不适用于以具有该接口的设备为目标的NAT策略的类型，策略会将该接口标记为“已删除”。在 NAT 策略中点击 **Save** 会自动从策略删除接口。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 配置 NAT 策略：

- 要修改策略名称或说明，请点击**名称 (Name)** 或**说明 (Description)** 字段，根据需要删除任何字符，然后输入新的名称或说明。在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。
- 要管理策略目标，请参阅配置 NAT 策略目标，第 504 页。
- 要保存策略更改，请点击**保存 (Save)**。
- 要向策略中添加规则，请点击**添加规则 (Add Rule)**。

- 要编辑现有规则，请点击规则旁边的编辑图标 ()。
- 要删除规则，请点击该规则旁边的删除图标 ()，然后点击**确定 (OK)**。
- 要启用或禁用现有规则，请右键点击规则，选择**状态 (State)**，然后选择**禁用 (Disable)** 或**启用 (Enable)**。
- 要显示特定规则属性的配置页面，请点击该规则对应行上的条件对应列中的名称、值或图标。例如，点击 **Source Networks** 列中的名称或值可显示所选规则的 Source Network 页面。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置 NAT 策略目标

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

创建或编辑策略时，可以确定要应用策略的受管设备。可以搜索一系列可用设备、7000 或 8000 系列堆栈和高可用性对，并将其添加到所选设备列表。

不能以运行不同版本的Firepower系统的堆叠设备作为目标（例如，如果其中一台设备的升级失败）。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

祖先域中的管理员可以将NAT策略设为针对后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略。如果NAT策略针对不同后代域中的设备，则后代域中的管理员可以查看有关仅属于其域的目标设备的信息。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击**策略分配 (Policy Assignments)**。

步骤 4 执行以下任一操作：

- 要将设备、堆栈、高可用性对或设备组分配给策略，请在**可用设备 (Available Devices)** 列表中将其选中，然后点击**添加到策略 (Add to Policy)**。还可以进行拖放。

- 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、堆栈、高可用性对或设备组旁边的删除图标 ( )。

步骤 5 点击**保存 (Save)**。
如果系统提示您确认该更改，请点击**确定 (OK)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

复制 NAT 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

您可以创建 NAT 策略的副本。该副本包含所有策略规则和配置。

在多域部署中，可以从当前域和祖先域复制策略。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要复制的 NAT 策略旁边的复制图标 ( )。

步骤 3 为策略输入唯一**名称 (Name)**。
在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

步骤 4 点击**确定 (OK)**。

第 28 章

7000 和 8000 系列设备的 NAT

以下主题介绍如何为 7000 和 8000 系列设备配置 NAT：

NAT 策略配置

可以用不同的方法配置 NAT 策略来管理特定的网络需求。您可以执行以下操作：

- 向外部网络开放内部服务器。
  在此配置中，可定义从外部 IP 地址转换为内部 IP 地址的静态转换，以便系统从网络外部访问内部服务器。发送到服务器的流量以外部 IP 地址或 IP 地址和端口为目标，并转换为内部 IP 地址或 IP 地址和端口。从服务器返回的流量重新转换为外部地址。
- 允许内部主机/服务器连接到外部应用。
  在此配置中，可定义从内部地址转换为外部地址的静态转换。这样的定义允许内部主机或服务器向预期内部主机或服务器有特定IP地址和端口的外部应用发起连接。因此，系统无法动态分配内部主机或服务器的地址。
- 隐藏来自外部网络的专有网络地址。

  可以使用以下任一配置隐藏内部网络地址：

  如果有足够数量的外部 IP 地址可满足内部网络需求，则可使用 IP 地址块。在此配置中，可创建动态转换，以自动将任何传出流量的源 IP 地址转换为来自外部目标 IP 地址的未使用的 IP 地址。

  如果没有足够数量的外部 IP 地址可满足内部网络需求，则可使用有限的 IP 地址块和端口转换。在此配置中，可创建动态转换，以自动将传出流量的源 IP 地址和端口转换为来自外部目标 IP 地址的未使用的 IP 地址。

注意 在 7000 或 8000 系列设备高可用性对中，如果 NAT 转换影响的所有网络都是专用网络，则只能在成对设备上为静态 NAT 规则选择单个对等接口。**请勿**将这些配置用于会影响公共网络与专用网络之间流量的静态 NAT 规则。

NAT 策略配置准则

要配置NAT策略，必须为策略提供一个唯一的名称，以及识别要部署策略的设备（又称为目标）。还可以添加、编辑、删除、启用和禁用 NAT 规则。创建或修改 NAT 策略后，可以将策略部署到全部或部分目标设备。

可以将 NAT 策略部署到 7000 或 8000 系列设备高可用性对（包括成对堆栈），就像应用于独立设备一样。但是，可以对单个成对设备或整个高可用性对上的接口定义静态NAT规则，并在源区域使用这些接口。对于动态规则，只可以在源或目标区域使用整个高可用性对的接口。

注意 在 7000 或 8000 系列设备高可用性对中，如果 NAT 转换影响的所有网络都是专用网络，则只能在成对设备上为静态 NAT 规则选择单个对等接口。**不**能将此配置用于会影响公共网络与专用网络之间流量的静态 NAT 规则。

如果在没有建立高可用性链路接口的设备高可用性对上配置动态 NAT，则两个成对设备将会独自分配动态 NAT 条目，系统将无法同步这两台设备之间的条目。

您可以将 NAT 策略部署到设备堆栈，就像应用于独立设备一样。如果从包含在 NAT 策略中的设备建立设备堆叠，且这些设备具有与作为堆叠成员的辅助设备的接口关联的规则，则辅助设备的接口将保留在 NAT 策略中。您可以保存并部署包含接口的策略，但规则不提供任何转换。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。祖先域中的管理员可以将NAT策略设为针对后代域中的设备，而后代域可以使用这些策略或者将其替换为自定义本地策略

NAT 策略中的规则组织

NAT 策略的 Edit 页面分别列出了静态 NAT 规则和动态 NAT 规则。系统按名称的字母顺序对静态规则进行排序，显示顺序不能更改。不能创建具有相同的匹配值的静态规则。系统会先检查匹配的静态转换，再检查所有动态转换。

动态规则按数字顺序处理。每个动态规则的数字位置显示在规则旁边的页面左侧。可以移动或插入动态规则，也可以更改规则顺序。例如，如果将动态规则 10 移动到动态规则 3 下方，规则 10 将会变成规则 4，而且所有后续编号将会相应地增大。

动态规则的位置很重要，因为系统会按策略的 Edit 页面中显示的规则数字顺序将数据包与动态规则进行比较。如果某个数据包符合某个动态规则的所有条件，系统会将该规则的条件应用于该数据包，并忽略该数据包的所有后续规则。

可以在添加或编辑动态规则时指定动态规则的数字位置。还可以在增加新的动态规则之前突出显示某个动态规则，以将新规则插入到突出显示的规则下方。

可以通过点击规则行的空白区域来选择一个或多个动态规则。可以将选定的动态规则拖放到新位置，从而更改移动的规则及其后续规则的位置。

可以剪切或复制选定的规则，并将其粘贴到现有规则的上方或下方。静态规则只能粘贴到静态转换列表中，动态规则只能粘贴到动态转换列表中。还可以删除选定的规则，并将新规则插入到现有规则列表中的任何位置。

可以显示解释性警告，用以识别由于被前置规则抢占而绝对不会匹配的规则。

如果在部署中有访问控制策略，系统会在流量通过访问控制后才对其进行转换。

组织 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 组织 NAT 规则：

- 要选择规则，请点击规则的对应行中的空白区域。
- 要清除规则选择，请点击页面右下方的重新加载图标 ( )。要清除单个规则，请按住 Ctrl 键并点击规则行的空白区域。
- 要剪切或复制所选规则，请右键点击所选规则的对应行中的空白区域，然后选择**剪切 (Cut)** 或**复制 (Copy)**。
- 要将已剪切或复制的规则粘贴到规则列表中，请右键点击要粘贴所选规则的规则的对应行中的空白区域，然后选择**粘贴在上方 (Paste above)** 或**粘贴在下方 (Paste below)**。
- 要移动所选规则，请在新位置下拖放所选规则，该位置通过拖动规则时指针上方显示的蓝色横线进行指示。
- 要删除规则，请点击该规则旁边的删除图标 ( )，然后点击**确定 (OK)**。
- 要显示警告，请点击**显示警告 (Show Warnings)**。

NAT 规则警告和错误

NAT 规则的条件可以抢占来自匹配流量的后续规则。任何类型的规则条件都可以抢占后续规则。

规则还会抢占所有配置条件都相同的完全一样的后续规则。只要任何一个条件不同，后续规则都不会被抢占。

如果创建导致NAT策略在部署时失败的规则，则该规则旁边会显示错误图标( )。如果静态规则中存在冲突，或者编辑策略中使用的但当前使策略无效的网络对象，将会出现错误。例如，如果将网络对象更改为只使用IPv6地址，并且使用该对象的规则不再有任何有效网络，但该规则要求至少有一个网络，将会出现错误。错误图标自动显示；无需点击 **Show Warnings**。

显示和隐藏 NAT 规则警告

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 要显示警告，请点击**显示警告 (Show Warnings)**。

页面即会更新，每个被抢占的规则旁边都显示警告图标 ( )。

步骤 4 要显示规则的警告，请将指针悬停在规则旁边的警告图标 ( ) 上方。

系统将显示一条消息，指明哪个规则抢占了该规则。

步骤 5 要清除警告，请点击**隐藏警告 (Hide Warnings)**。

页面即会刷新，警告消失。

NAT 策略规则选项

简单来说，NAT 规则是一组具有如下作用的配置和条件：

- 限定网络流量
- 指定那些符合资格的流量如何转换

可以在现有 NAT 策略中创建和编辑 NAT 规则。每个规则只属于一个策略。

用于添加或编辑规则的网络界面是类似的。在页面顶部指定规则的名称、状态、类型和位置（如果是动态规则）。在页面左侧使用选项卡建立条件；每种条件都有自己的选项卡。

以下列表总结了 NAT 规则的可配置组成部分。

Name

为每个规则提供唯一的名称。对于静态 NAT 规则，请使用最多 22 个字符。对于动态 NAT 规则，请使用最多 30 个字符。可以使用可打印字符，包括空格和特殊字符，但冒号 (:) 除外。

规则状态

默认情况下，规则处于启用状态。系统不使用已禁用的规则来评估要转换的网络流量。查看 NAT 策略中的规则列表时，已禁用的规则呈灰色显示，但这些规则仍可以修改。

Type

规则的类型决定系统如何处理与规则条件相匹配的流量。创建和编辑 NAT 规则时，可配置的组成部分因规则类型而异。

位置（仅适用于动态规则）

NAT 策略中的动态规则带有编号（从 1 开始）。系统按编号自上而下的顺序将流量与 NAT 规则进行匹配。

向策略添加规则时，可以使用规则编码作为参考点，通过将其置于特定规则**之上**或**之下**来确定它的位置。编辑现有规则时，可以通过类似的做法**移动**规则。

条件

规则条件确定要转换的特定流量。条件可以通过多个属性（包括安全区域、网络和传输协议端口）的任意组合来匹配流量。

创建和编辑 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的策略和规则，您可以对其进行编辑。系统还会显示在祖先域中创建的策略和规则，您不可以对其进行编辑。要查看和编辑在较低域中创建的规则，请切换至该域。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要向其添加规则的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 要添加新规则或编辑现有规则：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击要编辑的规则旁边的编辑图标 ()。

步骤 4 在**名称 (Name)** 中输入唯一的规则名称。

步骤 5 配置以下规则组成部分：

- 指定规则是否为 **Enabled**。
- 在**类型 (Type)** 中指定规则类型。
- 指定规则位置（仅适用于动态规则）。
- 配置规则的条件。

注释 静态规则必须包括原始目标网络。动态规则必须包含转换后的源网络。

步骤 6 点击 **Add**。

步骤 7 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

NAT 规则类型

每个 NAT 规则都有具有如下作用的相关类型：

- 限定网络流量
- 指定那些符合资格的流量如何转换

以下列表总结了 NAT 规则类型。

静态

静态规则提供对目标网络或者端口和协议的一对一转换。配置静态转换时，可以配置源区域、目标网络和目标端口。不能配置目标区域或源网络。

必须指定原始目标网络。对于目标网络，只能选择包含单个 IP 地址的网络对象和组，或者输入代表单个 IP 地址的文字 IP 地址。只能指定一个原始目标网络和一个转换后的目标网络。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

您可以指定一个原始目标端口和一个转换后的目标端口。在指定原始目标端口之前，必须指定原始目标网络。此外，必须满足以下条件才能指定转换后的目标端口：已经指定原始目标端口，且转换后的值与原始值的协议相匹配。

注意 对于高可用性对中的 7000 或 8000 系列设备上的静态 NAT 规则，如果所有受 NAT 转换影响的网络都是专用网络，则仅选择单个对等接口。不能将此配置用于会影响公共网络与专用网络之间流量的静态 NAT 规则。

仅动态 IP

“仅动态 IP”规则转换多对多源网络，但保留端口和协议。配置“仅动态 IP”转换时，可以配置区域、源网络、原始目标网络和原始目标端口。不能配置转换后的目标网络或转换后的目标端口。

必须至少指定一个转换后的源网络。如果转换后的源网络值的数量少于原始源网络的数量，系统将会显示针对的警告，指出在所有原始地址匹配之前可能用完转换后的地址。

如果有多个规则具有与同一个数据包相匹配的规则，优先级较低的规则将会变成死规则，这意味着，这些规则绝不会被触发。系统还会显示针对死规则的警告。可以查看工具提示来确定哪个规则取代了死规则。

注释 您可以保存并部署包含无效规则的策略，但此类规则无法提供任何转换。

在某些情况下，您可能希望以较大的范围创建带有有限范围前置规则的规则。例如：

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

在此示例中，与某些数据包匹配的规则 1 也与规则 2 相匹配。因此，规则 2 并没有完全死亡。

如果您仅指定原始目标端口，则无法指定转换后的目标端口。

动态 IP + 端口

“动态 IP 和端口”规则转换多对一或多对多的源网络、端口和协议。配置“动态 IP 和端口”转换时，可以配置区域、源网络、原始目标网络和原始目标端口。不能配置转换后的目标网络或转换后的目标端口。

必须至少指定一个转换后的源网络。如果有多个规则具有与同一个数据包相匹配的规则，优先级较低的规则将会变成死规则，这意味着，这些规则绝不会被触发。系统还会显示针对死规则的警告。可以查看工具提示来确定哪个规则取代了死规则。

注释 您可以保存并部署包含无效规则的策略，但此类规则无法提供任何转换。

如果您仅指定原始目标端口，则无法指定转换后的目标端口。

注释 如果创建动态 IP 和端口规则，并且系统传递没有使用接口的流量，流量不发生转换。例如，来自匹配源网络的 IP 地址的 ping (ICMP) 不会映射，因为 ICMP 不使用端口。

NAT 规则条件类型

下表总结了可以根据指定的 NAT 规则类型配置的 NAT 规则条件类型：

表 *64*: 每种 *NAT* 规则类型可用的 *NAT* 规则条件类型

情况	静态	动态（仅 IP 或 IP+ 端口）
源区域	可选	可选
目标区域	不允许	可选
原始源网络	不允许	可选
转换后的源网络	不允许	**必要**
原始目标网络	**必填**	可选
转换后的目标网络	可选；仅单个地址	不允许
原始目标端口	可选；仅限单个端口，且仅在定义了原始目标网络的情况下才可用	可选
转换后的目标端口	可选；仅限单个端口，且仅在定义了原始目标端口的情况下才可用	不允许

NAT 规则条件和条件机制

可以向NAT规则添加条件来识别与规则匹配的流量的类型。对于每种条件类型，从可用条件列表中选择要添加到规则的条件。如果适用，可使用条件过滤器来限制可用的条件。可用条件和选定条件的列表可以短至只包含一个条件，也可以长达多页。可以搜索可用条件，并仅显示那些与您在列表中键入的名称或值相匹配的条件（该列表会根据键入的内容同步更新）。

根据条件类型，可用条件的列表可能包含直接由思科提供或使用其他Firepower系统功能配置的条件的组合，包括使用对象管理器（**对象 (Objects)** > **对象管理 (Object Management)**）创建的对象、直接从个别条件页面创建的对象以及文字条件。

NAT 规则条件

可以设置 NAT 规则来匹配满足下表所述的任何条件的流量：

表 *65*: *NAT* 规则条件类型

情况	说明
区域	可以部署 NAT 策略的一个或多个路由接口的配置。区域提供用于对源接口和目标接口上的流量进行分类的机制；您可以向规则添加源区域条件和目标区域条件。
网络	明确指定或使用网络对象和组指定的单个IP地址、CIDR块和前缀长度的任意组合。可以将源和目标网络条件添加到 NAT 规则中。
目标端口	传输协议端口，包括基于传输协议创建的单个端口对象和端口对象组。

将条件添加到 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

对于每种条件，向NAT规则添加条件的操作基本相同。在左侧的可用条件列表中选择条件，然后将所选条件添加到右侧的一个或两个选定条件列表中。

对于所有条件类型，要选择一个或多个单独的可用条件，可通过点击来突出显示要选择的条件。可以点击两种列表之间的按钮将所选的可用条件添加到选定条件列表，也可以将所选的可用条件拖放到选定条件列表。

最多可以将同一类型的 50 个条件添加到选定条件列表。例如，最多可以添加 50 个源区域条件、50 个目标区域条件和 50 个源网络条件，等等，直至达到设备的上限。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Add Rule**（添加规则）。

步骤 4 为规则输入**名称 (Name)**。

步骤 5 为规则指定**类型 (Type)**。

步骤 6 点击要添加到规则的条件类型的选项卡。

步骤 7 执行下列操作之一：

- 要选择要添加到选定条件列表的可用条件，请点击可用条件。
- 要选择所有列出的可用条件，请右键点击任何可用条件的行，然后点击**全选 (Select All)**。
- 要选择可用条件或过滤器的列表，请在**搜索 (Search)** 字段中点击，然后输入搜索字符串。列表会在您键入内容时进行更新，以显示匹配的项目。
  您可以搜索对象名称以及为对象配置的值。例如，如果有一个名为 `Texas Office` 的网络对象，该对象配置了 `192.168.3.0/24` 这个值，且该对象包含在组对象 `US Offices` 中，则可以输入部分或完整的搜索字符串（例如 `Tex`）或者输入某个值（例如 `3`）来显示这两个对象。
- 要在搜索可用条件或过滤器时清除搜索，请点击“搜索”(Search) 字段上方的重新加载图标 ( ) 或点击“搜索”(Search) 字段中的清除图标 ( )。
- 要将可用条件列表中的选定区域条件添加到选定源条件或目标条件的列表，请点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。
- 要将可用条件列表中的选定网络和端口条件添加到选定源条件或已转换条件的列表，请点击**添加到原始 (Add to Source)** 或**添加到已转换 (Add to Translated)**。
- 要将选定的可用条件拖放到选定条件列表中，请点击选定的条件，然后将其拖放到选定条件列表。
- 要使用文字字段将文字条件添加到选定条件列表，请点击以删除文字字段中的提示，输入文字条件，然后点击**添加 (Add)**。网络条件提供一个用于添加文字条件的字段。
- 要使用下拉列表将文字条件添加到选定条件列表，请从下拉列表中选择一个条件，然后点击**添加 (Add)**。端口条件提供一个用于添加文字条件的下拉列表。
- 要添加单个对象或条件过滤器以供在可用条件列表中选择，请点击添加图标 ( )。
- 要从选定条件列表中删除单个条件，请点击该条件旁边的删除图标 ( )。
- 要从选定条件列表中删除条件，请右键点击以突出显示所选条件的行，然后点击**删除 (Delete)**。

步骤 8 点击 **Add** 保存配置。

NAT 规则中的文字条件

可以向以下条件类型的原始条件列表和转换后条件列表添加文字值。

- 网络
- 端口

对于网络条件，可在原始条件列表或转换后条件列表下方的配置字段中键入文字值。

对于端口条件，可从下拉列表中选择协议。当协议为 `All` 或 `TCP` 或 `UDP` 时，在配置字段输入端口号。

每个相关条件页面都提供添加文字值所需的控件。如果在配置字段中输入的值是无效的，将会显示为红色文本，直至被识别为是有效值。值被识别为有效值后，将会变为蓝色文本。识别到有效值后，呈灰色显示的 **Add** 按钮将会激活。添加的文字值立即显示在选定条件列表中。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

NAT 规则条件中的对象

在对象管理器 (**对象 (Objects)** > **对象管理 (Object Management)**) 中创建的对象会立即显示在相关的可用 NAT 规则条件列表中以供选择。

还可以通过NAT策略快速创建对象。相关条件页面上的控件提供对于在对象管理器中使用的相同配置控件的访问权限。

快速创建的各个对象会立即显示在可用对象列表中。可以将创建的对象添加到当前规则以及其他现有和将来的规则。在相关条件页面和策略Edit页面上，将指针悬停在单个对象上显示该对象的内容，将指针悬停在某个组对象上可显示该组中各个对象的编号。

NAT 规则中的区域条件

系统的安全区域包括受管设备的接口。添加到NAT规则的区域使规则以网络上在这些区域中有路由接口或混合接口的设备为目标。只能将带有路由接口或混合接口的安全区域添加为NAT规则条件。

可以将当前已分配给虚拟路由器的区域或独立接口添加到 NAT 规则。如果有未部署设备配置的设备，则“区域”(Zones)页面会在可用区域列表的顶部显示警告图标(⚠)，指示仅显示已部署的区域和接口。可以点击区域旁边的箭头图标 (▷) 来折叠或展开区域，以隐藏或查看其接口。

如果接口在高可用性对中的 7000 或 8000 系列设备上，则可用区域列表会显示来自该接口的额外分支，并以高可用性对中的其他接口作为该高可用性对中主用设备上的主接口的子级。您也可以点击箭头图标 (▷) 来折叠或展开配对设备接口，以隐藏或查看其接口。

注释 可以保存和部署包含已禁用接口的策略，但是规则无法提供任何转换，直至启用接口为止。

右侧列出的两个条目是供NAT规则用于匹配用途的源区域和目标区域。如果规则配置了值，当您编辑规则时，这些列表将显示现有值。如果源区域列表为空，规则将会匹配来自任何区域或接口的流量。如果目标区域列表为空，规则将会匹配流向任何区域或接口的流量。

对于带有绝不会在目标设备上触发的区域组合的规则，系统会显示警告。

注释 可以保存和部署包含这些区域组合的策略，但是规则将不提供任何转换。

可以通过选择区域中的某个项目或选择独立接口来添加各个接口。如果要向其添加接口的区域未添加到源区域列表或目标区域列表，则只能在该区域中添加接口。这些单独选定的接口不受区域更改的影响，即使您删除并将其添加到不同的区域。如果接口是高可用性对的主成员，并且配置的是动态规则，则只能将主接口添加到源区域或目标区域列表。对于静态规则，可以将各个高可用性对成员接口添加到源区域列表。仅当未添加高可用性对主接口的任何子级时才能添加此接口，并且仅当未添加高可用性对主接口时才能添加各个高可用性对接口。

如果添加区域，规则会使用与添加的区域关联的所有接口。如果从区域添加或删除接口，则规则不会使用区域的已更新版本，直至设备配置重新部署到接口所在的设备为止。

注释 在静态 NAT 规则中，只能添加源区域。在动态 NAT 规则中，可添加源区域和目标区域。

将区域条件添加到 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Add Rule**（添加规则）。

步骤 4 为规则输入**名称 (Name)**。

步骤 5 为规则指定**类型 (Type)**。

步骤 6 点击**区域 (Zones)** 选项卡。

步骤 7 在 **Available Zones** 列表中点击所需的区域或接口。

步骤 8 有以下选项可供选择：

- 要根据源区域匹配流量，请点击 **Add to Source**。
- 要根据目标区域匹配流量，请点击 **Add to Destination**。

注释　只能将源区域添加到静态 NAT 规则。此外，虽然可以向 NAT 规则中添加已禁用的接口，但是该规则不提供任何转换。

步骤 9　点击**添加 (Add)** 以保存新规则。

步骤 10　点击**保存 (Save)** 以保存已更改的策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

动态 NAT 规则中的源网络条件

可以配置数据包源 IP 地址的匹配值和转换值。如果原始源网络未配置，任何源 IP 地址都会匹配动态 NAT 规则。请注意，不能配置静态 NAT 规则的源网络。如果数据包与 NAT 规则相匹配，系统会使用转换后源网络的值来为源 IP 地址分配新值。对于动态规则，则必须配置至少有一个值的转换后源网络。

注意　如果更改或删除正被 NAT 规则使用的网络对象或对象组，可能导致规则无效。

可以将以下任何类型的源网络条件添加到动态 NAT 规则：

- 使用对象管理器创建的单个网络对象和成组网络对象
- 从 Source Network 条件页面添加的单个网络对象（这些对象随后可添加到当前规则以及其他现有和将来的规则）
- 单个文字 IP 地址、地址范围或地址块

注释　系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

将网络条件添加到动态 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

在已部署的策略中使用的动态规则中更新网络条件时，系统会使用现有已转换地址池丢弃任何网络会话。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Add Rule**（**添加规则**）。

步骤 4 为规则输入**名称 (Name)**。

步骤 5 为规则指定动态**类型 (Type)**。

- **仅动态 IP**
- **动态 IP + 端口**

步骤 6 点击**源网络 (Source Networks)** 选项卡。

步骤 7 或者，通过点击**可用网络 (Available Networks)** 列表上方的添加图标 () 向该列表添加单个网络对象。

可以向每个网络对象添加多个 IP 地址、CIDR 块和前缀长度。

步骤 8 在 **Available Networks** 列表中点击要添加的条件。

步骤 9 有以下选项可供选择：

- 要根据原始源网络匹配流量，请点击 **Add to Original**。
- 要为与转换后源网络匹配的流量指定转换值，请点击 **Add to Translated**。

步骤 10 要添加文字 IP 地址、范围或地址块，请执行以下操作：

a) 点击**原始源网络 (Original Source Network)** 或**转换后的源网络 (Translated Source Network)** 列表下方的**输入 IP 地址 (Enter an IP address)** 提示。

b) 输入 IP 地址、范围或地址块。

按以下格式添加地址范围：低位 IP 地址-高位 IP 地址。例如：`179.13.1.1-179.13.1.10`。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

c) 点击您输入的值旁边的**添加 (Add)**。

步骤 11 点击 **Add** 保存规则。

步骤 12 点击**保存 (Save)** 以保存已更改的策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

NAT 规则的目标网络条件

可以配置数据包目标 IP 地址的匹配值和转换值。请注意，不能为动态 NAT 规则配置转换后目标网络。

由于静态 NAT 规则是一对一转换，因此，**Available Networks** 列表仅包含只有一个 IP 地址的网络对象和网络对象组。对于静态转换，只能将一个对象或文字值添加到 **Original Destination Network** 或 **Translated Destination Network** 列表。

注意 如果更改或删除正被 NAT 规则使用的网络对象或对象组，可能导致规则无效。

可以将以下任何类型的目标网络条件添加到 NAT 规则：

- 使用对象管理器创建的单个网络对象和成组网络对象
- 从 Destination Network 条件页面添加的单个网络对象（这些对象随后可添加到当前规则以及其他现有和将来的规则）
- 单个文字 IP 地址、地址范围或地址块

  对于静态 NAT 规则，只能添加带子网掩码 /32 的 CIDR，并且只能在列表中不能已存在值的情况下添加。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

将目标网络条件添加到 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

在已部署的策略中使用的动态规则中更新网络条件时，系统会使用现有已转换地址池丢弃任何网络会话。

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Add Rule**（添加规则）。

步骤 4 为规则输入**名称 (Name)**。

步骤 5 为规则指定**类型 (Type)**。

步骤 6 点击**目标网络 (Destination Network)** 选项卡。

步骤 7 或者，通过点击**可用网络 (Available Networks)** 列表上方的添加图标 () 向该列表添加单个网络对象。

对于动态规则，可以向每个网络对象添加多个 IP 地址、CIDR 块和前缀长度。对于静态规则，只能添加一个 IP 地址。

步骤 8 点击**可用网络 (Available Networks)** 列表中的条件或对象。

步骤 9 有以下选项可供选择：

- 要根据原始目标网络匹配流量，请点击 **Add to Original**。
- 要为与转换后目标网络匹配的流量指定转换值，请点击 **Add to Translated**。

步骤 10 或者，点击**原始目标网络 (Original Destination Network)** 或**已转换目标网络 (Translated Destination Network)** 列表下方的**输入 IP 地址 (Enter an IP address)** 提示，输入 IP 地址或地址块，然后点击**添加 (Add)**。

步骤 11 点击 **Add**。

步骤 12 点击**保存 (Save)** 以保存对策略的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

NAT 规则中的端口条件

可以根据原始目标端口、转换后目标端口和用于转换的传输协议将端口条件添加到与网络流量匹配的规则。如果未配置原始端口，任何目标端口都会匹配该规则。如果数据包与NAT值相匹配，并且转换后目标端口已配置，系统会将端口转换为该值。请注意，对于动态规则，只能指定原始目标端口。对于静态规则，可以定义转换后目标端口，但前提是，转换后目标端口所带有的对象与原始目标端口对象或文字值使用相同的协议。

对于静态规则，系统会将目标端口与原始目标端口列表中端口对象或文字对象的值进行匹配；对于动态规则，会将目标端口与多个值进行匹配。

由于静态 NAT 规则是一对一转换，因此，**Available Ports** 列表仅包含只有一个端口的端口对象和端口对象组。对于静态转换，只能将一个对象或文字值添加到 **Original Port** 或 **Translated Port** 列表。

对于动态规则，可以添加一系列端口。例如，在指定原始目标端口时，可以添加 `1000-1100` 作为文字值。

注意 如果更改或删除正被 NAT 规则使用的对象或对象组，可能导致规则无效。

可以将以下任何类型的端口条件添加到 NAT 规则：

- 使用对象管理器创建的单个端口对象和成组端口对象
- 从 Destination Ports 条件页面添加的单个网络对象（这些对象随后可添加到当前规则以及其他现有和将来的规则）
- 文字端口值，由 TCP、UDP、All（TCP 和 UDP）传输协议和一个端口组成

将端口条件添加到 NAT 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	可控性	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **NAT**。

步骤 2 点击要修改的 NAT 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Add Rule**（**添加规则**）。

步骤 4 为规则输入**名称 (Name)**。

步骤 5 为规则指定**类型 (Type)**。

步骤 6 点击**目标端口 (Destination Port)** 选项卡。

步骤 7 或者，通过点击**可用端口 (Available Ports)** 列表上方的添加图标 ( ) 向该列表添加单个端口对象。您可以识别要添加的每个端口对象中的单个端口或端口范围。然后，可以选择添加为规则条件的对象。对于静态规则，只能使用带有单个端口的端口对象。

步骤 8 在 **Available Ports** 列表中点击要添加的条件。

步骤 9 有以下选项可供选择：

- 点击**添加到原始 (Add to Original)**。
- 点击**添加到已转换 (Add to Translated)**。
- 将可用端口拖放到列表。

步骤 10 要添加文字端口，请执行以下操作：

a) 从**原始端口 (Original Port)** 或**已转换端口 (Translated Port)** 列表下的**协议 (Protocol)** 下拉列表中选择条目。

b) 输入端口。

c) 点击 **Add**。

对于动态规则，可以指定单个端口或端口范围。

步骤 11 点击 **Add**。

步骤 12 点击**保存 (Save)** 以保存对策略的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

第 X 部分

7000 和 8000 系列高级部署选项

第 29 章

设置虚拟交换机

以下主题介绍如何在 FirePOWER 系统中设置虚拟交换机：

虚拟交换机

可以在第 2 层部署中配置 7000 或 8000 系列设备，使其在两个或多个网络之间提供数据包交换。在第 2 层部署中，可以配置虚拟机作为单独广播域运行，将网络划分为多个逻辑网段。虚拟交换机根据主机的媒体访问控制 (MAC) 地址来确定在哪里发送数据包。

当配置虚拟交换机时，交换机起初会通过交换机的每个可用端口来广播数据包。随着时间的推移，交换机使用标记的回传流量了解哪些主机驻留在连接到每个端口的网络上。

虚拟交换机必须包含两个或多个交换接口来处理流量。对于每个虚拟交换机，配置作为交换接口的组端口的流量受到限制。例如，如果用四个交换接口配置虚拟交换机，通过某个广播端口发送的数据包只能通过交换机的其余三个端口转发出去。

配置物理交换接口时，必须将它分配到虚拟交换机。还可以根据需要在物理端口定义其他逻辑交换接口。可以将多个物理接口组合到名为链路汇聚组 (LAG) 的单一逻辑交换接口中。该单一汇聚逻辑链路提供更高的带宽、冗余和两个终端之间的负载平衡。

注意 如果第二层部署因任何原因而失效，设备将不再传递流量。

交换接口配置

可以将交换接口设置成物理或逻辑配置。可以配置用于处理未标记 VLAN 流量的物理交换接口。还可以创建用于处理含指定 VLAN 标记的流量的逻辑交换接口。

在第二层部署，系统将删除在没有交换接口为其等待的外部物理接口上收到的所有流量。如果系统接收到没有 VLAN 标记的数据包且您没有为该端口配置物理交换接口，系统会删除该数据包。如果系统收到带有 VLAN 标记的数据包且您未配置逻辑交换接口，系统也会删除数据包。

系统在交换接口处理所接收的带有 VLAN 标记的流量，去除入口处最外层的 VLAN 标记，然后做出任何规则评估或转发决策。通过 VLAN 标记的逻辑交换接口离开设备的数据包将通过出口相关的 VLAN 标记封装。

请注意，如果将父物理接口更改为内联或被动接口，系统将删除所有关联的逻辑接口。

交换接口配置说明

可以在受管设备上配置一个或多个物理端口作为交换接口。必须将物理交换接口分配到虚拟交换机，物理接口才可以处理流量。只能为铜缆接口配置链路模式设置和 MDI/MDIX 设置。

注释 8000 系列设备上的接口不支持半双工选项。

对于每个物理交换接口，可以添加多个逻辑交换接口。必须将每个逻辑接口与 VLAN 标记关联，以处理物理接口接收的带有该特定标记的流量。必须指定一个逻辑交换接口作为虚拟交换机来处理流量。

配置交换接口时，MTU 的设置范围可能根据 Firepower 系统设备型号和接口类型而异。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

要编辑现有逻辑交换接口，请点击接口旁的编辑图标 ( )。

当删除逻辑交换接口时，会从其所在的物理接口将其删除，同时会还会删除与之相关的虚拟交换机和安全区域。

配置物理交换接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在需要配置交换接口的设备旁，点击编辑图标 ( )。

在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在需要配置为交换接口的接口旁边，点击编辑图标 ()。

步骤 4 点击**交换 (Switched)** 选项卡。

步骤 5 如果要将交换接口与安全区域相关联，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象，第 309 页。

步骤 6 如果要将交换接口与虚拟交换机相关联，请执行以下操作之一：

- 从**虚拟交换机 (Virtual Switch)** 下拉列表中选择现有虚拟交换机。
- 选择**新建 (New)** 以添加新的虚拟交换机；请参阅添加虚拟交换机，第 532 页。

步骤 7 选中**已启用 (Enabled)** 复选框以允许交换接口处理流量。

注释 如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8 从**模式 (Mode)** 下拉列表中，选择一个选项以指定链路模式，或者选择**自动协商 (Autonegotiation)** 以指定将接口配置为自动协商速度和双工设置。
模式设置仅适用于铜缆接口。

8000 系列设备上的接口不支持半双工选项。

步骤 9 从 **MDI/MDIX** 下拉列表中，选择一个选项以指定接口是配置用于 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。
默认情况下，MDI/MDIX 设置为 Auto-MDIX，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10 在 **MTU** 字段中，输入用于指定所允许的最大数据包的最大传输单位 (MTU)。
MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 11 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加逻辑交换接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在需要添加交换接口的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击 **Add Interface**。

步骤 4 点击**交换 (Switched)**。

步骤 5 从**接口 (Interface)** 下拉列表中，选择将接收 VLAN 标记的流量的物理接口。

步骤 6 在 **VLAN 标记 (VLAN Tag)** 字段中，输入将分配到此接口上的入站和出站流量的标记值。
该标记值可以是 1 到 4094 之间的任何整数。

步骤 7 如果要将交换接口与安全区域相关联，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象，第 309 页。

步骤 8 如果要将交换接口与虚拟交换机相关联，请执行以下操作之一：

- 从**虚拟交换机 (Virtual Switch)** 下拉列表中选择现有虚拟交换机。
- 选择**新建 (New)** 以添加新的虚拟交换机；请参阅添加虚拟交换机，第 532 页。

步骤 9 选中**已启用 (Enabled)** 复选框以允许交换接口处理流量。
如清除此复选框，则将禁用并强制性断开该接口。如果禁用物理接口，则会同时禁用与其相关的所有逻辑接口。

步骤 10 在 **MTU** 字段中，输入用于指定所允许的最大数据包的最大传输单位 (MTU)。
MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 11 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

删除逻辑交换接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要删除的包含交换接口的受管设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要删除的逻辑交换接口旁，点击删除图标 ( )。

步骤 4 出现提示时，请确认要删除接口。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

虚拟交换机配置

您必须先配置虚拟交换机并为其分配交换接口，然后才能在第二层部署中使用交换接口。虚拟交换机是通过网络处理入站和出站流量的一组交换接口。

虚拟交换机配置说明

可以从 Device Management 页面的 Virtual Switches 选项卡添加虚拟交换机。“虚拟交换机”(Virtual Switches) 选项卡显示已在设备上配置的所有虚拟交换机的列表。该页面包含有关每个交换机的摘要信息。

表 *66*：虚拟交换机表视图字段

字段	说明
Name	虚拟交换机的名称。
接口	已分配到虚拟交换机的所有交换接口。已从 Interfaces 选项卡禁用的接口将不可用。
Hybrid Interface	将虚拟交换机关联到虚拟路由器的可选择配置的混合接口。
Unicast Packets	虚拟交换机的单播数据包统计信息，包括： • 接收的单播数据包 • 转发的单播数据包（不包括主机丢包） • 无意间丢弃的单播数据包

字段	说明
Broadcast Packets	虚拟交换机的广播数据包统计信息，包括： • 接收的广播数据包 • 转发的广播数据包 • 无意间丢弃的广播数据包

在配置交换接口时也可以添加交换机。只能将交换接口分配到虚拟交换机。如果要在受管设备配置交换接口之前创建虚拟交换机，可以创建空的虚拟交换机并稍后为之添加接口。

提示

要编辑现有虚拟交换机，请点击交换机旁的编辑图标 ( )。

添加虚拟交换机

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在需要添加虚拟交换机的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟交换机 (Virtual Switches)** 选项卡。

步骤 4 点击 **Add Virtual Switch**。

步骤 5 在**名称 (Name)** 字段中输入名称。

步骤 6 从**可用 (Available)** 列表中，选择一个或多个要添加到虚拟交换机的交换接口。

提示 已从 Interfaces 选项卡中禁用的接口将不可用；添加接口后禁用接口会从配置中删除该接口。

步骤 7 点击 **Add**。

步骤 8 如果要将虚拟交换机绑定到虚拟路由器，请从**混合接口 (Hybrid Interface)** 下拉列表中选择混合接口。

步骤 9 或者，配置交换机的高级设置；请参阅 高级虚拟交换机设置 ， 第 533 页

步骤 10 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

高级虚拟交换机设置

添加静态 MAC 条目

随着时间的推移，虚拟交换机通过标记来自网络的回传流量来了解 MAC 地址。可以手动添加静态 MAC 条目，指定驻留在特定端口的 MAC 地址。不管是否收到来自该端口的流量，MAC 地址在表中将保持静态。可以为每个虚拟交换机指定一个或多个静态 MAC 地址。

启用生成树协议 (STP) 并丢弃网桥协议数据单元 (BPDU)。

STP 是一种用来防止网络环路的网络协议。BPDU 通过网络进行交换，并传输有关网络桥接的信息。如果网络中存在重复的链路，该协议将使用 BPDU 识别并选择最快的网络链路。如果网络链路发生故障，生成树会切换到现有的备用链路。

注释 思科强烈建议在配置计划在 7000 或 8000 系列设备高可用性对中部署的虚拟交换机时启用 STP。只有当虚拟交换机在多个网络接口之间交换流量时，才启用 STP。

如果虚拟交换机在 VLAN 之间路由，类似于单臂路由，BPDU 将通过不同的逻辑交换接口进出设备，但是在同一个物理交换接口。因此，STP 确认设备为冗余网络环路，可在特定第二层部署产生问题。为了防止这种情况出现，可在域级别配置虚拟交换机，让设备在监控流量时删除 BPDU。只有禁用 STP，才能丢弃 BPDU。

注释 只有当虚拟交换机通过单个物理接口在各个 VLAN 之间路由流量时，才能选择丢弃 BPDU。

启用严格 TCP 执行

为最大程度地提高 TCP 安全性，您可以启用严格执行，从而阻止未完成三次握手的连接。严格执行功能也阻止：

- 三次握手尚未完成的连接的非 SYN TCP 数据包
- TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
- TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

请注意，如果将虚拟交换机与逻辑混合接口关联，交换机使用与该逻辑混合接口关联的虚拟路由器相同的严格 TCP 执行设置。在这种情况下，不能在交换机上的指定严格 TCP 执行。

配置高级虚拟交换机设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要编辑的包含虚拟交换机的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟交换机 (Virtual Switches)** 选项卡。

步骤 4 在要编辑的虚拟交换机旁，点击编辑图标 ( )。

步骤 5 点击 **Advanced** 选项卡。

步骤 6 要添加静态 MAC 条目，请点击 **Add**。

步骤 7 在 **MAC 地址 (MAC Address)** 字段中，使用标准格式（即用冒号隔开的六组两位十六进制数字）输入地址（例如，01:23:45:67:89:AB）。

注释 广播地址（00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF）不能作为静态 MAC 地址来添加。

步骤 8 从**接口 (Interface)** 下拉列表中，选择要分配 MAC 地址的接口。

步骤 9 点击 **OK**。

步骤 10 如果要启用生成树协议，请选中**启用生成树协议 (Enable Spanning Tree Protocol)** 复选框。

步骤 11 如果要启用严格 TCP 执行，请选中**严格 TCP 执行 (Strict TCP Enforcement)** 复选框。
如果将虚拟交换机与逻辑混合接口关联，则不会显示此选项，并且交换机使用与该逻辑混合接口关联的虚拟路由器相同的设置。

步骤 12 如果要在域级丢弃 BPDU，请选中**丢弃 BPDU (Drop BPDU)** 复选框。

步骤 13 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改， 第 254 页。

删除虚拟交换机

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

删除虚拟交换机时，所有分配给交换机的交换接口可以纳入另一台交换机中。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要删除的包含虚拟交换机的受管设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟交换机 (Virtual Switches)** 选项卡。

步骤 4 在要删除的虚拟交换机旁，点击删除图标 ( )。

步骤 5 出现提示时，请确认要删除虚拟交换机。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 30 章

设置虚拟路由器

以下主题介绍如何在 FirePOWER 系统中设置虚拟路由器：

虚拟路由器

可在第 3 层部署中配置受管设备，使其在两个或多个接口之间路由流量。要路由流量，必须为每个接口分配一个 IP 地址，并将这些接口分配给虚拟路由器。分配给虚拟路由器的接口可以是物理接口、逻辑接口或链路汇聚组 (LAG) 接口。

可对系统进行配置，使其根据目标地址做出数据包转发决策，从而对数据包进行路由。配置为路由接口的接口将接收和转发第 3 层流量。路由器根据转发条件从输出接口获取目标，访问控制规则指定要应用的安全策略。

在第 3 层部署中，可定义静态路由。此外，可配置路由信息协议 (RIP) 和开放最短路径优先 (OSPF) 动态路由协议。还可进行组合配置，如静态路由和 RIP、静态路由和 OSPF 等组合。

请注意，只能在 7000 或 8000 系列设备上配置虚拟路由器、物理路由接口或逻辑路由接口。

注意 如果第 3 层部署出于任何原因失效，则设备将不再传递流量。

路由接口

可使用物理或逻辑配置设置路由接口。可以配置处理不带标记的 VLAN 流量的物理路由接口。还可创建逻辑路由接口，以处理带有指定 VLAN 标记的流量。

在第 3 层部署中，如果外部物理接口上收到的流量没有等待它的路由接口，系统会将其这些流量全部丢弃。如果出现以下情况，系统将丢弃数据包：

- 系统收到的数据包没有 VLAN 标记，且尚未给该端口配置物理路由接口。
- 系统收到带有 VLAN 标记的数据包，但尚未为该端口配置逻辑路由接口。

在处理交换接口上收到的带 VLAN 标记的流量时，系统会首先在入口处剥离最外层的 VLAN 标记，然后再进行任何规则评估或做出转发决策。当数据包通过带 VLAN 标记的逻辑路由接口离开设备时，系统会在出口处使用关联的 VLAN 标记对该数据包进行封装。剥离过程结束后，系统将丢弃接收到的所有带 VLAN 标记的任何流量。

可向路由接口添加静态地址解析协议 (ARP) 条目。当外部主机要将流量发送到本地网络上的目标 IP 地址时，如果其需要知道该目标 IP 地址的 MAC 地址，它将发送 ARP 请求。配置静态 ARP 条目时，虚拟路由器会使用 IP 地址和关联的 MAC 地址做出响应。

请注意，为逻辑路由接口禁用 **ICMP Enable Responses** 选项不会在所有情景下都阻止 ICMP 响应。您可向访问控制策略添加基于网络的规则，以丢弃目标 IP 为路由接口 IP 且协议为 ICMP 的数据包。

如果您在受管设备上启用**检查本地路由器流量 (Inspect Local Router Traffic)** 选项，则系统会在数据包到达主机之前将其丢弃，从而阻止所有响应。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

如果将父物理接口更改为内联或被动接口，系统将删除所有关联的逻辑接口。

配置物理路由接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可将受管设备上的一个或多个物理端口配置为路由接口。必须先向虚拟路由器分配物理路由接口，然后它才能路由流量。

注意 在 7000 和 8000 系列设备上添加路由接口对在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要修改的接口旁边，点击编辑图标 ( )。

步骤 4 点击 **Routed** 以显示路由接口选项。

步骤 5 如果要应用安全区域，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象 ， 第 309 页。

步骤 6 如果要指定虚拟路由器，请执行以下操作之一：

- 从**虚拟路由器 (Virtual Router)** 下拉列表选择现有虚拟路由器。
- 选择**新建 (New)** 以添加新虚拟路由器；添加虚拟路由器 ， 第 545 页。

步骤 7 选中**已启用 (Enabled)** 复选框以允许交换接口处理流量。如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8 从**模式 (Mode)** 下拉列表中，选择一个选项以指定链路模式，或者选择**自动协商 (Autonegotiation)** 以指定将接口配置为自动协商速度和双工设置。
模式设置仅适用于铜缆接口。

8000 系列设备上的接口不支持半双工选项。

步骤 9 从 **MDI/MDIX** 下拉列表中，选择一个选项以指定接口是配置用于 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。

通常，MDI/MDIX 会设置为 Auto-MDIX，此选项可自动处理 MDI 与 MDIX 之间的切换以获得链路。

MDI/MDIX 设置仅适用于铜缆接口。

步骤 10 在 **MTU** 字段中，选择用于指定所允许的最大数据包的最大传输单位 (MTU)。
MTU 是第 2 层 MTU/MRU，而非第 3 层 MTU。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 11 在 **ICMP** 旁边，选中**启用响应 (Enable Responses)** 复选框，以允许接口对 ICMP 流量做出响应，例如 ping 和 traceroute。

步骤 12 在 **IPv6 NDP** 旁边，选中**启用路由器通告 (Enable Router Advertisement)** 复选框，以使接口广播路由器通告。

步骤 13 要添加 IP 地址，请点击 **Add**。

步骤 14 在**地址 (Address)** 字段中，使用 CIDR 表示法输入路由接口的 IP 地址和子网掩码。
请注意以下提示：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 15 如果您的组织使用 IPv6 地址且您要自动设置接口的 IP 地址，请选中 **IPv6** 字段旁边的**地址自动配置 (Address Autoconfiguration)** 复选框。

步骤 16 对于**类型 (Type)**，选择**正常 (Normal)** 或 **SFRP**。
有关 SFRP 选项，请参阅配置 SFRP，第 544 页以了解详细信息。

步骤 17 点击 **OK**。

- 要编辑 IP 地址，请点击编辑图标 ( )。
- 要删除 IP 地址，请点击删除图标 ( )。

注释 向高可用性对中的 7000 或 8000 系列设备的路由接口添加 IP 地址时，必须向高可用性对的对等设备的路由接口添加相应的 IP 地址。

步骤 18 要添加静态 ARP 条目，请点击 **Add**。

步骤 19 在 **IP 地址 (IP Address)** 字段中，输入静态 ARP 条目的 IP 地址。

步骤 20 在 **MAC 地址 (MAC Address)** 字段中，输入与 IP 地址关联的 MAC 地址。使用标准地址格式（即用冒号隔开的六组两位十六进制数字，例如，01:23:45:67:89:AB）。

步骤 21 点击 **OK**。

提示 要编辑静态 ARP 条目，请点击编辑图标 ( )。要删除静态 ARP 条目，请点击删除图标 ( )。

步骤 22 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加逻辑路由接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

对于每个物理路由接口，可添加多个逻辑路由接口。必须将每个逻辑接口与 VLAN 标记关联，以处理物理接口接收的带有该特定标记的流量。必须向虚拟路由器分配逻辑路由接口以路由流量。

注意 在 7000 和 8000 系列设备上添加路由接口对在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击 **Add Interface**。

步骤 4 点击 **Routed** 以显示路由接口选项。

步骤 5 从**接口 (Interface)** 下拉列表中，选择要向其添加逻辑接口的物理接口。

步骤 6 在 **VLAN 标记 (VLAN Tag)** 字段中，输入将分配到此接口上的入站和出站流量的标记值。该值可以是 1 到 4094 之间的任意一个整数。

步骤 7 如果要应用安全区域，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象，第 309 页。

步骤 8 如果要指定虚拟路由器，请执行以下操作之一：

- 从**虚拟路由器 (Virtual Router)** 下拉列表选择现有虚拟路由器。
- 选择**新建 (New)** 以添加新虚拟路由器；添加虚拟路由器，第 545 页。

步骤 9 选中**已启用 (Enabled)** 复选框以允许交换接口处理流量。

如清除此复选框，则将禁用并强制性断开该接口。如果禁用物理接口，则会同时禁用与其相关的所有逻辑接口。

步骤 10 在 **MTU** 字段中，输入用于指定所允许的最大数据包的最大传输单位 (MTU)。
MTU 是第 2 层 MTU/MRU，而非第 3 层 MTU。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 11 在 **ICMP** 旁边，选中**启用响应 (Enable Responses)** 复选框以将更新或错误消息发送给其他路由器、中间设备或主机。

步骤 12 在 **IPv6 NDP** 旁边，选中**启用路由器通告 (Enable Router Advertisement)** 复选框，以使接口广播路由器通告。

步骤 13 要添加 IP 地址，请点击 **Add**。

步骤 14 在**地址 (Address)** 字段中，使用 CIDR 表示法输入 IP 地址。
请注意以下提示：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 15 如果您的组织使用 IPv6 地址且您要自动设置接口的 IP 地址，请选择 **IPv6** 字段旁边的**地址自动配置 (Address Autoconfiguration)** 复选框。

步骤 16 对于**类型 (Type)**，选择**正常 (Normal)** 或 **SFRP**。
有关 SFRP 选项，请参阅配置 SFRP，第 544 页以了解详细信息。

步骤 17 点击 **OK**。

- 要编辑 IP 地址，请点击编辑图标 ( )。
- 要删除 IP 地址，请点击删除图标 ( )。

注释 向高可用性对中的 7000 或 8000 系列设备的路由接口添加 IP 地址时，必须向高可用性对的对等设备的路由接口添加相应的 IP 地址。

步骤 18 要添加静态 ARP 条目，请点击 **Add**。

步骤 19 在 **IP 地址 (IP Address)** 字段中，输入静态 ARP 条目的 IP 地址。

步骤 20 在 **MAC 地址 (MAC Address)** 字段中，输入与 IP 地址关联的 MAC 地址。使用标准地址格式（即用冒号隔开的六组两位十六进制数字，例如，01:23:45:67:89:AB）。

步骤 21 点击 **OK**。静态 ARP 条目添加成功。

提示 要编辑静态 ARP 条目，请点击编辑图标 ( )。要删除静态 ARP 条目，请点击删除图标 ( )。

步骤 22 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

删除逻辑路由接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

删除逻辑路由接口时，会将它从其所驻留的物理接口删除，并会删除分配给它的的虚拟路由器和安全区域。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ()。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要删除的逻辑路由接口旁，点击删除图标 ()。

步骤 4 出现提示时，请确认要删除接口。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

SFRP

可以配置思科冗余协议 (SFRP) 以实现网络冗余，从而在 7000 或 8000 系列设备高可用性对或单个设备上实现高可用性。SFRP 可为 IPv4 和 IPv6 地址提供网关冗余。您可在路由接口和混合接口上配置 SFRP。

在单一设备配置的各个接口必须位于相同的广播域中。您必须将至少一个此类接口指定为主用接口，并指定相同数量的备用接口。对于每个 IP 地址，系统仅支持一个主用接口和一个备用接口。如果网络连接断开，系统会自动将备用接口升级为主用接口，以保持连接的稳定性。

对于一组 SFRP 接口中的所有接口，为 SFRP 设置的选项必须相同。一个接口组中的多个 IP 地址必须处于相同的主/备状态。因此，添加或编辑 IP 地址时，为该地址设置的状态将传播至其所在组的所有地址。出于安全考虑，必须输入相应组内所有接口所共享的 **Group ID** 和 **Shared Secret** 的值。

为了在虚拟路由器上启用 SFRP IP 地址，还必须至少配置一个非 SFRP IP 地址。

对于高可用性对中的 7000 或 8000 系列设备，请指定共享密钥，系统会将其和 SFRP IP 配置一起复制至对等的高可用性对。共享密钥用于验证对等数据。

配置 SFRP

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可以配置思科冗余协议 (SFRP) 以实现网络冗余，从而在 7000 或 8000 系列设备高可用性对或单个设备上实现高可用性。SFRP 可为 IPv4 和 IPv6 地址提供网关冗余。您可在路由接口和混合接口上配置 SFRP。

注释 思科不建议在的 7000 或 8000 系列设备高可用性对的路由或混合接口（已配置一个 SFRP IP 地址）上启用多个非 SFRP IP 地址。如果 7000 或 8000 系列设备高可用性对在备用模式下发生故障切换，则系统不会执行 NAT。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要为其配置 SFRP 的接口旁，点击编辑图标 ( )。

步骤 4 选择要配置 SFRP 的接口的类型，**路由 (Routed)** 或**混合 (Hybrid)**。

步骤 5 可在添加或编辑 IP 地址时配置 SFRP。点击**添加 (Add)** 以添加 IP 地址。要编辑 IP 地址，请点击编辑图标 ( )。

步骤 6 对于**类型 (Type)**，请选择 **SFRP** 以显示 SFRP 选项。

步骤 7 在 **Group ID** 字段中，输入为 SFRP 配置的一组主用接口或备用接口的值。

步骤 8 对于**优先级 (Priority)**，请选择**主用 (Master)** 或**备用 (Backup)** 以指定首选接口：

- 对于单台设备，必须在一台设备上将某一接口设置为主用接口，在另一设备上将另一接口设置为备用接口。
- 对于 7000 或 8000 系列设备高可用性对，在将某一接口设置为主用接口时，另一接口会自动成为备用接口。

步骤 9 在**共享密钥 (Shared Secret)** 字段中，输入共享密钥。
对于 7000 或 8000 系列设备高可用性对中的群组，“共享密钥”(Shared Secret) 字段会自动填充。

步骤 10 在 **Adv.Interval (seconds)** 字段中，输入第 3 层流量的路由通告间隔。

步骤 11 点击 **OK**。

步骤 12 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ，第 254 页。

虚拟路由器配置

注意 添加虚拟路由器在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

要在第 3 层部署中使用路由接口，必须首先配置虚拟路由器并向它们分配路由接口。虚拟路由器是可路由第 3 层流量的一组路由接口。

可仅将路由接口和混合接口分配至虚拟路由器。

为最大程度地提高 TCP 安全性，您可以启用严格执行，从而阻止未完成三次握手的连接。严格执行功能也阻止：

- 三次握手尚未完成的连接的非 SYN TCP 数据包
- TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
- TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
- 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

请注意，如将第 3 层接口的配置更改为非第 3 层接口或从虚拟路由器上移除某一第 3 层接口，路由器可能会陷入无效状态。例如，如将它用于 DHCPv6 中，可能会导致上行和下行不匹配。

添加虚拟路由器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可从“设备管理”(Device Management) 页面的**虚拟路由器 (Virtual Routers)** 选项卡中添加虚拟路由器。也可在配置路由接口时添加路由器。

如要先创建虚拟路由器，然后再在受管设备上配置接口，则可在创建一个空虚拟路由器之后再向其添加接口。

注意 添加虚拟路由器在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

提示 如果设备在高可用性对的堆栈中，请从**所选设备 (Selected Device)** 下拉列表中选择要修改的堆栈。

步骤 4 点击 **Add Virtual Router**。

步骤 5 在**名称 (Name)** 字段中，输入虚拟路由器的名称。可使用字母数字字符和空格。

步骤 6 通过选中或清除 **IPv6 支持 (IPv6 Support)** 复选框，在虚拟路由器上配置 IPv6 静态路由、OSPFv3 和 RIPng。

步骤 7 如果不想启用严格 TCP 执行，请清除**严格 TCP 执行 (Strict TCP Enforcement)** 复选框。默认情况下，此选项已启用。

步骤 8 从**接口 (Interfaces)** 下的**可用 (Available)** 列表中选择一个或多个接口，然后点击**添加 (Add)**。
可用 (Available) 列表包含设备上可分配至虚拟路由器上的所有已启用的第 3 层路由和混合接口。

提示 要从虚拟路由器移除路由或混合接口，请点击删除图标 ( )。在 Interfaces 选项卡上禁用已配置的接口也会将其移除。

步骤 9 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

DHCP 中继

DHCP 提供 Internet 主机的配置参数。尚未获得 IP 地址的 DHCP 客户端不能直接与广播域之外的 DHCP 服务器通信。要使 DHCP 客户端与 DHCP 服务器进行通信，可配置 DHCP 中继实例以处理客户端与服务器处于不同广播域的情况。

可为已配置的每个虚拟路由器设置DHCP中继。默认情况下，此功能处于禁用状态。可启用DHCPv4中继或 DHCPv6 中继。

注释 不能通过在同一设备上运行的两个或多个虚拟路由器运行 DHCPv6 中继链。

设置 DHCPv4 中继

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

以下步骤介绍如何在虚拟路由器上设置 DHCPv4 中继。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 选中 **DHCPv4** 复选框。

步骤 6 在**服务器 (Servers)** 字段下，输入服务器 IP 地址。

步骤 7 点击 **Add**。
最多可添加四个 DHCP 服务器。

步骤 8 在**最大跳数 (Max Hops)** 字段中，输入范围在 1 到 255 之间的最大跳数。

步骤 9 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

设置 DHCPv6 中继

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

不能通过在同一设备上运行的两个或多个虚拟路由器运行 DHCPv6 中继链。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要为其设置 DHCP 中继的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 选中 **DHCPv6** 复选框。

步骤 6 在**接口 (Interfaces)** 字段中，选中已分配到虚拟路由器的一个或多个接口旁边的复选框。

提示 在接口配置用于 DHCPv6 中继时，不能从**接口 (Interfaces)** 选项卡禁用该接口。只有先清除 DHCPv6 Relay Interfaces 复选框，才能保存配置。

步骤 7 在所选接口旁边，点击下拉图标并选择该接口是在**上游 (Upstream)**、**下游 (Downstream)** 还是**两者 (Both)** 中继 DHCP 请求。

注释 必须至少包含一个下游接口和一个上游接口。选择两者意味着接口既是下游接口，也是上游接口。

步骤 8 在**最大跳数 (Max Hops)** 字段中，输入范围在 1 到 255 之间的最大跳数

步骤 9 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

静态路由

静态路由可供您编写有关通过路由器的流量的 IP 地址的规则。因为无需就网络的当前拓扑与其他路由器进行通信，因此它是配置虚拟路由器的路径选择的最简便方式。

静态路由表包含有关每个路由的摘要信息，如下表所述。

表 *67*: 静态路由表视图字段

字段	说明
启用	指定此路由当前是否已启用。
Name	静态路由的名称。
目标	流量将路由至的目标网络。

字段	说明
Type	指定为此路由执行的操作，具体为下列某项： • IP - 指定路由将数据包转发至相邻路由器的地址。 • 接口 - 指定路由将数据包转发至流量被路由到直连网络上主机时所经由的接口。 • 放弃 (Discard) - 指定静态路由丢弃数据包。
网关	目标 IP 地址（如已选择 IP 作为静态路由类型）或接口（如已选择接口作为静态路由类型）。
偏好	确定路由选择。如有多条路由到达同一目标，系统会选择优先级高的路由。

查看静态路由表

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要查看的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要查看静态路由的虚拟路由器旁边，点击编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于后代域，或者您没有修改配置的权限。

步骤 5 点击**静态 (Static)** 选项卡。

添加静态路由

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要向其添加静态路由的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要向其添加静态路由的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 点击 **Static** 以显示静态路由选项。

步骤 6 点击 **Add Static Route**。

步骤 7 在**路由名称 (Route Name)** 字段中，输入静态路由的名称。可使用字母数字字符和空格。

步骤 8 对于**已启用 (Enabled)**，请选中该复选框以指定路由当前已启用。

步骤 9 在**首选项 (Preference)** 字段中，输入介于 1 和 65535 之间的数值以确定路由选择。
注释 如有多条路由到达同一目标，系统会使用优先级高的路由。

步骤 10 从**类型 (Type)** 下拉列表中，选择要配置的静态路由类型。

步骤 11 在**目标 (Destination)** 字段中，输入应路由流量的目标网络的 IP 地址。

步骤 12 在 **Gateway** 字段中，有两个选项：

- 如已选择 **IP** 作为所选静态路由类型，请选择 IP 地址。
- 如已选择**接口 (Interface)** 作为所选静态路由类型，请从下拉列表中选择已启用的接口。

提示 已从**接口 (Interfaces)** 选项卡中禁用的接口将无法使用；禁用已添加的接口会同时将其从配置中删除。

步骤 13 点击 **OK**。

步骤 14 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

动态路由

动态或自适应路由使用路由协议更改路由所经过的路径，以响应网络状况的变化。自适应旨在使尽可能多的路由保持有效状态，也就是说，在响应变化时有可到达的目标。这样，只要有其他选项可用，网络就可“绕过”故障，例如节点丢失或节点间连接断开。可配置无动态路由的路由器，也可配置路由信息协议 (RIP) 或开放最短路径优先 (OSPF) 路由协议。

RIP 配置

路由信息协议 (RIP) 是一种动态路由协议，专为小型 IP 网络设计，它依靠跳数确定路由。最佳路由采用的跳数最少。RIP 允许的最大跳数为 15。此跳数限值也限制 RIP 可支持的网络规模。

为 RIP 配置添加接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

在配置RIP时，必须从要配置RIP的虚拟路由器已包含的接口中选择接口。已禁用的接口无法使用。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **RIP** 以显示 RIP 选项。

步骤 7 在 **Interfaces** 下，点击添加图标 ( )。

步骤 8 从**名称 (Name)** 下拉列表中，选择要配置 RIP 的接口。
提示 已从 Interfaces 选项卡中禁用的接口将无法使用；禁用已添加的接口会同时将其从配置中删除。

步骤 9 在**度量 (Metric)** 字段中，输入接口的度量。如有来自不同 RIP 实例的路由可用且它们都有相同的优先级，则度量值最低的路由会成为首选路由。

步骤 10 从**模式 (Mode)** 下拉列表中，选择以下选项之一：

- **Multicast** - 默认模式。在此模式下，RIP 会将整个路由表组播至位于指定地址的所有邻接路由器。
- **Broadcast** - 即使有组播模式可供使用，也会强迫 RIP 使用广播模式（例如，RIPv1）。
- **Quiet** - RIP 不会将任何定期消息发送至该接口。
- **No Listen** - RIP 将发送消息至该接口，但不监听该接口。

步骤 11 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改， 第 254 页。

配置 RIP 配置的身份验证设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

RIP 身份验证使用您在虚拟路由器上配置的某一身份验证配置文件。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要向其添加 RIP 身份验证配置文件的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **RIP** 以显示 RIP 选项。

步骤 7 在**身份验证 (Authentication)** 下，从**配置文件 (Profile)** 下拉列表中选择现有虚拟路由器身份验证配置文件，或选择**无 (None)**。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改， 第 254 页。

配置 RIP 配置的高级设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可配置与影响协议行为的各种超时值和其他功能相关的高级 RIP 设置。

注意 如将任一高级 RIP 设置更改为错误值，将导致路由器无法与其他 RIP 路由器成功通信。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **RIP** 以显示 RIP 选项。

步骤 7 在**首选项 (Preference)** 字段中，输入路由协议首选项的数值（越高越好）。相比于静态路由，系统更偏向于使用通过 RIP 获悉的路由。

步骤 8 在**周期 (Period)** 字段中，输入定期更新之间的时间间隔，单位为秒。数值越小，收敛速度越快，但网络负载也越大。

步骤 9 在**超时时间 (Timeout Time)** 字段中，输入指定路由存续时间的数值（单位为秒）。过了该时间，路由将视为不可达。

步骤 10 在**垃圾时间 (Garbage Time)** 字段中，输入指定路由存续时间的数值（单位为秒）。过了该时间后，路由将被丢弃。

步骤 11 在**无限 (Infinity)** 字段中，输入在收敛计算中表示无限距离的数值。该值越大，协议收敛将越慢。

步骤 12 从**满足 (Honor)** 下拉列表中，选择下列选项之一，以指定何时满足删除路由表的请求：

- **Always** - 始终满足请求
- **Neighbor** - 仅满足由直连网络上主机发送的请求
- **Never** - 始终不满足请求

步骤 13 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

为 RIP 配置添加导入过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可添加导入过滤条件，以指定在由 RIP 进入路由表时，哪些路由会被接受或拒绝。导入过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导入过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。

提示

要编辑 RIP 导入过滤条件，请点击编辑图标 ( )。要删除 RIP 导入过滤条件，请点击删除图标 ( )。

开始之前

- 如添加虚拟路由器，第 545 页中所述，添加虚拟路由器。
- 如设置虚拟路由器过滤器，第 564 页中所述，在该虚拟路由器上配置过滤器。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要向其添加 RIP 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **RIP** 以显示 RIP 选项。

步骤 7 在 **Import Filters** 下方，点击添加图标 ( )。

步骤 8 从**名称 (Name)** 下拉列表中，选择要作为导入过滤器添加的过滤器。

步骤 9 在**操作 (Action)** 旁边，选择**接受 (Accept)** 或**拒绝 (Reject)**。

步骤 10 点击 **OK**。

提示 要更改导入过滤条件的顺序，请根据需要点击上移 ( ) 和下移 ( ) 图标。也可在列表中上下拖动过滤条件。

步骤 11 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

为 RIP 配置添加导出过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可添加导出过滤条件，以指定在从路由表导出至 RIP 时，哪些路由会被接受或拒绝。导出过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导出过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要向其添加 RIP 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **RIP** 以显示 RIP 选项。

步骤 7 在 **Export Filters** 下方，点击添加图标 ( )。

步骤 8 从**名称 (Name)** 下拉列表中，选择要作为导出过滤器添加的过滤器。

步骤 9 在**操作 (Action)** 旁边，选择**接受 (Accept)** 或**拒绝 (Reject)**。

步骤 10 点击 **OK**。

提示 要更改导出过滤条件的顺序，请根据需要点击上移 ( ) 和下移 ( ) 图标。也可在列表中上下拖动过滤条件。

步骤 11 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

OSPF 配置

开放最短路径优先 (OSPF) 是一个自适应路由协议，它使用链路状态通告获取来自其他路由器的信息并向其他路由器通告路由，从而动态地确定路由。路由器会保留其与目标之间的链路信息，以做出路由决定。OSPF 向每个路由接口分配一个开销，并将开销最低的路由视为最佳路由。

OSPF 路由区域

OSPF 网络可以构建或划分为多个路由区域，从而简化管理并优化流量和资源的使用。区域按 32 位数字识别，可简单表示为十进制数，或通常表示为基于八字节的的点十进制符号。

按照惯例，区域 0 或 0.0.0.0 代表 OSPF 网络的核心或骨干区域。可选择标识其他区域。通常，管理员会选择某一区域内主路由器的 IP 地址作为该区域的标识。每个额外区域都必须有到骨干 OSPF 区域的直接或虚拟连接。此类连接由互联的路由器维护，这些路由器称为区域边界路由器(ABR)。ABR 为其服务的各个区域维护单独的链路状态数据库，并为网络中的所有区域维护汇总路由。

添加 *OSPF* 区域

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **OSPF** 以显示 OSPF 选项。

步骤 7 在 **Areas** 下方，点击添加图标 ( )。

步骤 8 在**区域 ID (Area Id)** 字段中，输入区域的数值。该值可以是整数或 IPv4 地址。

步骤 9 或者，选中**末节网络 (Stubnet)** 复选框，以指定该区域不接收自治系统外部的路由器通告，并且从区域内进行的路由完全基于默认路由。如果清除此复选框，则该区域将成为骨干区域，否则将成为非末节区域。

步骤 10 在**默认成本 (Default cost)** 字段中，输入与该区域的默认路由相关联的开销。

步骤 11 在 **Stubnets** 下方，点击添加图标 ( )。

步骤 12 在 **IP 地址 (IP Address)** 字段中，使用 CIDR 表示法输入 IP 地址。

步骤 13 选中**隐藏 (Hidden)** 复选框以指示末节网络已隐藏。
隐藏的末节网络不会传播到其他区域。

步骤 14 选中**摘要 (Summary)** 复选框以指定属于此末节网络子网的默认末节网络已被抑制。

步骤 15 在**末节成本 (Stub cost)** 字段中，输入用于确定与路由至此末节网络相关联的成本的值。

步骤 16 点击 **OK**。

步骤 17 如果要添加网络，请点击**网络 (Networks)** 下的添加图标 ( )。

步骤 18 在 **IP 地址 (IP Address)** 字段中，使用 CIDR 表示法输入网络的 IP 地址。

步骤 19 选中**隐藏 (Hidden)** 复选框以指示网络已隐藏。隐藏的网络不会传播到其他区域。

步骤 20 点击 **OK**。

步骤 21 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

OSPF 区域接口

可为 OSPF 配置分配给虚拟路由器的接口子集。下表介绍了可在各个接口上指定的选项。

接口

选择要为其配置 OSPF 的接口。已从 Interfaces 选项卡中禁用的接口将无法使用

Type

从以下选项中选择 OSPF 接口的类型：

- Broadcast - 在广播网络中，泛洪和呼叫消息使用组播发送，即同一数据包会发送给所有邻居。此选项指定路由器负责同步链路状态数据库并发起网络链路状态通告。此网络类型不能用在物理上非广播多路访问 (NBMP) 网络及未编号的无适当 IP 前缀的网络上。
- Point-to-Point (PtP) - 点对点网络仅将两台路由器连接在一起。此选项不执行选举，也不会发起网络链路状态通告，因此连接起来更简单更快速。此网络类型不仅适用于物理上 PtP 的接口，同时适用于用作 PtP 链路的广播网络。此网络类型不能用于物理形态为 NBMP 的网络。
- Non-Broadcast - 在 NBMP 网络上，由于缺少组播功能，数据包被单独发送给各个邻居。类似于广播网络，此选项会指定一个路由器，该路由器在链路状态通告的传播上起着重要作用。此网络类型不能用于无编号网络。
- Autodetect - 系统根据指定的接口确定正确的类型。

成本

指定接口的输出开销。

Stub

指定接口是否应监听 OSPF 流量并发送自己的流量。

优先级

输入一个数字值，以指定用于指定路由器选举的优先级值。在每个多路访问网络上，系统会指定一个路由器和备用路由器。这些路由器在泛洪过程中有一些特殊的功能。优先级越高，在此选举中的优先级也越高。不能配置优先级为 0 的路由器。

Nonbroadcast

指定是否将 hello 数据包发给任何未定义的邻居。此交换机在所有 NBMA 网络均被忽略。

身份验证

从在虚拟路由器上配置的某一身份验证配置文件中选择此接口使用的 OSPF 身份验证配置文件，或选择 **None**。有关配置身份验证配置文件的详细信息，请参阅添加虚拟路由器身份验证配置文件，第 565 页。

Hello Interval

输入发送 hello 消息的间隔，单位为秒。

Poll

键入向 NBMA 网络上某些邻居发送 hello 消息时的间隔，单位为秒。

Retrans Interval

键入重新传输未确认更新之间的间隔，单位为秒。

Retrans Delay

键入在接口上传输链路状态更新数据包时估计需要的时间，单位为秒。

Wait Time

键入路由器在开始选举和建立邻接关系之间等待的时间，单位为秒。

Dead Interval

键入当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的时间，单位为秒。如已定义该值，则它会覆盖由失效计数计算而来的值。

Dead Count

键入一个数字值，该值与 问询间隔的乘积会指定当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的时间，单位为秒。

要编辑 OSPF 区域接口，请点击编辑图标 ( )。要删除 OSPF 区域接口，请点击删除图标 ( )。在 Interfaces 选项卡上禁用已配置的接口也会将其删除。

添加 OSPF 区域接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列 s	仅限枝叶	管理员/网络管理员

可为 OSPF 配置分配给虚拟路由器的接口子集。

只能选择一个接口以在 OSPF 区域中使用。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要向其添加 OSPF 接口的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要向其添加 OSPF 接口的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **OSPF** 以显示 OSPF 选项。

步骤 7 在 **Areas** 下方，点击添加图标 ( )。

步骤 8 点击 **Interfaces**。

步骤 9 点击添加图标 ( )。

步骤 10 执行 OSPF 区域接口，第 557 页 中描述的任意操作。

步骤 11 如果要添加网络，请点击**网络 (Networks)** 下的添加图标 ( )。

步骤 12 在 **IP 地址 (IP address)** 字段中，输入在非广播网络上从此接口接收问询消息的邻居的 IP 地址。

步骤 13 选中**合格 (Eligible)** 复选框以指示邻居有资格接收消息。

步骤 14 点击 **OK**。

提示 要编辑邻居，请点击编辑图标 ( )。要删除邻居，请点击删除图标 ( )。

步骤 15 点击 **OK**。

步骤 16 点击 **Save**。

步骤 17 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加 OSPF 区域虚拟链路

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

OSPF 自治系统中的所有区域均必须与骨干区域进行物理连接。在无法实现物理连接的情况下，可以使用虚拟链路，通过非骨干区域连接到骨干区域。虚拟链路也可用于通过非骨干区域连接一个分区骨干网的两个部分。

必须至少添加两个 OSPF 区域，然后才能添加虚拟链路。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **OSPF** 以显示 OSPF 选项。

步骤 7 在 **Areas** 下方，点击添加图标 ( )。

步骤 8 点击 **Vlinks**。

步骤 9 点击添加图标 ( )。

步骤 10 在**路由器 ID (Router ID)** 字段中，输入路由器的 IP 地址。

步骤 11 从**身份验证 (Authentication)**下拉列表中，选择虚拟链路将使用的身份验证配置文件。

步骤 12 在**消息间隔 (Hello Interval)** 字段中，输入发送 hello 消息的间隔（以秒为单位）。

步骤 13 在**重新传输间隔 (Retrans Interval)** 字段中，输入重新传输未确认更新之间的间隔（以秒为单位）。

步骤 14 在**等待时间 (Wait Time)** 字段中，输入路由器在开始选择和建立邻接关系之间等待的秒数。

步骤 15 在**静止间隔 (Dead Interval)** 字段中，输入当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的秒数。如已定义该值，则它会覆盖由失效计数计算而来的值。

步骤 16 在**静止计数 (Dead Count)** 字段中，输入一个数字值，该值与消息间隔的乘积会指定当路由器未收到来自邻居的消息时，在宣告邻居崩溃之前需等待的秒数。

步骤 17 点击 **OK**。

步骤 18 点击 **Save**。

步骤 19 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

为 OSPF 配置添加导入过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可添加导入过滤条件，以指定在由 OSPF 进入路由表时，哪些路由会被接受或拒绝。导入过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导入过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击 **Virtual Routers**。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 以显示动态路由选项。

步骤 6 点击 **OSPF** 以显示 OSPF 选项。

步骤 7 在 **Import Filters** 下方，点击添加图标 ( )。

步骤 8 从**名称 (Name)** 下拉列表中，选择要作为导入过滤器添加的过滤器。

步骤 9 在**操作 (Action)** 旁边，选择**接受 (Accept)** 或**拒绝 (Reject)**。

步骤 10 点击 **OK**。

提示 要更改导入过滤条件的顺序，请根据需要点击上移( )和下移( )图标。也可在列表中上下拖动过滤条件。

步骤 11 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

为 OSPF 配置添加导出过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可添加导出过滤条件，以指定在从路由表导出至 OSPF 时，哪些路由会被接受或拒绝。导出过滤条件的应用顺序与其在表中的出现顺序相同。

在添加导出过滤条件时，请使用在虚拟路由器上配置的过滤条件之一。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要向其添加 OSPF 虚拟路由器过滤条件的虚拟路由器旁，点击编辑图标 ( )。

步骤 5 点击**动态路由 (Dynamic Routing)** 选项卡以显示动态路由选项。

步骤 6 点击 **OSPF** 以显示 OSPF 选项。

步骤 7 在 **Export Filters** 下方，点击添加图标 ( )。

步骤 8 从**名称 (Name)** 下拉列表中，选择要作为导出过滤器添加的过滤器。

步骤 9 在**操作 (Action)** 旁边，选择**接受 (Accept)** 或**拒绝 (Reject)**。

步骤 10 点击 **OK**。

提示 要更改导出过滤条件的顺序，请根据需要点击上移 ( ) 和下移 ( ) 图标。也可在列表中上下拖动过滤条件。

步骤 11 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

虚拟路由器过滤器

过滤条件提供了一种匹配路由的方式，以将路由导入至虚拟路由器的路由表并将路由导出至动态协议。可创建和管理过滤条件列表。每个过滤条件都界定了特定的准则，以查找静态界定的路由或从动态协议获得的路由。

虚拟路由器过滤器表包含已在虚拟路由器上配置的每个过滤器的摘要信息，如下表所示。

表 *68*：虚拟路由器过滤器表视图字段

字段	说明
Name	过滤条件名称。
协议	发起路由所依据的协议： • Static - 作为本地静态路由发起的路由。 • RIP - 由动态 RIP 配置发起的路由。 • OSPF - 由动态 OSPF 配置发起的路由。
From Router	此过滤条件尝试在路由器中匹配的路由器 IP 地址。必须为静态和 RIP 过滤条件输入此值。
下一跳	使用此路由的数据包将被转发到的下一跳。必须为静态和 RIP 过滤条件输入此值。
Destination Type	数据包要发送到的目标类型： • 路由器 • 设备 • 丢弃
目标网络	此过滤条件尝试在路由中匹配的网络。
OSPF Path Type	仅适用于 OSPF 协议。路径类型可是以下其中一项： • Ext-1 • Ext-2 • Inter Area • Intra Area
OSPF Router ID	仅适用于 OSPF 协议。通告该路由/网络的路由器的路由器 ID。

查看虚拟路由器过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	任意	管理员/网络管理员

虚拟路由器编辑器的**过滤器 (Filter)**选项卡显示一个表，其中列出在虚拟路由器上已配置的所有过滤器。该表包括有关每个过滤器的摘要信息。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要查看的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要查看过滤器的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**过滤器 (Filter)** 选项卡。

设置虚拟路由器过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击**过滤器 (Filter)** 选项卡。

步骤 6 点击 **Add Filter**。

步骤 7 在**名称 (Name)** 字段中，输入过滤器名称。只能使用字母数字字符。

步骤 8 在**协议 (Protocol)** 下，选择**全部 (All)** 或选择应用于过滤器的协议。

步骤 9 如已选择“全部”(All)、“静态”(Static) 或 RIP 作为**协议**，则在**源路由器 (From Router)** 下，输入此过滤器尝试在路由中匹配的路由器 IP 地址。

注释 也可输入一个 32 位的 CIDR 数据块来表示 IPv4 地址和一个 128 位的前缀长度来表示 IPv6 地址。所有其他的地址块对于此字段都无效。

步骤 10 点击 **Add**。

步骤 11 如已选择“全部”(All)、“静态”(Static) 或 RIP 作为**协议**，则在**下一跳 (Next Hop)** 下，输入此过滤器尝试在路由中匹配的网关的 IP 地址。

注释　也可输入一个 32 位的 CIDR 数据块来表示 IPv4 地址和一个 128 位的前缀长度来表示 IPv6 地址。所有其他的地址块对于此字段都无效。

步骤 12 点击 **Add**。

步骤 13 在**目标类型 (Destination Type)** 下，选择适用于该过滤器的选项。

步骤 14 在**目标网络 (Destination Network)** 下，输入此过滤器将在路由中尝试匹配的网络的 IP 地址。

步骤 15 点击 **Add**。

步骤 16 如已选择“全部”(All) 或 OSPF 作为**协议**，则在**路径类型 (Path Type)** 下，选择应用于过滤器的选项。必须至少选择一种路径类型。

步骤 17 如已选择 OSPF 作为**协议**，则在**路由器 ID (Router ID)** 下，输入用作路由/网络通告路由器的路由器 ID 的 IP 地址。

步骤 18 点击 **Add**。

步骤 19 点击 **OK**。

步骤 20 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加虚拟路由器身份验证配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

可设置用于 RIP 和 OSPF 配置的身份验证配置文件。可配置简单的密码或指定共享的加密密钥。简单密码允许所有数据包携带密码的八个字节。如果接收到的数据包缺少此密码，系统会将其忽略。加密密钥可用于进行验证，它是一个根据密码生成的16字节长的摘要，用于附加到每个数据包上。

请注意，对于OSPF，每个区域均可能有不同的身份验证方法。因此，可创建能在许多区域之间共享的身份验证配置文件。无法为 OSPFv3 添加身份验证。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要修改的虚拟路由器旁边，点击编辑图标 ( )。

步骤 5 点击 **Authentication Profile**。

步骤 6 点击 **Add Authentication Profile**。

步骤 7 在**身份验证配置文件名称 (Authentication Profile Name)** 字段中，输入身份验证配置文件的名称。

步骤 8 从**身份验证类型 (Authentication Type)** 下拉列表中，选择**简单 (simple)** 或**加密 (cryptographic)**。

步骤 9 在**密码 (Password)** 字段中，输入安全密码。

步骤 10 在**确认密码 (Confirm Password)** 字段中，再次输入该密码以进行确认。

步骤 11 点击 **OK**。

步骤 12 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

查看虚拟路由器统计信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	任意	管理员/网络管理员

可查看每个虚拟路由器的运行时统计数据。这些统计数据显示了单播数据包、丢弃的数据包和针对 IPv4 和 IPv6 地址的不同的路由表。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要查看其统计信息的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要为其查看虚拟路由器统计数据的虚拟路由器旁，点击编辑图标 ( )。

删除虚拟路由器

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

删除虚拟路由器之后，向其分配的所有路由接口均可纳入另一路由器中。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要修改的设备旁边，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击**虚拟路由器 (Virtual Routers)** 选项卡。

步骤 4 在要删除的虚拟路由器旁，点击删除图标 ( )。

步骤 5 看到提示后，请确认要删除虚拟路由器。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 31 章

汇聚接口和 LACP

以下主题介绍汇聚接口配置以及 LACP 在受管设备上的运作方式：

汇聚接口

在Firepower系统中，您可以将多个物理以太网接口组合到受管设备上的单一逻辑链路，这些设备或者在提供网络间数据包交换的第 2 层部署中配置，或者在路由接口间流量的第 3 层部署中配置。该单一汇聚逻辑链路提供更高的带宽、冗余和两个终端之间的负载平衡。

可以通过创建一个交换或路由链路汇聚组或LAG来创建汇聚链路。当创建汇聚组时，会创建称为汇聚接口的逻辑接口。对一个上层实体而言，LAG看起来像单一逻辑链路，并且数据流量通过汇聚接口进行传输。通过将多条链路的带宽添加到一起，汇聚链路可增加带宽。通过负载均衡所有可用链路之间的流量，它还提供冗余。如果一条链路发生故障，系统自动负载均衡所有剩余的链路之间的流量。

LAG 中的终端可以是两台7000 或 8000 系列设备（如上图所示）或者是连接到第三方接入交换机或路由器的7000 或 8000 系列设备。两台设备无需匹配，但是必须具有相同的物理配置并且必须支持

IEEE 802.ad链路汇聚标准。LAG的典型部署可能是在两台受管设备之间汇聚访问链路，或者在受管设备和接入交换机或路由器之间创建点对点连接。

请注意，您无法在NGIPSv设备或ASA FirePOWER模块上配置汇聚接口。

LAG 配置

汇聚接口有两种类型：

- 交换 - 第 2 层汇聚接口
- 路由 - 第 3 层汇聚接口

通过使用链路汇聚组 (LAG) 可以实现链路汇聚。通过创建汇聚交换或路由接口，然后将一组物理接口与链路相关联，可以配置 LAG。所有物理接口必须具有相同的速度和介质。

您可以动态或静态创建汇聚链路。当静态链路汇聚不起作用时，动态链路汇聚使用链路汇聚控制协议 (LACP)，该协议是 IEEE 802.ad 链路汇聚标准的组件。LACP 启用 LAG 任一端上的每台设备，以交换链路和系统信息，从而确定汇聚中将主动使用哪些链路。静态LAG配置要求您手动维护链路汇聚以及部署负载均衡和链路选择策略。

当您创建交换或路由汇聚接口时，会自动创建同一类型的链路汇聚组并进行编号。例如，当您创建第一个 LAG（交换或路由）时，此汇聚接口可以使用受管设备的**接口 (Interfaces)** 选项卡上的 **lag0** 标记进行识别。将物理和逻辑接口与此 LAG 相关联时，在分层树菜单中的主要 LAG 下面以嵌套方式显示这些接口。请注意，交换LAG只能包含交换的物理接口，路由LAG只能包含路由物理接口。

当配置 LAG 时，请考虑以下要求：

- Firepower 系统最多支持 14 个 LAG，并为每个 LAG 接口分配一个唯一 ID，范围从 0 到 13。LAG ID 不可配置。
- 您必须在链路的两侧配置 LAG，并且必须将链路每侧的接口设置为具有相同的速率。
- 必须将每个 LAG 与最少两个、最多八个物理接口相关联。一个物理接口不能属于多个 LAG。
- 不能以任何其他操作模式将 LAG 中的物理接口用作内联或被动接口，或用作已标记流量的另一个逻辑接口的一部分。
- LAG 中的物理接口可以跨越多个 NetMod，但是不能跨越多个传感器（即，所有物理接口必须位于同一台设备上）。
- LAG 不能包含堆叠的 NetMod。

汇聚交换接口

您可以将受管设备上的两个和八个物理端口结合起来创建交换 LAG 接口。必须将交换 LAG 接口分配给虚拟交换机，然后该接口才可以处理流量。受管设备可支持多达 14 个 LAG 接口。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

汇聚路由接口

您可以在7000 或 8000 系列 设备上的两个和八个物理端口之间进行组合以创建路由 LAG 接口。必须先向虚拟路由器分配路由 LAG 接口，然后其才能路由流量。受管设备可支持多达 14 个 LAG 接口。

可向路由 LAG 接口添加静态地址解析协议 (ARP) 条目。当外部主机要将流量发送到本地网络上的目标 IP 地址时，如果其需要知道该目标 IP 地址的 MAC 地址，它将发送 ARP 请求。配置静态 ARP 条目时，虚拟路由器会使用 IP 地址和关联的 MAC 地址做出响应。

为路由 LAG 接口禁用 **ICMP 启用响应 (ICMP Enable Responses)** 选项并不会在所有情景下都阻止 ICMP 响应。您仍可使用访问控制规则来处理连接，其中目标 IP 为路由接口的 IP 且协议为 ICMP；请参阅端口和 ICMP 代码条件，第 274 页。

如果启用**检查本地路由器流量 (Inspect Local Router Traffic)** 选项，则系统会在数据包到达主机之前将其阻止，从而阻止所有响应。有关检查本地路由器流量的详细信息，请参阅高级设备设置，第 380 页。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

逻辑汇聚接口

对于每个交换或路由汇聚接口，均可添加多个逻辑接口。必须将每个逻辑 LAG 接口与 VLAN 标记相关联，以处理 LAG 接口接收的带有该特定标记的流量。将逻辑接口添加到交换或路由汇聚接口的方式与将逻辑接口添加到物理交换或路由接口的方式相同。

注释 当创建 LAG 接口时，默认情况下也会创建“未加标记的”逻辑接口。该逻辑接口用 **lag*n*.0** 标签进行识别，其中 ***n*** 是 0 到 13 之间的一个整数。每个 LAG 至少需要一个这样的逻辑接口才起作用。您可以将额外的逻辑接口与任何 LAG 相关联以处理 VLAN 标记的流量。每个额外逻辑接口都需要唯一的 VLAN 标记。Firepower 系统支持范围在 1 到 4094 之间的 VLAN 标记。

您也可以在逻辑路由接口上配置思科冗余协议 (SFRP)。SFRP 允许设备充当指定 IP 地址的冗余网关。

请注意，为逻辑路由接口禁用 **ICMP Enable Responses** 选项不会在所有情景下都阻止 ICMP 响应。您可向访问控制策略添加基于网络的规则，以丢弃目标 IP 为路由接口 IP 且协议为 ICMP 的数据包。

如果您在受管设备上启用**检查本地路由器流量 (Inspect Local Router Traffic)** 选项（受管设备上的高级设置），则该设备会在数据包到达主机之前将其丢弃，从而阻止所有响应。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

Load-balancing 算法

将出口负载均衡算法分配给确定如何将流量分布给 LAG 捆绑包的成员链路的 LAG。负载均衡算法基于各种数据包字段中的值作出散列决策，例如第 2 层 MAC 地址、第 3 层 IP 地址和第 4 层端口号（TCP/UDP 流量）。您选择的负载均衡算法适用于 LAG 捆绑包的所有成员链路。

配置 LAG 时，从以下选项选择支持您的部署方案的负载均衡算法：

- 目标 IP
- 目的 MAC
- 目标端口
- 源 IP
- 源 MAC
- 源端口
- Source and Destination IP
- Source and Destination MAC
- Source and Destination Port

注释 您应该将 LAG 的两端配置为具有相同的负载均衡算法。必要时，较高层的算法将回退到较低层的算法（例如，对于 ICMP 流量，第 4 层算法回退到第 3 层算法）。

链路选择策略

链路汇聚要求每条链路的速度和介质在两个终端上均相同。由于链路属性可以动态更改，因此，链路选择策略有助于确定系统如何管理链路选择过程。最大化最高端口数的链路选择策略支持链路冗余，同时最大化总带宽的链路选择策略支持总链路速度。稳定的链路选择策略尝试将链路状态下的额外更改减到最少。

注释 您应该将 LAG 的两端配置为具有相同的链路选择策略。

从以下选项中选择支持您的部署场景的链路选择策略：

- “最高端口数”(Highest Port Count) - 为最高总活动端口数选择此选项，以提供更多冗余。
- “最高总带宽”(Highest Total Bandwidth) - 选择此选项，为汇聚链路提供最高总带宽。
- “稳定”(Stable) - 如果您最关心链路稳定性和可靠性，请选择此选项。一旦配置 LAG 后，仅当绝对必要（例如链路故障）而不是为获得更多端口数或带宽时，活动链路才会更改。
- “LACP 优先级”(LACP Priority) - 选择此选项，以使用 LACP 算法确定在 LAG 中哪些链路处于活动状态。如果未定义部署目标，或者 LAG 另一端的设备并非由 Firepower 管理中心管理，则此设置是适当的。

LACP 是自动化支持动态链路汇聚的链路选择方法的一个主要方面。启用 LACP 后，基于 LACP 优先级的链路选择策略使用以下 LACP 属性：

LACP 系统优先级

您在运行 LACP 的每台合作设备上配置该值，以确定哪个在链路汇聚中更优越。具有较低值的系统具有较高的系统优先级。在动态链路汇聚中，具有较高 LACP 系统优先级的系统首先设置自己一侧的成员链路的选定状态，然后具有较低优先级的系统相应设置其成员链路。可指定 0 到 65535 之间的任意数字。如果未指定值，则默认优先级是 32768。

LACP 链路优先级

您在属于汇聚组的每条链路上配置该值。链路优先级确定在 LAG 中的活动和备用链路。具有较低值的链路具有较高优先级。如果活动链路出现故障，则选择具有最高优先级的备用链路来替换有故障的链路。但是，如果两个或多个链路具有相同的 LACP 链路优先级，则具有最低物理端口号的链路选定为备用链路。可指定 0 到 65535 之间的任意数字。如果未指定值，则默认优先级是 32768。

链路汇聚控制协议 (LACP)

链路汇聚控制协议 (LACP) 作为 IEEE 802.3ad 的组件，是交换系统和端口信息以创建和维护 LAG 捆绑包的一种方法。当启用 LACP 时，在 LAG 任一端的每台设备都使用 LACP 确定将在汇聚中主动使用哪些链路。LACP 通过在链路之间交换 LACP 数据包（或控制消息）提供可用性和冗余。它动态了解链路的功能并通知其他链路。一旦 LACP 确定正确匹配的链路，它就促进将链路组合到 LAG 中。如果链路发生故障，流量在剩余的链路继续通过。只有在 LAG 的两端都启用 LACP 才能使链路正常运行。

LACP

当启用 LACP 时，您需要为 LAG 的每一端指定一种传输方式，从而确定如何在伙伴设备之间交换 LACP 数据包。LACP 模式有 2 种选项：

- 主动 - 选择此模式会将设备置于主动协商状态，在此状态下，设备通过发送 LACP 数据包发起与远程链路的协商。
- 被动 - 选择此模式会将设备置于被动协商状态，在此状态下，设备对其接收的 LACP 数据包做出响应，但是不发起 LACP 协商。

注释 这两种模式允许 LACP 在链路之间协商，以根据标准（例如端口速度）确定链路是否可以构成链路捆绑包。但是，您应避免被动-被动配置，其实质上是将 LAG 两端置于侦听模式。

LACP 有一个计时器，其定义在设备之间发送 LACP 数据包的频率。LACP 以下面的速度交换数据包：

- 慢 - 30 秒
- 快 - 1 秒

此选项所应用的设备预期以该频率从 LAG 另一侧的合作设备接收 LACP 数据包。

注释 在作为设备堆栈一部分的受管设备上配置LAG时，只有主设备与合作伙伴系统参与LACP通信。所有辅助设备将 LACP 消息转发给主设备。主设备将所有动态 LAG 修改中继给辅助设备。

添加汇聚交换接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

您可以将受管设备上的两个和八个物理端口结合起来创建交换 LAG 接口。必须将交换 LAG 接口分配给虚拟交换机，然后该接口才可以处理流量。受管设备可支持多达 14 个 LAG 接口。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要配置交换式 LAG 接口的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 从**添加 (Add)** 下拉菜单中选择**添加汇聚接口 (Add Aggregate Interface)**。

步骤 4 点击 **Switched** 显示交换 LAG 接口选项。

步骤 5 如果要应用安全区域，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象 ， 第 309 页。

步骤 6 指定虚拟交换机：

- 从**虚拟交换机 (Virtual Switch)** 下拉列表中选择现有虚拟交换机。
- 选择**新建 (New)** 以添加新的虚拟交换机；请参阅添加虚拟交换机 ， 第 532 页。

步骤 7 选中**已启用 (Enabled)** 复选框以允许交换式 LAG 接口处理流量。
如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8 从**模式 (Mode)** 下拉列表中，选择用于指定链路模式的选项，或者选择**自动协商 (Autonegotiation)** 以指定该接口配置为自动协商速度和双工设置。
模式设置仅适用于铜缆接口。

8000 系列设备上的接口不支持半双工选项。当链路自动协商速度时，根据相同的速度设置为 LAG 选择所有活动链路。

步骤 9 从 **MDI/MDIX** 下拉列表中，选择一个选项以指定接口是配置用于 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。
MDI/MDIX 设置仅适用于铜缆接口。

默认情况下，MDI/MDIX 设置为 Auto-MDIX，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10 在 **MTU** 字段中输入最大传输单位 (MTU)。
MTU 的设置范围可能根据 Firepower 系统设备型号和接口类型而异。有关详细信息，请参阅7000 和 8000 系列设备与 NGIPSv 的 MTU 范围 ， 第 389 页。

步骤 11 在**链路汇聚 (Link Aggregation)** 下，从**可用接口 (Available Interfaces)** 中选择一个或多个物理接口以添加到 LAG 捆绑包。

提示 要从 LAG 捆绑包中删除物理接口，请选择一个或多个物理接口，然后点击删除所选项图标 ()。要从 LAG 捆绑包移除所有物理接口，请点击移除所有项图标 ()。从 Interfaces 选项卡删除 LAG 接口也会移除接口。

步骤 12 从**负载均衡算法 (Load-Balancing Algorithm)** 下拉列表中选择一个选项。

步骤 13 从下拉列表中选择**链路选择策略 (Link Selection Policy)**。

提示 如果是在 Firepower 系统设备与第三方网络设备之间配置汇聚接口，请选择 **LACP 优先级 (LACP Priority)**。

步骤 14 如果已选择 **LACP 优先级 (LACP Priority)** 作为**链路选择策略 (Link Selection Policy)**，请为**系统优先级 (System Priority)** 分配值，然后点击**配置接口优先级 (Configure Interface Priority)** 链接来为 LAG 中的每个接口都分配一个优先级值。

步骤 15 从**隧道级别 (Tunnel Level)** 下拉菜单中选择**内部 (Inner)** 或**外部 (Outer)**。

注释 仅在配置了第 3 层负载均衡时，隧道级别才适用于 IPv4 流量。外部隧道始终用于第 2 层和 IPv6 流量。如果未显式设置**隧道级别 (Tunnel Level)**，则默认值为**外部 (Outer)**。

步骤 16 在 **LACP** 下，选中**已启用 (Enabled)** 复选框以允许交换式 LAG 接口使用链路汇聚控制协议处理流量。

如果清除此复选框，则 LAG 接口变为静态配置，并且 Firepower 系统将使用为汇聚选择的所有物理接口。

步骤 17 选择**速率 (Rate)** 单选按钮，以设置用于确定从伙伴设备接收 LACP 控制消息的间隔的频率：

- 点击**慢速 (Slow)** 以每 30 秒接收数据包。
- 点击**快速 (Fast)** 以每 1 秒接收数据包。

步骤 18 点击**模式 (Mode)** 单选按钮以建立设备的侦听模式：

- 点击**主动 (Active)** 以通过向伙伴设备发送 LACP 数据包来发起与远程链路的协商。
- 点击**被动 (Passive)** 以对接收到的 LACP 数据包做出响应。

步骤 19 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加汇聚路由接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

您可以将受管设备上的两个和八个物理端口结合起来创建路由LAG接口。必须先向虚拟路由器分配路由 LAG 接口，然后其才能路由流量。受管设备可支持多达 14 个 LAG 接口。

注意 在 7000 和 8000 系列设备上添加路由接口对在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要配置路由式 LAG 接口的设备旁边的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 从**添加 (Add)** 下拉菜单中选择**添加汇聚接口 (Add Aggregate Interface)**。

步骤 4 点击**路由 (Routed)** 以显示路由式 LAG 接口选项。

步骤 5 如果要应用安全区域，请执行以下操作之一：

- 从**安全区域 (Security Zone)** 下拉列表中选择现有安全区域。
- 选择**新建 (New)** 以添加新的安全区域；请参阅创建安全区域对象，第 309 页。

步骤 6 指定虚拟路由器：

- 从**虚拟路由器 (Virtual Router)** 下拉列表选择现有虚拟路由器。
- 选择**新建 (New)** 以添加新虚拟路由器；添加虚拟路由器，第 545 页。

步骤 7 选中**已启用 (Enabled)** 复选框以允许路由式 LAG 接口处理流量。
如果清除此复选框，接口将被禁用，用户将因安全原因无法对其进行访问。

步骤 8 从**模式 (Mode)** 下拉列表中，选择一个选项以指定链路模式，或者选择**自动协商 (Autonegotiation)** 以指定将 LAG 接口配置为自动协商速度和双工设置。
模式设置仅适用于铜缆接口。

8000 系列设备上的接口不支持半双工选项。当链路自动协商速度时，根据相同的速度设置为 LAG 选择所有活动链路。

步骤 9 从**MDI/MDIX** 下拉列表中选择一个选项，以指定将接口配置为 MDI（介质相关接口）、MDIX（介质相关接口交叉）还是自动 MDIX。
MDI/MDIX 设置仅适用于铜缆接口。

默认情况下，MDI/MDIX 设置为 Auto-MDIX，自动处理 MDI 和 MDIX 之间的交换来建立链路。

步骤 10 在 **MTU** 字段中输入最大传输单位 (MTU)。
MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 11 如果要使 LAG 接口可以对 ICMP 流量（例如 ping 和 traceroute）作出响应，请选中 **ICMP** 旁边的**启用响应 (Enable Responses)** 复选框。

步骤 12 如果要启用 LAG 接口以广播路由器通告，请选中 **IPv6 NDP** 旁边的**启用路由器通告 (Enable Router Advertisement)** 复选框。

步骤 13 点击**添加 (Add)** 以添加 IP 地址。

步骤 14 在**地址 (Address)** 字段中，使用 CIDR 表示法输入路由式 LAG 接口的 IP 地址和子网掩码。
请注意以下提示：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 15 如果您的组织使用 IPv6 地址且您要自动设置 LAG 接口的 IP 地址，请选中 **IPv6** 字段旁边的**地址自动配置 (Address Autoconfiguration)** 复选框。

步骤 16 对于**类型 (Type)**，选择“正常”(Normal) 或 SFRP。

步骤 17 如果为**类型 (Type)** 选择 SFRP，请设置选项，如SFRP，第 543 页中所述。

步骤 18 点击 **OK**。

注释 向高可用性对中的 7000 或 8000 系列设备的路由接口添加 IP 地址时，必须向高可用性对等体的路由接口添加相应的 IP 地址。

步骤 19 点击**添加 (Add)** 以添加静态 ARP 条目。

步骤 20 在 **IP 地址 (IP Address)** 字段中输入 IP 地址。

步骤 21 在 **MAC 地址 (MAC Address)** 字段中输入与该 IP 地址关联的 MAC 地址。使用标准格式（例如，01:23:45:67:89:AB）。

步骤 22 点击 **OK**。

步骤 23 在**链路汇聚 (Link Aggregation)** 下，从**可用接口 (Available Interfaces)** 中选择一个或多个物理接口以添加到 LAG 捆绑包。

提示 要从 LAG 捆绑包中删除物理接口，请选择一个或多个物理接口，然后点击删除所选项图标 ()。要从LAG捆绑包移除所有物理接口，请点击移除所有项图标 ()。从**接口 (Interfaces)** 选项卡中删除 LAG 接口也会删除这些接口。

步骤 24 从下拉列表中选择**负载均衡算法 (Load-Balancing Algorithm)**。

步骤 25 从下拉列表中选择**链路选择策略 (Link Selection Policy)**。

提示 如果是在 Firepower 系统设备与第三方网络设备之间配置汇聚接口，请选择 **LACP 优先级 (LACP Priority)**。

步骤 26 如果已选择 **LACP 优先级 (LACP Priority)** 作为**链路选择策略 (Link Selection Policy)**，请为**系统优先级 (System Priority)** 分配值，然后点击**配置接口优先级 (Configure Interface Priority)** 链接来为 LAG 中的每个接口都分配一个优先级值。

步骤 27 从**隧道级别 (Tunnel Level)** 下拉菜单中选择**内部 (Inner)** 或**外部 (Outer)**。

注释 仅在配置了第 3 层负载均衡时，隧道级别才适用于 IPv4 流量。外部隧道始终用于第 2 层和 IPv6 流量。如果未显式设置**隧道级别 (Tunnel Level)**，则默认值为**外部 (Outer)**。

步骤 28 在 **LACP** 下，选中**已启用 (Enabled)** 复选框以允许路由式 LAG 接口使用链路汇聚控制协议处理流量。

如果清除此复选框，则LAG接口变为静态配置，并且Firepower系统会将所有物理接口都用于汇聚。

步骤 29 点击**速率 (Rate)** 单选按钮，以设置确定从伙伴设备接收 LACP 控制消息的频率。

- 点击**慢速 (Slow)** 以每 30 秒接收数据包。
- 点击**快速 (Fast)** 以每 1 秒接收数据包。

步骤 30 点击**模式 (Mode)** 单选按钮以建立设备的侦听模式。

- 点击**主动 (Active)** 以通过向伙伴设备发送 LACP 数据包来发起与远程链路的协商。

- 点击**被动 (Passive)** 以对接收到的 LACP 数据包做出响应。

步骤 31 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加逻辑汇聚接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

对于每个交换或路由汇聚接口，均可添加多个逻辑接口。必须将每个逻辑 LAG 接口与 VLAN 标记相关联，以处理LAG接口接收的带有该特定标记的流量。将逻辑接口添加到交换或路由汇聚接口的方式与将逻辑接口添加到物理交换或路由接口的方式相同。

注释 当创建 LAG 接口时，默认情况下也会创建“未加标记的”逻辑接口。该逻辑接口用 **lag*n*.0** 标签进行识别，其中 ***n*** 是 0 到 13 之间的一个整数。每个 LAG 至少需要一个这样的逻辑接口才起作用。您可以将额外的逻辑接口与任何 LAG 相关联以处理 VLAN 标记的流量。每个额外逻辑接口都需要唯一的 VLAN 标记。Firepower 系统支持范围在 1 到 4094 之间的 VLAN 标记。

注意 在 7000 和 8000 系列设备上添加路由接口对在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要添加逻辑 LAG 接口所在设备旁的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 从**添加 (Add)** 下拉菜单中，选择**添加逻辑接口 (Add Logical Interface)**。

步骤 4 点击**交换 (Switched)** 显示交换接口选项，或者点击**路由 (Routed)** 显示路由接口选项。

步骤 5 从**接口 (Interface)** 下拉列表中选择可用 LAG。汇聚接口用 **lag*n*** 标签进行标识，其中 ***n*** 是 0 到 13 之间的一个整数。

步骤 6 配置其余设置以适合选择的接口类型：

- 交换 - 有关将逻辑接口添加到交换接口的详细信息，请参阅添加逻辑交换接口，第 529 页。
- 路由 - 有关将逻辑接口添加到路由接口的详细信息，请参阅添加逻辑路由接口，第 541 页。

查看汇聚接口统计信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

您可以查看每个汇聚接口的协议和流量统计数据。统计数据显示 LACP 协议信息，例如 LACP 密钥和合作伙伴信息、接收的数据包、数据包发射器和丢弃的数据包。每个成员接口均可进一步优化统计数据，以按每端口显示流量和链路信息。

汇聚接口信息还通过预定义的控制面板构件提供给控制面板。Current Interface Status 构件显示设备上所有接口的状态，已启用或未使用。Interface Traffic 构件显示设备接口上在控制面板时间范围内的接收流量速率 (Rx) 和传输流量速率 (Tx)。请参阅预定义控制面板构件，第 182 页。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要查看逻辑汇聚接口统计数据所在设备旁的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击要查看接口统计数据所在接口旁的视图图标 ( )。

删除汇聚接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

汇聚接口用 **lag*n*** 标签进行标识，其中 ***n*** 可以是 0 到 13 之间的一个整数。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击要删除汇聚接口所在设备旁的编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 点击要删除的汇聚接口旁的删除图标 ( )。

步骤 4 当出现提示时，请确认要删除汇聚接口。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 32 章

混合接口

以下主题介绍如何配置本地混合接口：

混合接口基础知识

您可以在允许 Firepower 系统桥接虚拟路由器与虚拟交换机之间流量的受管设备上配置逻辑混合接口。如果虚拟交换机接口收到的 IP 流量发送至关联混合逻辑接口的 MAC 地址，则系统将其作为第 3 层流量处理，并根据目标 IP 地址对该流量进行路由或做出响应。如果系统收到任何其他流量，则将其作为第 2 层流量处理，并对其进行适当交换。您不能在 NGIPSv 设备上配置逻辑混合接口。

请注意，未同时与虚拟交换机和虚拟路由器关联的混合接口不可用于路由，也不会生成流量或对流量做出响应。

逻辑混合接口

如要桥接第 2 层和第 3 层之间的流量，您必须将逻辑混合接口与虚拟路由器和虚拟交换机相关联。您只能将单个混合接口与虚拟交换机关联。但是，您能将多个混合接口与虚拟路由器关联。

您也可以在逻辑混合接口上配置思科冗余协议 (SFRP)。SFRP 允许设备充当指定 IP 地址的冗余网关。

请注意，禁用混合接口的 **ICMP Enable Responses** 选项并不会阻止所有情形下的 ICMP 响应。您可向访问控制策略添加基于网络的规则，以丢弃目标 IP 为混合接口 IP 且协议为 ICMP 的数据包。

如您在受管设备上启用 **Inspect Local Router Traffic** 选项，则该设备在数据包到达主机之前将其丢弃，从而阻止所有响应。

MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意 当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

添加逻辑混合接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

注意 在 7000 和 8000 系列设备上添加路由接口对在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要向其添加混合接口的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 从**添加 (Add)** 下拉菜单中，选择**添加逻辑接口 (Add Logical Interface)**。

步骤 4 点击 **Hybrid** 以显示混合接口选项。

步骤 5 在**名称 (Name)** 字段中，输入接口名称。

步骤 6 从**虚拟路由器 (Virtual Router)** 下拉列表中，选择一个现有虚拟路由器、选择**无 (None)**，或选择**新建 (New)** 以添加新虚拟路由器。

注释 如果添加新虚拟路由器，则在完成混合接口设置之后，必须在“设备管理”(Device Management) 页面上配置该虚拟路由器。请参阅添加虚拟路由器，第 545 页。

步骤 7 从**虚拟交换机 (Virtual Switch)** 下拉列表中，选择一个现有虚拟交换机、选择**无 (None)**，或选择**新建 (New)** 以添加新虚拟交换机。

注释 如果添加新虚拟交换机，则在完成混合接口设置之后，必须在“设备管理”(Device Management) 页面上配置该虚拟路由器。请参阅添加虚拟交换机，第 532 页。

步骤 8 选中**已启用 (Enabled)** 复选框以允许混合接口处理流量。

注释 如清除此复选框，则将禁用并强制性断开该接口。

步骤 9 在 **MTU** 字段中，输入用于指定所允许的最大数据包的最大传输单位 (MTU)。
MTU 值的范围可以根据受管设备的型号和接口类型而异。

注意　当部署配置更改时，为非管理接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有非管理接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于受管设备的型号和接口类型。

步骤 10 在 **ICMP** 旁边，选中**启用响应 (Enable Responses)** 复选框，以允许接口对 ICMP 流量做出响应，例如 ping 和 traceroute。

步骤 11 在 **IPv6 NDP** 旁边，选中**启用路由器通告 (Enable Router Advertisement)** 复选框，以使接口广播路由器通告。只有添加了 IPv6 地址，才能启用此选项。

步骤 12 要添加 IP 地址，请点击 **Add**。

步骤 13 在**地址 (Address)** 字段中，输入 IP 地址和子网掩码。请注意以下提示：

- 不能添加网络和广播地址，或静态 MAC 地址 00:00:00:00:00:00 和 FF:FF:FF:FF:FF:FF。
- 无论子网掩码如何，均不能将多个相同的 IP 地址添加至虚拟路由器的接口。

步骤 14 或者，如果您有 IPv6 地址，请在 **IPv6** 字段旁边，选中**地址自动配置 (Address Autoconfiguration)** 复选框，以自动设置接口的 IP 地址。

步骤 15 对于**类型 (Type)**，选择“正常”(Normal) 或 SFRP。

步骤 16 如果为**类型 (Type)** 选择 SFRP，请设置选项，如SFRP，第 543 页中所述。

步骤 17 点击 **OK**。

步骤 18 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

删除逻辑混合接口

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	7000 和 8000 系列	仅限枝叶	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 在要从其中删除混合接口的设备旁，点击编辑图标 ( )。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 3 在要删除的逻辑混合接口旁，点击删除图标 ( )。

步骤 4 出现提示时，请确认要删除接口。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 33 章

网关 VPN

以下主题介绍如何管理 VPN 部署：

网关 VPN 基础知识

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在终端之间建立安全隧道。可以配置 Firepower 系统以在 Firepower 受管设备的虚拟路由器之间构建安全的 VPN 隧道。系统使用互联网协议安全 (IPSec) 协议套件构建隧道。

建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。连接包括两个网关的 IP 地址和主机名、网关后台的子网以及供两个网关互相进行身份验证的共享密钥。

各 VPN 终端利用 Internet 密钥交换 (IKE) 版本 1 或版本 2 协议相互进行身份验证，为隧道创建安全关联。系统使用 IPSec 身份验证标头 (AH) 协议或 IPSec 封装式安全负载 (ESP) 协议对进入隧道的数据进行身份验证。除具有与 AH 相同的功能之外，ESP 协议还可以对数据加密。

如果部署中有访问控制策略，系统在通过访问控制前不会发送 VPN 流量。此外，在隧道关闭时，系统不向公共资源发送隧道流量。

要为 Firepower 配置和部署 VPN，必须在每个目标受管设备上启用 VPN 许可证。此外，VPN 功能仅适用于 7000 和 8000 系列设备。

IPSec

IPsec 协议套件定义如何在 ESP 或 AH 安全协议中散列、加密和封装跨 VPN 隧道的 IP 数据包。Firepower 系统使用通过互联网密钥交换 (IKE) 协议在两个网关之间建立的安全关联 (SA) 的散列算法和加密密钥。

安全关联 (SA) 在两台设备之间建立共享安全属性并使 VPN 终端支持安全通信。SA 可使两个 VPN 终端处理相关参数，确保在两终端之间建立 VPN 隧道。

系统在协商 IPSec 连接以在终端和经过身份验证的密钥交换之间建立 VPN 初始阶段期间使用互联网安全关联与密钥管理协议 (ISAKMP)。IKE 协议驻留在 ISAKMP 之内。

AH 安全协议为数据包标头和数据提供保护，但不能对其进行加密。ESP 为数据包提供加密和保护，但不能保护最外层的 IP 标头。在许多情况下，并不需要此保护，由于 ESP 具有加密功能，大多数 VPN 部署更频繁地使用 ESP，较少使用 AH。由于 VPN 仅在隧道模式运行，因此，在 ESP 协议中，系统从第 3 层向上对整个数据包进行加密和身份验证。在隧道模式下，ESP 可对数据进行加密，并具有 AH 的加密功能。

IKE

Firepower 系统使用 IKE 协议对两个网关共同进行身份验证，并为隧道协商 SA。此流程包含两个阶段。

IKE 阶段 1 通过使用 Diffie - Hellman 密钥交换建立一个安全的经验证通信信道，生成一个预共享密钥对 IKE 通信进行进一步加密。此协商促成一个双向的 ISAKMP 安全关联。系统允许您使用预共享密钥执行身份验证。阶段 1 在主模式中运行，力图在协商期间保护所有数据，同时保护对等体的身份。

在 IKE 阶段 2 中，IKE 对等体使用在阶段 1 中建立的安全隧道代表 IPSec 协商安全关联。此协商促成至少两个单向的安全关联，一个为入站关联，一个为出站关联。

VPN 部署

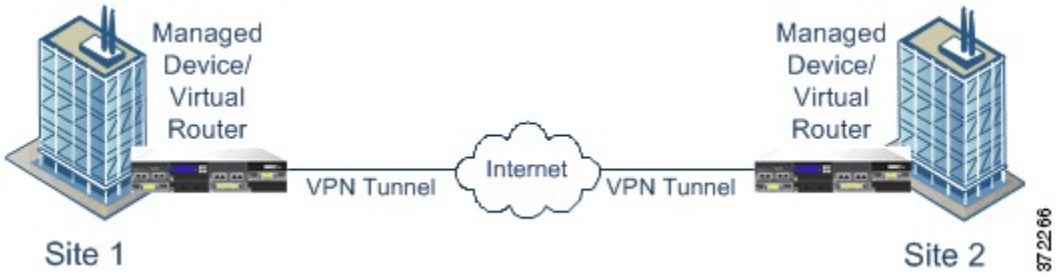
VPN 部署指定纳入 VPN 的终端和网络及其如何互相连接。在 Firepower 管理中心上配置 VPN 部署后，可将其部署到受管设备或由另一 Firepower 管理中心管理的设备。

系统支持三类 VPN 部署：点对点、星型和网格。

点对点 VPN 部署

在点对点VPN部署中，两个终端彼此直接通信。将两个终端配置为对等设备，任一台设备均可启动安全连接。在此配置中，每台设备必须为支持 VPN 的受管设备。

以下图表显示了一个典型点对点 VPN 部署。



星型 VPN 部署

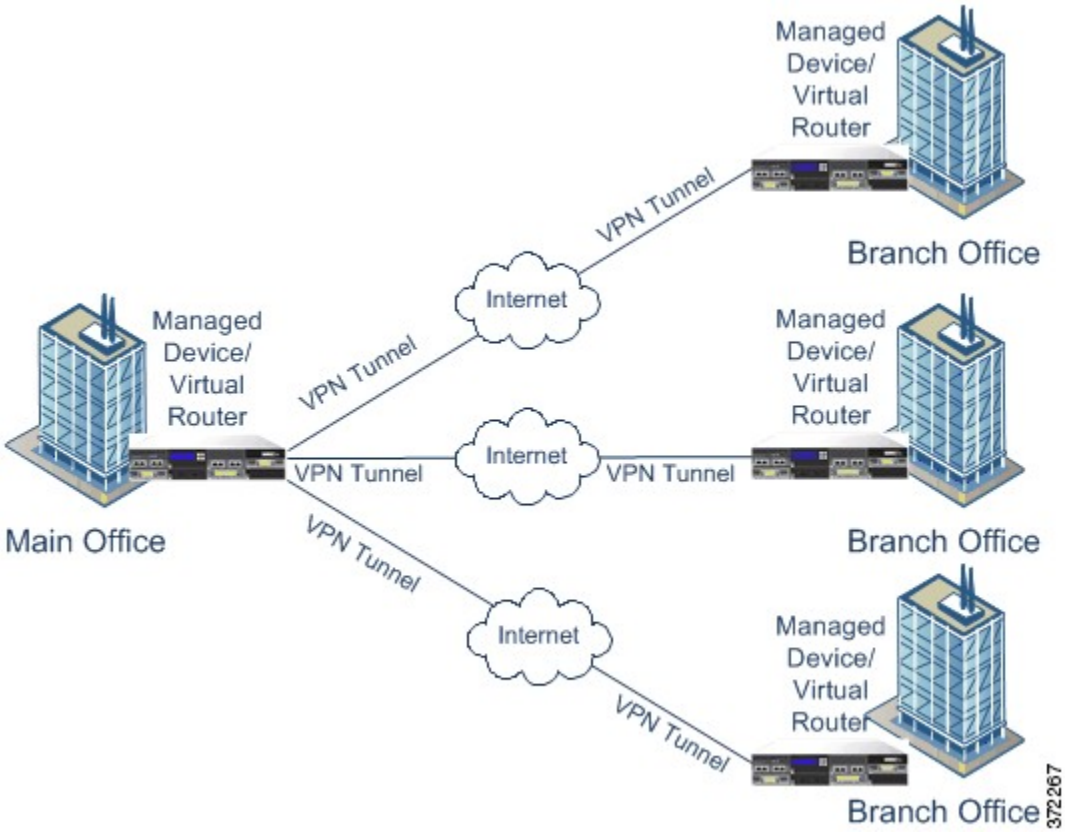
在星型VPN部署中，中央终端（集线器节点）建立与多个远程终端（叶节点）的安全连接。集线器节点与每个叶节点之间的每条连接均为独立VPN隧道。任何叶节点后台的主机均可通过集线器节点相互通信。

星型部署通常代表通过互联网或其他第三方网络建立安全连接，将公司总部和分公司相连的 VPN。星型 VPN 部署为所有员工提供对公司网络的受控访问权。

在典型星型部署中，集线器节点位于总部。叶节点位于分支机构并启动大部分流量。每个节点均必须属于支持 VPN 的受管设备。

星型部署仅支持 IKE 版本 2。

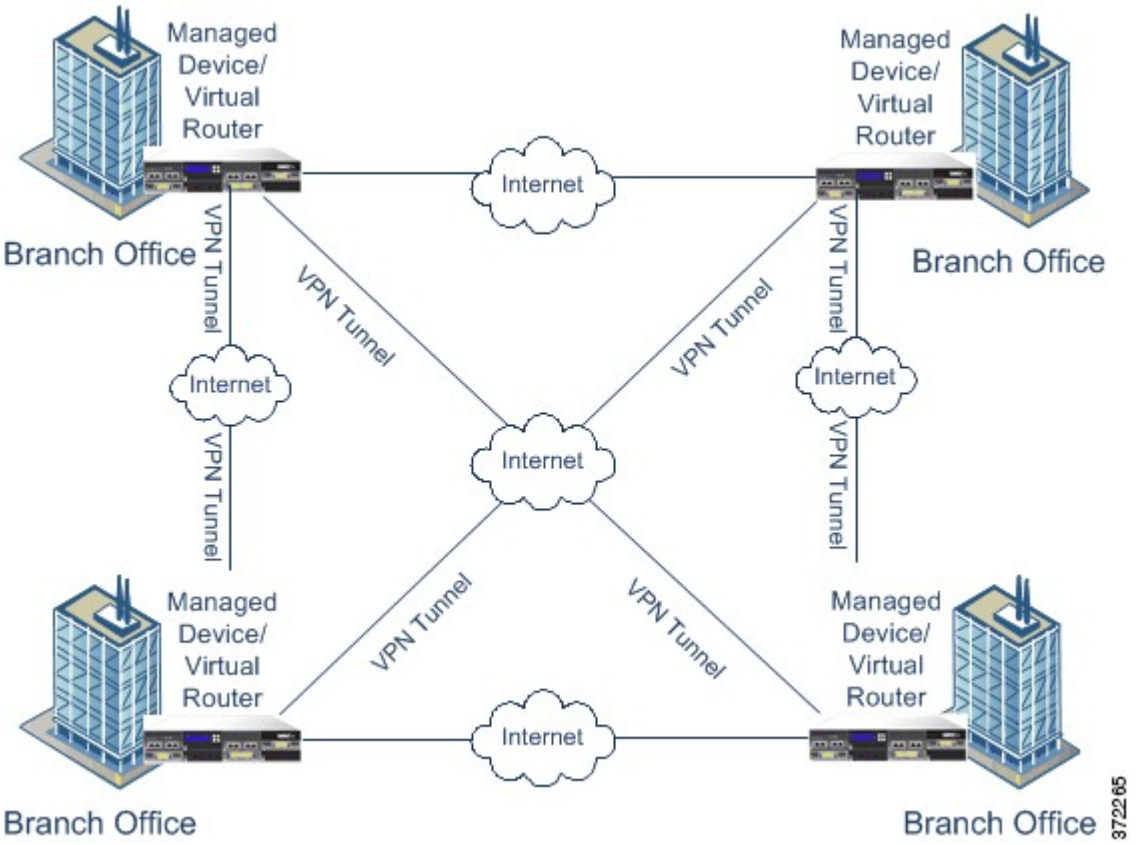
以下图表显示了一个典型的星型 VPN 部署。



网格 VPN 部署

在网格 VPN 部署中，所有终端均可通过单个 VPN 隧道与每个其他终端进行通信。网格部署可保证冗余，以便当一个终端发生故障时，其余终端仍可以互相通网格部署提供冗余节点信。此类部署通常代表连接一组分散式分公司地点的 VPN。在此配置中，所部署的支持 VPN 的受管设备数量取决于所需的冗余级别。每个终端均必须属于支持 VPN 的受管设备。

以下图表显示了典型的网格 VPN 部署。



VPN 部署管理

在 VPN 页面（**设备 (Devices)** > **VPN**）上，可以按名称查看所有当前 VPN 部署以及部署中包含的终端。通过此页面上的选项，可以查看VPN部署的状态，创建新部署，部署到受管设备以及编辑或删除部署。

请注意，将设备注册到 Firepower 管理中心时，已部署的 VPN 部署将在注册期间与 Firepower 管理中心同步。

VPN 部署选项

新建VPN部署时，必须至少为其提供一个唯一名称、指定部署类型并指定预共享密钥。有三类部署可供选择，每类部署均包含一组 VPN 隧道：

- 点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。
- 星型部署建立一组 VPN 隧道连接一个集线器终端与一组叶终端。
- 网格部署在一组终端当中建立一组 VPN 隧道。

在 VPN 部署中，只有思科受管设备可用作终端。不支持第三方终端。

必须为 VPN 身份验证定义一个预共享密钥。可指定一个默认密钥，用于在部署中生成的所有 VPN 连接。对于点对点部署，可为每对终端指定一个预共享密钥。

在多域部署中，可以跨域配置VPN部署；也就是说，可以将终端分配到属于不同域的设备。在此情况下，可以在相关的后代域中查看祖先部署但无法对其进行修改。向下展开以了解部署详细信息时，系统仅显示属于当前域的设备的信息。

点对点 VPN 部署选项

配置点对点 VPN 部署时，先定义一组终端对，然后在每个终端对的两个节点之间创建 VPN。

以下列表描述了在部署中可以指定的选项。

Name

为部署指定唯一名称。

Type

点击 **PTP** 表明正在配置点对点部署。

Pre-shared Key

定义一个用于身份验证的唯一预共享密钥。系统会将该密钥用于部署中的所有 VPN，除非为每个终端对指定一个预共享密钥。

设备

可以选择受管设备（包括设备堆栈或设备高可用性对）作为部署的终端。对于思科管理的设备（不受您使用的Firepower管理中心管理），请选择**其他 (Other)**，然后指定该终端的IP地址。

虚拟路由器

如果选择受管设备作为终端，请选择当前应用于所选设备的虚拟路由器。不能为多个终端选择同一虚拟路由器。

接口

如果选择受管设备作为终端，请选择分配到指定虚拟路由器的路由接口。

IP 地址

- 如果选择受管设备作为终端，请选择分配到指定路由接口的 IP 地址。
- 如果此受管设备是设备高可用性对，则只能从 SFRP IP 地址列表中进行选择。
- 如果选择不受 Firepower 管理中心管理的受管设备，请指定终端的 IP 地址。

Protected Networks

在部署中指定已加密的网络。为每个网络输入带 CIDR 块的子网。IKE 版本 1 仅支持一个受保护的网络。

请注意，VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络列表包含一个或多个 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（即 IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不得与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

Internal IP

如果终端驻留在带网络地址转换的防火墙后面，请选中此复选框。

Public IP

如果选中了**内部 IP (Internal IP)** 复选框，请指定防火墙的公共 IP 地址。如果终端为响应方，必须指定此值。

Public IKE Port

如果选中了**内部 IP (Internal IP)** 复选框，请为防火墙上向内部终端进行端口转发的 UDP 端口指定一个介于 1 与 65535 之间的数值。如果终端为响应方，且防火墙上正在转发的端口不是 500 或 4500，必须指定此值。

Use Deployment Key

选中此复选框，可使用为部署定义的预共享密钥。清除此复选框，可为此终端对指定用于VPN身份验证的预共享密钥。

Pre-shared Key

如已清除 **Use Deployment Key** 复选框，请在此字段中指定一个预共享密钥。

星型 VPN 部署选项

配置星型VPN部署时，需定义一个集线器节点终端和一组叶节点终端。必须定义集线器节点终端和至少一个叶节点终端才能配置部署。

以下列表描述了在部署中可以指定的选项。

Name

为部署指定唯一名称。

Type

单击 **Star** 指定正在配置星型部署。

Pre-shared Key

定义一个用于身份验证的唯一预共享密钥。

设备

可以选择受管设备（包括设备堆栈或设备高可用性对）作为部署的终端。对于思科管理的设备（不受您使用的Firepower管理中心管理），请选择**其他 (Other)**，然后指定该终端的IP地址。

虚拟路由器

如果选择受管设备作为终端，请选择当前应用于所选设备的虚拟路由器。不能为多个终端选择同一虚拟路由器。

接口

如果选择受管设备作为终端，请选择分配到所选虚拟路由器的路由接口。

IP 地址

- 如果选择受管设备作为终端，请选择分配到指定路由接口的 IP 地址。
- 如果此受管设备是设备高可用性对，则只能从 SFRP IP 地址列表中进行选择。
- 如果选择不受 Firepower 管理中心管理的受管设备，请指定终端的 IP 地址。

Protected Networks

在部署中指定已加密的网络。为每个网络输入带 CIDR 块的子网。

请注意，VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络列表包含一个或多个 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（即 IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不得与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

Internal IP

如果终端驻留在带网络地址转换的防火墙后面，请选中此复选框。

Public IP

如果选中了**内部 IP (Internal IP)** 复选框，请指定防火墙的公共 IP 地址。如果终端为响应方，必须指定此值。

Public IKE Port

如果选中了**内部 IP (Internal IP)** 复选框，请为防火墙上向内部终端进行端口转发的 UDP 端口指定一个介于 1 与 65535 之间的数值。如果终端为响应方，且防火墙上正在转发的端口不是 500 或 4500，必须指定此值。

网格 VPN 部署选项

配置网格 VPN 部署时，需定义一组 VPN 以连接一组特定终端的任何两点。

以下列表描述了在部署中可以指定的选项。

Name

为部署指定唯一名称。

Type

点击 **Mesh** 指定正在配置网格部署。

Pre-shared Key

定义一个用于身份验证的唯一预共享密钥。

设备

可以选择受管设备（包括设备堆栈或设备高可用性对）作为部署的终端。对于思科管理的设备（不受您使用的Firepower管理中心管理），请选择**其他 (Other)**，然后指定该终端的IP地址。

虚拟路由器

如果选择受管设备作为终端，请选择当前应用于指定设备的虚拟路由器。不能为多个终端选择同一虚拟路由器。

接口

如果选择受管设备作为终端，请选择分配到指定虚拟路由器的路由接口。

IP 地址

- 如果选择受管设备作为终端，请选择分配到所选路由接口的 IP 地址。
- 如果此受管设备是设备高可用性对，则只能从 SFRP IP 地址列表中进行选择。
- 如果选择不受 Firepower 管理中心管理的受管设备，请指定终端的 IP 地址。

Protected Networks

在部署中指定已加密的网络。为每个网络输入带 CIDR 块的子网。IKE 版本 1 仅支持一个受保护的网络。

请注意，VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络列表包含一个或多个 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（即 IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不得与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

Internal IP

如果终端驻留在带网络地址转换的防火墙后面，请选中此复选框。

Public IP

如果选中了**内部 IP (Internal IP)** 复选框，请指定防火墙的公共 IP 地址。如果终端为响应方，必须指定此值。

Public IKE Port

如果选中了**内部 IP (Internal IP)** 复选框，请为防火墙上向内部终端进行端口转发的 UDP 端口指定一个介于 1 与 65535 之间的数值。如果终端为响应方，且防火墙上正在转发的端口不是 500 或 4500，必须指定此值。

高级 VPN 部署选项

VPN 部署包含可在部署的 VPN 中共享的一些常见设置。每个 VPN 均可使用默认设置，也可覆盖这些默认设置。高级设置通常几乎不需要修改，并非在每个部署中都出现。

以下列表描述了在部署中可指定的高级选项。

Other Algorithm Allowed

选中此复选框可对算法列表中未列出、但远程对等体拟用的算法启用自动协商。

算法

在部署中指定第一阶段和第二阶段算法方案以保护数据。为两个阶段均选择**密码 (Cipher)**、**散列 (Hash)**, 和 Diffie-Hellman (**DH**) 组身份验证消息。

IKE Life Time

指定数值并为最大 IKE SA 重新协商间隔选择时间单位。可以指定最短 15 分钟和最长 30 天。

IKE v2

选中此复选框可指定系统使用 IKE 版本 2。此版本支持星型部署和多个受保护网络。

Life Time

指定一个数值并为最大 SA 重新协商间隔选择一个时间单位。可以指定最短 5 分钟和最长 24 小时。

Life Packets

指定在 IPsec SA 到期前可通过其传输的数据包的数量。可以使用 0 到 18446744073709551615 之间的任意整数。

Life Bytes

指定在 IPsec SA 到期前可通过其传输的字节数。可以使用 0 到 18446744073709551615 之间的任意整数。

AH

选中此复选框可指定系统使用身份验证报头安全协议以保护数据。清除此复选框，可使用加密服务有效载荷 (ESP) 协议。

管理 VPN 部署

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

注意 在 7000 或 8000 系列设备上添加或删除 VPN 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 管理您的 VPN 部署：

- 添加 - 要创建新 VPN 部署，请点击**添加 (Add)**，然后根据部署类型按如下所述继续操作：

  配置网格 VPN 部署， 第 598 页

  配置点对点 VPN 部署， 第 596 页

  配置星型 VPN 部署， 第 597 页

- 编辑 - 要修改现有 VPN 部署中的设置，请点击编辑图标 ( )；请参阅编辑 VPN 部署， 第 600 页。
- 删除 - 要删除 VPN 部署，请点击删除图标 ( )。
- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改， 第 254 页。
- 查看 VPN 状态 - 要查看现有 VPN 部署的状态，请点击状态图标；请参阅查看 VPN 状态， 第 601 页。

配置点对点 VPN 部署

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击 **Add**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 验证是否已选定 **PTP** 作为**类型 (Type)**。

步骤 5 在**预共享密钥 (Pre-shared Key)** 中输入唯一的预共享密钥。

步骤 6 点击 **Node Pairs** 旁边的添加图标 ( )。

步骤 7 配置 VPN 部署选项，如点对点 VPN 部署选项，第 591 页中所述。

步骤 8 点击**节点 A (Node A)** 下的**受保护网络 (Protected Networks)** 旁边的添加图标 ( )。

步骤 9 为受保护网络输入 CIDR 块。

步骤 10 点击 **OK**。

步骤 11 对于**节点 B (Node B)**，重复步骤 8 至步骤 10。

步骤 12 点击**保存 (Save)**。
系统将终端对添加到您的部署中。

步骤 13 点击**保存 (Save)** 完成配置您的部署。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置星型 VPN 部署

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击 **Add**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 点击 **Star** 以指定 **Type**。

步骤 5 在**预共享密钥 (Pre-shared Key)** 中输入唯一的预共享密钥。

步骤 6 点击 **Hub Node** 旁边的添加图标 ( )。

步骤 7 配置 VPN 部署选项，如星型 VPN 部署选项，第 592 页中所述。

步骤 8 点击 **Protected Networks** 旁边的添加图标 ( )。

步骤 9 输入受保护网络的 IP 地址。

步骤 10 点击 **OK**。

步骤 11 点击 **Save**。集线器节点添加到您的部署中。

步骤 12 点击 **Leaf Nodes** 旁边的添加图标 ( )。

步骤 13 重复第 7 步至第 10 步完成叶节点，该节点具有与集线器节点相同的选项。

步骤 14 点击**保存 (Save)**。
叶节点添加到您的部署中。

步骤 15 点击**保存 (Save)** 完成配置您的部署。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置网格 VPN 部署

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击 **Add**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 点击 **Mesh** 以指定 **Type**。

步骤 5 在**预共享密钥 (Pre-shared Key)** 中输入唯一的预共享密钥。

步骤 6 点击**节点 (Nodes)** 旁边的添加图标 ( )。

步骤 7 配置 VPN 部署选项，如网格 VPN 部署选项，第 593 页中所述。

步骤 8 点击 **Protected Networks** 旁边的添加图标 ( )。

步骤 9 为受保护网络输入 CIDR 块。

步骤 10 点击 **OK**。
受保护网络添加成功。

步骤 11 点击**保存 (Save)**。
系统将终端添加到您的部署中。

步骤 12 重复步骤 6 至步骤 11 以添加更多终端。

步骤 13 点击**保存 (Save)** 完成部署。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置高级 VPN 部署设置

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的VPN部署，您可以对其进行编辑。如果某个终端设备属于您的域，系统还会显示在祖先域中创建的VPN部署。您无法编辑在祖先域中创建的VPN配置。要查看和编辑在较低域中创建的 VPN 部署，请切换至该域。

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Advanced** 选项卡。

步骤 4 配置高级设置，如配置高级 VPN 部署设置，第 599 页中所述。

步骤 5 点击 **Algorithms** 旁边的添加图标 ( )。

步骤 6 为两个阶段均选择**密码 (Cipher)**、**散列 (Hash)**, 和 Diffie-Hellman (**DH**) 组身份验证消息。

步骤 7 点击 **OK**。

步骤 8 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

编辑 VPN 部署

注意 两个用户不应同时编辑同一部署；然而，请注意，网络界面不会阻止同时编辑。

在多域部署中，系统会显示在当前域中创建的VPN部署，您可以对其进行编辑。如果某个终端设备属于您的域，系统还会显示在祖先域中创建的VPN部署。您无法编辑在祖先域中创建的VPN配置。要查看和编辑在较低域中创建的 VPN 部署，请切换至该域。

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 修改所需设置：

- 高级设置；请参阅配置高级 VPN 部署设置，第 599 页。
- 网格部署设置；请参阅配置网格 VPN 部署，第 598 页。
- 点对点部署设置；请参阅配置点对点 VPN 部署，第 596 页。
- 星型部署设置；请参阅配置星型 VPN 部署，第 597 页。

提示 在最初保存部署之后，不能编辑部署类型。要更改部署类型，必须删除部署并新建一个部署。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

VPN 部署状态

配置 VPN 部署之后，可查看已配置的 VPN 隧道的状态。VPN 页面显示每个 VPN 部署（部署之后）的状态图标：

- () 图标表示所有 VPN 终端均已启用。
- () 图标表示所有 VPN 终端均已关闭。
- () 图标表示部分终端已启用，部分终端已关闭。

可点击状态图标，以查看部署状态及部署中终端的基本信息，如终端名称和IP地址。VPN状态每分钟更新一次，或在发生状态变化时更新，例如终端关闭或启用。

查看 VPN 状态

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的VPN部署。如果某个终端设备属于您的域，它还会显示在祖先域中创建的 VPN 部署。要查看在较低域中创建的 VPN 部署，请切换至该域。

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击要查看其状态的部署旁边的 VPN 状态图标。

步骤 3 点击 **OK**。

VPN 统计信息和日志

配置 VPN 部署之后，可查看有关横越已配置 VPN 隧道的统计数据。此外，还可查看每个终端的最新 VPN 系统和 IKE 日志。

系统将显示以下统计信息：

终端

到路由接口的设备路径和指定为 VPN 终端的 IP 地址。

状态

VPN 连接处于启用还是禁用状态。

协议

用于加密的协议，ESP 或 AH。

已接收数据包

在 IPsec SA 协商期间，VPN 隧道接收的每接口数据包数量。

已转发数据包

在 IPsec SA 协商期间，VPN 隧道传输的每接口数据包数量。

已接收字节

在 IPsec SA 协商期间，VPN 隧道收到的每接口字节数。

已转发字节

在 IPsec SA 协商期间，VPN 隧道传输的每个接口字节数。

创建时间

VPN 连接的创建日期和时间。

上次使用时间

用户上次启动 VPN 连接的时间。

NAT 遍历

如果显示“是”(Yes)，则至少有一个 VPN 终端会驻留在支持网络地址转换的设备之后。

IKE 状态

IKE SA 的状态：正在连接，已建立，正在删除或正在销毁。

IKE 事件

IKE SA 事件：重新身份验证或密钥更新。

IKE 事件时间

下一个事件应发生的时间（秒）。

IKE 算法

VPN 部署在使用的 IKE 算法。

IPSec 状态

IPSec SA 的状态：正在安装、已安装、正在更新、正在进行密钥更新、正在删除和正在毁坏。

IPSec 事件

IPSec SA 事件进行密钥更新时的通知。

IPSec 事件时间

距离下一个事件发生的秒数。

IPSec 算法

VPN 部署正在使用的 IPSec 算法。

查看 VPN 统计信息和日志

智能许可证	经典许可证	支持的设备	支持的域	Access
不适用	VPN	7000 和 8000 系列	任意	管理员/网络管理员

在多域部署中，系统会显示在当前域中创建的VPN部署。如果某个终端设备属于您的域，它还会显示在祖先域中创建的 VPN 部署。要查看在较低域中创建的 VPN 部署，请切换至该域。

过程

步骤 1 选择**设备 (Devices)** > **VPN**。

步骤 2 点击要为其查看统计信息的部署旁边的 VPN 状态图标。

步骤 3 点击视图统计信息图标 ( )。

步骤 4 或者，点击 **Refresh** 更新 VPN 统计信息。

步骤 5 或者，点击 **View Recent Log** 查看每个终端的最新数据日志。要查看高可用性对中的 7000 或 8000 系列设备和堆叠设备的日志，可点击主用设备/主设备或备用/辅助设备的链路。

第 XI 部分

访问控制

第 34 章

访问控制策略使用入门

以下主题介绍如何开始使用访问控制策略：

访问控制简介

访问控制是一项基于策略的分层功能，可用于指定、检查和记录（非快速路径）网络流量。此功能在多域部署中尤其有用，您可以嵌套访问控制策略。在这种情况下，每个策略都会继承祖先（或基本）策略的规则和设置。您可以执行此继承，或允许较低级别的策略覆盖其祖先。每个受管设备都可作为一个访问控制策略的目标。

策略的目标设备收集有关网络流量的数据可用于根据以下内容过滤和控制该流量：

- 简单、易于确定的传输层和网络层特征：源和目标、端口和协议等
- 流量的最新的上下文信息，包括诸如信誉、风险、业务相关性、使用的应用或访问的 URL 等特征
- 领域、用户、用户组或 ISE 属性
- 加密流量的特性；也可以解密此流量以进一步分析
- 未加密或已解密的流量包含禁止的文件、检测到的恶意软件还是入侵尝试

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。例如，基于信誉的黑名单使用简单的源和目标数据，因此，可以在过程的早期阻止禁止的流量。相反，检测和阻止入侵和漏洞则是最后一道防线。

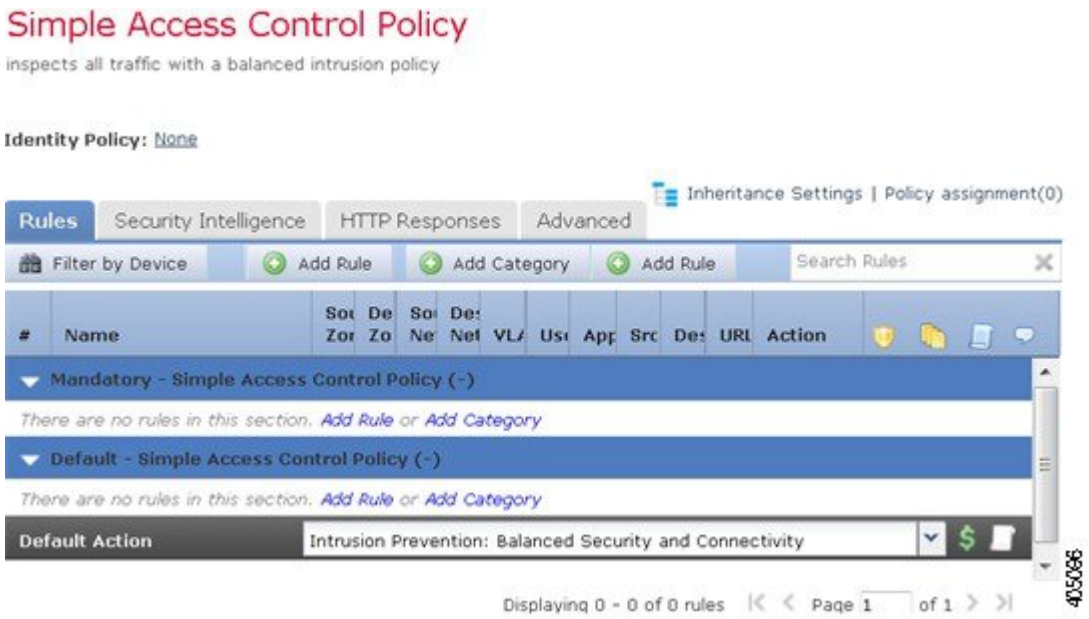
虽然无需为部署提供许可也可配置系统，但许多功能要求您在部署之前，先启用适当的许可证。此外，某些功能仅在特定设备型号上可用。警告图标和确认对话框会指出不支持的功能。

注释 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向受管设备部署相关配置。有时，系统会阻止您将内联配置部署到被动部署的设备，包括分流模式下的内联设备。在其他情况下，策略可成功部署，但尝试使用被动部署的设备阻止或修改流量可能会出现意外结果。例如，由于受阻连接在被动部署中未被阻止，因此系统可为每个受阻连接报告多个连接开始事件。

访问控制策略组件

新创建的访问控制策略指导其目标设备使用其默认操作处理所有流量。

在下图中，默认操作使用“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略，在允许流量流向其最终目标之前检查流量。



以下列表介绍可在创建简单策略后更改的配置。

注释 您只能编辑在当前域中创建的访问控制策略。此外，不能编辑由祖先访问控制策略锁定的设置。

名称和描述

每个访问控制策略必须拥有唯一的名称。说明是可选的。

沿用设置

通过策略继承，您可以创建访问控制策略的层次结构。父（或基本）策略定义和执行其后代的默认设置，这对于多域部署尤为有用。

策略的继承设置允许您选择其基本策略。您还可以锁定当前策略中的设置以强制所有后代继承这些设置。后代策略可以覆盖未锁定的设置。

Policy Assignment

每个访问控制策略可识别使用策略的设备。每台设备只能作为一个访问控制策略的目标。在多域部署中，可能需要一个域中的所有设备使用同一基本策略。

Rules

访问控制规则提供了一种精细的网络流量处理方法。访问控制策略中的规则从 1 开始进行编号，包括从祖先策略继承的规则。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

通常，系统根据第一个访问控制规则（其中所有规则的条件都与流量匹配）处理网络流量。条件可以简单也可以复杂，条件的使用通常取决于某些许可证。

默认操作

默认操作确定系统如何处理和记录不是由任何其他访问控制配置处理的流量。默认操作可以阻止或信任所有流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。

尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

安全情报

安全情报是抵御恶意互联网内容的第一道防线。此功能允许您根据最新的 IP 地址、URL 和域名信誉情报将连接列入黑名单（加以阻止）。要确保对重要资源的持续访问，您可以使用自定义白名单覆盖黑名单。

HTTP 响应

在系统阻止用户的网站请求时，您可以显示系统提供的通用响应页面或自定义页面。也可以显示一个警告用户，同时允许他们继续访问初始请求站点的页面。

高级访问控制选项

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。通常，默认设置就非常适合。可修改的高级设置包括流预处理、SSL 检查、身份和各种性能选项。

访问控制策略默认操作

在简单的访问控制策略中，默认操作指定目标设备如何处理所有流量。在更复杂的策略中，默认操作处理如下流量：

- 不受智能应用绕行信任
- 未被安全情报列入黑名单
- 未被 SSL 检查阻止（仅限加密流量）
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

访问控制策略默认操作可以阻止或信任流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。

注释 您**不能**对默认操作处理的流量执行文件或恶意软件检查。默认操作处理的连接的日志记录最初处于禁用状态，但是您可以启用该日志记录功能。

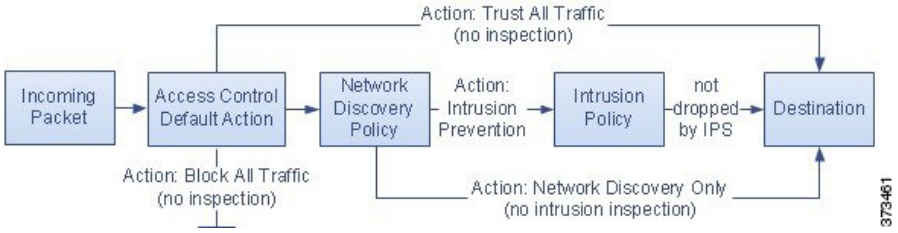
如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从其基本策略继承其默认操作，但您无法强制执行这一继承。

下表介绍了您可以对每个默认操作处理的流量执行的检查类型。

表 *69*：访问控制策略默认操作

默认操作	对流量的影响	检查类型和策略
访问控制：阻止所有流量	阻止，无需进一步检查	none
访问控制：信任所有流量	信任（允许流向其最终目标，而无需进一步检查）	none
入侵防御	允许，前提是其通过指定的入侵策略	入侵，使用指定的入侵策略和关联变量集，以及 发现，使用网络发现策略
仅网络发现	允许	仅发现，使用网络发现策略
继承自基本策略	在基本策略中定义	在基本策略中定义

下图对该表进行了展示。



下图展示了**阻止所有流量 (Block All Traffic)** 和**信任所有流量 (Trust All Traffic)** 默认操作。

下图展示了**入侵防御 (Intrusion Prevention)** 和**仅网络发现 (Network Discovery Only)** 默认操作。

提示

Network Discovery Only 的目的是在仅发现部署中提高性能。如果您仅对入侵检测和防御感兴趣，则不同的配置可以禁用发现。

访问控制策略继承

访问控制使用基于分层策略的实施，完善了多租户策略。正如创建域层次结构一样，您也可以创建访问控制策略的相应层次结构。后代或子访问控制策略继承其直接父策略或基本策略的规则和设置。该基础策略可能有其子级的父级策略，它从父级策略沿用规则和设置等。

访问控制策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。这种实施执行来自祖先策略的强制规则，但也允许当前策略写入规则以抢先于来自祖先策略的默认规则。

您可以锁定以下设置，以便在所有后代策略中执行它们。后代策略可以覆盖未锁定的设置。

- 安全情报 - 根据最新的 IP 地址、URL 和域名信誉情报将连接列入黑名单和白名单。
- HTTP 响应页面 - 在阻止用户的网站请求时显示自定义或系统提供的响应页面。
- 高级设置 - 指定关联的子策略、网络分析设置、性能设置和其他常规选项。

尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

策略继承和多租户

在典型的多域部署中，访问控制策略的层次结构与域结构相对应，您将最低级别的访问控制策略应用于受管设备。这种实施支持在较高的域级别选择性地执行访问控制，而低层域管理员可以定制特定部署的具体设置。（要限制后代域中的管理员，您必须使用角色而不能只靠策略继承和实施。）

例如，作为组织的全局域管理员，您可以在全局级别创建访问控制策略。然后，您可以要求所有设备（按功能分为子域）使用该全局级策略作为基本策略。

当子域管理员登录Firepower管理中心配置访问控制时，他们可以按原样部署该全局级策略。或者，他们也可以在该全局级策略的界限之内创建和部署后代访问控制策略。

注释 虽然这种最有用的访问控制继承和执行的实施方法可以完善多租户策略，但您也可以在单个域中创建访问控制策略的层次结构。您还可以在任意级别分配和部署访问控制策略。

管理访问控制策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 访问管理员 网络管理员

可以使用Firepower系统编辑系统提供的访问控制策略，并创建自定义访问控制策略。根据设备的初始配置，系统提供的策略可以包括：

- “默认访问控制”(Default Access Control) - 阻止所有流量，而不进行进一步检查。
- “默认入侵防御”(Default Intrusion Prevention) - 允许所有流量，但是还会使用“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略和默认入侵变量集进行检查。
- “默认网络发现”(Default Network Discovery) - 检查时允许发现数据的所有流量，但不允许入侵或漏洞的流量。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**。

步骤 2 管理访问控制策略：

- 复制 - 点击复制图标 ( )。
- 创建 - 点击**新建策略 (New Policy)**；请参阅创建基本访问控制策略，第 613 页。
- 删除 - 点击删除图标 ( )。
- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改，第 254 页。
- 编辑 - 点击编辑图标 ( )；请参阅 编辑访问控制策略，第 614 页
- 继承 - 点击具有后代的策略旁边的加号图标 ( )，展开策略层次结构视图。
- 导入/导出 - 点击**导入/导出 (Import/Export)**；请参阅配置导入和导出，第 149 页。
- 报告 - 点击报告图标 ( )；请参阅生成当前策略报告，第 262 页。

创建基本访问控制策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

创建新访问控制策略时，必须至少选择一个默认操作。

大多数情况下，初始时会禁用默认操作处理连接的日志记录。如果您在多域部署中创建子策略，则会出现例外。在那种情况下，系统会根据继承的默认操作的日志记录配置启用连接日志记录。

注意 初始时将访问控制策略部署到受管设备在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**。

步骤 2 点击 **New Policy**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 或者，从**选择基本策略 (Select Base Policy)** 下拉列表中选择基本策略。
如果已在您的域上执行访问控制策略，则此步骤不为可选步骤。必须选择已执行的策略或其后代之一作为基本策略。

步骤 5 指定初始**默认操作**：

- 如果已选择基本策略，则新策略会继承其默认操作。您无法在此对其进行更改。
- **Block all traffic** 通过 **Access Control: Block All Traffic** 默认操作创建策略。
- **入侵防御 (Intrusion Prevention)** 可以通过**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)** 默认操作创建策略，与默认入侵变量集相关联。
- **Network Discovery** 使用默认操作 **Network Discovery Only** 创建策略。

提示 如果要在默认情况下信任所有流量，或如果已选择基本策略但不想继承默认操作，则可以稍后更改默认操作。

步骤 6 或者，选择要部署策略的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。
如果要立即部署此策略，则必须执行此步骤。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 或者，进一步配置新策略，如编辑访问控制策略，第 614 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

编辑访问控制策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。

为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**。

步骤 2 点击要编辑的访问控制策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑访问控制策略：

- 名称和说明 - 点击任一字段并输入新信息。
- 默认操作 - 从**默认操作 (Default Action)** 下拉列表中选择一个值。

更改访问控制策略使用的入侵策略总数在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。通过以下方式更改入侵策略总数：将策略当前未使用的入侵策略与访问控制规则、默认操作或默认入侵策略关联；或者从其中任意一个中删除访问控制策略使用的最后一个入侵策略实例。

- 默认操作变量集 - 要更改与**入侵防御 (Intrusion Prevention)** 默认操作关联的变量集，请点击变量图标 ( )。在显示的弹出窗口中，选择新变量集并点击**确定 (OK)**。也可在新窗口中编辑所选变量集；点击编辑图标 ( )，然后如管理变量，第 324 页中所述继续操作。
- 默认操作日志记录 - 要配置默认操作所处理的连接的日志记录，请点击日志记录图标 ( )，然后如使用策略默认操作记录连接，第 1510 页中所述继续操作。
- HTTP 响应 - 要指定当系统阻止网站请求时用户在浏览器中所看到的内容，请点击 **HTTP 响应 (HTTP Responses)** 选项卡，然后如选择 HTTP 响应页面，第 646 页中所述继续操作。
- 继承：更改基本策略 - 要更改此策略的基本访问控制策略，请点击**继承设置 (Inheritance Settings)**，然后如选择基本访问控制策略，第 617 页中所述继续操作。
- 继承：锁定后代域中的设置 - 要在其后代策略中实施此策略的设置，请点击**继承设置 (Inheritance Settings)**，然后如锁定后代访问控制策略中的设置，第 618 页中所述继续操作。
- 策略分配：目标 - 要确定此策略所针对的受管设备，请点击**策略分配 (Policy Assignment)**，然后如设置访问控制策略的目标设备，第 619 页中所述继续操作。
- 策略分配：域中需要 - 要在子域中实施此策略，请点击**策略分配 (Policy Assignment)**，然后如在域中需要访问控制策略，第 619 页中所述继续操作。
- 规则 - 要使用入侵和文件策略来管理访问控制规则，以及检查和阻止恶意流量，请点击**规则 (Rules)** 选项卡，然后如创建和编辑访问控制规则，第 630 页中所述继续操作。
- 安全情报 - 要立即根据最新信誉情报将连接列入黑入单（阻止），请点击**安全情报 (Security Intelligence)** 选项卡，然后如配置安全情报，第 653 页中所述继续操作。
- 高级选项 - 要设置预处理、SSL检查、性能及其他高级选项，请点击**高级 (Advanced)** 选项卡并参阅访问控制策略高级设置，第 620 页。

- 警告 - 要查看访问控制策略（及其后代和关联策略）中的警告或错误列表，请点击**显示警告 (Show Warnings)**。警告和错误标记出会对流量分析和数据流产生不利影响或阻碍策略部署的配置。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

管理访问控制策略继承

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 编辑要更改其继承设置的访问控制策略；请参阅编辑访问控制策略，第 614 页。

步骤 2 管理策略继承：

- 更改基本策略 - 要更改此策略的基本访问控制策略，请点击**继承设置 (Inheritance Settings)**，然后如选择基本访问控制策略，第 617 页中所述继续操作。
- 锁定后代策略中的设置 - 要在此策略的所有后代策略中执行其设置，请点击**继承设置 (Inheritance Settings)**，然后如锁定后代访问控制策略中的设置，第 618 页中所述继续操作。
- 要求在域中提供 - 要在子域中执行此策略，请点击**策略分配 (Policy Assignment)**，然后如在域中需要访问控制策略，第 619 页中所述继续操作。
- 继承基本策略的设置 - 要继承基本访问控制策略的设置，请点击 **安全情报 (Security Intelligence)**、**HTTP 响应 (HTTP Responses)** 或**高级 (Advanced)** 选项卡，然后如继承基本策略的访问控制策略设置，第 617 页中所述继续操作。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

选择基本访问控制策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

可以使用一个访问控制策略作为另一个访问控制策略的基础（父级）。默认情况下，子策略从其基本策略继承其设置，但是可以更改未锁定的设置。

当更改当前访问控制策略的基本策略时，系统会使用新基本策略中的任何已锁定的设置来更新当前策略。

过程

步骤 1 在访问控制策略编辑器中，点击**继承设置 (Inheritance Settings)**。

步骤 2 从**选择基本策略 (Select Base Policy)** 下拉列表中选择策略。
在多域部署中，在当前域中可能需要访问控制策略。只能选择已执行的策略或其后代之一作为基本策略。

步骤 3 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

继承基本策略的访问控制策略设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

新的子策略继承其基本策略的许多设置。如果这些设置在基本策略中未锁定，您可以覆盖这些设置。

如果稍后重新继承基本策略的设置，系统会显示基本策略的设置且控件呈灰色。不过，系统会保存所做的覆盖，如果您再次禁用继承，则会恢复覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，点击**安全情报 (Security Intelligence)**、**HTTP 响应 (HTTP Responses)** 或**高级 (Advanced)** 选项卡。

步骤 2 选中要继承的每个设置所对应的**继承自基本策略 (Inherit from base policy)** 复选框。
如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

锁定后代访问控制策略中的设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

锁定访问控制策略中的设置，以便在所有后代策略中执行该设置。后代策略可以覆盖未锁定的设置。

当您锁定设置时，系统会保存后代策略中已经做出的覆盖，以便在您再次解锁设置时可以恢复这些覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，点击**继承设置 (Inheritance Settings)**。

步骤 2 在“子策略继承设置”(Child Policy Inheritance Settings) 区域中，选中要锁定的设置。
如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**确定 (OK)** 保存设置。

步骤 4 点击**保存 (Save)** 保存访问控制策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

在域中需要访问控制策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

您可以要求域中的每个设备都使用相同的基本访问控制策略或其后代策略之一。

开始之前

- 除全局域以外，至少配置一个域。

过程

步骤 1 在访问控制策略编辑器中，点击**策略分配 (Policy Assignments)**。

步骤 2 点击**在域中需要 (Required on Domains)** 选项卡。

步骤 3 构建域列表：

- 添加 - 选择要实施当前访问控制策略的域，然后点击**添加 (Add)** 或拖放到所选域列表中。
- 删除 - 点击枝叶域旁边的删除图标 ( )，或者右键点击祖先域并选择**删除所选项 (Delete Selected)**。
- 搜索 - 在搜索字段中键入搜索字符串。点击清除图标 ( ) 以清除搜索。

步骤 4 点击**确定 (OK)** 以保存域实施设置。

步骤 5 点击**保存 (Save)** 保存访问控制策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

设置访问控制策略的目标设备

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

访问控制策略指定使用策略的设备。每台设备只能作为一个访问控制策略的目标。在多域部署中，可能需要一个域中的所有设备使用同一基本策略。

过程

步骤 1 在访问控制策略编辑器中，点击**策略分配 (Policy Assignments)**。

步骤 2 在**目标设备 (Targeted Devices)** 选项卡上，建立目标列表：

- 添加 - 选择一个或多个**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)** 或拖放到**所选设备 (Selected Devices)** 列表。
- 删除 - 点击单个设备旁边的删除图标 ( )，或选择多个设备，点击右键，然后选择**删除所选项 (Delete Selected)**。
- 搜索 - 在搜索字段中键入搜索字符串。点击清除图标 ( ) 以清除搜索。

在**受影响的设备 (Impacted Devices)** 下，系统列出可以分配此访问控制策略但当前正使用另一个策略的所有设备。

步骤 3 或者，点击**域中需要 (Required on Domains)** 选项卡以要求您所选的子域中的所有设备使用同一基本策略。请参阅在域中需要访问控制策略，第 619 页。

步骤 4 点击**确定 (Ok)** 以保存目标设备设置。

步骤 5 点击**保存 (Save)** 保存访问控制策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

访问控制策略高级设置

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。默认设置适用于大多数的部署。请注意，规则更新可能会修改访问控制策略中的许多高级预处理和性能选项，如入侵规则更新，第 127 页中所述。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

常规设置

要自定义您为用户所请求的每个 URL 存储的字符数，请参阅限制长 URL 的日志记录，第 1511 页。

要自定义用户绕过初始阻止后您重新阻止网站前的时长；请参阅为受阻网站设置用户绕过超时，第 648 页。

禁用**重试 URL 缓存缺失查找 (Retry URL cache miss lookup)** 以在未缓存类别时允许系统立即将流量传递到URL 而无需进行云查找。系统将需要云查找的URL 视为“未分类”(Uncategorized)，直至对其他类别完成云查找为止。

要在部署配置更改时检查流量（除非特定配置需要重新启动Snort 进程），请确保**在策略应用期间检查流量 (Inspect traffic during policy apply)** 设置为其默认值（已启用）。启用此选项后，资源需求可能会导致丢弃少量数据包而不进行检查。有关详细信息，请参阅Snort® 在配置部署期间重新启动，第 257 页。

注意 部署配置更改时，禁用**在策略应用期间检查流量 (Inspect traffic during policy apply)** 会重启 Snort 进程。

关联策略

使用高级设置将子策略（SSL、身份）与访问控制相关联；请参阅将其他策略与访问控制相关联，第 622 页。

注意 部署配置更改时，关联 SSL 或身份策略，或者后续通过选择**无 (None)** 解除与此策略的关联，会重启 Snort 进程。

网络分析和入侵策略

高级网络分析和入侵策略设置可供您：

- 更改访问控制策略的默认入侵策略和关联的变量集，在系统可以准确确定如何检查流量之前，该默认入侵策略和关联的变量集用于对该流量进行初始检查。
- 更改访问控制策略的默认网络分析策略，该默认策略监管许多预处理选项。
- 使用自定义网络分析规则和网络分析策略根据特定安全区域、网络和VLAN 定制预处理选项。

有关详细信息，请参阅网络分析和入侵策略的高级访问控制设置，第 991 页。

文件和恶意软件设置

文件和恶意软件检测性能和存储调整，第 775 页 提供有关文件控制和面向 Firepower 的 AMP 的性能选项的信息。

注意 部署配置更改时，更改“文件和恶意软件设置”(Files and Malware Settings) 下的值会重启 Snort 进程。

智能应用绕行设置

智能应用绕行 (IAB) 是可用于指定应用的专家级配置，如果这些应用的流量超过所配置的检查性能和流阈值组合，则系统可以绕过该流量或将其识别为应已绕过。有关详细信息，请参阅智能应用绕行 (IAB)，第 671 页。

传输/网络层预处理器设置

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。有关详细信息，请参阅高级传输/网络预处理器设置，第 1069 页。

检测增强功能设置

借助高级检测增强功能设置，您可以使用自适应配置文件根据您的主机操作系统在被动部署中改善数据包分片和 TCP 流的重组。有关详细信息，请参阅自适应配置文件，第 1117 页。

性能设置和基于延迟的性能设置

概述：入侵防御性能调整，第 977 页提供在系统分析尝试入侵的流量时提高该系统的性能的有关信息。

将其他策略与访问控制相关联

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	因功能而异	因功能而异	任意	管理员/访问管理员/网络管理员

使用访问控制策略的高级设置将以下每一个子策略与该访问控制策略相关联：

- SSL 策略 - 用于监控、解密、阻止或允许使用安全套接字层 (SSL) 或传输层安全 (TLS) 加密的应用层协议流量。
- 身份策略 - 根据与流量关联的领域和身份验证方法执行用户身份验证。

注意 关联 SSL 或身份策略，或者随后通过选择**无 (None)** 取消关联该策略，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 在相应的“策略设置”(Policy Settings) 区域点击编辑图标 ( )。

如果改为显示查看图标 ()，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 从下拉列表中选择策略。
如果选择用户创建的策略，则可以点击显示的编辑图标来编辑策略。

步骤 4 点击 **OK**。

步骤 5 点击**保存 (Save)** 保存访问控制策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 35 章

访问控制规则

以下主题介绍如何配置访问控制规则：

访问控制规则简介

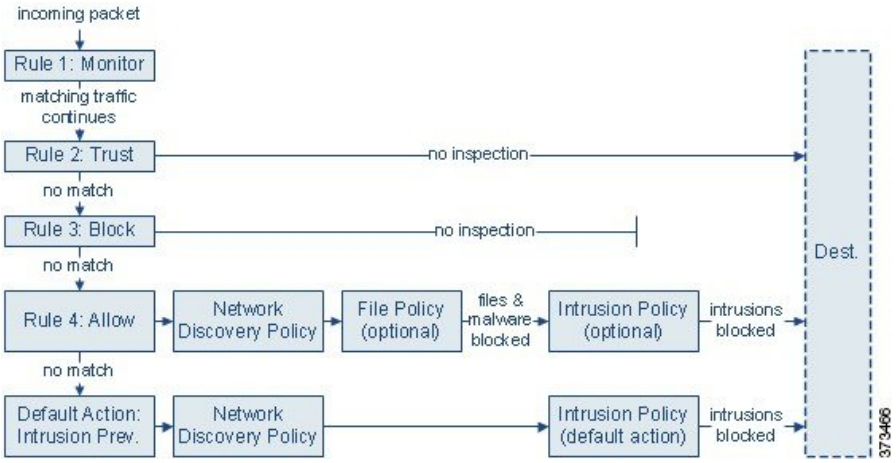
在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。

注释 8000 系列快速路径、安全情报过滤、SSL 检查、用户标识以及某些解码和预处理发生在访问控制规则评估网络流量之前。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。

每个规则也有操作，确定是否监控、信任、阻止或允许匹配的流量。当您允许流量时，可以指定在流量到达您的资产或退出您的网络之前，系统首先利用入侵或文件策略对其进行检查以阻止任何漏洞攻击、恶意软件或禁止的文件。

以下场景汇总了内联入侵防御部署中访问控制规则评估流量的方式。



在这种情况中，流量评估如下：

- **规则 1：Monitor** 第一次评估流量。Monitor 规则跟踪和记录网络流量，但不影响流量。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- **规则 2：Trust** 继续评估流量。系统允许匹配的流量传至目标，而无需进一步检查，但此类流量仍会受到身份要求的制约。不匹配的流量继续根据下一规则进行评估。
- **规则 3：Block** 第三次评估流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据最终规则进行评估。
- **规则 4：Allow** 是最终规则。对于此规则，允许匹配的流量；但检测和阻止流量内禁止的文件、恶意软件、入侵和漏洞。系统允许其余未阻止的非恶意流量传至目标，但此类流量仍受到身份要求的制约。您可以配置只执行文件检查、入侵检查或两类检查都不执行的“允许”(Allow) 规则。
- **Default Action** 处理不匹配任何规则的所有流量。在此情况下，默认操作在允许非恶意流量通过之前执行入侵防御。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。（您不能对默认操作处理的流量执行文件或恶意软件检测。）

无论是使用访问控制规则还是默认操作，您允许的流量都自动可用于根据网络发现策略检查主机、应用和用户数据。尽管可以增强或禁用发现功能，但不能明确启用该功能。但是，允许流量不会自动确保收集发现数据。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

请注意，当 SSL 检查配置允许已加密流量通过或者您不配置 SSL 检查时，访问控制规则处理已加密流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

访问控制规则管理

通过访问控制策略编辑器的**规则 (Rules)** 选项卡，您可以添加、编辑、分类、搜索、移动、启用、禁用、删除或以其他方式管理当前策略中的访问控制规则。

对于每个访问控制规则，策略编辑器显示其名称、条件概述、规则操作以及传达规则检测选项或状态的图标。这些图标代表：

- 入侵策略选项 ()
- 文件策略选项 ()
- 日志记录选项 ()
- 注释 ()
- 警告 ()
- 错误 ()
- 重要信息 ()

已禁用的规则在规则名称下方呈灰色显示并带有相应的标记 `(disabled)`。

要创建或编辑规则，请使用访问控制规则编辑器。您可以执行以下操作：

- 在编辑器的上部配置基本属性，如规则的名称、状态、位置和操作。
- 使用编辑器下部左侧的选项卡添加条件。
- 使用下部右侧的选项卡配置检测和日志记录选项，还可以向规则添加注释。为了方便，无论您在查看哪个选项卡，编辑器都列出规则的检测和日志记录选项。

注释 正确创建和排序访问控制规则是一项复杂的任务，但重要的是构建有效部署。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，访问控制策略接口具有规则的强大警告和错误反馈系统。

访问控制规则继承

每个访问控制策略具有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。所有访问控制规则都必须属于其中一个部分。访问控制策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。

您只能在当前编辑的策略中添加和编辑规则。在策略编辑器中，这些规则显示为最内部的规则。您无法查看或编辑后代策略中的规则；您可以查看但无法编辑祖先策略中的规则。

在一种典型的部署中，如果您在层次结构中部署最低级别的访问控制策略，则系统会根据每个策略中的“强制性”(Mandatory) 规则匹配流量，从最内部（最高级别）开始向内执行。如果流量不匹配任何强制性规则，则系统会使用每个策略中的“默认”(Default) 规则，从最内部（最低级别）开始向外执行。

虽然您可以严格执行后代策略中的设置，但您无法执行“默认”(Default) 规则或默认操作：

- “强制性”(Mandatory) 访问控制规则会抢占后代策略中的规则。在系统根据已部署策略中的规则匹配流量之前，它会根据每个祖先策略中的“强制性”(Mandatory) 规则匹配流量。如果您希

望一条规则在任何后代策略的规则之前处理流量，请将该规则置于“强制性”(Mandatory) 部分。

- “默认”(Default) 访问控制规则会抢占后代策略中的规则。如果您希望后代策略中的规则以不同方式处理目标流量，请将一条规则置于“默认”(Default) 部分。
- 如果流量既不匹配已部署策略中的规则，也不匹配已部署策略的祖先中的规则（非监控），则系统会使用已部署策略的默认操作。尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

例如，在编辑最低级别的策略时，分层访问控制策略可能会显示以下规则评估顺序：

- 强制性规则 - 全局策略

  强制性规则 - 子域策略

  默认规则 - 子域策略

- 默认规则 - 全局策略
- 默认操作 - 子域策略

访问控制规则组成部分

除唯一名称之外，每个访问控制规则都具有以下基本组件：

省/自治区

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

位

系统已对访问控制策略中的规则进行编号，从 1 开始。如果正在使用策略继承，则规则 1 是最外层策略的第一条规则。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

规则也可属于某个部分和某个类别，其仅有利于组织且不影响规则位置。规则位置跨越部分和类别。

部分和类别

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。要进一步组织访问控制规则，您可以在“强制性”(Mandatory) 和“默认”(Default) 部分中创建自定义规则类别。

如果正在使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。

条件

条件指定规则处理的特定流量。条件可以简单也可以复杂；条件的使用通常取决于许可证。

操作

规则操作确定系统如何处理匹配的流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检测）匹配的流量。系统**不会**对受信任、被阻止或加密的流量进行深度检查。

检查

深度检查选项管理系统如何检查和阻止您意外允许的恶意流量。通过规则允许流量时，可以指定系统先使用入侵或文件策略检测流量以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。一般来说，您可以在连接开始和/或结束时记录会话。您可以将连接记录到数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器。

备注

每次保存对访问控制规则所做的更改时，都可以添加注释。

访问控制规则顺序

系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。除了“监控”(Monitor) 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，不再继续根据其他低优先级规则评估流量。

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。要进一步组织，您可以在“强制性”(Mandatory) 和“默认”(Default) 部分中创建自定义规则类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

如果使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。规则 1 是最外层策略（不是当前策略）中的第一条规则，系统跨策略、部分和类别分配规则编号。

允许修改访问控制策略的任何预定义用户角色还允许您在规则类别内部和之间移动和修改访问控制规则。但是，可以创建自定义角色来限制用户移动和修改规则。允许修改访问控制策略的任意用户可以将规则添加到自定义类别，以及无限制的修改其中的规则。

提示 适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

添加访问控制规则类别

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

您可以将访问控制策略的“强制性”(Mandatory) 和“默认”(Default) 规则部分划分为自定义类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

过程

步骤 1 在访问控制策略编辑器中，点击**添加类别 (Add Category)**。

提示 如果您的策略已经包含规则，则可以点击现有规则在该行的空白区域，先设置新类别的位置，然后才能添加。还可以右键单击现有规则并选择 **Insert new category**。

步骤 2 输入 **Name**。

步骤 3 从**插入 (Insert)** 下拉列表中，选择要添加类别的位置：

- 要在某个部分中的所有现有类别下方插入类别，请选择**插入强制性类别 (into Mandatory)** 或**插入默认类别 (into Default)**。
- 要在现有类别上方插入类别，请选择**类别上方 (above category)**，然后选择类别。
- 要在访问控制规则上方或下方插入类别，请选择**规则上方 (above rule)** 或**规则下方 (below rule)**，然后输入现有规则编号。

步骤 4 点击 **OK**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

创建和编辑访问控制规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，您有以下选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击编辑图标 ()。

如果规则旁边改为显示查看图标 ()，则表明规则属于祖先策略，或者您没有修改配置的权限。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分，或接受默认值：

- 已启用 - 指定规则是否为**已启用 (Enabled)**。
- 位置 - 指定规则位置；请参阅访问控制规则顺序，第 629 页。
- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅访问控制规则操作，第 633 页。
- 条件 - 点击与要添加的条件对应的选项卡。有关详细信息，请参阅规则条件类型，第 268 页。
- 深度检查 - 对于“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则，点击入侵检测图标 () 或文件和恶意软件检测图标 () 以配置规则的**检查 (Inspection)** 选项。如果图标呈灰色显示，则表示没有为规则选择此类型的策略。有关详细信息，请参阅使用入侵和文件策略的访问控制，第 637 页。
- 日志记录 - 点击活动（蓝色）日志记录图标 () 以指定**日志记录 (Logging)** 选项。如果图标呈灰色显示，则表示对规则禁用连接日志记录。有关详细信息，请参阅连接日志记录策略，第 1502 页。
- 注释 - 点击注释列中的数值可添加**注释 (Comments)**。编号指示规则已包含的注释数。有关详细信息，请参阅访问控制规则注释，第 635 页。

步骤 4 保存规则。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

启用和禁用访问控制规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

创建访问控制规则时，默认情况下启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。在查看访问控制策略中的规则列表时，禁用的规则会呈灰色显示，不过，您仍然可以修改它们。

提示 您还可以使用规则编辑器启用或禁用访问控制规则。

过程

步骤 1 在访问控制策略编辑器中，右键点击规则并选择规则状态。

如果规则旁边改为显示查看图标 ( )，则表明规则属于祖先策略，或者您没有修改配置的权限。

步骤 2 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

定位访问控制规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

可以在访问控制策略内部（而非之间）移动现有规则。将某条规则添加或移动到某个类别时，系统会将其置于该类别的末尾。

提示 可以使用右键点击菜单选择规则，然后剪切并粘贴，以立即移动多条规则。

过程

步骤 1 在访问控制规则编辑器中，您有以下选择：

- 如果添加的是新规则，请使用**插入 (Insert)** 下拉列表。
- 如果编辑的是现有规则，请点击**移动 (Move)**。

步骤 2 选择要移动或插入规则的位置：

- 选择**插入强制性类别 (into Mandatory)** 或**插入默认类别 (into Default)**。
- 选择**插入强制性类别 (into Mandatory)**，然后选择用户定义的类别。
- 选择**规则上方 (above rule)** 或**规则下方 (below rule)**，然后键入相应的规则编号。

步骤 3 点击**保存 (Save)**。

步骤 4 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

访问控制规则操作

每个访问控制规则都具有用于确定系统如何处理和记录匹配流量的操作：您可以监控、信任、阻止或允许（执行或无需执行进一步检查）匹配流量。

访问控制策略的默认操作会处理不符合任何非 Monitor 访问控制规则条件的流量。

访问控制规则监控操作

Monitor 操作不影响流量；匹配的流量既不会被立即允许，也不会被立即拒绝。更确切地是，根据其他规则匹配流量以确定允许还是拒绝该流量。所匹配的第一个非 Monitor 规则确定流量和任何进一步的检查。如果没有其他匹配的规则，系统使用默认操作。

由于Monitor规则的主要目的是跟踪网络流量，因此系统会自动记录监控流量的连接结束事件。即，即使流量不匹配其他规则，且您不对默认操作进行日志记录，系统也会记录连接。

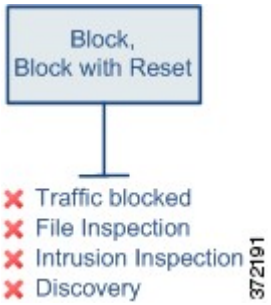
注释 如果本地约束的流量与第 3 层部署中的 Monitor 规则相匹配，则该流量可能绕过检查。为确保对流量进行检查，在路由流量的受管设备的高级设备设置中启用 **Inspect Local Router Traffic**。

访问控制规则信任操作

信任 (Trust) 操作允许流量通过，无需深度检查或网络发现。受信任的流量仍会受到身份要求的制约。

访问控制规则阻止操作

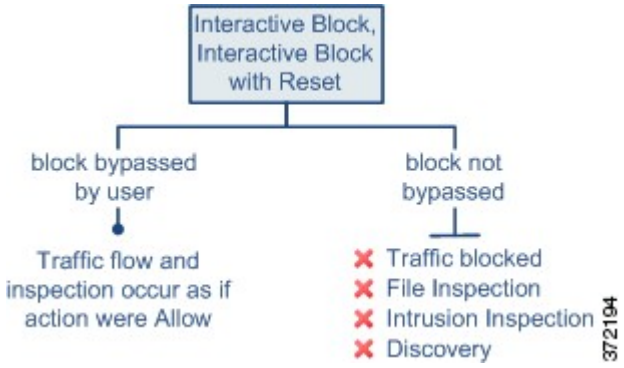
Block 和 **Block with reset** 操作拒绝流量，无需任何类型的进一步检测。Block with reset 规则也会重置连接。



可以在阻止 Web 请求时显示 *HTTP* 响应页面；请参阅HTTP 响应页面和交互式阻止，第 645 页。

访问控制规则交互式阻止操作

交互式阻止 (Interactive Block) 和**交互式阻止并重置 (Interactive Block with reset)** 操作使用户有机会通过点击可自定义的警告页面（称为 *HTTP* 响应页面）绕过网站阻止。Interactive Block with reset 规则也可以重置连接。有关详细信息，请参阅HTTP 响应页面和交互式阻止，第 645 页。



如果用户绕过拦截，该规则模拟 Allow 规则。因此，您可以将任一类型的 Interactive Block 规则与文件和入侵策略关联，以检测此用户允许的流量。系统也可以使用网络发现进行检查。

如果用户不（或无法）绕过拦截，该规则模拟 Block 规则。匹配流量会被拒绝，无需进一步检测。

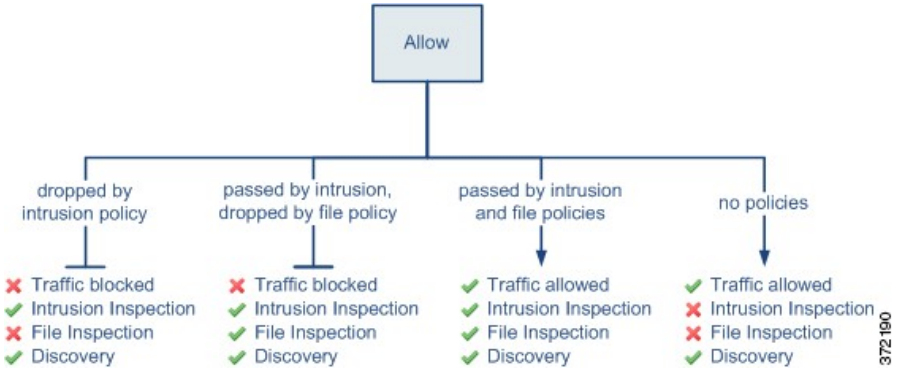
访问控制规则允许操作

允许 (Allow) 操作允许匹配的流量通过，但是仍会受到身份要求的制约。

或者，您可以使用深度检查以在未加密或已解密流量到达目的地之前进一步对其进行检查和阻止：

- 您可以使用入侵策略，以便根据入侵检测和防御配置来分析网络流量，并根据配置丢弃恶意数据包。
- 您可使用文件策略执行文件控制。借助文件控制，可以检测和阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。
- 您还可以使用文件策略执行基于网络的高级恶意软件防护 (AMP)。面向 Firepower 的 AMP 可以检查文件中的恶意软件，并根据配置阻止检测到的恶意软件。

下图展示对满足“允许”(Allow) 规则（或用户绕过的“交互式阻止”[Interactive Block] 规则）条件的流量执行的检查类型。请注意，文件检测会在入侵检测之前发生；被阻止文件不会进行入侵相关漏洞检测。



为简单起见，该图显示入侵和文件策略均与访问控制规则相匹配（或都不匹配）的情况下的流量。但是，您可以单独配置其中一个。没有文件策略时，流量由入侵策略确定；没有入侵策略时，流量由文件策略确定。

不管入侵或文件策略会检测还是丢弃流量，系统都可以使用网络发现功能进行检查。但是，允许流量不会自动确保发现检查。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

访问控制规则注释

创建或编辑访问控制规则时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。您可以显示规则的所有注释列表，以及添加每条注释的用户以及添加注释的日期。

保存规则时，自上次保存所做的所有注释都将变为只读。

将注释添加到访问控制规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制规则编辑器中，点击**注释 (Comments)** 选项卡。

步骤 2 点击 **New Comment**。

步骤 3 输入注释，然后点击**确定 (OK)**。您可以在保存规则之前编辑或删除此注释。

步骤 4 点击**保存 (Save)**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 36 章

使用入侵和文件策略的访问控制

以下主题介绍如何配置访问控制策略以使用入侵和文件策略：

深度检查简介

入侵策略和文件策略共同用作允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。
- 文件策略监管系统的文件控制和面向 Firepower 的 AMP 功能。

访问控制发生在深度检查之前；访问控制规则和访问控制默认操作确定哪些流量由入侵和文件策略检测。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

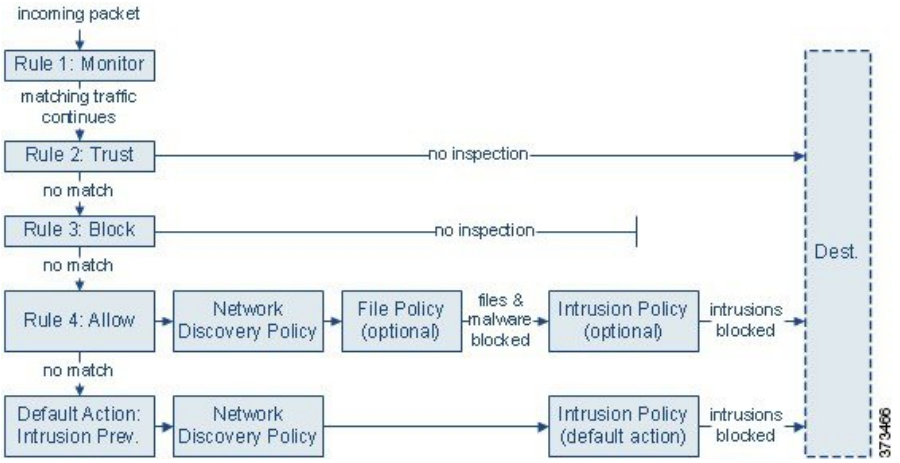
注释 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

系统也可以从 AMP 云接收面向终端的 AMP 数据，然后与任何面向 Firepower 的 AMP 数据并排呈现此数据。

访问控制流量处理

访问控制规则提供跨多个受管设备处理网络流量的精细方法。系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。访问控制规则的操作决定系统如何处理匹配流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检测）匹配的流量。

下图显示内联入侵防御和面向 Firepower 的 AMP 部署中的流量，它受包含四种不同类型的访问控制规则和默认操作的访问控制策略监管。



在上面的情景中，策略中的前三条访问控制规则 — Monitor、Trust 和 Block — 无法检查匹配的流量。Monitor 规则跟踪和记录但不检查网络流量，因此，系统继续将流量与其他规则进行匹配以确定是允许还是拒绝该流量。Trust 和 Block 规则处理匹配流量，无需任何何类型的进一步检查，不匹配的流量继续进入下一条访问控制规则。

策略中的第四个也是最后一条规则（Allow 规则）按照以下顺序调用各种其他策略以检查和处理匹配的流量：

- **发现：网络发现策略** - 首先，网络发现策略检查流量是否存在发现数据。发现是被动分析，并不影响流量的流动。尽管不显式启用发现，但您可以增强或禁用它。但是，允许流量不会自动确保收集发现数据。系统仅对涉及网络发现策略显式监控的 IP 地址的连接进行发现。
- **面向 Firepower 的 AMP 和文件控制：文件策略** - 在流量由发现检查之后，系统可以检查其中是否存在受禁文件和恶意软件。面向 Firepower 的 AMP 会检测并选择性阻止许多类型的文件（包括 PDF、Microsoft Office 文档及其他）中的恶意软件。如果贵组织不仅要阻止传输恶意软件文件，还要阻止特定类型的所有文件（无论文件是否包含恶意软件），则 *file control* 可供您监控网络流量中特定文件类型的传输，然后阻止或允许文件。
- **入侵防御：入侵策略** - 在文件检查之后，系统可以检查流量中是否存在入侵和漏洞。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。
- **目标** - 通过上述所有检查的流量将传递到其目标。

“交互式阻止”(Interactive Block) 规则（未显示在图中）具有与“允许”(Allow) 规则相同的检查选项。因此，您可以在用户通过点击警告页面绕过已阻止网页时检测流量是否存在恶意内容。

不与策略中任何非监控访问控制规则相匹配的流量由默认操作来处理。在这种情况下，默认操作是入侵防御操作，只要流量由您指定的入侵策略进行传递，它就允许流量到达其最终目的地。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。请注意，系统可能检测默认操作允许的流量是否存在发现数据和入侵，而不是检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

注释 有时，当访问控制策略分析某条连接时，系统必须处理该连接中的头几个数据包，**从而让其通过**，然后才能确定哪个访问控制规则（如有）将处理流量。因此，这些数据包不会未经检测就到达其目的地，您可以使用称为默认入侵策略的入侵策略对其进行检测并生成入侵事件。

文件和入侵检查顺序

在您的访问控制策略中，您可以将多个 Allow 和 Interactive Block 规则与不同的入侵和文件策略相关联，以使检查配置文件匹配各种流量类型。

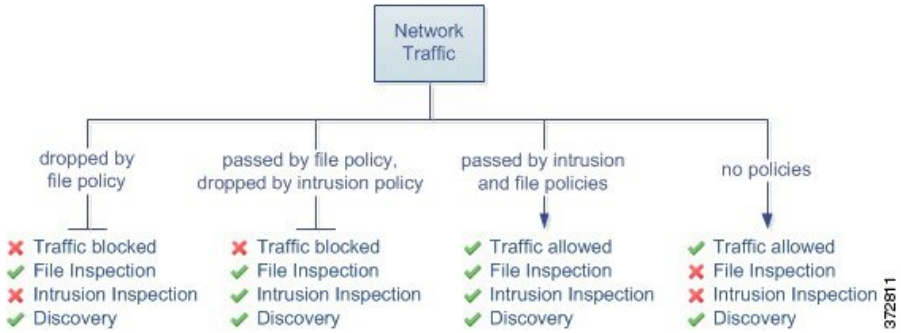
注释 可检测 Intrusion Prevention 或 Network Discovery Only 默认操作允许的流量是否存在发现数据和入侵，但不能检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

您不必在同一规则中同时执行文件和入侵检测。对于符合 Allow 或 Interactive Block 规则的连接：

- 没有文件策略，数据流取决于入侵策略
- 没有入侵策略，数据流取决于文件策略
- 若以上两者都没有，仅由网络发现检查允许的流量

提示 系统不会对受信任的流量执行任何种类的检查。虽然没有使用入侵或文件策略配置Allow规则可以放行流量，就像 Trust 规则那样，但 Allow 规则让您可以对匹配的流量执行发现。

下图说明对符合 Allow 或用户绕过的 Interactive Block 访问控制规则的条件的流量执行的检查类型。为简单起见，该图显示入侵策略和/或文件策略与单个访问控制规则关联的情况的流量。



对由访问控制规则处理的任何单条连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。

例如，请考虑按照访问控制规则中所定义通常要允许特定网络流量的情况。但是，作为预防措施，您希望阻止下载可执行文件，检查恶意软件的已下载的 PDF 并阻止找到的所有实例，然后对流量执行入侵检查。

您可以使用与自己想要暂时允许通过的流量的特征相匹配的规则创建访问控制策略，然后将其与入侵策略和文件策略相关联。文件策略阻止所有可执行文件的下载，也可检测和阻止包含恶意软件的 PDF：

- 首先，系统根据文件策略中指定的简单类型匹配阻止所有可执行文件的下载。由于会立即遭到阻止，因此这些文件既无法执行恶意软件检查也无法执行入侵检查。
- 接着，系统对下载到网络主机的PDF执行恶意软件云查找。具有恶意软件处置情况的任何PDF均被阻止，且不接受入侵检查。
- 最后，系统使用与访问控制规则关联的入侵策略检测任何剩余流量，包括文件策略未阻止的文件。

注释 文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

用于执行文件控制和恶意软件防护的访问控制规则配置

访问控制策略可能有多个与文件策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达其最终目的地之前，将不同的文件和恶意软件检测配置文件与其匹配。

当系统根据文件策略中的设置检测到受禁文件（包括恶意软件）时，会自动将事件记录到Firepower管理中心数据库中。如果您不想记录文件或恶意软件事件，则可按每条访问控制规则禁用此日志记录功能。

无论调用访问控制规则的日志记录配置如何，系统都还会将关联连接的末端记录到Firepower管理中心数据库。

配置访问控制规则以执行文件控制和 AMP

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（文件控制）恶意软件 (AMP)	保护（文件控制）恶意软件 (AMP)	任何环境	任何环境	管理员/访问管理员/网络管理员

注意 将第一个文件策略与访问控制规则关联，或从访问控制策略中删除所有文件策略，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在访问控制规则编辑器中，选择**操作 (Action)** 为**允许 (Allow)**、**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**。

步骤 2 点击**检查 (Inspection)** 选项卡。

步骤 3 选择**恶意软件策略 (Malware Policy)**（文件策略）以检查与访问控制规则相匹配的流量，或选择**无 (None)** 以禁用匹配流量的文件检查。

步骤 4 （可选）通过点击**日志记录 (Logging)** 选项卡并取消选中**日志文件 (Log Files)** 为匹配连接禁用文件或恶意软件文件的日志记录。

注释 思科建议您保持启用文件和恶意软件日志记录。

步骤 5 保存规则。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

用于执行入侵防御的访问控制规则配置

访问控制策略可能有多个与入侵策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达最终目的地之前，使不同的入侵检测配置文件与其匹配。

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

提示 即使您使用系统提供的入侵策略，思科也强烈建议您配置系统的入侵变量以准确反映您的网络环境。至少，要修改默认变量集中的默认变量。

了解系统提供的入侵策略和自定义入侵策略

思科通过 Firepower 系统提供多种入侵策略。通过使用系统提供的入侵策略，您可以利用 Cisco Talos 安全情报和研究小组 (Talos) 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，并提供高级设置的初始配置。可以按现状使用系统提供的策略，也可以将其用作自定义策略的基础。构建自定义策略可以提高系统在您的环境中的性能，并提供网络上发生的恶意流量和策略违规行为的集中视图。

连接和入侵事件日志记录

当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，它会将此事件保存到 Firepower 管理中心。无论访问控制规则采用何种日志记录配置，系统都会将发生入侵的连接的结束自动记录到 Firepower 管理中心数据库。

访问控制规则配置和入侵策略

除了您创建的自定义入侵策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个入侵策略使用平衡安全性和连接入侵策略作为其基本策略。两者之间的唯一区别是其**内联时丢弃 (Drop When Inline)** 设置，该设置在内联策略中启用丢弃行为，在被动策略中禁用该行为。

请注意，您在单个访问控制策略中可以使用的唯一入侵策略的数量取决于目标设备型号；设备的功能越强大，处理的策略就越多。每个唯一的入侵策略和变量集**对均**视为一个策略。虽然您可以将不同的入侵策略-变量集对与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则（以及默认操作）相关联，但是，如果目标设备没有足够的资源可按照配置执行检测，则无法部署访问控制策略。

配置访问控制规则以执行入侵防御

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

注意 更改访问控制策略使用的入侵策略总数在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。通过以下方式更改入侵策略总数：将策略当前未使用的入侵策略与访问控制规则、默认操作或默认入侵策略关联；或者从其中任意一个中删除访问控制策略使用的最后一个入侵策略实例。

过程

步骤 1 在访问控制策略编辑器中，创建新规则或编辑现有规则；请参阅访问控制规则组成部分，第 628 页。

步骤 2 确保规则操作设置为 **Allow**、**Interactive Block** 或 **Interactive Block with reset**。

步骤 3 如果**检查** 选项卡。

步骤 4 选择系统提供的或自定义**入侵策略 (Intrusion Policy)**，或选择**无 (None)** 以禁用对与访问控制规则相匹配的流量进行的入侵检查。

步骤 5 如果要更改与入侵策略关联的变量集，请从**变量集 (Variable Set)** 下拉列表中选择值。

步骤 6 点击 **Save** 保存规则。

步骤 7 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 37 章

HTTP 响应页面和交互式阻止

以下主题介绍如何配置自定义页面以在系统阻止 Web 请求时显示：

关于 HTTP 响应页面

作为访问控制的一部分，您可以使用访问控制规则或访问控制策略默认操作配置在系统阻止 Web 请求时要显示的 HTTP 响应页面。

可以选择系统提供的通用响应页面，也可以输入自定义 HTML。所显示的响应页面取决于阻止会话的方式：

- 阻止或阻止并重置 - 受阻会话超时或重置。**阻止响应页面 (Block Response Page)** 覆盖用于说明拒绝连接的默认浏览器或服务器页面。
- 交互式阻止或交互式阻止并重置 - 系统可以显示**交互式阻止响应页面 (Interactive Block Response Page)** 以警告用户，并且还允许其点击按钮（或刷新页面）以加载原先请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

当系统阻止网络流量时，HTTP 响应页面并非始终显示；请参阅对 HTTP 响应页面的限制，第 645 页。

对 HTTP 响应页面的限制

当系统阻止网络流量时，并不总是显示 HTTP 响应页面。

除访问控制规则之外的配置

系统仅为被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的未加密连接或解密连接显示响应页面。对于以下连接，系统不会显示响应页面：

- 被安全情报列入黑名单的连接
- 被 SSL 策略阻止的加密连接

提升的访问控制规则

如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。

识别 URL 之前

如果网络流量在系统识别请求的 URL 之前被阻止，则系统不会显示响应页面；请参阅对 URL 过滤的限制，第 285 页。

加密流量

如果会话已加密或曾加密，则系统不会显示响应页面。

选择 HTTP 响应页面

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

HTTP 响应页面能否稳定显示取决于页面的网络配置、流量负载和大小。较小的页面更有可能成功显示。

过程

步骤 1 在访问控制策略编辑器中，点击 **HTTP 响应 (HTTP Responses)** 选项卡。
如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 选择**阻止响应页面 (Block Response Page)** 和**交互式阻止响应页面 (Interactive Block Response Page)**：

- “系统提供”(System-provided) - 显示常规响应。点击查看图标 () 可查看此页面的代码。
- “自定义”(Custom) - 创建自定义响应页面。屏幕上将显示一个弹出窗口，其中预先填充有系统提供的代码，您可以通过点击编辑图标()来替换或修改此代码。计数器显示已使用的字符数量。

- “无”(None) - 在没有交互或说明的情况下禁用响应页面并阻止会话。要对整个访问控制策略快速禁用交互式阻止，请选择此选项。

步骤 3 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

对 HTTP 响应页面的交互式阻止

配置交互式阻止时，用户可在看到警告后加载原先请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

提示 要对整个访问控制策略快速禁用交互式阻止，既不要显示系统提供的页面，也不要显示自定义页面。然后，系统会阻止所有连接而不交互。

如果用户不绕过交互式阻止，则会拒绝匹配流量而不进行进一步检查。如果用户绕过交互式阻止，则访问控制规则会允许流量，不过，流量仍然可能受到深度检查和阻止。

默认情况下，用户绕行的有效时间为 10 分钟（600 秒），而在在后续访问时不显示警告页面。可以将持续时间设置为长达一年，也可以强制用户每次都绕过阻止。此设置适用于策略中的每条“交互式阻止”规则。不能对每条规则都设置限制。

以交互方式阻止的流量的日志记录选项与允许的流量中的日志记录选项相同，但如果用户不绕过交互式阻止，则系统只能记录连接开始事件。在系统最初警告用户时，它会使用 `Interactive Block` 或 `Interactive Block with reset` 操作标记任何已记录的连接开始事件。如果用户绕过阻止，则为会话记录的其他连接事件具有操作 `Allow`。

配置交互式阻止

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 访问管理员 网络管理员

过程

步骤 1 作为访问控制的一部分，请配置与网络流量匹配的访问控制规则；请参阅创建和编辑访问控制规则，第 630 页：

- 操作 - 将规则操作设置为**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**；请参阅访问控制规则交互式阻止操作，第 634 页。
- 条件 - 使用 URL 条件指定要进行交互式阻止的网络流量；请参阅URL 条件（URL 过滤），第 280 页。
- 日志记录 - 假设用户将绕过阻止并相应地选择日志记录选项；请参阅允许连接的日志记录，第 1507 页。
- 检测 - 假设用户将绕过阻止并相应地选择深度检查选项；请参阅使用入侵和文件策略的访问控制，第 637 页。

步骤 2 （可选）在访问控制策略 **HTTP 响应 (HTTP Responses)** 选项卡上，选择自定义交互式阻止 HTTP 响应页面；请参阅选择 HTTP 响应页面，第 646 页。

步骤 3 （可选）在访问控制策略**高级 (Advanced)** 选项卡上，更改用户绕行超时；请参阅为受阻网站设置用户绕过超时，第 648 页。
在用户绕过阻止后，系统允许用户浏览到该页面而不发出警告，直至经过超时期为止。

步骤 4 保存访问控制策略。

步骤 5 部署配置更改；请参阅部署配置更改，第 254 页。

为受阻网站设置用户绕过超时

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击 General Settings 旁边的编辑图标 ()。
如果改为显示查看图标 ()，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 在 **Allow an Interactive Block to bypass blocking for (seconds)** 字段中，键入用户绕过到期之前必须经过的秒数。指定零会强制用户每次都绕过阻止。

步骤 4 点击 **OK**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 38 章

安全情报黑名单

以下主题提供安全情报的概述，包括用于将流量和基本设置列入黑名单和白名单。

安全情报基础知识

作为防御恶意互联网内容的第一道防线，安全情报使用信誉情报快速阻止与IP地址、URL和域名的连接。这称为列入安全情报黑名单。

在系统执行需要更多资源的评估之前，安全情报是访问控制的第一阶段。黑名单通过快速排除不需要检测的流量来提高性能。

注释 您无法将使用快速路径的流量列入黑名单。8000 系列快速路径操作发生在安全情报过滤之前。使用快速路径的流量会绕过所有的进一步评估，包括安全情报。

虽然您可以配置自定义黑名单，但思科提供对定期更新的情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。

您可以利用白名单和仅监控的黑名单缩小安全情报黑名单范围。这些机制可以使流量免于列入黑名单，但**不会**自动信任匹配流量或对其使用快速路径。在安全情报阶段已被列入白名单或受到监控的流量需要使用其余访问控制方法特意进行进一步的分析。

安全情报配置

如果要将特定IP地址、URL或域名列入白名单、黑名单或进行监控，则必须配置自定义对象、列表或源。您有以下选择：

- 要配置网络、URL 或 DNS 源，请参阅创建安全情报源，第 331 页。
- 要配置网络、URL 或 DNS 列表，请参阅更新安全情报列表，第 334 页。
- 要配置网络对象和对象组，请参阅创建网络对象，第 306 页。
- 要配置 URL 对象和对象组，请参阅创建 URL 对象，第 312 页。

根据 DNS 列表或源将流量列入黑名单、白名单或进行监控还要求：

- 创建 DNS 策略。有关详细信息，请参阅创建基本 DNS 策略，第 659 页。
- 配置引用 DNS 列表或源的 DNS 规则。有关详细信息，请参阅创建和编辑 DNS 规则，第 662 页。

由于DNS策略部署为访问控制策略的一部分，因此必须将两个策略均进行关联。有关详细信息，请参阅DNS 策略部署，第 668 页。

安全情报战略

安全情报战略包括使用：

- 思科提供的源 - 思科提供对定期更新的情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。
- 第三方源 - 可以使用第三方信誉源（通常是Firepower管理中心定期从互联网下载的动态列表）补充思科提供的源。
- 全局和自定义黑名单 - 将特定IP地址、URL或域名列入黑名单。为提高性能，您可能想要锁定执行目标，例如将列入垃圾邮件黑名单的范围限定于处理邮件流量的安全区域。
- 列入白名单以消除误报 - 当黑名单范围太宽泛或抢先阻止您想要使用其余访问控制方法进一步分析的流量时，可以使用自定义白名单覆盖黑名单。
- 监控而非列入黑名单 - 在被动部署中以及对于在实施源之前对其进行测试尤其有用；可以只监控并记录违规会话而不阻止它们，从而生成连接结束事件。

注释

在被动部署中，为优化性能，思科建议始终使用仅监控设置。被动部署的受管设备无法影响流量；与将系统配置为阻止流量相比，没有任何优势。此外，因为阻止的连接实际上在被动部署中并未被阻止，因此，系统可能针对每条已阻止连接报告多个连接开始事件。

示例：白名单

例如，如果信誉良好的源不适当地阻止对重要资源的访问，但其整体而言对于您的组织有用，则可以仅将分类不当的 IP 地址列入白名单，而不是从黑名单中删除整个源。

示例：按区域划分安全情报

您可以将分类不当的 URL 列入白名单，但随后使用您的组织中需要访问这些 URL 的人员所使用的安全区域来限制白名单对象。这样，只有有业务需要的人员才能访问列入白名单的 URL。或者，您可以使用第三方垃圾邮件源将邮件服务器安全区域上的流量列入黑名单。

示例：仅监控黑名单

考虑一下这样的情况，在使用第三方源实施阻止之前，想要先对该源进行测试。当将源设置为仅监控时，系统允许已被阻止的连接，以便系统能对其进行进一步的分析，但是也会记录这些连接中的每一个连接，以供进行评估。

配置安全情报

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

每个访问控制策略都具有安全情报选项。可以将网络对象、URL 对象和列表以及安全情报源和列表列入白名单或黑名单，全部都可通过安全区域进行限制。您还可以将DNS策略与访问控制策略相关联，并将域名列入白名单或黑名单。

注意 修改“安全情报”(Security Intelligence) 列表，但通过右键点击情景菜单上的**立即将 IP 列入白名单 (Whitelist IP Now)** 或**立即将 IP 列入黑名单 (Blacklist IP Now)** 选项进行修改除外，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

最多可以向白名单和黑名单添加总共 255 个网络对象以及 32767 个 URL 对象和列表。即，白名单中的对象数加上黑名单中的数量不能超过 255 个网络对象或 32767 个 URL 对象和列表。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 在被动部署中，或者如果要将安全情报过滤设置为仅监控，请启用日志记录；请参阅使用安全情报记录连接，第 1508 页。

过程

步骤 1 在访问控制策略编辑器中，点击**安全情报 (Security Intelligence)** 选项卡。
如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 您有以下选择：

- 点击**网络 (Networks)** 选项卡以添加网络对象。
- 点击 **URL** 选项卡以添加 URL 对象。

步骤 3 查找要添加到白名单或黑名单中的**可用对象 (Available Objects)**。您有以下选择：

- 通过在**按名称或值搜索 (Search by name or value)** 字段中输入内容，搜索可用对象。通过点击重新加载 ( ) 或清除 ( ) 来清除搜索字符串。
- 如果现有列表或源不满足需求，请点击添加图标 ( )，选择**新建网络列表 (New Network List)** 或**新建 URL 列表 (New URL List)**，然后继续操作，如创建安全情报源，第 331 页或将新的安全情报列表上传到 Firepower 管理中心，第 333 页中所述。
- 如果现有对象不满足需求，请点击添加图标 ( )，选择**新建网络对象 (New Network Object)** 或**新建 URL 对象 (New URL Object)**，然后继续操作，如创建网络对象，第 306 页中所述。

安全情报会忽略使用 /0 掩码的 IP 地址块。

步骤 4 在**可用对象 (Available Objects)** 中选择一个或多个要添加的可用对象。

步骤 5 或者通过选择一个**可用区域**，按区域限制选定对象。
不能按区域限制系统提供的安全情报列表。

步骤 6 点击**添加到白名单 (Add to Whitelist)** 或**添加到黑名单 (Add to Blacklist)**，或者点击所选对象并将其拖至任一列表。

要从白名单或黑名单中删除对象，请点击其删除图标 ( )。要删除多个对象，请选择这些对象并右键点击**删除所选项 (Delete Selected)**。

步骤 7 或者，右键单击 **Blacklist** 下的对象，然后选择 **Monitor-only (do not block)**，将列入黑名单的对象设置为仅监控。
不能将系统提供的安全情报列表设置为仅监控。

步骤 8 从 **DNS 策略 (DNS Policy)** 下拉列表中选择 DNS 策略。

注意 将自定义 DNS 策略与安全情报相关联在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。您可在访问控制策略中的“安全情报”(Security Intelligence) 选项卡上关联 DNS 策略。

步骤 9 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

安全情报选项

使用访问控制策略编辑器中的“安全情报”(Security Intelligence) 选项卡配置网络（IP 地址）和 URL 安全情报，以及将访问控制策略与 DNS 策略相关联。

对象、区域和黑名单图标

在访问控制策略编辑器的“安全情报”(Security Intelligence) 选项卡上，每种类型的对象或区域使用不同的图标进行区分。

在黑名单中，设置为阻止的对象标有阻止图标 ( )，而仅监控的对象标有监控图标 ( )。仅监控使得系统不仅可以使用访问控制处理涉及列入黑名单的 IP 地址和 URL 的连接，而且也会将连接的匹配项记录到黑名单。

因为白名单会覆盖黑名单，如果您向两个列表添加相同的对象，系统会显示带删除线的已列入黑名单对象。

区域限制

除系统提供的全局列表之外，您可以按照区域限制安全情报过滤。如要在多个区域上实施对象的安全情报过滤，对于每个区域，都必须将对象分别添加至白名单或黑名单。

日志记录

启用安全情报日志记录（默认情况下处于启用状态）会记录由访问控制策略的目标设备处理的所有受阻和受监控的连接。然而，系统不会记录白名单匹配项；列入白名单的连接的记录取决于其最终的性质。必须为列入黑名单的连接启用日志记录，然后才能将列入黑名单的对象设置为仅监控。

安全情报类别

Security Intelligence Category	说明
攻击者	出站恶意活动已知的活动扫描工具和列入黑名单的主机
Bogon	Bogon 网络和未分配的 IP 地址
Bots	托管二进制恶意软件丢弃程序的站点
CnC	托管僵尸网络的命令和控制服务器的站点
Dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法
Exploitkit	指定用于识别客户端中的软件漏洞的软件包

Security Intelligence Category	说明
恶意软件	托管恶意软件二进制或漏洞包的站点
OpenProxy	允许匿名 Web 浏览的开放代理
OpenRelay	已知用于垃圾邮件的开放邮件中继
网络钓鱼	托管网络钓鱼页面的站点
解决方案	主动参与恶意或可疑活动的 IP 地址和 URL
垃圾邮件	已知用于发送垃圾邮件的邮件主机
可疑	看似可疑并具有类似于已知恶意软件的特征的文件
TorExitNode	Tor 出口节点

第 39 章

DNS 策略

以下主题介绍 DNS 策略、DNS 规则，以及向受管设备部署 DNS 策略的方法。

DNS 策略概述

通过基于DNS的安全情报功能，您可以根据客户端请求的域名，将流量加入白名单或黑名单中。思科提供可用于过滤流量的域名情报；您还可以根据部署配置域名的自定义列表和源。

根据DNS策略列入黑名单的流量会被立即阻止，因此不会执行任何进一步入侵、攻击、恶意软件等检查，也不会用于网络发现。您可以使用白名单覆盖黑名单以强制执行访问控制规则评估，在被动部署中，建议您在安全情报过滤中使用“仅监控”(monitor-only) 设置。这使系统能够分析本应被列入黑名单的连接，但也将匹配项记录至黑名单并生成连接结束安全情报事件。

注释 基于 DNS 的安全情报可能无法为域名实现预期功能，除非 DNS 服务器由于到期删除域缓存条目，或者客户端的 DNS 缓存或本地 DNS 服务器的缓存被清除或已到期。

您可使用 DNS 策略及关联的 DNS 规则配置基于 DNS 的安全情报。要将配置部署到设备，您必须将 DNS 策略与访问控制策略相关联，然后将配置部署到受管设备。

DNS 策略组件

通过 DNS 策略，您可以根据域名将连接列入白名单或黑名单。以下列表介绍可在创建 DNS 策略后更改的配置。

名称和描述

每个 DSN 策略必须拥有唯一的名称。说明是可选的。

在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

Rules

规则提供一种基于域名处理网络流量的精细方法。DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。

创建 DNS 策略时，系统使用默认的“全局 DNS 白名单”(Global DNS Whitelist) 规则和默认的“全局 DNS 黑名单”(Global DNS Blacklist) 规则填充该策略。两个规则均固定到其各自类别中的第一个位置。您无法修改这些规则，但是可以将其禁用。

在多域部署中，系统还会将后代 DNS 白名单和后代 DNS 黑名单规则添加到后代域中的 NDS 策略。这些规则固定到其各自类别中的第一个位置。

注释 如果为 Firepower 管理中心启用多租户，则系统组成域的层次结构，包括祖先域和后代域。这些域截然不同并独立于 DNS 管理中所使用的域名。

后代列表包含由 Firepower 系统子域用户列入白名单或黑名单的域。从祖先域中，您无法查看后代列表的内容。如果您不希望子域用户将域列入白名单或黑名单，请执行以下操作：

- 禁用后代列表规则，并且
- 使用访问控制策略继承设置执行安全情报

系统按照以下顺序评估规则：

- “全局 DNS 白名单”(Global DNS Whitelist) 规则（如果启用）
- “后代 DNS 白名单”(Descendant DNS Whitelists) 规则（如果启用）
- “白名单”(Whitelist) 规则
- “全局 DNS 黑名单”(Global DNS Blacklist) 规则（如果启用）
- “后代 DNS 黑名单”(Descendant DNS Blacklists) 规则（如果启用）
- “黑名单”(Blacklist) 和“监控”(Monitor) 规则

通常，系统根据第一个 DNS 规则（其中所有规则的条件都与流量匹配）处理基于 DN 的网络流量。如果没有任何 DNS 规则与流量匹配，则系统根据关联的访问控制策略规则继续评估流量。DNS 规则条件可以简单，也可以复杂。

创建基本 DNS 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **DNS**。

步骤 2 点击**添加 DNS 策略 (Add DNS Policy)**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 或者，进一步配置新策略，如使用安全情报记录连接，第 1508 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

编辑 DNS 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

一个用户一次只能使用一个浏览器窗口编辑一个DNS策略。如果多个用户尝试保存同一策略，系统会仅保留第一组保存的更改。

为保护会话隐私，在策略编辑器上 30 分钟未执行任何操作之后，系统将显示警告。在 60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **DNS**。

步骤 2 点击要编辑的 DNS 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 要编辑 DNS 策略，请执行以下操作：

- 名称和说明 - 要更改名称或说明，请点击相应的字段并键入新信息。
- 规则 - 要添加、分类、启用、禁用或以其他方式管理 DNS 规则，请点击**规则 (Rules)** 选项卡，然后如创建和编辑 DNS 规则，第 662 页中所述继续操作。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

管理 DNS 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

使用“DNS 策略”(DNS Policy) 页面（**策略 (Policies)** > **访问控制 (Access Control)** > **DNS**）管理自定义 DNS 策略。除了您创建的自定义策略，系统会提供使用默认黑名单和白名单的默认 DNS 策略。您可以编辑并使用系统提供的这一自定义策略。在多域部署中，默认策略使用默认的全局DNS黑名单、全局 DNS 白名单、后代 DNS 黑名单和后代 DNS 白名单，并且只能在全局域中编辑。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **DNS**。

步骤 2 要管理 DNS 策略，请执行以下操作：

- 比较 - 要比较 DNS 策略，请点击**比较策略 (Compare Policies)**，然后如比较策略，第 261 页中所述继续操作。
- 复制 - 要复制 DNS 策略，请点击复制图标 ()，然后如编辑 DNS 策略，第 659 页中所述继续操作。
- 创建 - 要创建新的 DNS 策略，请点击**添加 DNS 策略 (Add DNS Policy)**，然后如创建基本 DNS 策略，第 659 页中所述继续操作。
- 删除 - 要删除 DSN 策略，请点击删除图标 ()，然后确认要删除策略。

- 编辑 - 要修改现有 DNS 策略，请点击编辑图标 ()，然后如编辑 DNS 策略，第 659 页中所述继续操作。

DNS 规则

DNS 规则根据主机请求的域名处理流量。作为安全情报的一部分，此评估发生在所有流量解密之后以及访问控制评估之前。

系统按照您指定的顺序将流量与DNS规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中规则的所有条件都与流量匹配）处理网络流量。创建DNS规则时，系统会将白名单规则放置在监控和黑名单规则之前，并先根据白名单规则评估流量。

除其唯一名称之外，每个 DNS 规则都具有以下基本组件：

省/自治区

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

DNS 策略中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。DNS 规则必须包含 DNS 源或列表条件，还可以按安全区域、网络或 VLAN 匹配流量。

操作

规则的操作确定系统如何处理匹配流量：

- 允许列入白名单的流量，需进一步进行访问控制检查。
- 受监控的流量将根据其余 DNS 黑名单规则进行进一步评估。如果流量不匹配 DNS 黑名单规则，则将使用访问控制规则进行检查。系统会记录流量的安全情报事件。
- 列入黑名单的流量将被丢弃，无需进一步检查。您还可以返回“找不到域”(Domain Not Found)响应，或将 DNS 查询重定向到 Sinkhole 服务器。

创建和编辑 DNS 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

在 DNS 策略中，最多可以向白名单和黑名单规则中添加总共 32767 个 DNS 列表；即，DNS 策略中的列表数不能超过 32767。

过程

步骤 1 在 DNS 策略编辑器中，可进行以下选择：

- 要添加新规则，请点击**添加 DNS 规则 (Add DNS Rule)**。
- 要编辑现有规则，请点击编辑图标 ( )。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分，或接受默认值：

- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅DNS 规则操作，第 664 页。
- 条件 - 配置规则的条件；请参阅DNS 规则条件，第 665 页。
- 已启用 - 指定规则是否为**已启用 (Enabled)**。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

DNS 规则管理

通过 DNS 策略编辑器的**规则 (Rules)** 选项卡，您可以添加、编辑、移动、启用、禁用、删除或以其他方式管理策略中的 DNS 规则。

对于每个规则，策略编辑器会显示其名称和条件摘要，以及规则操作。其他图标表示警告 ( )、错误 ( ) 和其他重要信息 ( )。已禁用的规则在规则名称下方呈灰色显示并带有相应的标记 `(disabled)`。

启用和禁用 DNS 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

创建DNS规则时，默认情况下会启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。查看DNS策略中的规则列表时，已禁用的规则呈灰色显示，但这些规则仍可以修改。请注意，也可使用 DNS 规则编辑器启用或禁用 DNS 规则。

过程

步骤 1 在 DNS 策略编辑器中，右键点击规则并选择规则状态。

步骤 2 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

DNS 规则顺序评估

DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中所有规则的条件都与流量相匹配）处理网络流量。

- 对于“监控”(Monitor) 规则，系统会记录流量，然后根据优先级较低的 DNS 黑名单规则继续评估流量。
- 对于非“监控”(Monitor) 规则，在流量匹配规则后系统不会根据其他优先级较低的 DNS 规则继续评估流量。

对规则排序时，请注意：

- “全局白名单”(Global Whitelist) 始终排在首位，优先于所有其他规则。
- “后代 DNS 白名单”(Descendant DNS Whitelists) 规则仅在多域部署的非枝叶域中显示。它始终排在第二位，且优先于除“全局白名单”(Global Whitelist) 之外的所有其他规则。
- “白名单”(Whitelist) 部分优先于“黑名单”(Blacklist) 部分；白名单规则始终优先于其他规则。
- “全局黑名单”(Global Blacklist) 始终排在“黑名单”(Blacklist) 部分的首位，优先于所有其他“监控”(Monitor) 和黑名单规则。

- “后代 DNS 黑名单”(Descendant DNS Blacklists) 规则仅在多域部署的非枝叶域中显示。它始终排在“黑名单”(Blacklist) 部分的第二位，且优先于除“全局黑名单”(Global Blacklist) 之外的所有其他“监控”(Monitor) 和黑名单规则。
- “黑名单”(Blacklist) 部分包含“监控”(Monitor) 和黑名单规则。
- 首次创建 DNS 规则时，如果分配**白名单 (Whitelist)** 操作，系统会将其放在“白名单”(Whitelist) 部分的最后；如果分配任何其他操作，模块会将其放在“黑名单”(Blacklist) 部分的最后。

可以通过拖放规则来为规则重新排序。

DNS 规则操作

每个 DNS 规则都有确定匹配流量的以下过程的操作：

- 处理 - 首先，规则操作管理系统是否将与规则条件匹配的流量列入白名单、监控或黑名单。
- 日志记录 - 该规则操作确定何时以及如何记录有关匹配的流量的详细信息

请记住，只有内联部署的设备才可以将流量列入黑名单。被动部署或在分流模式下部署的设备可以记录流量并将其列入白名单，但是不影响流量。

“白名单”(Whitelist) 操作

白名单 (Whitelist) 操作允许匹配的流量通过。将流量列入白名单时，系统会根据与访问控制规则的匹配情况或访问控制策略的默认操作进行进一步检查。

系统不会记录白名单匹配项。但是，是否记录列入白名单的连接取决于其最终的安全状态。

“监控”(Monitor) 操作

监控 (Monitor) 操作不影响流量；匹配的流量既不会被立即列入白名单，也不会被立即列入黑名单。更确切地是，根据其他规则匹配流量以确定允许还是拒绝该流量。所匹配的第一个非“监控”(Monitor) DNS 规则可确定系统是否将流量列入黑名单。如果没有其他匹配的规则，流量会进行访问控制评估。

对于 DNS 策略监控的连接，系统会记录连接结束的安全情报和 Firepower 管理中心数据库的连接事件。

“黑名单”(Whitelist) 操作

黑名单操作会将流量列入黑名单，无需任何类型的进一步检查：

- **丢弃 (Drop)** 操作会丢弃流量。
- **找不到域 (Domain Not Found)** 操作会针对 DNS 查询返回“不存在的互联网域”响应，防止客户端解析 DNS 请求。
- **Sinkhole** 操作会返回 Sinkhole 对象的 IPv4 或 IPv6 地址以响应 DNS 查询。Sinkhole 服务器可以记录或记录并阻止 IP 地址的后续连接。如果配置 **Sinkhole** 操作，还必须配置 Sinkhole 对象。

对于根据**丢弃 (Drop)** 或**找不到域 (Domain Not Found)** 操作列入黑名单的连接，系统会记录连接开始的安全情报和连接事件。因为列入黑名单的流量会被立即拒绝，无需进一步检测，所以，没有要记录的唯一连接终止。

对于根据 **Sinkhole** 操作列入黑名单的连接，日志记录取决于 Sinkhole 对象配置。如果将 Sinkhole 对象配置为仅记录 Sinkhole 连接，则系统会记录后续连接的连接结束的连接事件。如果将 Sinkhole 对象配置为记录并阻止 Sinkhole 连接，则系统会记录后续连接的连接开始的连接事件，然后阻止该连接。

注释 在 ASA FirePOWER 设备上，如果您使用 Sinkhole 操作配置 DNS 规则且流量匹配规则，则默认情况下 ASA 会阻止后续 Sinkhole 连接。对此的解决方法是，从 ASA 命令行运行以下命令：

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
```

如果 ASA 继续阻止连接，请联系支持部门。

DNS 规则条件

DNS 规则的条件识别该规则处理的流量的类型。条件可以简单，也可以复杂。您必须在 DNS 规则中定义 DNS 源或列表条件。还可以选择按安全区域、网络或 VLAN 控制流量。

将条件添加到 DNS 规则时：

- 如果不为规则配置特定条件，系统将不基于此标准匹配流量。
- 您可以为每个规则配置多个条件。为使规则应用于流量，流量必须匹配规则中的**所有**条件。例如，包含 DNS 源或列表条件和网络条件，但没有 VLAN 标记条件的规则会根据域名以及源或目标评估流量，无论会话采用任何 VLAN 标记。
- 可以为规则中的每个条件最多可以添加 50 个标准。匹配**所有**条件的标准的流量满足该条件。例如，您可以使用单一规则根据最多 50 个 DNS 列表和源将流量列入黑名单。

根据 DNS 和安全区域控制流量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

通过DNS规则中的区域条件，您可以根据其源和目标安全区域控制流量。安全区域是一个或多个接口的分组，可位于多个设备之间。在设备的初始设置过程中，您选择的称为其检测模式的选项，可以确定系统如何对该设备的接口进行初始配置，以及那些接口是否属于安全区域。

过程

步骤 1 在 DNS 规则编辑器中，点击**区域 (Zones)** 选项卡。

步骤 2 从 **Available Zones** 中查找并选择您想要添加的区域。要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

步骤 3 点击选择一个区域，或右键点击，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 5 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

根据 DNS 和网络控制流量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

DNS 规则中的网络条件可以根据源 IP 地址控制流量。您可以为要控制的流量显式指定源 IP 地址。

过程

步骤 1 在 DNS 规则编辑器中，点击**网络 (Networks)** 选项卡。

步骤 2 从 **Available Networks** 中查找并选择您想要添加的网络，如下所示：

- 要即时添加可随后添加到条件中的网络对象，请点击**可用网络 (Available Networks)** 列表上方的添加图标 ( )，然后如创建网络对象，第 306 页中所述继续操作。
- 要搜索要添加的网络对象，请点击**可用网络 (Available Networks)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象名称或对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 4 添加要手动指定的任何源 IP 地址或地址块。点击**源网络 (Source Networks)** 列表下方的**输入 IP 地址 (Enter an IP address)** 提示，然后键入 IP 地址或地址块，并点击**添加 (Add)**。
系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

根据 DNS 和 VLAN 控制流量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

通过 DNS 规则中的 VLAN 条件，您可以控制 VLAN 标记流量。系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。

构建基于 VLAN 的 DNS 规则条件时，可以手动指定 VLAN 标记。或者，也可以使用 VLAN 标记对象配置 VLAN 条件，这些对象可重用，并会将名称与一个或多个 VLAN 标记相关联。

过程

步骤 1 在 DNS 规则编辑器中，选择 **VLAN 标记 (VLAN Tags)** 选项卡。

步骤 2 查找并选择您要从 **Available VLAN Tags** 添加的 VLAN，如下所述：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击“可用 VLAN 标记”(Available VLAN Tags) 列表上方的添加图标 () 并继续操作，如创建 VLAN 标记对象，第 311 页中所述。
- 要搜索要添加的 VLAN 标记对象和组，请点击**可用 VLAN 标记 (Available VLAN Tags)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的一个 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 添加要手动指定的任何 VLAN 标记。点击 **Selected VLAN Tags** 列表下方的 **Enter a VLAN Tag** 提示，然后键入 VLAN 标记或范围并点击 **Add**。可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。
系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

根据 DNS 列表、源或类别控制流量

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

如果 DNS 列表、源或类别包含客户端请求的域名，则 DNS 规则中的 DNS 条件可用于控制流量。您必须在 DNS 规则中定义 DNS 条件。

无论向 DNS 条件中添加全局或自定义白名单还是黑名单，系统都会将所配置的规则操作应用于流量。例如，如果向规则中添加全局白名单，并配置**丢弃 (Drop)** 操作，则系统会将应已列入白名单的所有流量都列入黑名单。

过程

步骤 1 在 DNS 规则编辑器中，点击 **DNS** 选项卡。

步骤 2 从 **DNS 列表和源 (DNS Lists and Feeds)** 中查找并选择要添加的 DNS 列表和源，如下所示：

- 要动态添加可随后添加到条件中的 DNS 列表和源，请点击 **DNS 列表和源 (DNS Lists and Feeds)** 列表上方的添加图标 ( )，然后如创建安全情报源，第 331 页中所述继续操作。
- 要搜索将添加的 DNS 列表、源或类别，请点击 **DNS 列表和源 (DNS Lists and Feeds)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象名称或其中一个对象的组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

DNS 策略部署

智能许可证	经典许可证	支持的设备	支持的域
威胁	保护	任何环境	任何环境

完成 DNS 策略配置更新后，您必须将其部署为访问控制配置的一部分。

- 将 DNS 策略与访问控制策略相关联，如配置安全情报，第 653 页中所述。

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 40 章

智能应用绕行 (IAB)

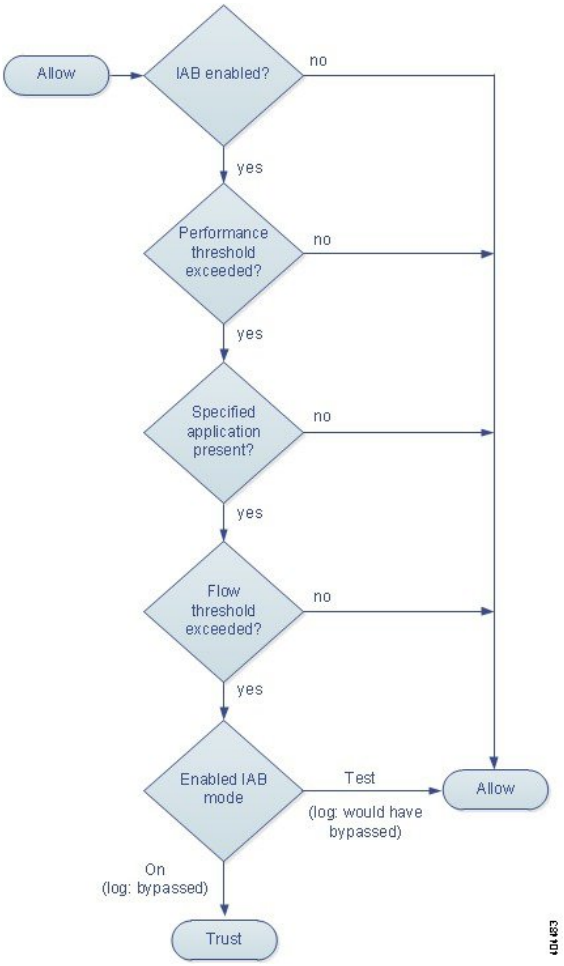
以下主题介绍如何配置访问控制策略以使用智能应用绕行：

IAB 简介

智能应用绕行 (IAB) 可识别您信任其流经您的网络而无需进一步检查（如果超出性能和数据流阈值）的应用。例如，如果每次晚间的备份会显著影响系统的性能，您可以配置某些阈值，当超过这些阈值时则信任备份应用产生的流量。

在对流量进行深度检查之前，系统会对访问控制规则或访问控制策略的默认操作所允许的流量实施 IAB。您可以通过一种测试模式确定是否已超过阈值，如果已超过，则识别出在您实际启用了 IAB 的情况下会被绕过的应用数据流（称为绕行模式）。

下图展示 IAB 决策过程：



配置 IAB

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员 访问管理员 网络管理员

注意 并非所有部署都需要IAB，而那些需要IAB的部署也仅以有限的方式进行使用。除非您具备网络流量（特别是应用流量）和系统性能（包括可预测的性能问题的原因）方面的专业知识，否则不要启用 IAB。在绕行模式下运行 IAB 之前，请确保信任指定的流量不会使您处于风险中。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，然后点击**智能应用绕行设置 (Intelligent Application Bypass Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 配置 IAB 选项：

- 状态 (State) - **关闭**或**打开** IAB，或在**测试**模式下启用 IAB。
- 性能采样间隔 (Performance Sample Interval) - 输入 IAB 性能采样扫描之间的间隔时间（以秒为单位）。如果启用 IAB，即使在测试模式下，也请输入非零值。输入 0 可禁用 IAB。
- 可绕行的应用和过滤器 (Bypassable Applications and Filters) - 点击绕过的应用和过滤器数量并指定要绕过其流量的应用；请参阅配置应用条件和过滤器，第 277 页。
- 检查性能阈值 (Inspection Performance Thresholds) - 点击**配置 (Configure)** 并输入至少一个阈值。
- 流绕行阈值 (Flow Bypass Thresholds) - 点击**配置 (Configure)** 并输入至少一个阈值。

必须指定至少一个检查性能阈值和一个流绕行阈值；必须超过这两个阈值，IAB 才可信任流量。如果为每种类型输入多个阈值，则仅必须超过每种类型的一个阈值。有关详细信息，请参阅IAB 选项，第 673 页。

步骤 3 点击**确定 (OK)** 保存 IAB 设置。

步骤 4 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

IAB 选项

省/自治区

启用或禁用 IAB。

选择项	说明
关闭	禁用 IAB。
测试	在测试模式下启用 IAB。连接事件和自定义控制面板构件会记录会在绕行模式下绕过的流量。

选择项	说明
On（打开）	在绕行模式下启用 IAB。连接事件和自定义控制面板构件会记录超过配置的阈值时可靠地流经网络的流量。

性能采样间隔 (Performance Sample Interval)

指定两次 IAB 性能采样扫描间隔的时间（秒），系统会在此期间收集系统性能指标以与 IAB 性能阈值进行比较。值 0 会禁用 IAB。

可绕行应用和过滤器 (Bypassable Applications and Filters)

提供您可以在其中指定可绕行应用和应用集（过滤器）的编辑器。请参阅应用条件（应用控制），第 276 页。

检查性能阈值 (Inspection Performance Thresholds)

检查性能阈值提供入侵检查性能限值，如果超过该限值，则会触发流阈值检查。IAB 不使用设置为 0 的检查性能阈值。

注释 如果启用多个性能或流阈值，则必须超过至少一个类型的阈值，才能使IAB考虑是否信任流量。

丢弃百分比 (Drop Percentage)

因昂贵入侵规则、文件策略、解压等引起的性能过载导致的数据包丢弃时，丢弃的平均数据包数占总数据包数的百分比。这并不是指入侵规则等正常配置丢弃的数据包数。请注意，当丢弃指定百分比的数据包时，指定大于 1 的整数会激活 IAB。指定 1 时，任何从 0 到 1 的百分比都会激活 IAB。这允许少量数据包激活 IAB。

处理器利用率百分比 (Processor Utilization Percentage)

使用的处理器资源的平均百分比。

数据包延迟 (Package Latency)

平均数据包延迟（微秒）。

流量

系统处理流的速率，以每秒的流数进行测量。请注意，此选项可配置 IAB 以测量流速率，而不是流计数。

流绕行阈值 (Flow Bypass Thresholds)

流绕行阈值提供流限值，如果超过该限值，则会触发 IAB 信任绕行模式下的可绕行应用流量或允许应用流量在测试模式下接受进一步检查。IAB 不使用设置为 0 的流绕行阈值。

注释 如果启用多个性能或流阈值，则必须超过至少一个类型的阈值，才能使IAB考虑是否信任流量。

单位流字节数 (Bytes per Flow)

一个流可以包含的最大千字节数。

单位流数据包数 (Packets per Flow)

一个流可以包含的最大数据包数。

流持续时间 (Flow Duration)

一个流保持开放的最大秒数。

流速 (Flow Velocity)

最高传输速率（千字节/秒）。

IAB 日志记录和分析

无论是否启用连接日志记录，IAB 都会强制连接结束事件记录已绕过的流和应已绕过的流。连接事件指示在绕行模式下绕过的流或在测试模式下应已绕过的流。基于连接事件的自定义控制面板构件和报告可以显示已绕过和应已绕过的流的长期统计信息。

IAB 连接事件

操作

当**原因 (Reason)** 包括 `Intelligent App Bypass` 时：

Allow -

指示已应用的 IAB 配置处于测试模式，并且**应用协议 (Application Protocol)** 指定的应用的流量仍可供检查。

Trust -

指示已应用的 IAB 配置处于绕行模式，并且**应用协议 (Application Protocol)** 指定的应用的流量受信任，可流经网络而不进行进一步检查。

Reason

`Intelligent App Bypass` 指示 IAB 在绕行或测试模式下触发了事件。

应用协议

此字段显示触发了事件的应用协议。

示例

在以下截断的图形中，某些字段已省略。该图形显示根据两个单独访问控制策略中的不同 IAB 设置产生的两个连接事件的**操作 (Action)**、**原因 (Reason)** 和**应用协议 (Application Protocol)** 字段。

对于第一个事件，`Trust` 操作指示 IAB 在绕行模式下已启用，并且 Bonjour 协议流量受信任可通过而不进行进一步检查。

对于第二个事件，`Allow` 操作指示 IAB 在测试模式下已启用，因此 Ubuntu 更新管理器流量会接受进一步检查，但如果 IAB 在绕行模式下已启用，则应已绕过该流量。

示例

在以下截断的图形中，某些字段已省略。第二个事件中的流同时按照入侵规则（**原因 [Reason]**：`Intrusion Monitor`）进行绕过（**操作 [Action]**：`Trust`；**原因 [Reason]**：`Intelligent App Bypass`）和检查。`Intrusion Monitor` 原因指示检测到设置为**生成事件 (Generate Events)** 的入侵规则，但在连接过程中未阻止漏洞。在示例中，此情况发生在检测到应用之前。在检测到应用后，IAB 将应用识别为可绕过且受信任的流。

IAB 自定义控制面板构件

可以创建自定义分析控制面板构件以根据连接事件显示长期 IAB 统计信息。创建构件时，请指定以下信息：

- **预设 (Preset)**：`None`
- **表 (Table)**：`Application Statistics`
- **字段 (Field)**：any
- **汇聚 (Aggregate)**：以下任一：

  `IAB Bypassed Connections`

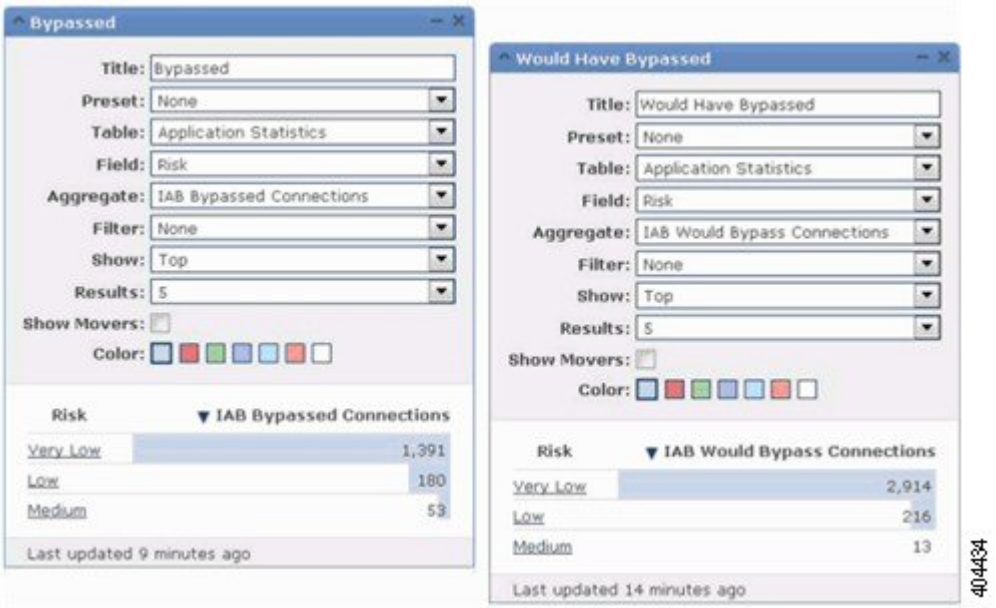
  `IAB Would Bypass Connections`

- **过滤器 (Filter)**：any

示例

在以下自定义分析控制面板构件示例中：

- “已绕过”示例显示由于在已部署的访问控制策略中应用指定为可绕过且IAB在绕行模式下已启用而绕过的应用流量的统计信息。
- “应已绕过”示例显示由于在已部署的访问控制策略中应用指定为可绕过且IAB在测试模式下已启用而应已绕过的应用流量的统计信息。.



IAB 自定义报告

可以创建自定义报告以根据连接事件显示长期 IAB 统计信息。创建报告时，请指定以下信息：

- **表 (Table)**：`Application Statistics`
- **预设 (Preset)**：`None`
- **过滤器 (Filter)**：any
- **X 轴 (X-Axis)**：any
- **Y 轴 (Y-Axis)**：以下任一：

```
IAB Bypassed Connections

IAB Would Bypass Connections
```

示例

下图中显示两个缩写的报告示例：

- “已绕过”示例显示由于在已部署的访问控制策略中应用指定为可绕过且IAB在绕行模式下已启用而绕过的应用流量的统计信息。
- “应已绕过”示例显示由于在已部署的访问控制策略中应用指定为可绕过且IAB在测试模式下已启用而应已绕过的应用流量的统计信息。

第 XII 部分

加密流量的处理

第 41 章

了解流量解密

以下主题概述 SSL 检查，介绍 SSL 检查配置的前提条件，并详细说明部署场景。

流量解密概述

默认情况下，系统无法检查使用安全套接字层 (SSL) 协议或其后续的传输层安全 (TLS) 协议加密的流量。借助 *SSL* 检查功能，您可以阻止已加密流量而不进行检查，或者使用访问控制检查已加密或解密的流量。系统在处理已加密会话时会记录流量的详细信息。检查已加密流量与分析已加密会话数据双管齐下，可以更好地了解和控制网络中的已加密应用和流量。

SSL 检查是一种基于策略的功能。在 Firepower 系统中，访问控制策略是一种可调用子策略和其他配置（包括 SSL 策略）的主配置。如果将 SSL 策略与访问控制相关联，则系统会在使用访问控制规则评估加密会话前使用该 SSL 策略对其进行处理。如果没有配置 SSL 检查或设备不支持，则访问控制规则将处理所有加密流量。

请注意，当您的 SSL 检查配置允许加密流量通过时，访问控制规则也会对其进行处理。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

如果系统通过 TCP 连接检测到 SSL 握手，则其会确定是否可以解密检测到的流量。如果不能，则将应用已配置的操作：

- 阻止已加密流量
- 阻止已加密流量并重置 TCP 连接
- 不解密已加密的流量

如果系统能够解密流量，则它将阻止流量而不进行进一步检查、使用访问控制评估未解密流量或使用以下方法之一解密该流量：

- 采用已知的私钥解密。在外部主机启动与网络上某台服务器的SSL握手时，系统将交换的服务器证书与之前上载至设备的服务器证书相匹配。然后使用上载的私钥解密流量。
- 通过重签服务器证书进行解密。在网络上的某台主机启动与外部服务器的SSL握手时，系统将使用之前上载的证书颁发机构 (CA) 证书重签交换的服务器证书。然后使用上载的私钥解密流量。

已解密流量将受到与原先未加密流量相同的流量处理和分析：基于网络、信誉和用户的访问控制；入侵检测和防御；思科高级恶意软件防护（思科AMP）以及发现。如果系统在分析已解密流量后未阻止该流量，则会重新对其加密，然后再将其传递到目标主机。

SSL 检查要求

SSL 检查需要一台 7000 或 8000 系列设备，或一个 ASA FirePOWER 模块。

除了您的配置设置和许可证之外，如何在网络中部署设备也会影响到您控制和解密已加密流量时可以采取的操作。请审查您的映射操作列表、现有网络部署和总体要求以确定是否有一种或其他类型的部署更适合贵组织。

用内联、路由式、交换式或混合接口配置和部署的设备可以修改流量。这些设备可以监控、阻止、允许和解密入站和出站流量。

用被动或内联（分路模式）接口配置和部署的设备无法影响流量。这些设备只能监控、允许和解密入站流量。请注意，被动部署不支持解密采用瞬时 Diffie-Hellman (DHE) 或椭圆曲线 Diffie-Hellman (ECDHE) 密码套件加密的流量。

SSL检查需要公钥证书和配对的私钥才能执行某些功能。您必须将证书和配对的私钥上载到Firepower管理中心以根据加密会话特性解密和控制流量。

SSL 规则配置必备条件信息

SSL 检查依赖于大量支持公钥基础架构 (PKI) 信息。考虑贵组织的流量模式以确定可配置的匹配规则条件。

表 *70*: *SSL* 规则条件必备条件

要匹配…	收集…
检测到的服务器证书，包括自签的服务器证书	服务器证书
受信任的服务器证书	CA 证书
检测到的服务器证书主体或颁发机构	服务器证书主体 DN 或颁发机构 DN

决定是否不解密、阻止、监控或解密作为您匹配规则之依据的已加密流量。将这些决策映射至 SSL 规则操作、无法解密的流量操作和 SSL 策略默认操作。

表 *71*: *SSL* 解密必备条件

要解密…	收集...
您控制的服务器的入站流量	服务器证书文件和配对的私钥文件
外部服务器的出站流量	CA 证书文件和配对的私钥文件 还可以生成 CA 证书和私钥。

在您收集此信息后，请将其上载到系统并配置可重复使用的对象。

SSL 检查设备部署情景

本小节提供了若干情景，在其中 Life Insurance Example, Inc. life insurance company (LifeIns) 对已加密流量使用 SSL 检查以帮助审核其流程。根据其业务流程，LifeIns 计划部署：

- 被动部署中的一台 7000 或 8000 系列设备，供客户服务部门使用
- 内联部署中的一台 7000 或 8000 系列设备，供保险部门使用
- 用于管理上述两台设备的一台Firepower 管理中心

客户服务业务流程

LifeIns 为客户创建了面向客户的网站。LifeIns 通过其网站和邮件接收来自潜在客户的有关保单的已加密问题和请求。LifeIns的客户服务部门在24小时内处理并返回请求的信息。客户服务部门希望扩展其传入联络指标收集LifeIns 已为客户服务部门建立内部审核机制。

LifeIns还在线接收已加密的应用。客户服务部门在将案例文件发送到保险部门之前，在24小时内处理申请。客户服务部门过滤出通过在线表单发送的所有明显错误的申请，这将消耗他们不少时间。

保险业务流程

LifeIns 的保险员在线向 Medical Repository Example，LLC medical data repository （MedRepo ）提交已加密的医疗信息请求。MedRepo 在 72 小时内审查该请求并将已加密记录传输到 LifeIns。保险员随后签署接受申请并提交保单和费率决定。保险部门希望扩展其指标收集。

最近，未知源总是发送欺骗响应到LifeIns。虽然LifeIns的保险员接受过正确使用互联网的培训，但 LifeIns 的 IT 部门首先要分析采用医疗响应形式的所有已加密流量，然后要阻止所有欺骗尝试。

LifeIns对初级保险员提供六个月的培训。最近，这些保险员错误地向MedRepo的客户服务部门提交了已加密的医疗法规请求。作为回应，MedRepo 多次向 LifeIns 提出投诉。LifeIns 计划延长这些新保险员的培训期，并且审核保险员对 MedRepo 提交的请求。

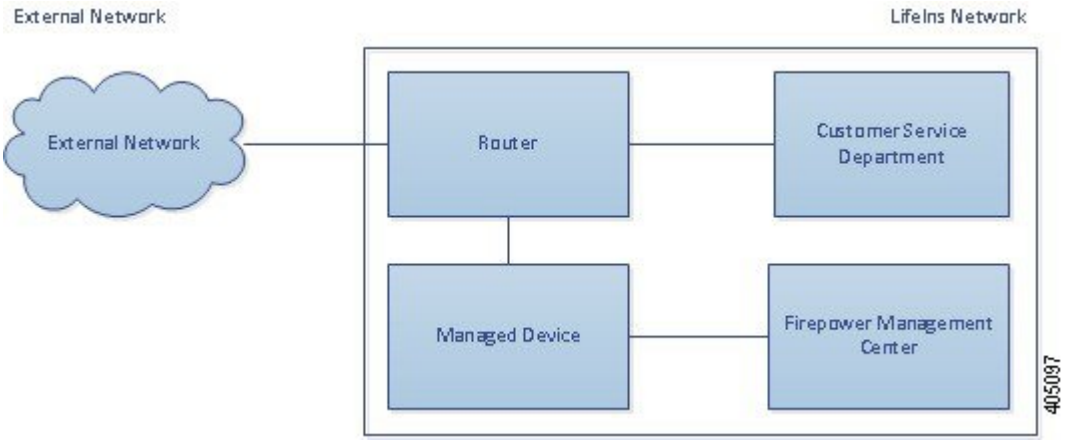
被动部署中的流量解密

LifeIns 的业务要求客户服务部门必须：

- 在 24 小时内处理所有请求和申请
- 改善其传入联系指标收集流程
- 标识并丢弃传入错误申请

客户服务部门无需额外的审核。

LifeIns 计划以被动方式部署客户服务部门的受管设备。



来自外部网络的流量进入 LifeIns 的路由器。该路由器将流量路由到客户服务部门并将流量的副本镜像到受管设备进行检查。

在管理Firepower 管理中心上，具有访问控制和 SSL 编辑器自定义角色的用户配置 SSL 检查完成以下任务：

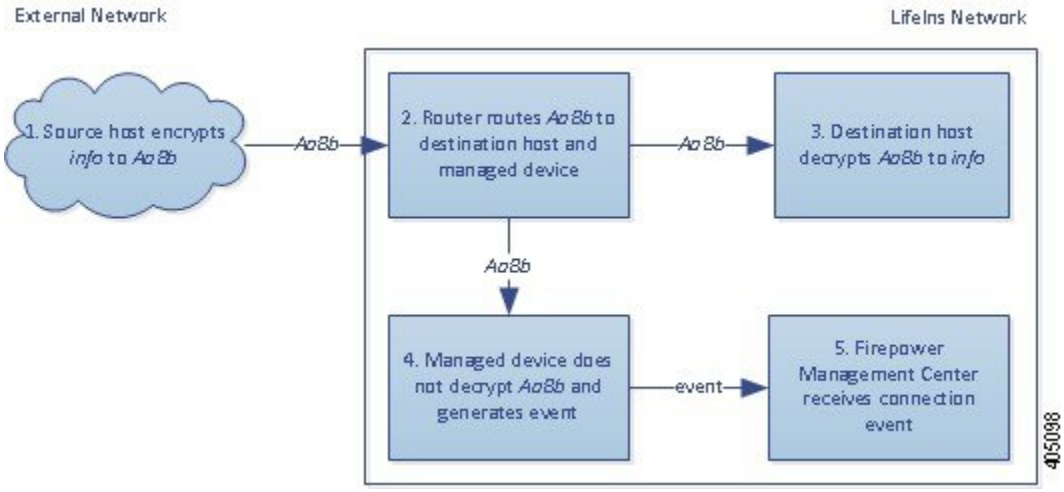
- 记录发送到客户服务部门的所有已加密流量
- 解密使用在线申请表发送到客户服务部门的已加密流量
- 不解密发送到客户服务部门的所有其他已加密流量，包括使用在线请求表发送的流量

用户也可以配置访问控制以检查已加密的申请表流量是否存在虚假的申请数据，并在检测到虚假数据时予以记录。

在以下情景中，用户向客户服务部门提交在线表单。用户的浏览器建立与服务器的 TCP 连接，然后启动 SSL 握手。受管设备接收该流量的副本。客户端和服务器完成 SSL 握手，建立已加密会话。系统根据握手和连接详情记录连接并对已加密流量的副本执行操作。

被动部署中的加密流量监控

对于发送到客户服务部门的所有 SSL 加密流量，受管设备都会记录连接。



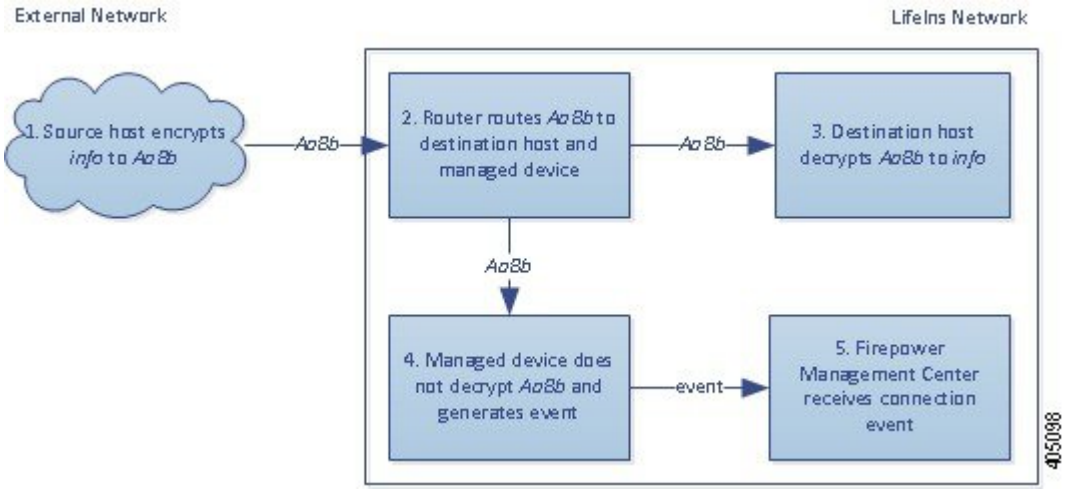
发生接下来的步骤：

1. 用户提交纯文本请求 (`info`)。客户端加密此 (`AaBb`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`info`)。
4. 受管设备不解密流量。

   访问控制策略继续处理已加密的流量并允许其通过。设备在会话结束后生成连接事件。
5. Firepower 管理中心 接收连接事件。

被动部署中未解密的已加密流量

对于包含有关策略的请求的所有 SSL 加密流量，设备允许该流量通过而不将其解密，并会记录连接。



发生接下来的步骤：

1. 用户提交纯文本请求 (`info`)。客户端加密此 (`AaBb`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`info`)。
4. 受管设备不解密流量。

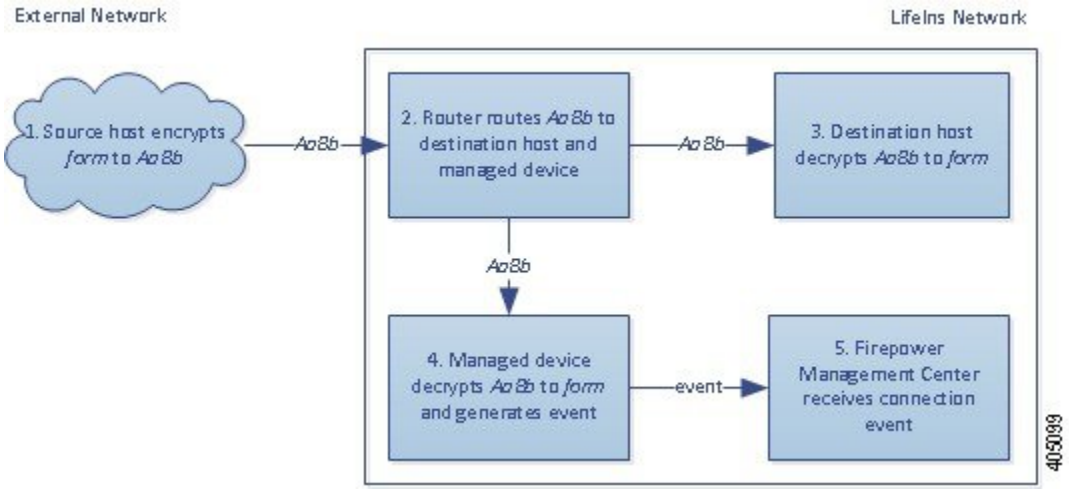
   访问控制策略继续处理已加密的流量并允许其通过。设备在会话结束后生成连接事件。
5. Firepower 管理中心 接收连接事件。

在被动部署中使用私钥检查已加密的流量

对于包含申请表单数据的所有 SSL 加密流量，系统均解密该流量加密并记录连接。

注释 在被动部署中，如果流量采用 DHE 或 ECDHE 密码套件加密，则您无法使用已知私钥解密该流量。

对于包含合法的申请表信息的流量，系统将记录连接。

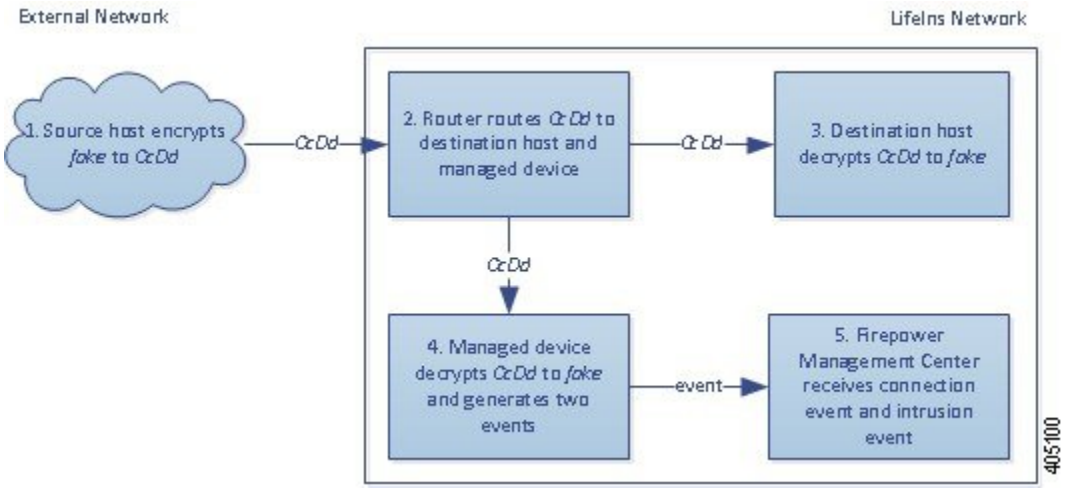


发生接下来的步骤：

1. 用户提交纯文本请求 (`form`)。客户端加密此 (`AaBb`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密信息请求 (`AaBb`) 并将其解密为纯文本 (`form`)。
4. 受管设备使用通过上载的已知私钥获取的会话密钥将该已加密流量解密为纯文本 (`form`)。

   访问控制策略继续处理已解密的流量且不查找虚假的申请信息。设备在会话结束后生成连接事件。
5. Firepower 管理中心接收包含有关已加密和解密流量的信息的连接事件。

相反，如果已解密流量包含虚假申请数据，则系统记录连接和虚假数据。



发生接下来的步骤：

1. 用户提交纯文本请求 (`fake`)。客户端加密此 (`CcDd`) 并将已加密流量发送到客户服务部门。
2. LifeIns 的路由器接收已加密流量并将其路由到客户服务部门服务器。它还将副本镜像到受管设备。
3. 客户服务部门服务器接收已加密的信息请求 (`CcDd`) 并将其解密为纯文本 (`fake`)。
4. 受管设备使用通过上载的已知私钥获取的会话密钥将此已加密流量解密为纯文本 (`fake`)。

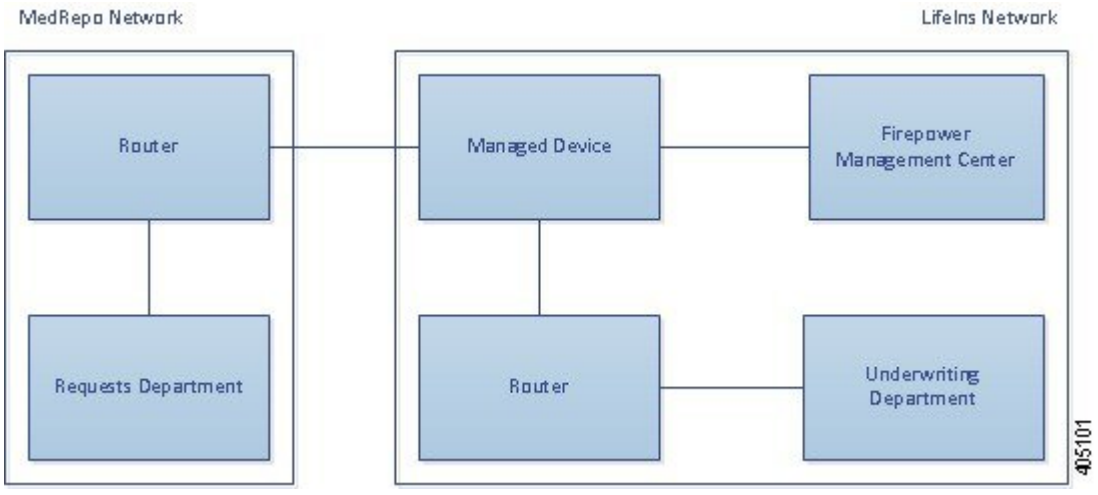
   访问控制策略继续处理已解密的流量并查找虚假的申请信息。设备生成入侵事件。设备在会话结束后生成连接事件。
5. Firepower 管理中心接收包含有关已加密和解密流量的信息的连接事件，以及虚假申请数据的入侵事件。

内联部署中的流量解密

LifeIns 的业务要求规定保险部门必须：

- 审核新的和初级保险员，确认其提交给 MedRepo 的信息请求符合所有适用的法规
- 改善其保险指标收集流程
- 检查似乎来自 MedRepo 的所有请求，然后丢弃所有欺骗尝试
- 丢弃从保险部门发送到 MedRepo 客户服务部门的所有不当法规请求
- 不审核高级保险员

LifeIns 计划在内联部署中部署一台设备供保险部门使用。



来自 MedRepo 网络的流量进入 LifeIns 的路由器。该路由器将流量路由到 LifeIns 的网络。受管设备接收流量，将允许的流量传递到 LifeIns 的路由器，并向管理Firepower 管理中心发送事件。LifeIns 的路由器将流量路由到目标主机。

在管理Firepower 管理中心上，具有访问控制和 SSL 编辑器自定义角色的用户配置 SSL 检查完成以下任务：

- 记录发送到保险部门的所有已加密流量
- 阻止从 LifeIns 的保险部门错误发送到 MedRepo 客户服务部门的所有已加密流量
- 解密从 MedRepo 发送到 LifeIns 的保险部门以及从 LifeIns 的初级保险员发送到 MedRepo 的请求部门的所有已加密流量
- 不解密从高级保险员发送的已加密流量

用户还可以将访问控制配置为使用自定义入侵策略检查已解密的流量，并且：

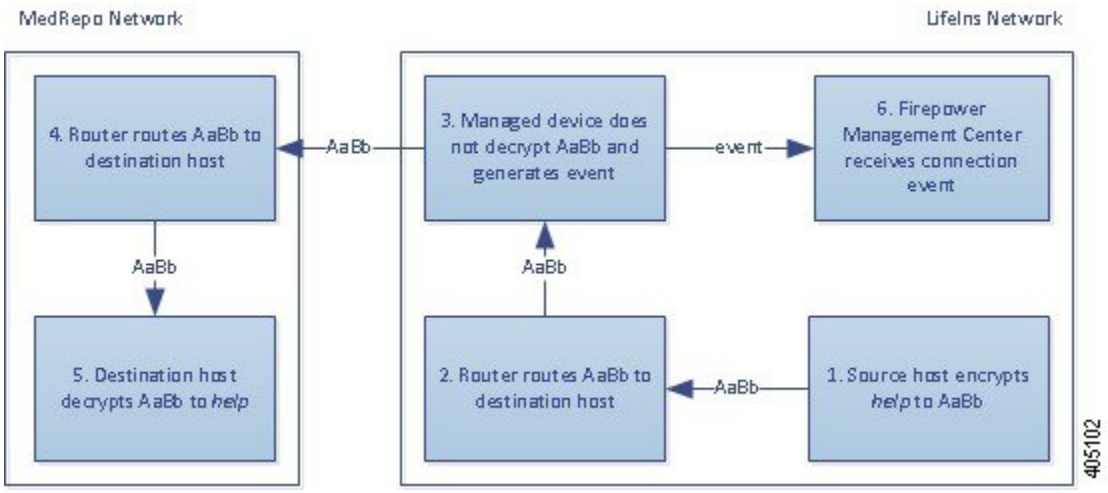
- 如果已解密流量包含欺骗尝试，则将其阻止并记录欺骗尝试
- 阻止包含不符合法规的信息的已解密流量，并记录不当信息
- 允许所有其他的已加密和已解密流量

系统在将允许的已解密流量发送到目标主机之前对其重新加密。

在以下情景中，用户在线向远程服务器提交信息。用户的浏览器建立与服务器的 TCP 连接，然后启动 SSL 握手。受管设备接收此流量；系统基于握手和连接详情记录连接并对流量执行相应操作。如果系统阻止流量，则也会关闭 TCP 连接。否则，客户端和服务器完成 SSL 握手，从而建立已加密会话。

内联部署中的加密流量监控

对于发往保险部门或从其发出的所有 SSL 加密流量，系统将记录连接。



发生接下来的步骤：

1. 用户提交纯文本请求 (`help`)。客户端加密此 (`AaBb`) 并将已加密流量发送到 MedRepo 的请求部门服务器。

2 LifeIns 的路由器接收已加密流量并将其路由到请求部门服务器。

3 受管设备不解密流量。

访问控制策略继续处理已加密流量并允许其通过，然后在会话结束后生成连接事件。

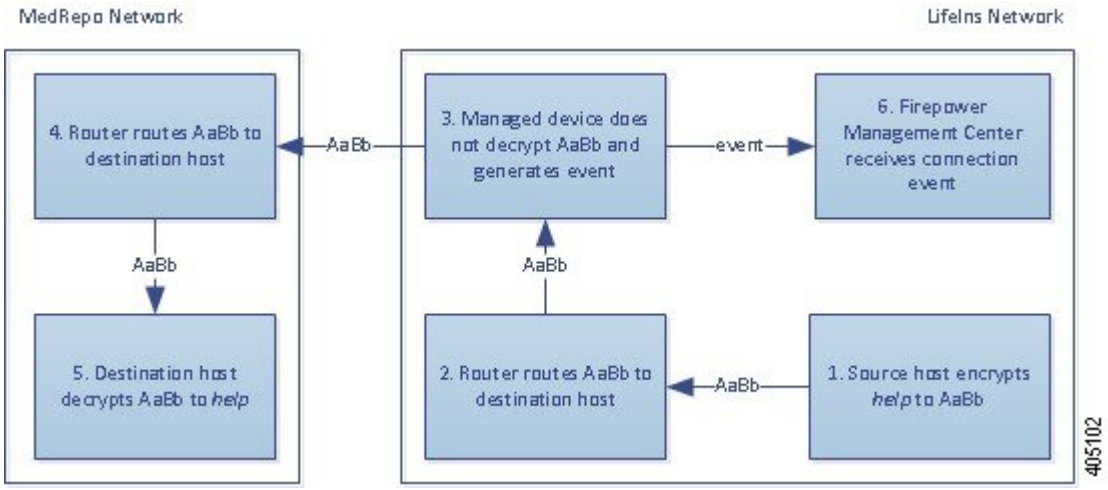
4 外部路由器接收流量并将其路由到请求部门服务器。

5 保险部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`help`)。

6 Firepower 管理中心 接收连接事件。

内联部署中未解密的已加密流量

对于来自高级保险员的所有 SSL 加密流量，受管设备均允许该流量通过而不进行解密，并记录连接。



发生接下来的步骤：

1 用户提交纯文本请求 (`help`)。客户端加密此 (`AaBb`) 并将已加密流量发送到 MedRepo 的请求部门服务器。

2 LifeIns 的路由器接收已加密流量并将其路由到请求部门服务器。

3 受管设备不解密此流量。

访问控制策略继续处理已加密流量并允许其通过，然后在会话结束后生成连接事件。

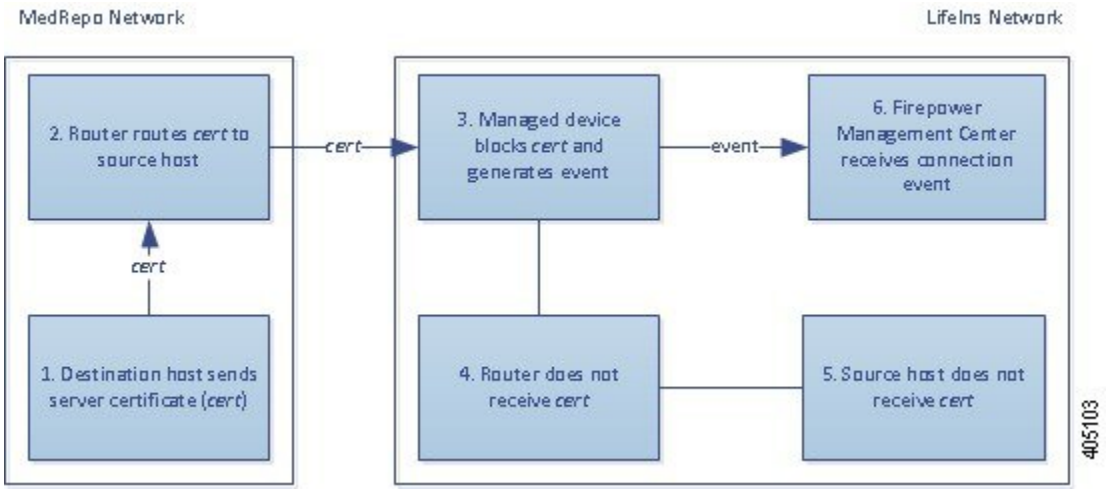
4 外部路由器接收流量并将其路由到请求部门服务器。

5 请求部门服务器接收已加密的信息请求 (`AaBb`) 并将其解密为纯文本 (`help`)。

6 Firepower 管理中心 接收连接事件。

内联部署中的加密流量阻止

对于从 LifeIns 的保险部门错误发送到 MedRepo 的客户服务部门的所有 SMTPS 邮件流量，系统在 SSL 握手期间均阻止该流量不进行进一步检查，并记录连接。

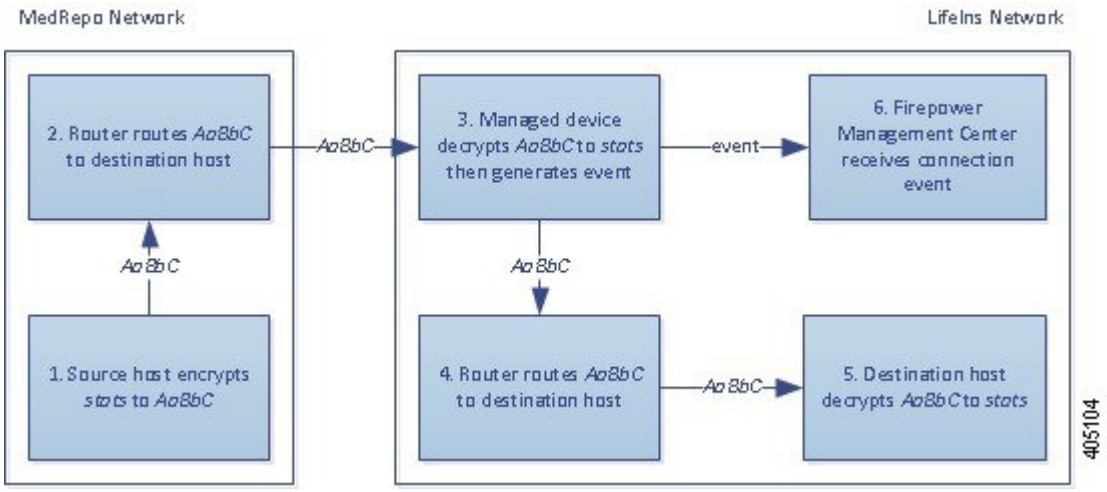


发生接下来的步骤：

1. 客户服务部门服务器从客户端浏览器收到建立 SSL 握手的请求后，客户服务部门服务器向 LifeIns 保险员发送服务器证书 (`cert`) 作为 SSL 握手的下一步。
2. MedRepo 的路由器接收证书并将其路由到 LifeIns 保险员。
3. 受管设备阻止流量并且不执行进一步检查，然后终止 TCP 连接。设备生成连接事件。
4. 内部路由器不会接收阻止的流量。
5. 保险员不会接收阻止的流量。
6. Firepower 管理中心 接收连接事件。

在内联部署中使用私钥检查加密流量

对于从 MedRepo 发送到 LifeIns 保险部门的所有 SSL 加密流量，系统将使用上载的服务器私钥来获取会话密钥，然后解密流量并记录连接。合法流量将被允许通过并在发送到保险部门之前重新加密。

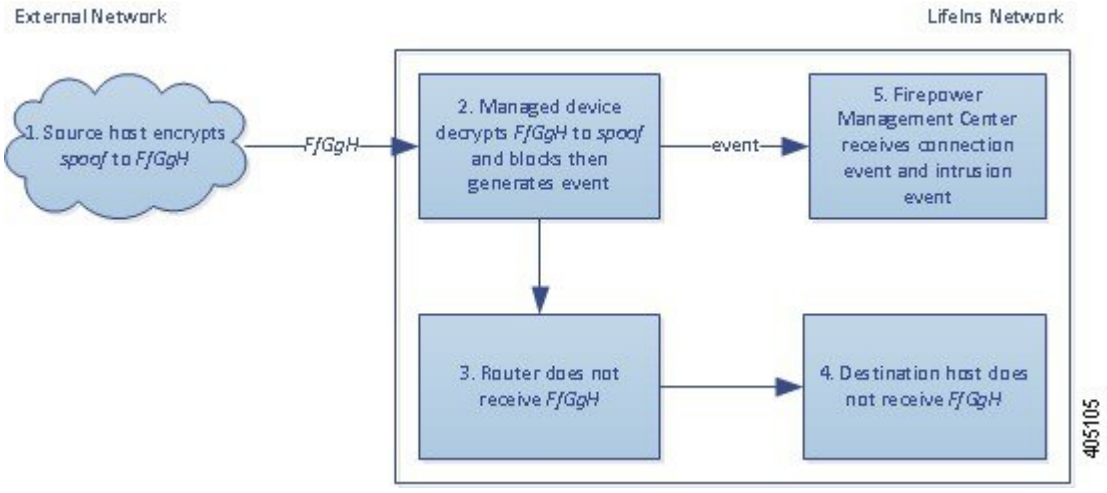


发生接下来的步骤：

1. 用户提交纯文本请求 (stats)。客户端加密此 (AaBbC) 并将已加密流量发送到保险部门服务器。
2. 外部路由器接收流量并将其路由到保险部门服务器。
3. 受管设备使用通过上载的已知私钥获取的会话密钥将此流量解密为纯文本 (stats)。

   访问控制策略继续使用自定义入侵策略处理已解密的流量，且不查找欺骗尝试。设备传输已加密流量 (AaBbC)，然后在会话结束后生成连接事件。
4. 内部路由器接收流量并将其路由到保险部门服务器。
5. 保险部门服务器接收已加密信息 (AaBbC) 并将其解密为纯文本 (stats)。
6. Firepower 管理中心接收到包含有关已加密和解密流量的信息的连接事件。

相反，实际为欺骗尝试的任何已解密流量将被丢弃。系统记录连接和欺骗尝试。



发生接下来的步骤：

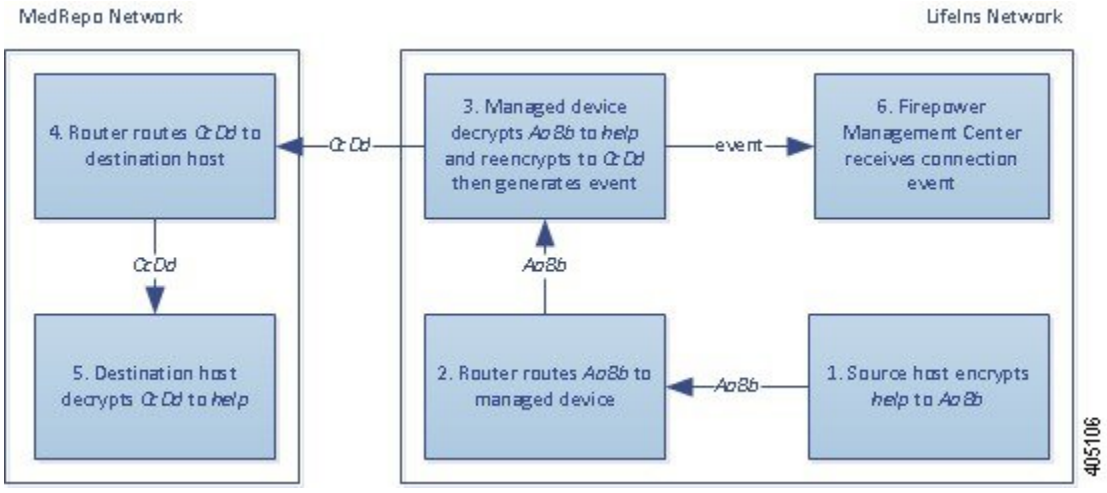
1. 用户提交纯文本请求 (`spoof`)，将流量修改为像是来自 MedRepo, LLC。客户端加密此 (`FfGgH`) 并将已加密流量发送到保险部门服务器。
2. 受管设备使用通过上载的已知私钥获取的会话密钥将此流量解密为纯文本 (`spoof`)。

   访问控制策略继续使用自定义入侵策略处理已解密的流量，且查找欺骗尝试。设备阻止流量，然后生成入侵事件。设备在会话结束后生成连接事件。
3. 内部路由器不会接收阻止的流量。
4. 保险部门服务器不会接收阻止的流量。
5. Firepower 管理中心接收包含有关已加密和解密流量的信息的连接事件，以及欺骗尝试的入侵事件。

内联部署中通过重签名证书进行的加密流量检查

对于从新保险员和初级保险员向MedRepo请求部门发送的所有SSL加密流量，系统将使用重签服务器证书来获取会话密钥，然后解密流量并记录连接。合法流量将被允许通过并在发送到MedRepo之前重新加密。

注释 当在内联部署中通过重签服务器证书解密流量时，设备作为中间人。它创建两个 SSL 会话，一个是客户端与受管设备之间的会话，一个是受管设备与服务器之间的会话。因此，每个会话包含不同的加密会话详细信息。



发生接下来的步骤：

1. 用户提交纯文本请求 (`help`)。客户端加密此 (`AaBb`) 并将已加密流量发送到请求部门服务器。
2. 内部路由器接收流量并将其路由到请求部门服务器。

3 受管设备使用通过重签服务器证书获取的会话密钥和私钥将此流量解密为纯文本 (help)。

访问控制策略继续使用自定义入侵策略处理已解密的流量，且不查找不当请求。设备重新加密流量 (CcDd)，允许其通过。设备在会话结束后生成连接事件。

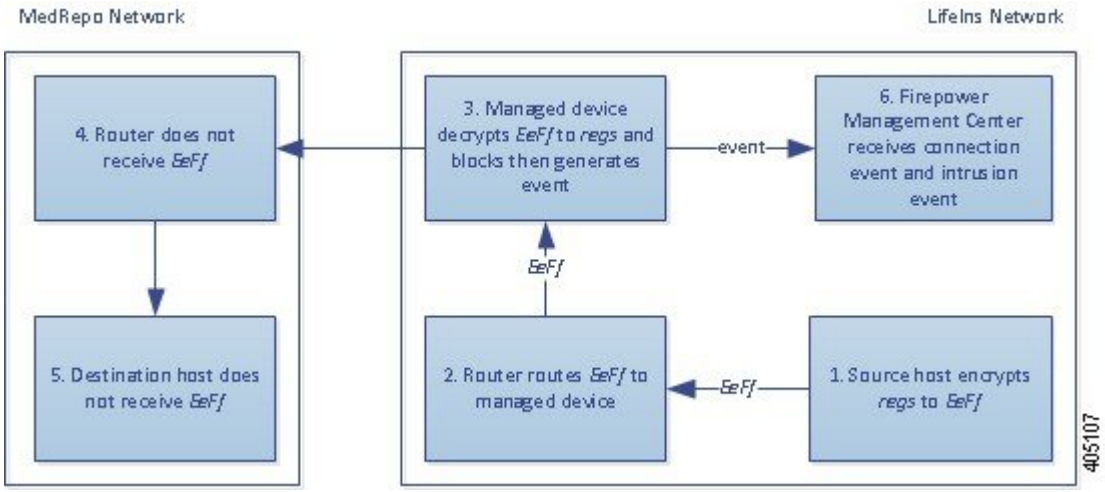
4 外部路由器接收流量并将其路由到请求部门服务器。

5 请求部门服务器接收已加密信息 (CcDd) 并将其解密为纯文本 (help)。

6 Firepower 管理中心接收到包含有关已加密和解密流量的信息的连接事件。

注释 使用重新签名的服务器证书加密的流量会导致出现浏览器警告，指出证书不受信任。要避免此问题，请将 CA 证书添加到组织的域根受信任证书存储或客户端受信任证书存储。

相反，包含不符合法规要求的任何已解密流量均将被丢弃。系统记录连接和不符信息。



发生接下来的步骤：

1 用户提交不符合法规要求的纯文本请求 (regs)。客户端加密此 (EeFf) 并将已加密流量发送到请求部门服务器。

2 内部路由器接收流量并将其路由到请求部门服务器。

3 受管设备使用通过重签服务器证书获取的会话密钥和私钥将此流量解密为纯文本 (regs)。

访问控制策略继续使用自定义入侵策略处理已解密流量并查找不当请求。设备阻止流量，然后生成入侵事件。设备在会话结束后生成连接事件。

4 外部路由器不会接收阻止的流量。

5 请求部门服务器不会接收阻止的流量。

6 Firepower 管理中心接收到包含有关已加密和解密流量的信息的连接事件，以及不当请求的入侵事件。

第 42 章

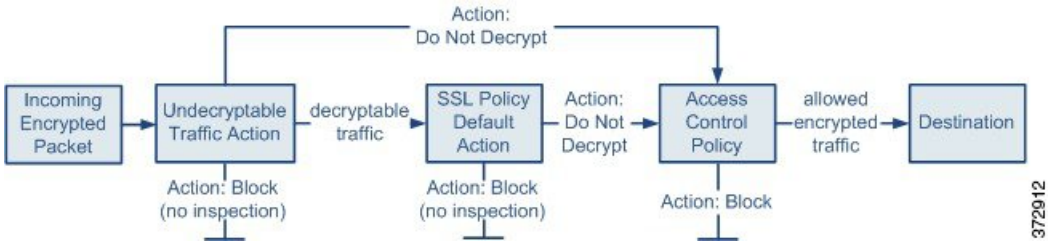
SSL 策略使用入门

以下主题概述 SSL 策略的创建、部署、管理和日志记录。

SSL 策略概述

SSL 策略确定系统如何处理网络上的加密流量。可以配置一个或多个 SSL 策略。将 SSL 策略与访问控制策略相关联，然后将该访问控制策略部署到受管设备。当设备检测到 TCP 握手时，访问控制策略首先处理并检查流量。如果它随后识别出通过 TCP 连接建立的 SSL 加密会话，则 SSL 策略将接管、处理和解密已加密的流量。

最简单的 SSL 策略（如下图所示）引导其部署所在设备，以使用单个默认操作处理加密流量。可将默认操作设置为阻止可解密流量，无需进一步检查，或者使用访问控制检查未解密的可解密流量。然后系统可以允许或阻止已加密的流量。如果设备检测到无法解密的流量，它会阻止该流量，无需进一步检查或不对其进行解密，而是使用访问控制对其进行检查。



更为复杂的 SSL 策略可通过不同的操作处理不同类型无法解密的流量，根据证书颁发机构 (CA) 是否颁发或信任加密证书而控制流量，以及使用 SSL 规则对已加密流量的日志记录和处理进行精细控制。这些规则可能很简单，也可能很复杂，使用多个条件匹配和检查已加密的流量。

SSL 策略默认操作

SSL 策略的默认操作确定系统如何处理与策略中任何非监控规则不匹配的无法解密的已加密流量。当部署不包含任何 SSL 规则的 SSL 策略时，默认操作确定如何处理网络上所有无法解密的流量。请注意，对于默认操作阻止的已加密流量，系统不会执行任何类型的检查。

表 *72*: *SSL* 策略默认操作

默认操作	对已加密流量的影响
Block	阻止 SSL 会话，无需进一步检查
阻止并重置	阻止 SSL 会话并且无需进一步检查，然后重置 TCP 连接
不解密	使用访问控制检查已加密的流量

无法解密流量的默认处理选项

表 *73*: 无法解密的流量类型

类型	说明	默认操作	可用操作
压缩的会话	此 SSL 会话应用数据压缩方法。	继承默认操作	不解密 Block Block with reset 继承默认操作

类型	说明	默认操作	可用操作
SSLv2 会话	此会话使用 SSL V2 加密。 请注意，如果 ClientHello 消息为 SSL 2.0，并且已传输流量的剩余部分为 SSL 3.0，则流量可解密。	继承默认操作	不解密 Block Block with reset 继承默认操作
Unknown Cipher Suite	系统无法识别该密码套件。	继承默认操作	不解密 Block Block with reset 继承默认操作
Unsupported Cipher Suite	系统不支持根据检测到的密码套件进行解密。	继承默认操作	不解密 Block Block with reset 继承默认操作
会话无法缓存	SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。	继承默认操作	不解密 Block Block with reset 继承默认操作
握手错误	在 SSL 握手协商时出错。	继承默认操作	不解密 Block Block with reset 继承默认操作
解密错误	在流量解密时出错。	Block	Block 阻止并重置

首次创建 SSL 策略时，默认情况下将禁用记录默认操作所处理的连接。由于默认操作的日志记录设置也适用于无法解密的流量处理，默认情况下也将禁用记录无法解密的流量操作所处理的连接。

请注意，如果浏览器使用证书锁定验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。由于您仍然可以通过访问控制检查此流量，因此不会通过无法解密的流量操作进行处理。如果要允许此流量，请配置一个 SSL 规则，将“不解密”(Do not decrypt) 操作与服务器证书公用名或可分辨名称相匹配。

注释 如果 HTTP 代理位于客户端和受管设备之间，并且客户端和服务器使用 CONNECT HTTP 方法建立隧道化 SSL 连接，则系统无法解密流量。**Handshake Errors** 无法解密操作将决定系统如何处理此流量。

管理 SSL 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

在 SSL 策略编辑器中，可以执行以下操作：

- 配置策略
- 添加、编辑、删除、启用、禁用和组织 SSL 规则
- 添加受信任 CA 证书
- 确定系统无法解密的已加密流量的处理
- 记录由默认操作和无法解密的流量操作处理的流量

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 2 管理 SSL 策略：

- 关联 - 要将 SSL 策略与访问控制策略相关联，请参阅将其他策略与访问控制相关联，第 622 页。
- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 261 页。
- 复制 - 点击复制图标 ( )。
- 创建 - 点击**新建策略 (New Policy)**；请参阅创建基本 SSL 策略，第 699 页。
- 删除 - 点击删除图标 ( )。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改，第 254 页。

- 编辑 - 点击编辑图标 ( )；请参阅编辑 SSL 策略，第 700 页。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。
- 导入/导出 - 请参阅配置导入/导出简介，第 149 页。
- 报告 - 点击报告图标 ( )；请参阅生成当前策略报告，第 262 页。

创建基本 SSL 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

要配置 SSL 策略，必须为策略提供唯一的名称并指定默认操作。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 2 点击 **New Policy**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 指定**默认操作 (Default Action)**；请参阅SSL 策略默认操作，第 696 页。

步骤 5 如使用策略默认操作记录连接，第 1510 页所述，配置默认操作的日志记录选项。

步骤 6 点击**保存 (Save)**。

后续操作

- 配置规则以添加到 SSL 策略中；请参阅创建和修改 SSL 规则，第 706 页。
- 为无法解密的流量设置默认处理，请参阅为无法解密的流量设置默认处理，第 700 页。
- 为无法解密的流量设置默认处理的日志记录选项，请参阅使用策略默认操作记录连接，第 1510 页。
- 将 SSL 策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 622 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

为无法解密的流量设置默认处理

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

您可以在 SSL 策略级别设置无法解密的流量操作以处理系统无法解密或检查的某些类型的已加密流量。部署不包含任何 SSL 规则的 SSL 策略时，无法解密的流量操作确定如何处理网络上的所有无法解密的已加密流量。

视乎无法解密的流量类型，您可以选择：

- 阻止连接
- 阻止连接，然后重置连接
- 使用访问控制检查已加密的流量
- 继承 SSL 策略的默认操作

过程

步骤 1 在 SSL 策略编辑器中，点击**无法解密的操作 (Undecryptable Actions)** 选项卡。

步骤 2 对于每个字段，请选择要对无法解密的流量类型执行的 SSL 策略的默认操作或其他操作。有关详细信息，请参阅无法解密流量的默认处理选项，第 696 页和SSL 策略默认操作，第 696 页。

步骤 3 点击 **Save** 保存策略。

接下来的操作

- 为无法解密的流量操作所处理的连接配置默认日志记录；请参阅使用策略默认操作记录连接，第 1510 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

编辑 SSL 策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 2 点击要配置的 SSL 策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 配置 SSL 策略：

- 说明 - 如果要更新 SSL 策略说明，请点击**说明 (Description)** 字段并输入新的说明。
- 记录 - 如果要为无法解密的流量处理以及不匹配 SSL 规则的流量记录连接，请参阅使用策略默认操作记录连接，第 1510 页。
- 重命名 - 如果要对 SSL 策略进行重命名，请点击**名称 (Name)** 字段并输入新名称。
- 设置默认操作 - 如果要配置 SSL 策略如何处理不匹配 SSL 规则的流量，请参阅SSL 策略默认操作，第 696 页。
- 为无法解密的流量设置默认操作 - 如果要配置 SSL 策略如何处理无法解密的流量，请参阅为无法解密的流量设置默认处理，第 700 页。
- 信任 - 如果要将受信任 CA 证书添加到 SSL 策略，请参阅信任外部证书颁发机构，第 739 页。

步骤 4 编辑 SSL 策略中的规则：

- 添加 - 如果要添加规则，请点击**添加规则 (Add Rule)**。
- 复制 - 如果要复制规则，请右键点击所选规则并选择**复制 (Copy)**。
- 剪切 - 如果要剪切规则，请右键点击所选规则并选择**剪切 (Cut)**。
- 删除 - 如果要删除规则，请点击该规则旁边的删除图标 ( )，然后点击**确定 (OK)**。
- 禁用 - 如果要禁用已启用的规则，请右键点击所选规则，选择**状态 (State)**，然后选择**禁用 (Disable)**。
- 显示 - 如果要显示特定规则属性的配置页面，请在规则行上点击条件列中的名称、值或图标。例如，点击 **Source Networks** 列中的名称或值，以便显示选定规则的 Networks 页面。有关详细信息，请参阅基于网络的 SSL 规则条件，第 720 页。
- 编辑 - 如果要编辑规则，请点击该规则旁边的编辑图标 ( )。
- 启用 - 如果要启用已禁用的规则，请右键点击所选规则，选择**状态 (State)**，然后选择**启用 (Enable)**。已禁用的规则在规则名称下方呈灰色显示并带有相应的标记 `(disabled)`。
- 粘贴 - 如果要粘贴已剪切或复制的规则，请右键点击所选规则并选择**粘贴在上方 (Paste Above)** 或者**粘贴在下方 (Paste Below)**。

步骤 5 保存或丢弃您的配置：

- 要保存更改并继续编辑，请点击**保存 (Save)**。
- 要放弃更改，请点击 **Cancel**；如果出现提示，点击 **OK**。

接下来的操作

- 如果 SSL 策略尚未与访问控制策略相关联，请对其进行关联，如将其他策略与访问控制相关联，第 622 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

第 43 章

SSL 规则使用入门

以下主题概述 SSL 规则的创建、配置、管理和故障排除：

SSL 规则概述

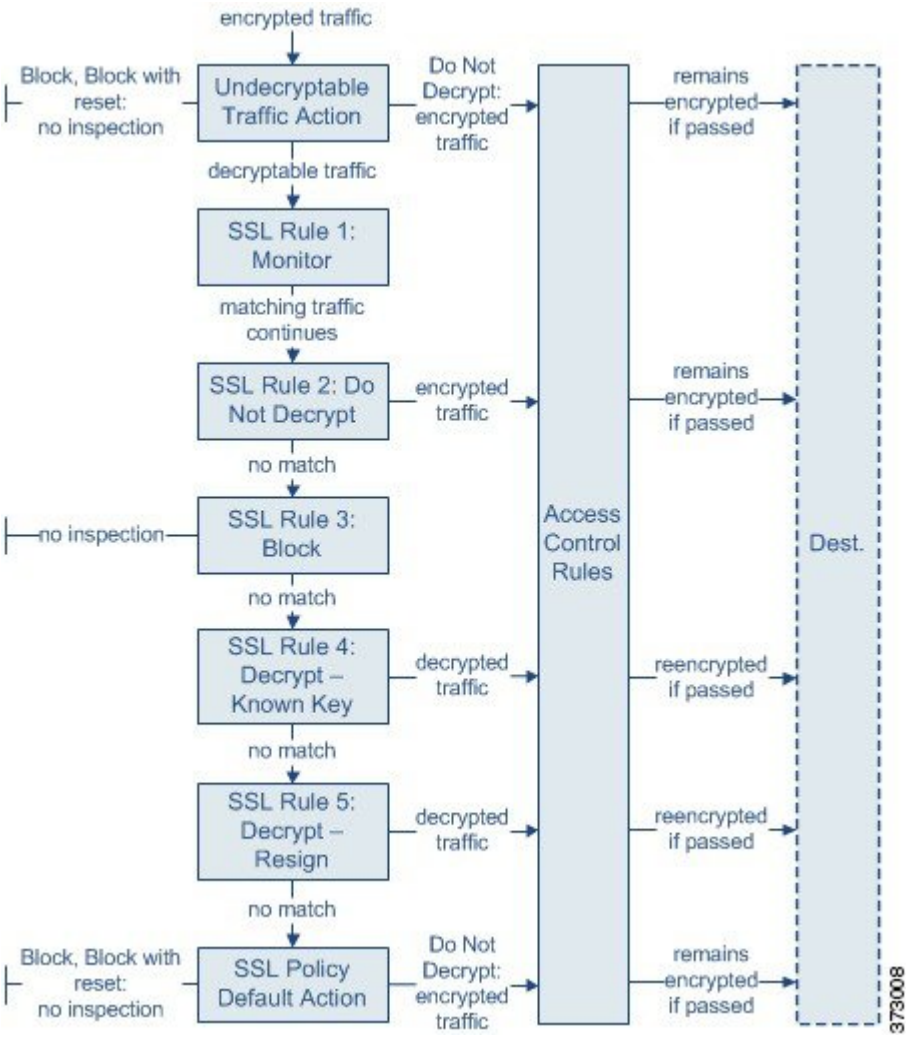
在 SSL 策略中，*SSL* 规则提供一种精细的方法来跨多台受管设备处理加密流量：阻止流量而不进一步检查；不解密流量并通过访问控制对其进行检查；或者解密流量以进行访问控制分析。

SSL 规则流量处理

系统会按照您所指定的顺序将流量与 SSL 规则相匹配。在大多数情况下，系统根据第一个 SSL 规则（使用规则的所有条件来匹配流量）处理加密流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统**不会**进一步检查其阻止的加密流量，而是会通过访问控制来检查加密流量和无法解密的流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。

下述场景概括说明了 SSL 规则在内联部署中处理流量的方式。



在这种情况中，流量评估如下：

- 首先，“**无法解密的流量操作**”**(Undecryptable Traffic Action)** 会评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 其次，使用 **SSL Rule 1: Monitor** 评估加密流量。Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- 第三，使用 **SSL 规则 2：不解密 (SSL Rule 2: Do Not Decrypt)** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **SSL Rule 3: Block** 评估加密流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据下一规则进行评估。
- 第五，使用 **SSL 规则 4：解密 - 已知密钥 (SSL Rule 4: Decrypt - Known Key)** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以

阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与SSL规则不匹配的流量继续根据下一规则进行评估。

- **SSL 规则 5：解密 - 重新签名 (SSL Rule 5: Decrypt - Resign)** 是最终规则。如果流量与此规则相匹配，则系统使用已上传的CA证书对服务器证书重新签名，然后充当中间人解密流量。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与SSL 规则不匹配的流量继续根据下一规则进行评估。
- **SSL Policy Default Action** 处理所有不与任何 SSL 规则相匹配的流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

加密流量检查配置

您必须创建可重用公共密钥基础设施 (PKI) 对象才能基于加密会话特性控制加密流量并解密加密流量。可以在将受信任证书颁发机构 (CA) 证书上传到 SSL 策略并创建 SSL 规则条件，以及在此过程中创建关联对象时随时添加此信息。不过，提前配置这些对象可降低不正确创建对象的几率。

使用证书和配对密钥解密加密流量

如果通过上传用于会话加密的服务器证书和私钥来配置内部证书对象，则系统可以解密传入的加密流量。如果在包含 **Decrypt - Known Key** 操作的 SSL 规则中引用该对象并且流量与该规则相匹配，则系统会使用上传的私钥来解密会话。

如果通过上传CA证书和私钥来配置内部CA对象，则系统还可以解密传出流量。如果在包含 **Decrypt - Resign** 操作的 SSL 规则中引用该对象并且流量与该规则相匹配，则系统会对传递到客户端浏览器的服务器证书重新签名，然后充当中间人来解密会话。

根据加密会话特性控制流量

系统可以根据用于协商会话的密码套件或服务器证书来控制加密流量。您可以从多个不同的可重用对象中选择一个进行配置，并在 SSL 规则条件中参照该对象来匹配流量。下表介绍可以配置的不同类型的可重用对象：

如果配置.....	可以根据是否存在以下内容控制加密流量.....
包含一个或多个密码套件的密码套件列表	用于协商加密会话的密码套件与密码套件列表中的密码套件相匹配
受信任 CA 对象（通过上传组织信任的 CA 证书）	受信任 CA 根据以下情况来确定是否信任用于加密会话的服务器证书： • CA 直接颁发证书 • CA 向颁发服务器证书的中间 CA 颁发证书
外部证书对象（通过上传服务器证书）	用于加密会话的服务器证书与上传的服务器证书相匹配
包含证书主题或颁发者可分辨名称的可分辨名称对象	用于加密会话的证书上的主题或颁发者通用名称、国家/地区、组织或组织单位与已配置的可分辨名称相匹配

SSL 规则组成部分

除了其唯一名称之外，每个 SSL 规则都具有以下基本组件。

省/自治区

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

SSL 策略中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。条件可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书主题或颁发者、证书状态、密码套件或加密协议版本来匹配流量。使用条件取决于目标设备许可证。

操作

规则操作确定系统如何处理匹配的流量。您可以对加密的匹配流量执行监控、允许、阻止或解密操作。解密和允许的加密流量会受到进一步检查。请注意，系统不对被阻止的加密流量执行检查。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。您可以在系统阻止加密会话或允许其未经解密便通过（取决于 SSL 策略中的设置）时记录连接。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。您可以将连接记录到Firepower 管理中心数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器中。

提示 正确创建 SSL 规则并对其排序是一项复杂的任务。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，SSL 策略接口具有功能强大的规则警告和错误反馈系统。

创建和修改 SSL 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 2 点击 SSL 策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 有以下选项可供选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击编辑图标 ()。

步骤 4 输入 **Name**。

步骤 5 配置规则组件，如上汇总。可以配置以下内容或接受默认设置：

- 指定规则是否为 **Enabled**。
- 指定规则位置；请参阅SSL 规则顺序评估，第 707 页。
- 选择规则**操作 (Action)**；请参阅配置 SSL 规则操作，第 713 页。
- 配置规则的条件；请参阅SSL 规则条件类型，第 709 页。
- 指定 **Logging** 选项；请参阅使用 SSL 规则记录可解密连接，第 1507 页。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

SSL 规则顺序评估

首次创建 SSL 规则时，请使用规则编辑器中的**插入 (Insert)** 下拉列表指定该规则的位置。SSL 策略中的 SSL 规则从 1 开始进行编号。系统将按照规则编号的升序顺序，自上而下将流量与 SSL 规则相匹配。

在大多数情况下，系统根据第一个 SSL 规则（其中所有规则的条件都与流量相匹配）处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，**不再**继续根据其他低优先级规则评估流量。

提示 正确的 SSL 规则顺序可减少处理网络流量所需的资源，并防止规则争抢。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

将 SSL 规则添加到规则类别

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，从 **Insert** 下拉列表中选择 **Into Category**，然后选择要使用的类别。

步骤 2 点击**保存 (Save)**。

提示 保存规则时，系统将其置于该类别的最后位置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

按编号确定 SSL 规则位置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，从 **Insert** 下拉列表中选择 **above rule** 或 **below rule**，然后键入相应的规则编号。

步骤 2 点击**保存 (Save)**。

提示 保存规则时，系统将其置于您指定的位置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

SSL 规则条件

SSL 规则的条件识别该规则处理的加密流量的类型。条件可以简单也可以复杂，并且可以指定每个规则有多个条件类型。仅当流量满足规则中的所有条件时，该规则才适用于此流量。

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话 SSL 或 TLS 版本如何，具有证书条件但不具有版本条件的规则根据用于协商会话的服务器证书来评估流量。

每个 SSL 规则都具有对匹配的加密流量确定以下处理的关联操作：

- 处理 - 首先，规则操作管理系统是监控、信任、阻止还是解密与规则条件匹配的加密流量
- 日志记录 - 规则操作确定何时以及如何记录有关匹配的加密流量的详细信息。

SSL 检查配置会处理、检查并记录解密流量：

- SSL 策略的无法解密的操作处理系统无法解密的流量。
- 策略的默认操作处理不满足任何非监控器 SSL 规则的条件的流量。

当系统阻止或信任加密会话时，可以记录连接事件。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。已加密会话的连接日志包含有关加密的详细信息，例如用于加密该会话的证书。您可以仅记录连接结束事件，但是：

- 对于受阻连接（Block、Block with reset），系统会立即结束会话并生成事件
- 对于受信任连接 (Do not decrypt)，系统在会话结束时生成事件

SSL 规则条件类型

当添加或编辑 SSL 规则时，请使用规则编辑器下部左侧的选项卡添加和编辑规则条件。

表 *74*: *SSL* 规则条件类型

此条件...	与加密流量相匹配.....	Details
区域	通过特定安全区域中的一个接口进入或离开设备	安全区域是根据部署和安全策略划分的一个或多个接口的逻辑分组。一个区域中的接口可能跨多个设备分布。
网络	按照其源或目标 IP 地址、国家/地区或大洲	您可以明确指定 IP 地址。利用地理定位功能还可以根据源或目标国家/地区或大洲控制流量。
VLAN Tags	按照 VLAN 进行标记	系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。
端口	按照其源端口或目标端口	可以根据 TCP 端口控制加密流量。

此条件...	与加密流量相匹配.....	Details
用户	按照参与会话的用户	根据登录到加密、受监控会话中涉及的主机的 LDAP 用户，可以控制加密流量。可以根据从 Microsoft Active Directory 服务器检索的单个用户或组控制流量。
应用	按照会话中检测的应用	可以控制对加密会话中单个应用的访问，或者根据基本特性（类型、风险、业务相关性和类别）过滤访问。
类别	按会话中请求的 URL（根据证书主题可分辨名称）	可以根据 URL 的通用分类和风险级别限制网络上的用户可以访问的网站。
Distinguished Names	按用于协商加密会话的服务器证书的主题或颁发者可分辨名称	可以根据颁发服务器证书的 CA 或服务器证书持有者来控制加密流量。
证书	按用于协商加密会话的服务器证书	可以根据为协商加密会话而传递到用户浏览器的服务器证书来控制加密流量。
Certificate Status	按用于协商加密会话的服务器证书的属性	可以根据服务器证书的状态来控制加密流量。
Cipher Suites	按用于协商加密会话的密码套件	可以根据由服务器选择用于协商加密会话的密码套件来控制加密流量。
个版本	按用于加密会话的 SSL 或 TLS 的版本	可以根据用于加密会话的 SSL 或 TLS 的版本来控制加密流量。

请注意，虽然您可以使用保护许可证和 7000 或 8000 系列设备控制和检测加密流量，但是使用检测到的应用、URL 类别或用户来控制流量需要其他许可证。此外，过于复杂的规则会消耗过多资源，并在某些情况下阻止您部署策略。

SSL 规则操作

SSL 规则监控操作

Monitor 操作不影响加密流量；既不会立即允许也不会拒绝匹配流量。相反，系统会根据其他规则（如果有）来匹配流量，以确定信任、阻止还是解密该流量。所匹配的第一个非 Monitor 规则确定流量和任何进一步的检查。如果没有其他匹配的规则，系统使用默认操作。

由于“监控”(Monitor) 规则的主要目的是跟踪网络流量，因此系统会自动将受监控流量的连接结束事件记录到 Firepower 管理中心数据库，而无论稍后处理该连接的规则或默认操作的日志记录配置如何。

SSL 规则不解密操作

Do not decrypt 操作使加密流量通过，以通过访问控制策略的规则和默认操作进行评估。由于某些访问控制规则条件需要未加密的流量，因此该流量可能与较少的规则相匹配。系统无法对加密流量执行深入检查，例如入侵或文件检查。

SSL 规则阻止操作

Block 和 **Block with reset** 操作类似于访问控制规则操作 Block 和 Block with reset。这些操作防止客户端和服务器建立 SSL 加密会话并允许加密流量通过。Block with reset 规则也会重置连接。

请注意，系统不会显示被阻止加密流量的已配置响应页面。相反，请求禁止的URL的用户将连接重置或超时。

提示

请注意，在被动或内联（触点模式）部署中不能使用 Block 或 Block with reset 操作，因为设备不是直接检查流量。如果创建具有 Block 或 Block with reset 操作的规则，该规则在安全区域条件内包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告图标 ( )。

SSL 规则解密操作

Decrypt - Known Key 和 **Decrypt - Resign** 操作会对加密流量进行解密。系统通过访问控制来检查解密流量。访问控制规则以相同方式处理已解密和未加密的流量，您可以检查该流量来获得发现数据，并检测和阻止入侵、禁止的文件及恶意软件。系统在将允许的流量传递到其目标之前会将其重新加密。

SSL 规则解密机制和准则

当配置 **Decrypt - Known Key** 操作时，可以将一个或多个服务器证书和配对私钥与该操作相关联。如果流量与规则相匹配，并且用于加密流量的证书与操作的关联证书相匹配，则系统会使用相应的私钥获取会话加密和解密密钥。由于您必须有权访问私钥，此操作最适合于解密传入到组织控制的服务器的流量。

同样，可以将一个证书颁发机构证书和私钥与 **Decrypt - Resign** 操作相关联。如果流量与此规则相匹配，则系统会使用 CA 证书对服务器证书重新签名，然后充当中间人。它创建两个 SSL 会话，一个是客户端与受管设备之间的会话，一个是受管设备与服务器之间的会话。每个会话包含不同的加密会话详细信息，并且允许系统解密并重新加密流量。此操作更适用于传出流量，因为证书的私钥会替换为您控制用于获取会话密钥的私钥。

对服务器证书重新签名涉及将证书的公钥替换为 CA 证书公钥，或者替换整个证书。通常，如果替换整个服务器证书，则在建立 SSL 连接时，客户端浏览器会发出警告，表明证书未由受信任机构签名。但是，如果客户端浏览器信任策略中的CA，则浏览器不发出表明证书不可信的警告。如果原始服务器证书是自签名证书，系统会更换整个证书，并且信任重新签名的CA，但是用户浏览器不发出表明证书是自签名的警告。在这种情况下，仅替换服务器证书公钥会导致客户端浏览器确实发出表明证书是自签名的警告。

如果配置具有 **Decrypt - Resign** 操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您将一个 CA 证书与 **Decrypt - Resign** 操作相关联，因此无法创建用来解密使用不同签名算法加密的多种类型的传出流量的 SSL 规则。此外，添加到规则中的任何外部证书对象和密码套件都必须与关联的 CA 证书加密算法类型相匹配。

例如，仅当操作引用基于椭圆曲线 (EC) 的 CA 证书时，使用 EC 算法加密的传出流量才会与 **Decrypt - Resign** 规则相匹配；如果要创建证书和密码套件规则条件，必须将基于 EC 的外部证书和密码套件添加到该规则。同样，引用基于 RSA 的 CA 证书的 **Decrypt - Resign** 规则仅与使用 RSA 算法加密的传出流量相匹配；使用 EC 算法加密的传出流量与该规则不匹配，即使所有其他已配置的规则条件都匹配也如此。

请注意以下提示：

- 如果用于建立 SSL 连接的密码套件应用 Diffie-Hellman 短时 (DHE) 或椭圆曲线 Diffie-Hellman 短时 (ECDHE) 密钥交换算法，则在被动部署中无法使用 **Decrypt - Known Key** 操作。如果 SSL 策略面向具有被动或内联（触点模式）接口的设备，并且包含具有密码套件条件（含有 DHE 或 ECDHE 密码套件）的 **Decrypt - Known Key** 规则，则系统会在该规则旁边显示信息图标 ()。如果以后向包含被动或内联（触点模式）接口的 SSL 规则中添加区域条件，系统会显示警告图标 ()。
- 在被动或内联（触点模式）部署中无法使用 **Decrypt - Resign** 操作，因为设备不会直接检查流量。如果创建具有 **Decrypt - Resign** 操作的规则，该规则在安全区域中包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告图标()。如果 SSL 策略面向具有被动或内联（触点模式）接口的设备，并且包含 **Decrypt - Resign** 规则，则系统在该规则旁边显示信息图标()。如果以后向包含被动或内联（触点模式）接口的 SSL 规则中添加区域条件，系统会显示警告图标 ()。如果将包含**解密 - 重新签名 (Decrypt - Resign)** 规则的 SSL 策略部署到具有被动或内联（分流模式）接口的设备，则与该规则相匹配的任何 SSL 会话都会失败。
- 如果客户端不信任用于对服务器证书重新签名的 CA，则会警告用户不应信任该证书。为避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织具有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。
- 系统无法解密使用匿名密码套件加密的流量。如果向**密码套件 (Cipher Suite)** 条件中添加匿名密码套件，则在 SSL 规则中无法使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作。
- 如果 HTTP 代理位于客户端和受管设备之间，并且客户端和服务器使用 CONNECT HTTP 方法建立隧道化 SSL 连接，则系统无法解密流量。**Handshake Errors** 无法解密操作将决定系统如何处理此流量。
- 系统无法解密强制网络门户用户的 Web 浏览器与受管设备上的强制网络门户后台守护程序之间的强制网络门户身份验证连接中的流量。
- 创建具有 **Decrypt - Known Key** 操作的 SSL 规则时，无法使用 **Distinguished Name** 或 **Certificate** 条件进行匹配。此限制基于这样一种假设：如果此规则与流量相匹配，则证书、主题 DN 和颁发者 DN 已经与规则的关联证书相匹配。

- 如果创建内部 CA 对象并选择生成证书签名请求 (CSR)，那么在将签名证书上传到对象之前，会无法对 **Decrypt - Resign** 操作使用此 CA。
- 如果配置具有 **Decrypt - Resign** 操作的规则，并且不匹配一个或多个外部证书对象或密码套件的签名算法类型，则策略编辑器在该规则旁边显示信息图标()。如果所有外部证书对象或所有密码套件的签名算法类型不匹配，则策略在该规则旁边显示警告图标()，并且无法部署与 SSL 策略相关联的访问控制策略。
- 如果浏览器使用证书锁定验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。如果要允许此流量，请配置一个 SSL 规则，将**不解密 (Do not decrypt)** 操作与服务器证书公用名或可分辨名称相匹配。
- 如果解密流量与具有 **Interactive Block** 或 **Interactive Block with reset** 操作的访问控制规则相匹配，则系统阻止匹配的连接而不交互，并且系统**不**显示响应页面。
- 如果启用内联规范化预处理器中的 **Normalize Excess Payload** 选项，则预处理器在规范化解密流量时，可能会丢弃数据包并将其替换为修整过的数据包。这不会结束SSL会话。如果允许流量，则修整过的数据包会作为 SSL 会话的一部分加密。

配置 SSL 规则操作

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 策略编辑器中，您有以下选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击编辑图标 ()。

步骤 2 从**操作 (Action)** 下拉列表中选择规则操作。

- 要阻止加密流量，请选择**阻止 (Block)**。
- 要阻止加密流量并重置连接，请选择**阻止并重置 (Block with reset)**。
- 要解密传入流量，请参阅配置解密-已知密钥操作，第 714 页以了解详细信息。
- 要解密传出流量，请参阅配置解密-重新签名操作，第 714 页以了解详细信息。
- 要记录加密流量，请选择**监控 (Monitor)**。
- 要不解密加密流量，请选择**不解密 (Do not decrypt)**。

步骤 3 点击 **Add**。

接下来的操作

- 配置规则条件，如基于网络的 SSL 规则条件，第 720 页、基于用户的 SSL 规则条件，第 726 页、基于信誉的 SSL 规则条件，第 727 页和基于服务器证书的 SSL 规则条件，第 734 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

配置解密-重新签名操作

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，从**操作 (Action)** 下拉列表中选择**解密 - 重新签名 (Decrypt - Resign)**。

步骤 2 从下拉列表中选择内部 CA 证书对象。

步骤 3 如果要替换证书公钥而不是整个证书，则必须选择**替换密钥 (Replace Key)**。

步骤 4 点击 **Add**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置解密-已知密钥操作

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，从**操作 (Action)** 下拉列表中选择**解密 - 已知密钥 (Derypt - Known Key)**。

步骤 2 点击 **Click to select decryption certs** 字段。

步骤 3 在**可用证书 (Available Certificates)** 列表中，选择一个或多个内部证书对象，然后点击**添加到规则 (Add to Rule)**。

步骤 4 点击 **OK**。

步骤 5 点击 **Add**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

SSL 规则管理

通过 SSL 策略编辑器的“规则”(Rules) 选项卡，您可以添加、编辑、搜索、移动、启用、禁用、删除或以其他方式管理策略中的 SSL 规则。

SSL 规则搜索

可以使用字母数字字符串（包括空格和可打印的特殊字符）在 SSL 规则列表中搜索匹配值。搜索会检查规则名称和已添加至规则的任意规则条件。对于规则条件，搜索会匹配可以为每个条件类型（区域、网络、应用程序等）添加的任意名称或值。这包括各个对象名称或值、组对象名称、组内的各个对象名称或值以及文本值。

可以使用部分或完整的搜索字符串。对于每个匹配规则，匹配值列将会突出显示。例如，如果在所有或部分规则上搜索字符串 `100Bao`，已添加 100Bao 应用程序的每个规则的 Applications 列都会突出显示。如果您还具有名为 `100Bao` 的规则，则 Name 和 Applications 列均会突出显示。

可以导航至每个上一个或下一个匹配规则。状态消息会显示当前的匹配项以及匹配项的总数量。

匹配可能会出现在多页规则列表的任意页面上。当第一个匹配项不在第一个页面上时，屏幕上将会显示第一个匹配项所在的页面。当您处于最后一个匹配项时，选择下一匹配项会使您到达第一个匹配项，当处于第一个匹配项时，选择上一匹配项会到达最后一个匹配项。

搜索 SSL 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 策略编辑器中，点击**搜索规则 (Search Rules)** 提示，键入搜索字符串，然后按 Enter 键。

提示 带有匹配值的规则列会被突出显示，其突出显示方式与指示的（第一个）匹配项不同。

步骤 2 查找感兴趣的规则：

- 要在匹配规则之间导航，可以点击下一匹配项 ( ) 或上一匹配项 ( ) 图标。
- 要刷新页面并清除搜索字符串和所有突出显示的内容，请点击清除图标 ( )。

启用和禁用 SSL 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

SSL 规则在创建时，默认会处于启用状态。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。查看 SSL 策略中的规则列表时，已禁用的规则会灰显，但仍然可以对其进行修改。请注意，也可使用规则编辑器启用或禁用 SSL 规则。

过程

步骤 1 在 SSL 策略编辑器中，右键点击规则并选择规则状态。

步骤 2 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

移动 SSL 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 策略编辑器中，通过点击各规则的空白区域来选择规则。

步骤 2 右键点击规则，然后选择**剪切 (Cut)**。

步骤 3 在要粘贴剪切规则的位置旁边，右键点击规则的空白区域并选择**粘贴在上方 (Paste above)** 或**粘贴在下方 (Paste below)**。

提示 不能在两个不同的 SSL 策略之间复制并粘贴 SSL 规则。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加新 SSL 规则类别

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

可以在标准规则和根规则类别之间创建自定义类别，以进一步组织规则，而无需创建额外的策略。可以重命名和删除添加的类别。不能移动这些类别，但可以将规则移入其中以及从中移出。

过程

步骤 1 在 SSL 策略编辑器中，点击**添加类别 (Add Category)**。

提示 如果您的策略已经包含规则，则可以点击现有规则在该行的空白区域，先设置新类别的位置，然后才能添加。还可以右键单击现有规则并选择 **Insert new category**。

步骤 2 键入**名称 (Name)**。

步骤 3 有以下选项可供选择：

- 从第一个**插入 (Insert)** 下拉列表中选择**类别上方 (above Category)**，然后从第二个下拉列表中选择要在其上放置规则的类别。
- 从下拉列表中选择**规则下方 (below rule)**，然后输入现有的规则编号。仅当策略中存在至少一个规则时，该选项才有效。
- 从下拉列表中选择**规则上方 (above rule)**，然后输入现有的规则编号。仅当策略中存在至少一个规则时，该选项才有效。

步骤 4 点击 **OK**。

提示　删除的类别中的规则将会添加至以上类别。

步骤 5　点击保存 (Save)。

SSL 规则故障排除

正确配置 SSL 规则是一项复杂任务，但是对于构建用于处理加密流量的有效部署至关重要。规则可以互相抢占，需要其他许可证或包含无效配置。周全配置的 SSL 规则还可以减少处理网络流量所需的资源。创建过度复杂的规则和对规则错误排序会影响性能。有关详细信息，请参阅规则性能准则，第 292 页。

SSL 规则的无效配置警告

因为 SSL 策略所依赖的外部设置可能会变化，因此原先有效的 SSL 策略可能会变得无效。请考虑以下示例：

- 包含 URL 类别条件的规则可能有效，直至将没有 URL 过滤许可证的设备设为目标为止。此时，在规则旁边会显示错误图标，并且在编辑或删除规则、将策略重新设为目标或启用适当的许可证之前，无法将策略部署到设备。
- 如果创建**解密 - 重新签名 (Decrypt-Resign)** 规则，然后向区域条件中添加具有被动接口的安全区域，则系统会在该规则旁边显示警告图标。由于无法通过在被动部署中对证书重新签名来解密流量，因此规则不会生效，直至从规则中移除被动接口或更改规则操作为止。
- 如果向规则中添加领域或用户，请更改领域设置以排除该领域或用户，规则将不会生效。

第 44 章

使用 SSL 规则调整解密

以下主题概述如何配置 SSL 规则条件：

SSL 规则条件概述

基本 SSL 规则将其规则操作应用于由设备检查的所有加密流量。为更好地控制和解密加密流量，可以配置规则条件来处理和记录特定类型的流量。每个 SSL 规则可包含 0 个、1 个或多个规则条件；仅当流量与该 SSL 规则中的每个条件匹配时，规则才会匹配流量。

注释 当流量匹配规则时，设备会将配置的规则操作应用于流量。当连接结束时，设备会记录流量（如果配置为执行此操作）。

每个规则条件允许指定要与其相匹配的流量的一个或多个属性；这些属性包括下列各项的详细信息：

- 流量，包括其流经的安全区域、IP 地址和端口、源或目标国家/地区以及源或目标 VLAN
- 与检测到的 IP 地址关联的用户
- 流量负载，包括流量中检测到的应用
- 连接加密，包括用于加密连接的 SSL/TLS 协议版本和密码套件及服务器证书
- 服务器证书的可分辨名称中指定的 URL 的类别和信誉

基于网络的 SSL 规则条件

SSL 策略中的 SSL 规则对加密流量日志记录和处理实行精细控制。通过基于网络的条件，可以使用以下一个或多个标准管理哪些加密流量可穿越网络：

- 通过SSL规则中的区域条件，可以按加密流量的源和目标安全区域对其进行控制。安全区域是一个或多个接口的分组，可位于多个设备之间。在设备的初始设置过程中，您选择的称为其检测模式的选项，可以确定系统如何对该设备的接口进行初始配置，以及那些接口是否属于安全区域。
- 通过 SSL 规则中的网络条件，可以按加密流量的源和目标 IP 地址对其进行控制和解密。您可以明确指定要控制的加密流量的源和目标 IP 地址，或者使用地理位置功能（将 IP 地址与地理位置相关联）根据加密流量的源或目标国家/地区或大洲对其进行控制
- 通过 SSL 规则中的 VLAN 条件，可以控制 VLAN 标记的流量。系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。
- 通过 SSL 规则中的端口条件，可以按加密流量的源和目标 TCP 端口对其进行控制。

可以将基于网络的条件相互结合以及与其他类型的条件结合来创建 SSL 规则。这些规则可以简单也可以复杂，使用多个条件来匹配和检查流量。

网络区域 SSL 规则条件

在单一区域条件中最多可向每个**源区域 (Sources Zones)** 和**目标区域 (Destination Zones)** 添加 50 个区域：

- 要匹配从区域中的某个接口传出设备的加密流量，请将该区域添加到 **Destination Zones**。

  因为被动部署的设备不会传输流量，所以，您不能在 **Destination Zone** 条件中使用包含被动接口的区域。

- 要匹配从区域中的某个接口传入设备的加密流量，请将该区域添加到 **Source Zone**。

如果同时向一条规则添加源区域和目标区域条件，则匹配流量必须源自其中一个指定源区域**并**通过其中一个目标区域流出。

请注意，如同区域中的所有接口都必须为相同类型（全都为内联、全都为被动、全都为交换或全都为路由）一样，SSL 规则的区域条件中使用的所有区域也都必须为相同类型。也就是说，不能编写与出入不同类型的区域的加密流量相匹配的单一规则。

警告图标指示无效配置，例如不包含接口的区域。如欲查看详细信息，请将鼠标指针悬停在该图标上。

按网络区域控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 Zones 选项卡。

步骤 2 从**可用区域 (Available Zones)** 中查找要添加的区域。要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

步骤 3 点击以选择区域。要选择所有区域，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。

提示 您也可以拖放选定区域。

步骤 5 保存或继续编辑规则。

示例

简答举例来说，当您使用 **Inline** 检测模式注册设备时，Firepower 管理中心会创建两个区域：Internal 和 External，并将设备上的第一对接口分配到这些区域。在内侧连接至网络的主机代表您的受保护资产。

要扩展此场景，可以部署其他配置相同的设备（由同一Firepower 管理中心管理）来保护若干不同位置中的类似资源。与第一个设备类似，这些设备中的每个设备都会保护其 Internal 安全区域中的资产。

注释 您不需要将所有内部（或外部）接口分组至单个区域。选择对您的部署和安全策略有意义的分组。

在此部署中，您可以决定，尽管希望这些主机可以不受限制地访问互联网，但是想要通过解密并检查传入加密流量来保护这些主机。

要实现此目的，请为 SSL 规则配置**目标区域 (Destination Zone)** 设置为**内部 (Internal)** 的区域条件。此简单 SSL 规则与从 Internal 区域中的任何接口传出设备的流量相匹配。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

网络或地理位置 SSL 规则条件

构建基于网络的SSL规则条件时，可以手动指定IP地址和地理位置。另外，您可以使用网络和地理位置对象配置网络条件，这些对象可重复使用，可以将名称与一个或多个IP地址、地址块、国家/地区、大陆等相关联。

注释 如果要编写按地理位置控制流量的规则，以确保使用最新地理位置数据过滤流量，思科强烈建议定期更新 Firepower 管理中心上的地理位置数据库 (GeoDB)。

在单一网络条件中，您可以向每个 **Source Networks** 和 **Destination Networks** 最多添加 50 项，而且可以混用基于网络和基于地理位置的配置。

- 要与来自 IP 地址或地理位置的加密流量相匹配，请配置 **Source Networks**。
- 要与到 IP 地址或地理位置的加密流量相匹配，请配置 **Destination Networks**。

如果向规则中同时添加源和目标网络条件，则匹配的加密流量必须源于其中一个指定的IP地址，**并且**是发往其中一个目标 IP 地址。

构建网络条件时，警告图标指明无效的配置。如欲查看详细信息，请将鼠标指针悬停在该图标上。

按网络或地理位置控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

开始之前

- 更新 Firepower 管理中心上的地理位置数据库 (GeoDB)，如地理位置数据库更新，第 136 页中所述。

过程

步骤 1 在 SSL 规则编辑器中，选择 Networks 选项卡。

步骤 2 从**可用网络 (Available Networks)** 中查找要添加的网络，如下所示：

- 点击 Networks 选项卡，以显示要添加的网络对象和组；点击 Geolocation 选项卡，以显示地理位置对象。
- 要即时添加可随后添加到条件中的网络对象，请点击“可用网络”(Available Networks) 列表上方的添加图标 ( )。

- 要搜索要添加的网络或地理位置对象，请选择相应的选项卡，点击**可用网络 (Available Networks)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象名称或该对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。

提示 您也可以拖放选定对象。

步骤 5 添加您想要手动指定的任何源或者目标 IP 地址或地址块。点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示，然后键入 IP 地址或地址块，并点击 **Add**。

步骤 6 保存或继续编辑规则。

示例

下图显示 SSL 规则的网络条件，该规则阻止源于内部网络并尝试访问位于开曼群岛或 182.16.0.3 处一家离岸控股公司服务器上的资源的加密连接。

该示例手动指定离岸控股公司的服务器 IP 地址，并使用系统提供的开曼群岛地理定位对象表示开曼群岛 IP 地址。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

VLAN SSL 规则条件

在构建基于 VLAN 的 SSL 规则条件时，可以手动指定从 1 到 4094 的 VLAN 标记。或者，也可以使用 VLAN 标记对象配置 VLAN 条件，这些对象可重用，并会将名称与一个或多个 VLAN 标记相关联。

提示 在创建 VLAN 标记对象之后，不仅可以使用其构建 SSL 规则，还可以表示系统 Web 界面中各种其他位置的 VLAN 标记。可以使用对象管理器创建 VLAN 标记对象，也可以在配置访问控制规则时即时创建这些对象。

在单个 VLAN 标记条件中，最多可向 **Selected VLAN Tags** 添加 50 项。在构建 VLAN 标记条件时，警告图标指示无效配置。如欲查看详细信息，请将鼠标指针悬停在该图标上。

控制加密 VLAN 流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 VLAN Tags 选项卡。

步骤 2 从**可用 VLAN 标记 (Available VLAN Tags)** 中查找要添加的 VLAN，如下所述：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击“可用 VLAN 标记”(Available VLAN Tags) 列表上方的添加图标 ( )。
- 要搜索要添加的 VLAN 标记对象和组，请点击**可用 VLAN 标记 (Available VLAN Tags)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的一个 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击 **Add to Rule**（**添加至规则**）。

提示 您也可以拖放选定对象。

步骤 5 添加要手动指定的任何 VLAN 标记。点击 **Selected VLAN Tags** 列表下方的 **Enter a VLAN Tag** 提示，然后键入 VLAN 标记或范围并点击 **Add**。可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

步骤 6 保存或继续编辑规则。

示例

下图显示 SSL 规则的 VLAN 标记条件，该规则与面向公众的 VLAN（以 VLAN 标记对象组表示）以及手动添加的 VLAN 42 上的加密流量相匹配。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

端口 SSL 规则条件

在构建基于端口的 SSL 规则条件时，可以手动指定 TCP 端口。此外，您可以使用端口对象配置端口条件，这些对象可重复使用，可将名称与一个或多个端口相关联。

在单一网络条件中，您可以向每个 **Selected Source Ports** 和 **Selected Destination Ports** 列表最多添加 50 项：

- 要与来自 TCP 端口的加密流量相匹配，请配置 **Selected Source Ports**。
- 要与传到 TCP 端口的加密流量相匹配，请配置 **Selected Destination Ports**。
- 要与源自 TCP **所选目标端口 (Selected Source Ports)**和发往 TCP **所选目标端口 (Selected Destination Ports)** 的加密流量均匹配，请同时配置两者。

只能使用 TCP 端口配置 **Selected Source Ports** 和 **Selected Destination Ports** 列表。包含非 TCP 端口的端口对象在 **Available Ports** 列表中灰显。

构建端口条件时，警告图标指明无效的配置。例如，您可以使用对象管理器来编辑正在使用的端口对象，以使使用这些对象组的规则变得无效。如欲查看详细信息，请将鼠标指针悬停在该图标上。

按端口控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 Ports 选项卡。

步骤 2 从**可用端口 (Available Ports)** 中查找要添加的 TCP 端口，如下所示：

- 要即时添加可随后添加到条件中的 TCP 端口对象，请点击“可用端口”(Available Ports) 列表上方的添加图标 ( )。
- 要搜索要添加的基于 TCP 的端口对象和组，请点击**可用端口 (Available Ports)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中端口的值。列表会在您键入内容时进行更新，以显示匹配的对象。例如，如果键入 443，Firepower 管理中心将显示系统提供的 HTTPS 端口对象。

步骤 3 要选择基于 TCP 的端口对象，请点击该对象。要选择所有基于 TCP 的端口对象，请点击右键，然后选择**全选 (Select All)**。如果对象包含不是基于 TCP 的端口，则无法将其添加到端口条件中。

步骤 4 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。

提示 您也可以拖放选定对象。

步骤 5 在**所选源端口 (Selected Source Ports)** 或**所选目标端口 (Selected Destination Ports)** 列表下输入**端口 (Port)**，以手动指定源端口或目标端口。您可以为单个端口指定从 0 到 65535 之间的一个值。

步骤 6 点击 **Add**。

注释 Firepower 管理中心不会将会导致无效配置的端口添加到规则条件。

步骤 7 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

基于用户的 SSL 规则条件

您可以将 SSL 规则配置为根据领域、组或用户来匹配流量。通过 SSL 规则中的领域、组和用户条件，可以执行用户控制以通过将授权用户与 IP 地址相关联来管理哪些流量可以流经网络。

为使流量与具有用户条件的 SSL 规则相匹配，受监控会话中的源或目标主机的 IP 地址必须与已登录的授权的用户相关联。您可以根据领域、个别用户或这些用户所属的组来控制流量。

根据用户控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

开始之前

- 配置一个或多个授权用户身份源，如用户身份源，第 1197 页中所述。

- 配置领域，如创建领域，第 1235 页中所述。

过程

步骤 1 在 SSL 规则编辑器中，选择 Users 选项卡。

步骤 2 按**可用领域 (Available Realms)** 列表上方的名称或值进行搜索并选择一个领域。

步骤 3 按**可用用户 (Available Users)** 列表上方的名称或值进行搜索并选择用户或组。

步骤 4 点击 **Add to Rule**（**添加至规则**）。

提示 也可以拖放选定的用户和组。

步骤 5 保存或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

基于信誉的 SSL 规则条件

SSL 规则中基于信誉的条件允许您通过将网络流量情景化并对其进行适当限制，来管理哪些加密流量可以穿越网络。SSL 规则监管以下类型的基于信誉的控制：

- 通过应用条件，可以执行应用控制。当系统分析加密 IP 流量时，它可以在解密加密会话之前识别和分类网络上的常用加密应用。系统使用此基于发现的应用感知功能，允许您控制网络上的加密应用流量。

  在单个 SSL 规则中，可以选择单个应用，包括自定义应用。可以使用系统提供的应用过滤器，此类过滤器是根据应用的基本特性（类型、风险、业务相关性和类别）组织的命名应用集。

- URL 条件允许您根据网站的分配的类别和信誉来控制网络流量。

SSL 规则中的所选应用和过滤器

思科通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他检测器。您还可以创建自己的检测器，并指定其所检测的应用的特征（风险和关联性等）。通过根据应用特性使用过滤器，可以确保系统使用最新的检测器来监控应用流量。

为使流量与具有应用条件的 SSL 规则相匹配，流量必须与向 **Selected Applications and Filters** 列表中添加的其中一个过滤器或应用相匹配。

注释 使用访问控制规则过滤应用流量时，可以使用应用标签作为过滤条件。但是，因为没有好处，不能使用应用标记过滤加密流量。系统在加密流量中可以检测的所有应用都标记为 **SSL Protocol**；只能在未加密或已解密的流量中检测到没有此标记的应用。

在单一应用条件中，最多可以向**所选应用和过滤器 (Selected Applications and Filters)** 列表中添加 50 个项目。下列每项均视为一个项目：：

- **Application Filters** 列表中的一个或多个过滤器（单独或自定义组合）。此项表示应用集（按特性分组）。
- 通过保存 **Available Applications** 列表中应用的搜索创建的过滤器。此项表示应用集（按子字符串匹配分组）。
- **Available Applications** 列表中的每项应用。

在 Web 界面中，添加到条件的过滤器会在上方列出并与单独添加的应用分别列出。

请注意，当部署 SSL 策略时，对于具有应用条件的每个规则，系统会生成要匹配的唯一应用的列表。换句话说，可以使用重叠过滤器和逐一指定的应用确保完整覆盖。

SSL 规则中的应用过滤器

在 SSL 规则中构建应用条件时，使用 **Application Filters** 列表可创建要匹配其流量的按特性分组的应用集。

为方便起见，系统会按类型、风险、业务关联性、类别和标签确定每个应用的特征。可以使用这些标准作为过滤器或创建过滤器的自定义组合来执行应用控制。

请注意，过滤 SSL 规则中的应用的机制与使用对象管理器创建可重用、自定义应用过滤器的机制相同。您还可以将在访问控制规则中动态创建的多个过滤器另存为新的可重复使用的过滤器。如果您的过滤器中包括其他用户创建的过滤器，则该过滤器无法保存，因为系统不允许嵌套用户创建的过滤器。

了解过滤器组合方式

选择过滤器时（单一或组合），**Available Applications** 列表会更新为仅显示符合条件的应用。可以选择系统提供的组合形式的过滤器，但不能选择自定义过滤器。

系统将同一类型的多个过滤器与 OR 操作关联。例如，如果您在 Risks 类型下选择 Medium 和 High 过滤器，则产生的过滤器为：

```
Risk: Medium OR High
```

如果 Medium 过滤器包含 110 个应用，而 High 过滤器包含 82 个应用，则系统将在 **Available Applications** 列表中显示全部 192 个应用。

系统将不同类型的过滤器与 AND 操作关联。例如，如果您选择 Risks 类型下的 Medium 和 High 过滤器，以及 Business Relevance 类型项下的 Medium 和 High 过滤器，则所产生的过滤器为：

```
Risk: Medium OR High
```

```
AND
Business Relevance: Medium OR High
```

在此情况下，系统仅显示 Medium 或 High Risk 类型和 Medium 或 High Business Relevance 类型中均包含的应用。

查找和选择过滤器

要选择过滤器，请点击过滤器类型旁边的箭头以展开该类型，然后选择或清除要显示或隐藏其应用的每个过滤器旁边的复选框。您还可以右键点击思科提供的过滤器类型（**风险 [Risks]**、**业务关联性 [Business Relevance]**、**类型 [Types]** 或 **类别 [Categories]**），然后选择**全部选中 (Check All)** 或**取消全部选中 (Uncheck All**）。

要搜索过滤器，请点击 **Available Filters** 列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的过滤器。

选择过滤器完成后，请使用**可用应用 (Available Applications)** 列表将这些过滤器添加到规则中。

SSL 规则中的可用应用

在 SSL 规则中构建应用条件时，请使用 **Available Applications** 列表选择要匹配其流量的应用。

浏览应用列表

首次开始构建条件时，该列表不受限制，并且显示系统检测的每个应用（一次 100 个）：

- 要翻页浏览应用，请点击列表下方的箭头。
- 要打开弹出窗口，显示有关应用特性的摘要信息以及可点选的互联网搜索链接，请点击应用旁边的信息图标 ()。

查找要匹配的应用

为帮助查找要匹配的应用，您可以通过以下方式限制 **Available Applications** 列表：

- 要搜索应用，请点击列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的应用。
- 要通过应用过滤器来限制应用，请使用**应用过滤器 (Application Filters)** 列表。**Available Applications** 列表在您应用过滤器时进行更新。

进行限制后，在 **Available Applications** 列表顶部会出现 **All apps matching the filter** 选项。

注释 如果您在 Application Filters 列表中选择一个或多个过滤器，并在这种状态下搜索 **Available Applications** 列表，系统会使用 AND 运算将您的选择与搜索过滤出的 **Available Applications** 列表进行组合。也就是说，**All apps matching the filter** 条件包括 **Available Applications** 列表中当前显示的所有个别条件以及在 **Available Applications** 列表上方输入的搜索字符串。

在条件中选择要匹配的单个应用

找到要匹配的应用，然后点击将其选定。要选择当前受限制视图中的所有应用，请右键点击并选择**全选 (Select All)**。

在单个应用条件中，可以通过逐个选择应用来匹配最多 50 个应用；要添加 50 个以上的应用，必须创建多个 SSL 规则或使用过滤器对应用进行分组。

为条件选择与某个过滤器匹配的所有应用

通过搜索或使用 **Application Filters** 列表中的过滤器进行限制后，在 **Available Applications** 列表的顶部会出现 **All apps matching the filter** 选项。

通过此选项，可以将受限制的**可用应用 (Available Applications)** 列表中的整个应用集一次性添加到**所选应用和过滤器 (Selected Applications and Filters)** 列表。与逐个添加应用相比，无论组成此应用集的单个应用的数量如何，添加此应用集都仅计为一项，而不是最多 50 项。

以此方式构建应用条件时，您添加到 **Selected Applications and Filters** 列表的过滤器名称会显示为一个串联字符串，其中包括该过滤器中代表的过滤器类型，每种类型后会最多显示三个过滤器名称。超过三个相同类型的过滤器后面会加上省略号 (.....)。例如，以下过滤器名称在 Risks 类型下包含两个过滤器，在 Business Relevance 下包括四个过滤器：

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

使用**所有匹配过滤器的应用 (All apps matching the filter)** 添加的过滤器中未显示的过滤器类型不包含在所添加的过滤器名称中。当您将指针悬停在**所选应用和过滤器 (Selected Applications and Filters)** 列表中的过滤器名称上时显示的说明文本表示这些过滤器类型设置为 *any*；即，这些过滤器类型不限制过滤器，因此对于这些过滤器允许任意值。

可以向应用条件中添加 **All apps matching the filter** 的多个实例，其中每个实例计为 **Selected Applications and Filters** 列表中的单独项。例如，可以将所有高风险应用添加为一项，然后清除选择，再将所有低业务关联性应用添加为另一项。此应用条件会匹配风险高或业务关联性低的应用。

基于应用的 SSL 规则条件要求

为使加密流量与具有应用条件的 SSL 规则相匹配，流量必须与向 **Selected Applications and Filters** 列表中添加的其中一个过滤器或应用相匹配。

每个条件最多可以添加 50 项，并且添加到条件中的过滤器列出在上方并与逐个添加的应用分隔开来。构建应用条件时，无效的配置会以警告图标加以指示。如欲查看详细信息，请将鼠标指针悬停在该图标上。

将应用条件添加到 SSL 规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 Applications 选项卡。

步骤 2 如果要限制**可用应用 (Available Applications)** 列表中显示的应用列表，必须在**应用过滤器 (Application Filters)** 列表中选择一个或多个过滤器。有关详细信息，请参阅SSL 规则中的应用过滤器，第 728 页。

步骤 3 从 **Available Applications** 列表查找并选择要添加的应用。可以搜索并选择个别应用，或者在列表受限制时，选择 **All apps matching the filter**。有关详细信息，请参阅SSL 规则中的可用应用，第 729 页。

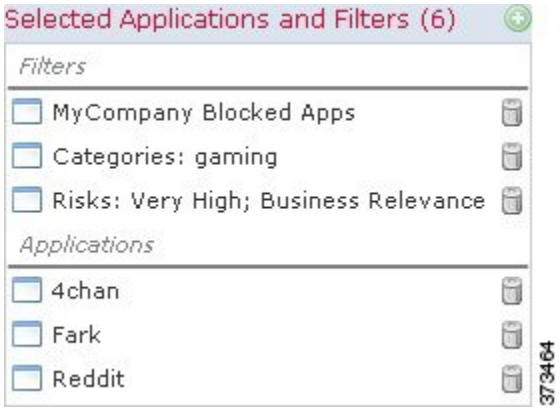
步骤 4 点击 **Add to Rule**（添加至规则）。

提示 点击**清除所有过滤器 (Clear All Filters)** 可清除现有选择。您也可以拖放所选应用和过滤器。

步骤 5 保存或继续编辑规则。

示例

下图显示用于解密以下自定义应用组的 SSL 规则的应用条件：MyCompany 的应用，具有高风险和低业务相关性的所有应用、游戏应用以及单独选择的一些应用。



接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

对加密应用控制的限制

加密应用识别

系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS 之类的应用。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书使用者可分辨名称值来识别某些加密应用。

应用识别的速度

系统在以下情况之前无法对加密流量执行应用控制：

- 在客户端和服务器之间建立加密连接，并且
- 系统识别加密会话中的应用

此识别发生在服务器证书交换之后。如果在 SSL 握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。为便于识别，受影响的规则会以信息图标 () 标记。

在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。

自动启用应用检测器

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。

加密流量中基于信誉的 URL 阻止

通过 URL 过滤许可证，SSL 规则中的 URL 条件可以基于所请求 URL 的类别和信誉控制对加密网站的访问。有关详细信息，请参阅URL 条件（URL 过滤），第 280 页。

提示 SSL 规则中的 URL 条件不支持手动 URL 过滤。应使用与主题公用名匹配的可分辨名称条件。

执行基于信誉的 URL 阻止

智能许可证	经典许可证	支持的设备	支持的域	Access
URL 过滤	URL 过滤	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择“类别”(Category) 选项卡。

步骤 2 从**类别 (Categories)** 列表中查找要添加的 URL 的类别。要匹配加密网络流量（无论类别如何），请选择 **Any** 类别。要搜索要添加的类别，请点击**类别 (Categories)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入类别名称。列表会在您键入内容时进行更新，以显示匹配的类别。

步骤 3 要选择类别，请点击该类别。

提示 虽然可以右键单击并选择 **Select All** 来选择所有类别，但是以此方式添加所有类别会超过 SSL 规则的 50 项最大限制值。请改用 **Any**。

步骤 4 如果要限定类别选择，必须从**信誉 (Reputations)** 列表中选择一个信誉级别。只能选择一个信誉级别。如果不指定信誉级别，则系统默认为 **Any**（表示所有级别）。

- 如果规则阻止 Web 访问或解密流量（规则操作为 **Block**、**Block with reset**、**Decrypt - Known Key**、**Decrypt - Resign** 或 **Monitor**），则选择信誉级别还将选择严重性高于该级别的所有信誉。例如，如果将规则配置为阻止 **Suspicious sites**（2 级），则系统还会自动阻止 **High Risk**（1 级）站点。
- 如果规则根据访问控制允许 Web 访问（规则操作为 **Do not decrypt**），则选择信誉级别还将选择严重性低于该级别的所有信誉。例如，如果您将规则配置为允许 **Benign sites**（第 4 级），系统还会自动允许 **Well known**（第 5 级）站点。

  注释 如果更改规则的规则操作，系统根据上述几点自动更改 URL 条件中的信誉级别。

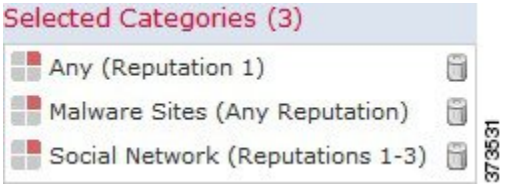
步骤 5 点击**添加到规则 (Add to Rule)** 以将所选项添加到**所选类别 (Selected Categories)** 列表中。

提示 您也可以拖放选定项。

步骤 6 保存或继续编辑规则。

示例

下图显示用于阻止以下内容的示例访问控制规则的URL条件：所有恶意软件站点、所有高风险站点以及所有非良性社交网站。



下表总结如何构建上图所示条件。

表 *75*：示例：构建 *URL* 条件

要阻止.....	请选择此类别或 URL 对象.....	和该信誉.....
恶意软件站点，无论信誉如何	Malware Sites	任意
具有高风险（1 级）的任何 URL	任意	1 - High Risk
风险大于良性（1 至 3 级）的社交网站	社交网络	3 - Benign sites with security risks

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

基于服务器证书的 SSL 规则条件

SSL 规则可以根据服务器证书特征来处理和解密已加密的流量。您可以根据以下服务器证书属性配置访问规则：

- 通过可分辨名称，您可以根据颁发服务器证书的 CA 或证书使用者来处理和检查加密流量。根据颁发者可分辨名称，可以根据颁发站点服务器证书的 CA 处理流量。
- 通过 SSL 规则中的证书条件，可以根据用于对加密流量进行加密的服务器证书来处理和检查该流量。可以配置具有一个或多个证书的条件；如果证书与该条件的任何证书相匹配，则流量与规则相匹配。
- 通过 SSL 规则中的证书状态条件，可以根据用于加密流量的服务器证书的状态（包括证书是否有效、已撤销、已到期、尚未生效、自签名或由受信任 CA 签名）来处理和检查加密流量。
- 通过 SSL 规则中的密码套件条件，可以根据用于协商加密会话的密码套件来处理和检查加密流量。
- 通过 SSL 规则中的会话条件，可以根据用于加密流量的 SSL 或 TLS 版本来检查加密流量。

要检测规则、证书颁发者或证书持有者中的多个密码套件，可以创建可重用密码套件列表和可分辨名称对象并将其添加到规则中。要检测服务器证书和某些证书状态，必须为规则创建外部证书和外部 CA 对象。

证书可分辨名称 SSL 规则条件

当配置规则条件时，可以手动指定文本值，引用可分辨名称对象，或者引用包含多个对象的可分辨名称组。

注释 如果还选择了**解密 - 已知密钥 (Derypt - Known Key)** 操作，则无法配置可分辨名称条件。由于该操作要求选择服务器证书来解密流量，因此证书已经与流量相匹配。

可以在单个证书状态规则条件中根据多个主题和颁发者可分辨名称进行匹配，只需匹配一个公用名或可分辨名称即可与规则相匹配。

如果手动添加可分辨名称，则其可以包含公用名属性 (**CN**)。如果添加不带 `CN=` 的公用名称，系统会在名称前面加上 `CN=`，再保存对象。

还可以添加具有下列属性各一（以逗号隔开）的可分辨名称：**C**、**CN**、**O**、**OU**。

在单个 DN 条件中，可以向**使用者 DN (Subject DNs)** 添加最多 50 个文本值和可分辨名称对象，并向**颁发者 DN (Issuer DNs)** 添加最多 50 个文本值和可分辨名称对象。

系统提供的 DN 对象组 Cisco-Undecryptable-Sites 包含系统无法解密其流量的网站。可以向 DN 条件中添加该组来阻止或不解密出入于这些网站的流量，而不会浪费系统资源尝试解密该流量。可以修改组中的单个条目。不能删除该组。系统更新可以修改此列表中的条目，但是，系统会保留用户更改。

按证书可分辨名称控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 DN 选项卡。

步骤 2 从**可用 DN (Available DNs)** 中查找要添加的可分辨名称，如下所示：

- 要即时添加可随后添加到条件中的可分辨名称，请点击**可用 DN (Available DNs)** 列表上方的添加图标 ()。
- 要搜索要添加的可分辨名称对象和组，请点击**可用 DN (Available DNs)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击**添加到使用者 (Add to Subject)** 或**添加到颁发者 (Add to Issuer)**。

提示 您也可以拖放选定对象。

步骤 5 添加要手动指定的所有文本公用名或可分辨名称。点击**使用者 DN (Subject DNs)** 或**颁发者 DN (Issuer DNs)** 列表下方的**输入 DN 或 CN (Enter DN or CN)** 提示；然后键入公用名或可分辨名称并点击**添加 (Add)**。

步骤 6 添加或继续编辑规则。

示例

下图说明用于搜索向 goodbakery.example.com 颁发或由 goodca.example.com 颁发的证书的可分辨名称规则条件。根据访问控制，允许通过这些证书加密的流量。

示例

下图说明用于搜索向 badbakery.example.com 和关联域颁发的证书或由 badca.example.com 颁发的证书的可分辨名称规则条件。通过这些证书加密的流量使用重新签名的证书进行解密。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

证书 SSL 规则条件

构建基于证书的 SSL 规则条件时，可以上传服务器证书；将证书另存为外部证书对象，该对象可重用并会将名称与服务器证书相关联。或者，可以使用现有外部证书对象和对象组来配置证书条件。

可以根据以下证书可分辨名称特性在外部证书对象或对象组所基于的规则条件中搜索 **Available Certificates** 字段：

- 主题或颁发者公用名 (CN)
- 主题或颁发者组织 (O)
- 主题或颁发者组织单位 (OU)

您可以选择根据单个证书规则条件中的多个证书进行匹配；如果用于加密流量的证书与上传的任何证书相匹配，则加密流量与规则相匹配。

在单个证书条件中，可以向 **Selected Certificates** 添加最多 50 个外部证书对象和外部证书对象组。

请注意以下提示：

- 如果还选择 **Decrypt - Known Key** 操作，则无法配置证书条件。由于该操作要求选择服务器证书来解密流量，因此结果是证书已经与流量相匹配。
- 如果使用外部证书对象配置证书条件，则添加到密码套件条件中的任何密码套件或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与外部证书的签名算法类型相匹配。例如，如果规则的证书条件引用基于 EC 的服务器证书，则添加的任何密码套件或与 **Decrypt - Resign** 操作相关

联的CA证书也必须基于EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告图标。

按证书控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 Certificate 选项卡。

步骤 2 从**可用证书 (Available Certificates)** 中查找要添加的服务器证书，如下所示：

- 要动态添加可随后添加到条件中的外部证书对象，请点击**可用证书 (Available Certificates)** 列表上方的添加图标 ( )。
- 要搜索将添加的证书对象和组，请点击**可用证书 (Available Certificates)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击 **Add to Rule**（添加至规则）。

提示 您也可以拖放选定对象。

步骤 5 添加或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

证书状态 SSL 规则条件

对于配置的每个证书状态 SSL 规则条件，可以根据给定状态存在还是缺失来匹配流量。可以在一个规则条件中选择若干状态，如果证书与任何所选状态相匹配，则规则与流量相匹配。

可以选择根据单个证书状态规则条件中多个证书状态的存在或缺失进行匹配；证书只需匹配其中一个标准即可与规则相匹配。

下表介绍系统如何根据加密服务器证书的状态评估加密流量。

表 *76*：证书状态规则条件标准

状态检查	状态设置为 **Yes**	状态设置为 **No**
Revoked	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书包含用于撤销服务器证书的 CRL。	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书不包含用于撤销证书的 CRL。
自签名	检测到的服务器证书包含相同的主题和颁发者可分辨名称。	检测到的服务器证书包含不同的主题和颁发者可分辨名称。
有效	以下所有情况都成立： • 策略信任颁发证书的 CA • 签名有效 • 颁发者有效 • 策略的受信任 CA 未撤销证书 • 当前日期介于证书的 Valid From 和 Valid To 日期之间	至少以下情况之一成立： • 策略不信任颁发证书的 CA • 签名无效 • 颁发者无效 • 策略中的受信任 CA 已撤销证书 • 当前日期在证书的 Valid From 日期之前 • 当前日期在证书的 Valid To 日期之后
签名无效	无法根据证书的内容正确验证证书的签名。	根据证书的内容正确验证证书的签名。
颁发者无效	颁发者 CA 证书未存储在策略的受信任 CA 证书列表中。	颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
Expired	当前日期在证书的 Valid To 日期之后。	当前日期在证书的 Valid To 日期之前或当日。
尚未生效	当前日期在证书的 Valid From 日期之前。	当前日期在证书的 Valid From 日期之后或当日。

请注意，即使证书可能匹配多个状态，但是规则仅对流量执行一次操作。

检查颁发或撤销证书的 CA 是否要求将根 CA 证书和中间 CA 证书以及关联的 CRL 作为对象进行上传。然后，将这些受信任 CA 对象添加到 SSL 策略的受信任 CA 证书列表。

信任外部证书颁发机构

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

您可以通过向 SSL 策略中添加根 CA 证书和中间 CA 证书来信任 CA，然后使用这些受信任 CA 验证用于加密流量的服务器证书。

如果受信任 CA 证书包含上传的证书撤销列表 (CRL)，则还可以验证受信任 CA 是否已撤销加密证书。

过程

步骤 1 在 SSL 规则编辑器中，选择**受信任 CA 证书 (Trusted CA Certificates)** 选项卡。

步骤 2 从**可用受信任 CA (Available Trusted CAs)** 中查找要添加的受信任 CA，如下所示：

- 要即时添加可随后添加到条件中的受信任 CA 对象，请点击**可用受信任 CA (Available Trusted CAs)** 列表上方的添加图标 ( )。
- 要搜索要添加的受信任 CA 对象和组，请点击**可用受信任 CA (Available Trusted CAs)** 列表上方的**按名称或值搜索 (Search by name or value)**，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击 **Add to Rule**（**添加至规则**）。

提示 您也可以拖放选定对象。

步骤 5 添加或继续编辑规则。

接下来的操作

- 将证书状态 SSL 规则条件添加到 SSL 规则。有关详细信息，请参阅按证书状态匹配流量，第 740 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

受信任外部证书颁发机构配置

已验证的服务器证书包括由受信任 CA 签名的证书。将受信任 CA 证书添加到 SSL 策略后，可以将具有证书状态条件的 SSL 规则配置为根据此流量进行匹配。

提示 将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。此外，如果将证书状态条件配置为根据根颁发者 CA 来信任流量，则可以允许而不解密受信任 CA 的信任链中的所有流量，而不是不必要地将其解密。

创建 SSL 策略时，系统使用默认受信任 CA 对象组“思科受信任机构”(Cisco Trusted Authorities) 填充“受信任 CA 证书”(Trusted CA Certificates) 选项卡。

可以修改组中的单个条目，并且选择是否在 SSL 策略中包含该组。不能删除该组。系统更新可以修改此列表中的条目，但会保留用户更改。

按证书状态匹配流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

开始之前

- 向 SSL 策略中添加可信 CA 对象或组。有关详细信息，请参阅信任外部证书颁发机构，第 739 页。

过程

步骤 1 在 SSL 规则编辑器中，选择 Cert Status 选项卡。

步骤 2 对于每个证书状态，具有以下选项：

- 选择 **Yes** 可根据该证书状态是否存在进行匹配。
- 选择 **No** 可根据该证书状态是否缺失进行匹配。
- 选择 **Do Not Match** 将不匹配该证书状态。

步骤 3 添加或继续编辑规则。

示例

组织信任 Verified Authority 证书颁发机构。组织不信任 Spammer Authority 证书颁发机构。系统管理员将 Verified Authority 证书和由 Verified Authority 颁发的中间 CA 证书上传到系统。由于 Verified Authority 已撤销其以前颁发的证书，因此系统管理员上传该 Verified Authority 分发的 CRL。

下图说明用于检查有效证书、由 Verified Authority 颁发的证书、不在 CRL 上的证书以及仍在 Valid From 和 Valid To 日期内的证书的证书状态规则条件。受配置原因的影响，未通过访问控制来解密和检查使用这些证书加密的流量。

下图说明用于检查状态是否缺失的证书状态规则条件。在此情况下，由于配置原因，它与使用尚未到期的证书加密的流量相匹配并监控该流量。

下图说明根据若干状态的存在或缺失进行匹配的证书状态规则条件。由于配置原因，如果规则与使用由无效用户颁发的证书、自签名证书、无效证书或已到期证书加密的传入流量相匹配，则该规则使用已知密钥来解密流量。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

密码套件 SSL 规则条件

思科提供可向密码套件规则条件中添加的预定义密码套件。您还可以添加包含多个密码套件的密码套件列表对象。

注释 不能添加新的密码套件。不能修改和删除预定义密码套件。

在单个密码套件条件中，可以向**所选密码套件 (Selected Cipher Suites)** 添加最多 50 个密码套件和密码套件列表。系统支持向密码套件条件添加以下密码套件：

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

请注意以下提示：

- 如果添加部署不支持的密码套件，则无法部署配置。例如，被动部署不支持使用任何短 Diffie-Hellman (DHE) 或短椭圆曲线 Diffie-Hellman (ECDHE) 密码套件来解密流量。使用这些密码套件创建规则将会阻止部署访问控制策略。

- 如果使用密码套件配置密码套件条件，则添加到证书条件中的任何外部证书对象或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与密码套件的签名算法类型相匹配。例如，如果规则的密码套件条件引用基于 EC 的密码套件，则添加的任何服务器证书或与 **Decrypt - Resign** 操作相关联的CA证书也必须基于EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告图标。
- 系统无法解密使用匿名密码套件加密的流量。如果向**密码套件 (Cipher Suite)** 条件中添加匿名密码套件，则在 SSL 规则中无法使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作。

按密码套件控制加密流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 Cipher Suite 选项卡。

步骤 2 从**可用密码套件 (Available Cipher Suites)** 中查找要添加的密码套件，如下所示：

- 要即时添加可随后添加到条件中的密码套件列表，请点击**可用密码套件 (Available Cipher Suites)** 列表上方的添加图标 ( )。
- 要搜索要添加的密码套件和列表，请点击**可用密码套件 (Available Cipher Suites)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入密码套件的名称或密码套件中的值。列表会在您键入内容时进行更新，以显示匹配的密码套件。

步骤 3 要选择密码套件，请点击该密码套件。要选择所有密码套件，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击 **Add to Rule**（**添加至规则**）。

提示 您也可以拖放所选密码套件。

步骤 5 添加或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

加密协议版本 SSL 规则条件

可以选择根据使用 SSL V3.0 或 TLS V1.0、V1.1 或 V1.2 加密的流量进行匹配。默认情况下，在创建规则时会选择所有协议版本；如果选择多个版本，则与任何所选版本相匹配的加密流量都与该规则相匹配。保存规则条件时，必须至少选择一个协议版本。

可以在版本规则条件中选择 SSL V2.0；系统不支持解密使用 SSL V2.0 加密的流量。可以配置无法解密的操作来允许或阻止此流量而不进一步检查。

按加密协议版本控制流量

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 规则编辑器中，选择 Version 选项卡。

步骤 2 选择要依据其进行匹配的协议版本。

步骤 3 添加或继续编辑规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 XIII 部分

高级恶意软件防护 (AMP) 和文件控制

第 45 章

文件策略和面向 Firepower 的 AMP

以下主题概述文件控制、文件策略、文件规则，AMP 云连接和动态分析连接。

文件策略和面向 Firepower 的 AMP 概述

恶意软件可以通过多种途径进入企业网络。为帮助您识别并减轻恶意软件的影响，Firepower 系统的面向 *Firepower* 的高级恶意软件防护（面向 Firepower de AMP）功能可以检测、跟踪、存储、分析并选择性阻止网络流量中恶意软件的传输。

您可在整体访问控制配置过程中配置面向 Firepower 的 AMP 和文件控制（允许控制特定类型的所有文件，而不考虑文件是否包含恶意软件）。您创建并与访问控制规则关联的文件策略会处理与规则匹配的网络流量。您可以下载在该流量中检测到的文件，并运行本地恶意软件分析以确定文件是否包含恶意软件。您还可以将文件提交到 AMP Threat Grid 云以进行动态分析，从而确定文件是否表示恶意软件。

系统自动为活动文件策略启用文件事件、恶意软件事件和捕获文件日志记录。当文件策略生成文件或恶意软件事件或者捕获文件时，系统还会自动将关联连接的结尾记录到 Firepower 管理中心数据库。

注释 通过检查 NetBIOS-ssn (SMB) 流量生成的文件事件不会立即生成连接事件，因为客户端和服务器建立持久连接。系统在客户端或服务器结束会话后生成连接事件。

要使分析更具针对性，可以使用恶意软件文件的网络文件轨迹页面跟踪个别威胁随时间推移跨主机进行的传播，从而在最有用的方面集中开展爆发控制和防御工作。

提示 如果您的组织使用面向终端的AMP，则系统可以导入并显示基于终端的数据以及由面向Firepower的 AMP 收集的任何数据。导入此功能无需许可证。

如果您的组织需要额外的安全或要限制外部连接，则您可以使用思科AMP专用云虚拟设备(AMPv)。AMPv 私下收集面向终端的 AMP 事件并将其转发到 Firepower 管理中心。

文件控制和思科 AMP 基础知识

面向 Firepower 的 AMP

借助面向 Firepower 的 AMP，您可以使用内联部署的受管设备检测、存储、跟踪、分析和阻止网络中的恶意软件。面向Firepower的AMP可以阻止许多不同类型的恶意软件文件，包括PDF和Microsoft Office 文档。

文件检测和存储

通过面向 Firepower 的 AMP，受管设备可以监控用于传输特定文件类型的网络流量。

当设备检测到合格文件时，会将该文件的 SHA-256 散列值发送到 Firepower 管理中心。Firepower 管理中心会执行恶意软件云查找，向AMP云查询文件处置情况。设备还可以使用文件存储功能将合格文件存储到硬盘或恶意软件存储包中。您可以在事件查看器中查看捕获的文件信息，并下载副本进行离线分析。

文件分析

系统运用多种文件检测和分析方法来确定文件是否包含恶意软件。

注释 根据您的配置，您可以在系统首次检测到某个文件时对其进行检查并等待云查找结果，也可以在首次检测到文件时不等待云查找结果即对文件放行。

根据您是否启用文件规则中的相关选项，系统将按照以下顺序检查文件：

Spero 分析

如果文件是合格的可执行文件，则设备可以分析文件的结构，并将产生的 Spero 签名提交到 AMP Threat Grid 云。云使用此签名确定文件是否包含恶意软件。

本地恶意软件分析

设备使用本地恶意软件检测引擎检查合格文件，阻止包含恶意软件的文件或者按照配置的文件规则阻止文件，并生成恶意软件事件。

设备还会生成文件构成报告，详细列明文件属性、嵌入的对象和潜在恶意软件。

动态分析

如果设备将文件预分类为潜在恶意软件，则无论设备是否存储文件，都会将这些文件提交到 AMP Threat Grid 云或AMP Threat Grid 本地部署设备进行动态分析。

AMP Threat Grid 云或本地部署的AMP Threat Grid 设备在沙盒环境中运行文件来确定文件是否为恶意文件，然后返回威胁评分，指明文件包含恶意软件的可能性。您可以通过威胁评分查看动态分析摘要报告，该报告详细解释了云给出该威胁评分的原因。

文件和恶意软件事件以及捕获的文件

根据文件分析结果，您可以在事件查看器中查看捕获的文件以及生成的恶意软件和文件事件。您可以仔细查阅文件的构成、处置情况、威胁评分和动态分析摘要报告（如果有这些信息），从而进一步了解恶意软件分析。您还可以访问网络文件轨迹（该图显示文件如何穿过您的网络，在主机间传递）以及各种文件属性。

存档文件

如果文件是存档（例如 `.zip` 或 `.rar` 存档文件），系统可以检查最外层存档文件（级别 0）以下的最多三级嵌套文件。如有任何单个文件与包含阻止操作的文件规则相匹配，系统将阻止整个存档而非该单个文件。系统还可以阻止超过指定嵌套级别的存档，或者内容已加密或无法检查的存档。

文件跟踪

如果文件在 AMP 云中的处置情况据您所知不正确，您可向文件列表中添加该文件的 SHA−-256 值：

- 要好像 AMP 云已为文件分配了干净的处置一样对其进行处理，请将文件添加到干净列表。
- 要好像 AMP 云已为文件分配了恶意软件处置一样对其进行处理，请将文件添加到自定义检测列表。

在后续检测中，设备无需重新评估文件处置情况即可允许或阻止该文件。您可以按文件策略使用干净的列表或自定义检测列表。

注释 您必须将文件策略中的一条规则配置为对匹配的文件执行恶意软件云查找或阻止恶意软件，这样才能计算文件的 SHA-256 值。

恶意软件处置情况

系统根据 AMP 云返回的处置情况来确定文件处置情况。为了提高性能，如果系统已经根据文件的 SHA-256 值知道其处置情况，Firepower 管理中心会使用缓存的处置情况而不是查询 AMP 云。系统可以根据处置情况来阻止文件。如果存档文件中的任何嵌套文件被阻止，系统将阻止整个存档文件。

由于向文件列表中进行添加或由于威胁评分，文件可具有以下其中一个文件处置情况：

- `恶意软件 (Malware)` 表示 AMP 云将文件分类为恶意软件，本地恶意软件分析识别恶意软件，或者文件的威胁评分超过文件策略中定义的恶意软件阈值。

- 干净 (Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。
- 未知 (Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。
- Custom Detection 表示用户将文件添加到自定义检测列表。
- 不可用 (Unavailable) 表示系统无法查询 AMP 云。您可以查看很少一部分事件发生此情况；这是预期行为。

存档文件所具有的性质是基于分配给存档内文件的性质。对于包含已确定的恶意软件文件的**所有**存档，将赋予其 Malware 性质。对于不含已确定恶意软件文件的存档，如果其包含任何未知文件，则其性质为 Unknown；如果其仅包含安全文件，则其性质为 Clean。

表 77：按内容划分的存档文件处置情况

存档文件性质	未知文件数	安全文件数	恶意软件文件数
未知	1 个或更多	任意	0
清洁	0	1 个或更多	0
恶意软件	任何环境	任何环境	1 个或更多

存档文件与其他文件一样可以具有自定义检测 (Custom Detection) 或不可用 (Unavailable) 处置情况（如果符合这些处置情况的条件）。

提示 如果在很短时间内连续看到多个不可用 (Unavailable) 恶意软件事件，请确保 Firepower 管理中心可以与 AMP 云联系。

请注意，文件性质可以更改。例如，AMP 云可以确定先前被视为干净的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是干净的。如果上周查询过的文件的处置情况发生变化，AMP 云会通知系统，使其在下次检测到该文件进行传输时可以自动采取措施。已更改的处置情况称为追溯性处置情况。

从 AMP 云查询返回的处置情况、关联的威胁评分以及本地恶意软件分析分配的处置情况都具有生存时间 (TTL) 值。保持某种处置情况而无更新达到 TTL 值中指定的持续时间后，系统会清除缓存的信息。性质及关联的威胁评分具有以下 TTL 值：

- Clean - 4 小时
- Unknown - 1 小时
- Malware - 1 小时

如果对缓存进行查询发现已超时的缓存处置情况，系统会向 AMP 云重新查询新的处置情况。

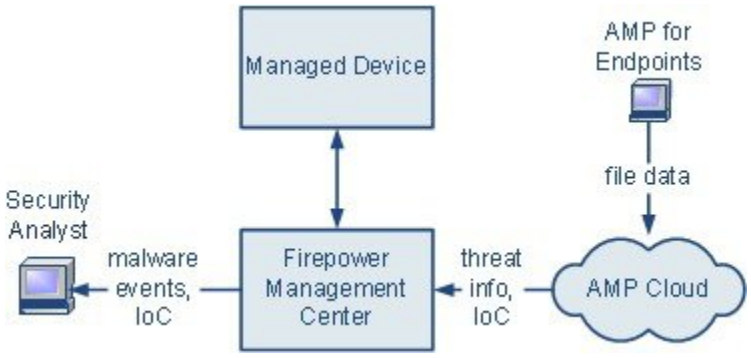
不使用面向 Firepower 的 AMP 的文件控制

如果贵组织不仅要阻止恶意软件文件的传输，还要阻止所有特定类型的文件的传输（无论文件是否包含恶意软件），则可通过文件控制功能来做到这一点。与使用面向 Firepower 的 AMP 一样，受管设备也会监控特定文件类型传输的网络流量，然后阻止或允许文件。

系统可以检测恶意软件的所有文件类型以及许多其他文件类型都支持文件控制。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。请注意，与面向 Firepower 的 AMP 不同，文件控制不需要查询 AMP 云。

面向终端的 AMP

面向终端的AMP是思科的企业级高级恶意软件防护解决方案，能够发现、了解和阻止高级恶意软件爆发、高级持续威胁和针对性攻击。下图详细介绍使用面向终端的 AMP 的一般信息流。



如果您的组织使用面向终端AMP，则个人用户可以在终端（计算机和移动设备）上安装轻量级连接器。连接器可在进行上传、下载、执行、打开、复制、移动等操作后检查文件。这些连接器与AMP云进行通信，以确定检查的文件是否包含恶意软件。

文件被确定为恶意软件后，AMP云会向Firepower管理中心发送威胁识别。AMP云还可以向Firepower管理中心发送其他类型的信息，包括有关扫描、隔离、受阻执行和云召回的数据。Firepower管理中心将这些信息记录为恶意软件事件。

当主机的安全可能受到损害时，面向终端的AMP可以生成危害表现(IOC)。Firepower系统可以为其受监控的主机显示此IOC信息。思科会不时为基于终端的恶意软件事件开发新的IOC类型，系统可自动下载这些类型。

通过面向终端的AMP，您不仅可以根据恶意软件事件配置管理中心发起的纠错和警报，还可以使用面向终端的 AMP 管理控制台帮助您降低恶意软件造成的影响。管理控制台提供稳健灵活的 Web 界面，您可以通过该界面控制面向终端的AMP部署的所有方面并管理爆发的所有阶段。您可以执行以下操作：

- 为整个组织配置自定义恶意软件检测策略和配置文件，以及对所有用户的文件执行快速扫描和全面扫描
- 执行恶意软件分析，包括查看热图、详细文件信息、网络文件轨迹和威胁根本原因

- 配置爆发控制的多个方面，包括自动隔离、用于阻止运行非隔离可执行文件的应用阻止，以及排除列表
- 创建自定义保护，根据组策略阻止某些应用的执行，并创建自定义白名单

提示 有关面向终端的 AMP 的详细信息，请参阅面向终端的 AMP 管理控制台。

面向 Firepower 的 AMP 与面向终端的 AMP

您可以将 Firepower 系统与来自面向 Firepower 的 AMP 和面向终端的 AMP 的数据配合使用。

由于面向终端的AMP恶意软件检测是在恶意软件下载或执行时在终端执行的，而受管设备则是检测网络流量中的恶意软件，因此这两种恶意软件事件中的信息是不同的。例如，基于终端的恶意软件事件包含有关文件路径、调用客户端应用等等的信息，而网络流量中的恶意软件检测则包含有关用于传输文件的连接的端口、应用协议和始发 IP 地址信息。

再例如，在基于网络的恶意软件事件中，用户信息向用户展示此用户最近登录的主机是恶意软件的攻击目标，并且恶意软件是由网络发现功能确定的。但是，面向终端的AMP报告的用户是指当前登录其中检测到恶意软件的终端的用户。

注释 根据您的部署，面向终端的 AMP 监控的终端可能不是与面向 Firepower 的 AMP 监控的终端相同的主机。因此，基于终端的恶意软件事件不将主机添加到网络映射。但是，系统会使用 IP 和 MAC 地址数据标记具有从面向终端的 AMP 部署获取的危害表现的受监控主机。如果不同 AMP 解决方案监控的两个不同主机具有相同的IP和MAC地址，则系统可能会错误地标记具有面向终端的 AMP 危害表现 (IOC) 的受监控主机。

下表总结了这两种策略之间的差异。

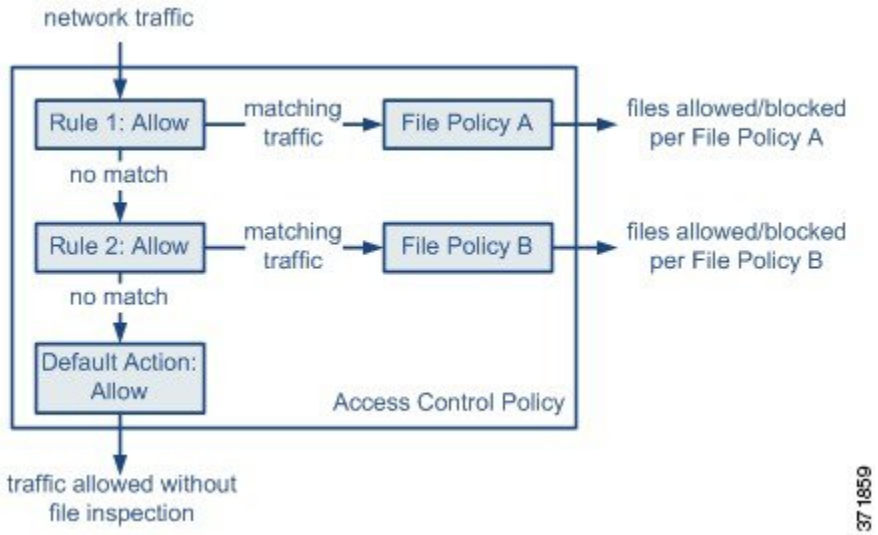
表 *78*：基于网络的高级恶意软件防护策略与基于终端的高级恶意软件防护策略

特性	面向 Firepower 的 AMP	面向终端的 AMP
文件类型检测和阻止方法（文件控制）	在网络流量中，使用访问控制和文件策略	不支持
恶意软件检测和阻止方法	在网络流量中，使用访问控制和文件策略	在单个终端上，使用与 AMP 云进行通信的连接器
检查的网络流量	流量传递通过受管设备	无；终端上安装的连接器直接检查文件
恶意软件检测稳健性	有限的文件类型	所有文件类型
恶意软件分析方案	基于管理中心的分析，以及在 AMP 云中的分析	基于管理中心的分析，以及面向终端的 AMP 管理控制台上的其他方案

特性	面向 Firepower 的 AMP	面向终端的 AMP
恶意软件缓解	网络流量中的恶意软件阻止，管理中心发起的纠错	基于面向终端的 AMP 的隔离和爆发控制方案，管理中心发起的纠错
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于管理中心	基于管理中心的分析，以及面向终端的 AMP 管理控制台上的其他方案
必需许可证或订用	执行文件控制和面向 Firepower 的 AMP 所需的许可证	面向终端的 AMP 订用（并非基于许可证）

文件策略

文件策略是一系列配置，系统将其用作整体访问控制配置的一部分，以执行面向 Firepower 的 AMP 和文件控制。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。在内联部署中，可考虑下图所示的简单访问控制策略。



策略有两个访问控制规则，两者都使用 Allow 操作并与文件策略关联。策略的默认操作也是允许流量，但不执行文件策略检查。在本示例中，流量处理如下：

- 与 `Rule 1` 匹配的流量根据 `File Policy A` 进行检查。

- 与 Rule 1 不匹配的流量根据 Rule 2 进行评估。与 Rule 2 匹配的流量根据 File Policy B 进行检查。
- 允许与任一规则不匹配的流量；不能将文件策略与默认操作关联。

可以将单个文件策略与其操作为 **Allow**、**Interactive Block** 或 **Interactive Block with reset** 的访问控制规则关联。这样，系统将会使用该文件策略检查符合访问控制规则条件的网络流量。

通过将不同文件策略与不同访问控制规则相关联，可以精细控制如何识别并阻止网络上传输的文件。但请注意，您**不能**使用文件策略检查由访问控制默认操作处理的流量。

文件策略高级配置

高级文件检查配置说明

在文件策略中，可以配置高级选项以阻止自定义检测列表上的文件，允许干净列表上的文件，以及设置威胁评分阈值（高于该阈值的文件被视为恶意软件）。

您还可以将文件策略配置为检查存档文件的内容，从而允许根据您的组织的需求分析和阻止存档文件。所有适用于未压缩的文件的功能（例如，动态分析和文件存储）也适用于存档文件中的嵌套文件。

存档文件检查说明

某些存档文件包含其他的存档文件（以此类推）。文件嵌套的级别是其存档文件深度。请注意，深度计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

虽然系统最多只能检查 3 级嵌套存档文件，但是可以将文件策略配置为阻止超过该深度（或指定的较低最文件深度）的存档文件。如果要进一步限制嵌套文件，则可以选择配置较低的最大文件深度（2 或 1）。

如果您选择不阻止超过最大存档文件深度 3 的文件，当受监控流量中出现包含某些可提取内容和某些嵌套深度为 3 或更大值的内容的存档文件时，系统仅检查其能够检查的文件并报告相关数据。

注释 如果包含存档文件的流量被安全情报列入黑名单或白名单，或者，如果顶级存档文件的 SHA - 256 值在自定义检测列表中，则系统将不检查该存档文件的内容。如果嵌套文件被列入黑名单，则整个存档也将被阻止；但是，如果嵌套文件被列入白名单，则存档不会自动通过（取决于任何其他嵌套文件和特性）。

如将文件策略配置为检查存档文件内容，当存档文件出现在文件事件、恶意软件事件或捕获的文件中时，可以使用事件查看器上下文菜单和网络文件轨迹查看器查看有关存档内部文件的信息。

存档的所有文件内容均以表形式列出，同时显示其相关信息的摘要：名称、SHA-256 哈希值、类型、类别和存档深度。每个文件旁边都会显示一个网络文件轨迹图标，点击该图标即可查看有关该特定文件的详细信息。

文件策略配置说明和限制

- 对于新策略，网络界面会指出该策略未在使用。如果编辑的是使用中的文件策略，则网络界面会告知您使用该文件策略的访问控制策略的数量。在任一情况下，可以点击文本以跳至“访问控制策略”(Access Control Policies) 页面。
- 对于使用适合于 FTP 的具有 **Block Malware** 规则的访问控制策略，如果将默认操作设置为已禁用 **Drop when Inline** 的入侵策略，则系统会为检测到的与规则匹配的文件或恶意软件生成事件，但不丢弃文件。要阻止FTP文件传输并使用入侵策略作为在其中选择文件策略的访问控制策略的默认操作，必须选择已启用 **Drop when Inline** 的入侵策略。

管理文件策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（文件控制） 恶意软件（面向 Firepower 的 AMP）	保护（文件控制） 恶意软件（面向 Firepower 的 AMP）	任何环境	任何环境	管理员/访问管理员

“文件策略”(File Policies) 页面显示现有文件策略的列表及其上次修改日期。您可以使用此页面来管理文件策略。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

注释 系统会检查 AMP 云以获取适合于动态分析的文件类型列表的更新（最多一天一次）。如果合格文件类型列表更改，这会构成文件策略发生更改；任何使用该文件策略的访问控制策略在部署于任何设备时都会标记为过期。在更新的文件策略可在设备上生效之前，必须先部署策略。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **恶意软件和文件 (Malware & File)**。

步骤 2 管理文件策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 261 页。
- 创建 - 要创建文件策略，请点击**新建文件策略 (New File Policy)**，然后如创建文件策略，第 758 页中所述继续操作。
- 复制 - 要复制文件策略，请点击复制图标 ()。

  如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

- 删除 - 如果要删除文件策略，请点击删除图标 ( )，然后按照提示点击**是 (Yes)** 和**确定 (OK)**。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改，第 254 页。
- 编辑 - 如果要修改现有文件策略，请点击编辑图标 ( )。
- 报告 - 点击报告图标 ( )；请参阅生成当前策略报告，第 262 页。

创建文件策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（文件控制） 恶意软件（面向 Firepower 的 AMP）	保护（文件控制） 恶意软件（面向 Firepower 的 AMP）	任何环境	任何环境	管理员/访问管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **恶意软件和文件 (Malware & File)**。

提示 要复制现有文件策略，请点击复制图标 ( )，然后在出现的对话框中为新策略键入唯一名称。然后就可以修改副本。

步骤 2 点击 **New File Policy**。

步骤 3 输入新策略的**名称 (Name)** 和可选**说明 (Description)**。

步骤 4 点击**保存 (Save)**。

步骤 5 如创建文件规则，第 764 页中所述，向文件策略添加一个或多个规则。

步骤 6 或者，也可以选择“高级”(Advanced) 选项卡，并如高级和存档文件检查选项，第 759 页中所述配置高级选项。

步骤 7 保存文件策略。

接下来的操作

- 如用于执行文件控制和恶意软件防护的访问控制规则配置，第 640 页中所述，将该文件策略添加到访问控制规则。
- 部署配置更改；请参阅部署配置更改，第 254 页。

高级和存档文件检查选项

文件策略编辑器中的“高级”(Advanced) 选项卡具有以下常规选项：

- **首次文件分析 (First Time File Analysis)** - 为系统首次检测到的文件分析提交文件。该文件必须与配置为执行恶意软件云查找和 Spero、本地恶意软件或动态分析的规则相匹配。如果禁用此选项，则会将首次检测到的文件标记为具有“未知”(Unknown) 处置情况。
- **启用自定义检测列表 (Enable Custom Detection List)** - 阻止自定义检测列表上的文件
- **启用干净列表 (Enable Clean List)** - 允许干净列表上的文件
- **根据动态分析威胁评分将文件标记为恶意软件 (Mark files as malware based on dynamic analysis threat score)** - 设置阈值威胁评分；评分等于或低于阈值的文件被视为恶意软件

  如果选择更低的阈值，请增加被视为恶意软件的文件数。根据文件策略中选择的操作，这可能导致受阻文件数增加。

文件策略编辑器中的“高级”(Advanced) 选项卡具有以下存档文件检查选项：

- **检查存档 (Inspect Archives)** - 允许检查存档文件的内容

  注意 启用或禁用存档文件检查在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

- **阻止已加密存档 (Block Encrypted Archives)** - 允许阻止具有加密内容的存档文件
- **阻止不可检查存档 (Block Uninspectable Archives)** - 允许阻止系统因加密以外的其他原因而无法检查其内容的存档文件；这通常适用于受损文件或超过指定的最大存档深度的存档文件。
- **最大存档深度 (Max Archive Depth)** - 允许阻止超过指定深度的嵌套存档文件；此计数未考虑顶级存档文件；第一个嵌套文件的深度从 1 开始

编辑文件策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（文件控制） 恶意软件（面向 Firepower 的 AMP）	保护（文件控制） 恶意软件（面向 Firepower 的 AMP）	任何环境	任何环境	管理员/访问管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **恶意软件和文件 (Malware & File)**。

步骤 2 点击要编辑的文件策略旁边的编辑图标 ( )。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 您有以下选择：

- 通过选择**添加文件规则 (Add File Rule)** 来添加文件规则。有关详细信息，请参阅文件规则，第 760 页。
- 通过点击要编辑的规则旁边的编辑图标 ( ) 来编辑现有文件规则。
- 配置高级选项，如高级和存档文件检查选项，第 759 页中所述。

注释 文件策略编辑器显示使用当前正在编辑的文件策略的访问控制策略数量。可以点击通知以显示父策略的列表，并或者转至 Access Control Policies 页面。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

文件规则

文件策略（例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

文件与某个规则匹配后，规则可以：

- 根据简单文件类型匹配允许或阻止文件
- 根据处置情况阻止文件
- 将捕获文件存储到设备
- 提交捕获的文件以进行本地恶意软件、Spero 或动态分析

此外，文件策略还可以：

- 根据白名单或自定义检测列表中的条目自动将文件视为安全文件或恶意软件
- 在文件的威胁评分超过可配置阈值时将文件视为恶意软件
- 检查存档文件（例如，`.zip` 或 `.rar`）的内容
- 阻止内容已加密，嵌套超过指定的最大存档深度或因其他原因无法检查的存档文件

文件规则组成部分

表 *79*: 文件规则组成部分

文件规则组件	说明
应用协议	系统可以检测和检查通过 FTP、HTTP、SMTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传输的文件。**Any**（默认值）检测 HTTP、SMTP、IMAP、POP3、FTP 和 NetBIOS-ssn (SMB) 流量中的文件。为了提高性能，可以逐个文件规则将文件检测仅限于其中一种应用协议。
传输方向	对于已下载的文件，可以检查通过 FTP、HTTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传入的流量；对于已上传的文件，可以检查通过 FTP、HTTP、SMTP 和 NetBIOS-ssn (SMB) 传出的流量。 **提示** 无论用户是发送还是接收，使用 **Any** 都可通过多种应用协议检测文件。
文件类别和类型	系统检测各种类型的文件。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。可以配置用于检测个别文件类型或整个类别的文件类型的规则。 例如，可以阻止所有多媒体文件，或者仅阻止 ShockWave Flash (swf) 文件。或者，可以将系统配置为会在用户下载 BitTorrent (torrent) 文件时向您发出警报。 **注释** 频繁触发的文件规则可能会影响系统性能。例如，检测 HTTP 流量（例如 YouTube，用于传输重要的 Flash 内容）中的多媒体文件可能会产生可能生成数量巨大的事件。
文件规则操作	文件规则操作用于确定系统如何处理与规则条件相符的流量。 根据所选操作，您可以配置系统是存储文件还是对文件执行 Spero、本地恶意软件或动态分析。如果选择“阻止”(Block) 操作，还可以配置系统是否还重置受阻连接。 **注释** 文件规则是以规则操作顺序而非数字顺序进行评估。

文件规则操作和评估顺序

文件策略必须包含一个或多个规则才能生效。借助文件规则，可以精细控制要对其记录、阻止或扫描恶意软件的文件类型。

每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。可以在文件策略中设置单独的规则，以对不同的文件类型、应用协议或传输方向采取不同操作。简单阻止优先于恶意软件检查和阻止，后者优先于简单检测和日志记录。

规则操作如下（按规则操作顺序列出）：

- 阻止文件 *(Block Files)* 规则允许您阻止特定文件类型。您可以配置选项，以在阻止文件传输时重置连接并将已捕获的文件存储到受管设备。

- 阻止恶意软件 *(Block Malware)* 规则允许您计算特定文件类型的 SHA-256 散列值，查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止表示为威胁的文件。
- 恶意软件云查找 *(Malware Cloud Lookup)* 规则允许您获取并记录通过网络传输的文件的处置情况，同时仍允许文件传输。
- 检测文件 *(Detect Files)* 规则允许您将特定文件类型的检测记录到数据库，同时仍允许文件传输。

注意 将文件规则操作更改为**检测文件 (Detect Files)** 或**阻止恶意软件 (Block Malware)** 或从其进行更改，或者启用或禁用**存储文件 (Store files)**，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

您可以根据每项文件规则操作配置选项，以在阻止文件传输后重置连接，将捕获的文件存储到受管设备，在本地对文件进行恶意软件分析，将捕获的文件提交到 AMP 云进行动态分析和 Spero 分析，并存储当前无法提交到云的文件以便稍后提交。

表 *80*：文件规则操作

文件规则操作选项	能否阻止文件？	能否阻止恶意软件？	能否检测文件？	能否进行恶意软件云查找？
MSEXE 的 Spero 分析	否	是，可以提交可执行文件	否	是，可以提交可执行文件
动态分析	否	是，可以提交具有未知文件处置情况的可执行文件	否	是，可以提交具有未知文件处置情况的可执行文件
容量处理	否	是	否	yes
本地恶意软件分析	否	是	否	yes
重置连接	是（推荐）	是（推荐）	否	否
存储文件	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型

文件策略说明和限制

文件规则配置说明和限制

- 配置为在被动部署中阻止文件的规则不会阻止匹配的文件。由于连接继续传输文件，因此如果配置规则以记录连接的开始，则您可能会看到为此连接记录的多个事件。
- 如果文件规则配置有**恶意软件云查找 (Malware Cloud Lookup)** 或**阻止恶意软件 (Block Malware)** 操作，并且Firepower 管理中心无法与 AMP 云建立连接，则系统无法执行任何已配置的规则操作选项，直到恢复连接为止。
- 思科建议启用**重置连接 (Reset Connection)**（适用于**阻止文件 [Block Files]** 和**阻止恶意软件 [Block Malware]** 操作）以防止受阻应用会话保持打开，直到 TCP 连接重置为止。如果不重置连接，则客户端会话会保持打开，直到 TCP 连接重置为止。
- 如果监控大量流量，请**勿**存储所有捕获文件，或者将所有捕获文件提交进行动态分析。否则可能对系统性能产生不利影响。
- 不能对系统检测到的所有文件类型都执行恶意软件分析。从 **Application Protocol**、**Direction of Transfer** 和 **Action** 下拉列表中选择值之后，系统会对文件类型的列表进行约束。

文件检测说明和限制

- 如果文件与带有应用协议条件的规则相匹配，在系统成功确定该文件的应用协议之后，会生成文件事件。无法识别的文件不生成文件事件。
- FTP 通过不同信道传输命令和数据。在被动或内嵌分路器模式部署中，FTP 数据会话中的流量及其控制会话可能不会被负载均衡到同一个 Snort。
- 如果 POP3、POP、SMTP 或 IMAP 会话中文件的所有文件名的总字节数超过 1024，则会话中的文件事件可能无法反映文件名缓冲区填充后检测到的文件的正确文件名。
- 当通过 SMTP 传输基于文本的文件时，某些邮件客户端会将换行符转换为 CRLF 换行符标准。由于基于 MAC 的主机使用回车 (CR) 字符，并且基于 Unix/Linux 的主机使用换行 (LF) 字符，因此，邮件客户端进行的换行可能修改文件的大小。注意某些邮件客户端在处理无法识别的文件类型时默认进行换行。

文件阻止说明和限制

- 无论使用何种传输协议，如果未检测到文件的文件结尾标记，**Block Malware** 规则或自定义检测列表不会阻止该文件。系统会等待接收整个文件后再阻止文件（如文件结尾标记所指示），并在检测到该标记后阻止文件。
- 如果 FTP 文件传输的文件结尾标记单独从最后一个数据段进行传输，则会阻止该标记，并且 FTP 客户端会指示文件传输失败，但是文件实际上将完整传输到磁盘。

- 具有 **Block Files** 和 **Block Malware** 操作的文件规则会阻止通过 HTTP 自动恢复文件下载，方法是在进行初始文件传输尝试后检测到相同的文件、URL、服务器和客户端应用达到 24 小时的情况下阻止新会话。
- 在极少数情况下，如果来自 HTTP 上传会话的流量顺序错误，则系统无法正确重组流量，并因此不会阻止该会话或生成文件事件。
- 如果通过 NetBios-ssn 传输使用 **Block Files** 规则阻止的文件（例如 SMB 文件传输），则目标主机上可能会显示文件。但是，该文件不可用，原因是在下载启动后阻止了该文件，导致文件传输未完成。
- 如果创建文件规则以检测或阻止通过 NetBios-ssn 传输的文件（例如 SMB 文件传输），则系统不检查在部署调用文件策略的访问控制策略前启动的已建立的 TCP 或 SMB 会话中传输的文件，因此不会检测或阻止这些文件。

创建文件规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（文件控制） 恶意软件（面向 Firepower 的 AMP）	保护（文件控制） 恶意软件（面向 Firepower 的 AMP）	任何环境	任何环境	管理员/访问管理员

注意 添加或删除文件类型或文件类别，将文件规则操作更改为**检测文件 (Detect Files)** 或**阻止恶意软件 (Block Malware)** 或从其进行更改；或者启用或禁用**存储文件 (Store files)**在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在文件策略编辑器中，点击**添加文件规则 (Add File Rule)**。

步骤 2 选择**应用协议 (Application Protocol)** 和**传输方向 (Direction of Transfer)**，如文件规则组成部分，第 761 页中所述。

步骤 3 选择一个或多个**文件类型**。可以通过以下方式过滤文件类型列表：

- 在**文件类型类别 (File Type Categories)** 中选择一个或多个文件类型类别，然后点击**所选类别中的所有类型 (All types in selected Categories)**。
- 按名称或描述搜索文件类型。例如，在 **Search name and description** 字段中键入 Windows 将会显示 Microsoft Windows 专用文件的列表。

提示　将指针悬停在文件类型上方可查看其描述。

步骤 4　在操作 **(Action)** 中选择文件规则操作，如文件规则操作和评估顺序，第 761 页中所述。

步骤 5　根据选择的操作，配置是否要执行以下操作：

- 在阻止文件后重置连接
- 存储匹配文件
- 启用 Spero 分析
- 启用本地恶意软件分析
- 启用动态分析和容量处理

如文件规则操作和评估顺序，第 761 页中所述。

步骤 6　点击 **Add**。

步骤 7　点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

云连接

Firepower 系统提供到以下基于公共云的服务器的连接，以帮助您执行思科高级恶意软件防护 (AMP)：

- AMP 云 - 您可通过其检索面向 Firepower 的 AMP 恶意软件处置情况和更新，以及面向终端的 AMP 扫描记录、恶意软件检测、隔离和危害表现 (IOC)
- AMP Threat Grid 云 - 您可通过其提交合格文件以用于面向 Firepower 的 AMP 动态分析，并且检索威胁评分和动态分析报告

根据您的组织的隐私或安全需求，您还可以部署私有云服务器：

- AMP 私有云虚拟设备 (AMPv) 用作压缩的内部 AMP 云。
- AMP Threat Grid 设备用作不联系公共 AMP Threat Grid 云的内部 AMP Threat Grid 云。

AMP 云连接

高级恶意软件防护 (AMP) 云是一种思科托管服务器，它使用大数据分析和持续分析帮助您检测和阻止网络上的恶意软件。两种思科 AMP 解决方案都使用 AMP 云：

- 面向 Firepower 的 AMP 使用 AMP 云检索由受管设备在网络流量中检测到的潜在恶意软件的处置情况，并获取本地恶意软件分析结果和文件预分类更新信息。

- 面向终端的 AMP 是思科的企业级 AMP 解决方案。个人用户在其通过 AMP 云通信的计算机和移动设备上安装轻量级连接器。然后，Firepower管理中心可导入扫描记录、恶意软件检测和隔离以及危害表现 (IOC)。

根据您的部署，面向终端的 AMP 监控的终端可能不是与面向 Firepower 的 AMP 监控的终端相同的主机。因此，基于终端的恶意软件事件不将主机添加到网络映射。但是，系统会使用 IP 和 MAC 地址数据标记具有从面向终端的 AMP 部署获取的危害表现的受监控主机。如果不同 AMP 解决方案监控的两个不同主机具有相同的 IP 和 MAC 地址，则系统可能会错误地标记具有面向终端的 AMP 危害表现 (IOC) 的受监控主机。

使用 AMP 管理页面（**AMP** > **AMP 管理 (AMP Management)**）管理与 AMP 云的连接。默认情况下，为面向 Firepower 的 AMP 配置并启用与美国 (US) AMP 公共云的连接。您无法删除或禁用面向 Firepower 的 AMP 云连接，但是可以在欧盟 (EU) 和美国 (US) AMP 云之间切换，或者配置私有云 (AMPv) 连接。

要为终端添加单独的FireAMP连接，您必须在FireAMP门户中拥有帐户。尚未成功注册到门户的面向终端的 AMP 连接不会禁用面向 FirePOWER 的 AMP。

AMP 云连接的要求

- 面向网络的 AMP - 无论您使用公共还是私有 AMP 云，系统都会使用端口 443 为面向网络的 AMP 执行恶意软件云查找。您必须从 Firepower 管理中心打开用于通信的端口（出站）。
- 面向终端的 AMP - 系统使用端口 443/HTTPS 连接到思科云（公共或私有）以接收基于终端的恶意软件事件。您必须通过 Firepower 管理中心打开用于通信的端口（出站和入站）。此外，Firepower 管理中心必须可以直接访问互联网。默认运行状况策略包括 AMP 状态监控，如果 Firepower 管理中心在初始成功连接后无法连接到云，或者如果使用 AMP 门户注销了连接，则会向您发出警告。

要使用传统端口进行 AMP 通信，请参阅综合安全情报通信配置选项，第 772 页。

AMP 云连接和多租户

在多域部署中，您只能在全局级别配置面向 Firepower 的 AMP 连接。每个 Firepower 管理中心只能有一个面向 Firepower 的 AMP 连接。假设您为每个连接使用单独的面向终端的 AMP 帐户，则您可以在所有域级别配置面向终端的AMP连接。例如，MSSP 的每个客户端都可能拥有自己的面向终端的 AMP 部署。

注意 思科强烈建议您仅在枝叶级别配置面向终端的 AMP 连接，尤其是如果您的枝叶域拥有重叠的 IP 空间。如果多个子域具有IP-MAC地址对相同的主机，则系统可能会将基于终端的恶意软件事件保存到错误的枝叶域，或将 IOC 与错误的主机相关联。

配置面向终端的 AMP 云连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果您的组织已部署面向终端的 AMP，则可以将威胁识别、危害表现 (IOC) 和其他恶意软件相关信息从 AMP 云导入到系统。即使已配置面向 Firepower 的 AMP 连接，也必须配置面向终端的 AMP 连接。

注意 在多域部署中，思科强烈建议仅在枝叶级别配置面向终端的 AMP 连接，尤其是在枝叶域具有重叠的 IP 空间的情况下。如果多个子域具有 IP-MAC 地址对相同的主机，则系统可能会将基于终端的恶意软件事件保存到错误的枝叶域，或将 IOC 与错误的主机相关联。

开始之前

- 如果您是在将 Firepower 管理中心恢复为出厂默认设置或还原为先前版本之后连接到 AMP 云，请使用面向终端的 AMP 管理控制台删除先前连接。

过程

步骤 1 选择**AMP** > **AMP 管理 (AMP Management)**。

步骤 2 点击**创建 AMP 云连接 (Create AMP Cloud Connection)**。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择要使用的云：

- 对于欧盟 AMP 云，选择 **EU 云 (EU Cloud)**。
- 对于美国 AMP 云，选择 **US 云 (US Cloud)**。
- 对于 AMPv，选择**私有云 (Private Cloud)**，然后如思科 AMP 私有云，第 768 页中所述继续操作。

步骤 4 如果要将此云用于面向 Firepower 的 AMP 和面向终端的 AMP，请选中**用于面向 Firepower 的 AMP (Use for AMP for Firepower)** 复选框。
在多域部署中，此复选框仅显示在全局域中。每个 Firepower 管理中心只能有一个面向 Firepower 的 AMP 连接。

步骤 5 点击 **Register**。
旋转状态图标指示连接处于待处理状态，例如，在 Firepower 管理中心上配置连接后，但在使用面向终端的 AMP 管理控制台对其进行授权之前。失败或拒绝图标 ( ) 表示云已拒绝连接，或者连接因其他原因而失败。

步骤 6 确认是否要继续访问面向终端的 AMP 管理控制台，然后登录管理控制台中。

步骤 7 使用管理控制台，授权 AMP 云以将面向终端的 AMP 数据发送到 Firepower 管理中心。

步骤 8 如果要限制接收的数据，请选择您的组织中要为其接收信息的特定组。
默认情况下，AMP 云发送所有组的数据。要管理组，请在面向终端的 AMP 管理控制台上依次选择**管理 (Management)** > **组 (Groups)**。有关详细信息，请参阅设备管理器联机帮助。

步骤 9 点击**允许 (Allow)** 以启用连接并开始传输数据。

点击**拒绝 (Deny)** 会将您返回到 Firepower 管理中心，其中连接标记为已拒绝。如果离开面向终端的 AMP 管理控制台上的“应用”(Applications) 页面，并且既未拒绝也未允许连接，则连接在 Firepower 管理中心的 Web 界面上标记为待处理。运行状况监控器在其中任一情况下不提示您连接失败。如果稍后要连接到 AMP 云，请删除失败或待处理的连接，然后重新创建连接。

面向终端的 AMP 连接注册不完整不会禁用面向 Firepower 的 AMP 连接。

思科 AMP 私有云

您可以配置思科 AMP 私有云虚拟设备 (AMPv) 以收集与您的网络有关的终端数据。AMPv 是一台思科专有虚拟机，用作压缩内部版 AMP 云。

所有面向终端的 AMP 连接器将数据发送到 AMPv，AMPv 会将该数据转发到 Firepower 管理中心。AMPv 不通过外部连接共享任何终端数据。Firepower 管理中心连接到公共 AMP 云，对在网络流量中检测到的文件进行处置情况查询并接收追溯性恶意软件事件。

每个私有云可支持多达 10,000 个面向终端的 AMP 连接器，并且您还可以配置多个私有云。

使用 Firepower 管理中心上的“AMP 管理”(AMP Management) 页面（**AMP** > **AMP 管理 (AMP Management)**），管理到 AMPv 的连接。

注释 动态分析（一个面向 FirePOWER 的 AMP 的组件）要求受管设备具有对 AMP Threat Grid 云或端口 443 上的内部 AMP Threat Grid 设备的直接或代理访问权限。AMPv 既不支持动态分析，也不支持匿名检索其他依靠思科综合安全情报 (CSI)（例如，URL 和安全情报过滤）的功能的威胁情报。

连接到 *AMPv*

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件（面向 Firepower 的 AMP） 任意（面向终端的 AMP）	恶意软件（面向 Firepower 的 AMP） 任意（面向终端的 AMP）	任何环境	任何环境	管理

开始之前

- 根据 AMPv 文档中的方向配置思科 AMP 私有云。在配置过程中，请记下私有云的主机名。稍后需要使用此主机名配置 Firepower 管理中心上的连接。
- 确保 Firepower 管理中心可与 AMPv 通信，并确认 AMPv 可访问互联网，以便它可与 AMP 云通信。

过程

步骤 1 选择**AMP** > **AMP 管理 (AMP Management)**。

步骤 2 点击**创建 AMP 云连接 (Create AMP Cloud Connection)**。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择**私有云 (Private Cloud)**。

步骤 4 输入 **Name**。
此信息显示在 AMPv 生成或传输的恶意软件事件中。

步骤 5 在**主机 (Host)** 字段中，输入在设置 AMPv 时配置的私有云主机名。

步骤 6 点击**证书上传路径 (Certificate Upload Path)** 旁边的**浏览 (Browse)**，浏览至 AMPv 的有效 TLS 或 SSL 加密证书的位置。有关详细信息，请参阅 AMPv 文档。

步骤 7 如果要将此私有云用于面向 Firepower 的 AMP 和面向终端的 AMP，请选中**用于面向 Firepower 的 AMP (Use for AMP for Firepower)** 复选框。
如果配置其他私有云来处理面向 Firepower 的 AMP 通信，则可以清除此复选框；如果这是唯一的 AMPv 连接，则无法清除。

在多域部署中，此复选框仅显示在全局域中。每个 Firepower 管理中心只能有一个面向 Firepower 的 AMP 连接。

步骤 8 要使用代理与 AMPv 进行通信，请选中**使用代理连接 (Use Proxy Connections)** 复选框。

步骤 9 点击**注册 (Register)**，确认要禁用到 AMP 云的现有直接连接，并最终确认要继续至 AMPv 管理控制台以完成注册。

步骤 10 登录管理控制台并完成注册过程。有关进一步说明，请参阅 AMPv 文档。

管理 AMP 云和 AMPv 连接

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件（面向 Firepower 的 AMP） 任意（面向终端的 AMP）	恶意软件（面向 Firepower 的 AMP） 任意（面向终端的 AMP）	任何环境	任何环境	管理

如果不想再从云接收恶意软件相关信息，请使用 Firepower 管理中心删除 AMP 云或 AMPv 连接。请注意，使用面向终端的 AMP 或 AMPv 管理控制台注销连接不会从系统中删除连接。注销连接会在 Firepower 管理中心 Web 界面上显示失败状态。

您还可以临时禁用连接。当重新启用云连接时，云恢复向系统发送数据，包括禁用期内的已排队数据。

注意 对于已禁用的连接，AMP 云和 AMPv 可以存储恶意软件事件和危害表现等，直到重新启用连接。在极少数情况下（例如，事件率超高或连接长时间禁用），云可能无法存储在连接处于禁用状态时生成的所有信息。

在多域部署中，系统会显示在当前域中创建的连接，您可以对其进行编辑。系统还会显示在祖先域中创建的连接，您不可以对其进行管理。要管理较低域中的连接，请切换至该域。每个 Firepower 管理中心只能具有一个属于全局域的面向 Firepower 的 AMP 连接。

过程

步骤 1 选择**AMP** > **AMP 管理 (AMP Management)**。

步骤 2 管理 AMP 云连接：

- 删除 - 点击删除图标 ( )，然后确认选择。
- 启用或禁用 - 点击滑块，然后确认选择。

动态分析连接

AMP Threat Grid 云在沙盒环境中运行文件。面向 FirePOWER 的 AMP 使用云，为提交进行动态分析的文件检索威胁评分和动态分析报告。通过适当的许可证，系统会自动访问云。

如果您的组织的安全策略不允许 FirePOWER 系统发送网络外部的文件，则您可以配置内部 AMP Threat Grid设备。有关详细信息，请参阅《思科 *AMP Threat Grid* 设备设置和配置指南》。

使用 Firepower 管理中心上的“动态分析连接”(Dynamic Analysis Connections) 页面（**AMP** > **动态分析连接 (Dynamic Analysis Connections)**），管理到 AMP Threat Grid云的公共动态分析连接，以及到本地 AMP Threat Grid设备的私有动态分析连接。

查看默认动态分析连接

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任意	仅全局	管理员/访问管理员/网络管理员

默认情况下，Firepower 管理中心可以连接到 AMP Threat Grid 公共云提交文件并检索报告。您既不能配置也不能删除此连接。

过程

步骤 1 选择**AMP** > **动态分析连接 (Dynamic Analysis Connections)**。

步骤 2 点击编辑图标 ( )。

Threat Grid 内部设备

如果您的组织担心提交文件到公共 AMP Threat Grid 云可能会造成隐私或安全问题，您可以部署内部 AMP Threat Grid 设备。如同公共云一样，内部设备在沙盒环境下运行合格文件，然后向 Firepower 系统传回威胁评分和动态分析报告。但是，内部设备不会与公共云或位于您的网络外部的任何其他系统通信。

可以将一个内部 AMP Threat Grid 设备连接到 Firepower 管理中心。有关详细信息，请参阅《思科 *AMP Threat Grid* 设备设置和配置指南》。

如果配置与内部设备的动态分析连接，则系统使用公共 AMP 云执行恶意软件云查找，并验证文件是否先前未提交进行动态分析。

系统还使用与 AMP 云的默认公共动态分析连接进行公共报告检索。如果内部设备未生成文件的动态分析报告，则系统会查询 AMP 云以获取动态分析报告。除非您的组织提交文件，否则只能查看包含有限数据的已清理报告。

配置本地动态分析连接

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任意	仅全局	管理员/访问管理员/网络管理员

如果在网络上安装内部 AMP Threat Grid 设备，则可以配置动态分析连接以提交文件并从该设备中检索报告。当配置内部设备动态分析连接时，可将 Firepower 管理中心注册到内部设备。

开始之前

- 设置内部 AMP Threat Grid 设备；请参阅《思科 *AMP Threat Grid* 设备设置和配置指南》。
- 从 AMP Threat Grid 设备下载公钥证书以用于登录内部设备；请参阅《思科 *AMP Threat Grid* 设备管理员指南》。
- 如果要使用代理连接到内部设备，请配置代理；请参阅编辑管理接口，第 443 页。

过程

步骤 1 选择**AMP** > **动态分析连接 (Dynamic Analysis Connections)**。

步骤 2 点击**添加新连接 (Add New Connection)**。

步骤 3 输入 **Name**。

步骤 4 输入**主机 URL (Host URL)**。

步骤 5 在**证书上传 (Certificate Upload)** 中，点击**浏览 (Browse)** 以上传要用于与内部设备建立连接的公钥证书。

步骤 6 如果要使用已配置的代理建立连接，请选择**在可用时使用代理 (Use Proxy When Available)**。

步骤 7 点击 **Register**。

步骤 8 点击**是 (Yes)** 以显示内部 AMP Threat Grid 设备登录页面。

步骤 9 将用户名和密码输入到内部 AMP Threat Grid 设备。

步骤 10 点击 **Sign in**（登录）。

步骤 11 您有以下选择：

- 如果先前将 Firepower 管理中心注册到内部设备，请点击**返回 (Return)**。
- 如果未注册 Firepower 管理中心，请点击**激活 (Activate)**。

综合安全情报通信配置

Firepower 系统针对信誉、风险和威胁情报使用思科的综合安全情报 (CSI)。通过正确的许可证，您可以为 URL 过滤和面向 Firepower 的 AMP 功能指定通信选项。

综合安全情报通信配置选项

启用 URL 过滤

允许根据网站的一般分类或类别和风险级别或信誉来进行流量过渡。添加URL过滤许可证将自动启用**启用 URL 过滤 (Enable URL Filtering)** 和**启用自动更新 (Enable Automatic Updates)**。必须启用 URL 过滤后才能选择其他 URL 过滤选项。

启用 URL 过滤后，Firepower 管理中心会从思科 CSI 检索 URL 数据（具体取决于上一次启用 URL 过滤的时间，或者是不是首次启用 URL 过滤）。

由于内存限制，某些设备型号以规模较小、精细程度较低的类别和信誉集执行URL过滤。例如，如果父 URL 的子站点具有不同的 URL 类别和信誉，有些设备可能会对所有子站点使用父 URL 的数据。具体举例而言，系统可能会使用 google.com 的类别和信誉来评估 mail.google.com。受影响设备包括 7100 系列和以下 ASA 型号：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X 和 ASA5525-X。对于虚拟设备，请参阅《《*Firepower* 系统虚拟安装指南》》以了解有关分配正确的内存量来执行基于类别和信誉的 URL 过滤的信息。

启用自动更新

允许 Firepower 管理中心自动更新您的部署的 URL 数据。URL 数据通常每天更新一次，但启用自动更新会强制 Firepower 管理中心每 30 分钟检查一次。虽然每日更新通常是小量更新，但如果距离上一次更新超过五天，新的URL数据最多可能需要20分钟才能下载完，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

如果需要严格控制系统联系外部资源的时间，可以禁用自动更新而改为使用调度程序。

注释 思科建议启用自动更新或使用调度程序安排更新。虽然可以通过点击**立即更新 (Update Now)** 手动执行按需更新，但自动执行更新过程可确保获得最新、最相关的数据。如果有更新正在进行，则不能启动按需更新。

向思科 CSI 查询未知 URL (Query Cisco CSI for Unknown URLs)

当用户浏览的网站的类别和信誉不在本地数据集中时，允许系统提交URL进行威胁情报评估。如果不想提交未分类 URL（例如，出于隐私原因），请禁用此选项。

与未分类 URL 的连接**不**与使用基于类别或信誉的 URL 条件的规则进行匹配。在这种情况下，您将无法手动对该 URL 指定类别或信誉。

启用自动本地恶意软件检测更新 (Enable Automatic Local Malware Detection Updates)

本地恶意软件检测引擎使用思科提供的签名对文件进行静态分析和预分类。如果启用此选项，则 Firepower 管理中心每 30 分钟检查一次签名更新。

与思科共享恶意软件事件中的 URI (Share URI from Malware Events with Cisco)

系统可以向 AMP 云发送有关网络流量中检测到的文件的信息。此信息包括与被检测的文件相关联的 URI 信息及其 SHA-256 散列值。虽然共享功能是可选的，不过向思科传输此信息对未来的恶意软件识别和跟踪工作有帮助。

对面向 Firepower 的 AMP 使用传统端口 32137 (Use Legacy Port 32137 for AMP for Firepower)

默认情况下，面向 Firepower 的 AMP 使用端口 443/HTTPS 与 AMP 云（或 AMPv）通信。此选项允许面向 Firepower 的 AMP 使用端口 32137。如果系统是从旧版本更新而来，可启用此选项。

配置与综合安全情报的通信

智能许可证	经典许可证	支持的设备	支持的域	Access
URL 过滤（URL 过滤） 恶意软件（面向 Firepower 的 AMP）	URL 过滤（URL 过滤） 恶意软件（面向 Firepower 的 AMP）	任何环境	任何环境	管理

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**思科 CSI (Cisco CSI)** 选项卡。

步骤 3 配置思科 CSI 通信，如综合安全情报通信配置选项， 第 772 页中所述。

步骤 4 点击**保存 (Save)**。

第 46 章

文件和恶意软件检测性能和存储调整

以下主题介绍如何配置文件和恶意软件检测性能和存储：

概述：文件和恶意软件检测性能和存储调整

如果执行文件控制或使用面向 FirePOWER 的 AMP，可以设置以下高级文件和恶意软件检查选项：

- 限制检测文件类型时检查的字节数
- 如果“阻止恶意软件”(Block Malware) 规则匹配没有缓存处置情况的文件，且大量时间过后仍未获得处置情况，则允许文件通过
- 如果文件大于特定大小，则避免存储文件，对文件执行恶意软件云查找，或阻止自定义检测列表中的文件
- 指定要存储的最小和最大文件大小
- 指定要提交进行动态分析的最小和最大文件大小

这些选项可能会影响系统性能和文件存储。

文件和恶意软件检测性能和存储选项

提高文件大小会影响系统的性能。

表 *81*：高级访问控制文件和面向 ***Firepower*** 的 ***AMP*** 选项

字段	说明	允许的值	说明
限制进行文件类型检测时检查的字节的数量	指定执行文件类型检测时检查的字节数。	0 - 4294967295 (4GB)	输入 0 可移除限制。 默认值是 TCP 数据包的最大分片大小。在大多数情况下，系统可以使用第一个数据包确定常见的文件类型。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	指定进行恶意软件云查找时，没有缓存的处置情况，系统将会保持匹配**阻止恶意软件 (Block Malware)** 规则的文件的最后一个字节的时长。如果该时间过去，系统没有获得处置，文件将会通过。不可用的处置不会被缓存。	0 - 30 秒	由于连接故障，思科建议使用默认值以避免阻止流量。如未联系支持部门，**请勿**将此选项设置为 0。
Do not calculate SHA-256 hash values for files larger than (in bytes)	禁止系统存储大于特定大小的文件，对文件进行恶意软件云查找或阻止文件（如果已添加到自定义检测列表）。	0 - 4294967295 (4GB)	输入 0 可移除限制。 该值必须大于或等于**可存储的最大文件大小（字节）**和**用于动态分析测试的最大文件大小（字节）**。
可存储的最小文件大小（字节）	指定系统使用文件规则可以存储的最小文件大小。	0 - 10485760 (10MB)	输入 0 以禁用文件存储。 此字段的值必须小于或等于**可存储的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。
可存储的最大文件大小（字节）	指定系统使用文件规则可以存储的最大文件大小。	0 - 10485760 (10MB)	输入 0 以禁用文件存储。 此字段的值必须大于或等于**可存储的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。

字段	说明	允许的值	说明
用于动态分析测试的最小文件大小（字节）	指定系统可以提交到AMP云以供动态分析的最小文件大小。	0 -104857600 (100MB)	此字段的值必须小于或等于**用于动态分析测试的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。 如果将访问控制策略部署到运行 5.x 版本 Firepower 系统的设备，则系统会将任何小于 15360 的值修改为 15360。 系统会检查AMP云以更新可以提交的最小文件大小（一天不超过一次）。如果新的最小值大于当前值，当前值会更新为新的最小值，而且策略会标记为过期。
用于动态分析测试的大小文件大小（字节）	指定系统可以提交到AMP云以供动态分析的最大文件大小。	0 -104857600 (100MB)	此字段的值必须大于或等于**用于动态分析测试的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 哈希值（以字节为单位）**。 如果将访问控制策略部署到运行 5.x 版本 Firepower 系统的设备，则系统会将任何大于 2097152 的值修改为 2097152。 系统会检查AMP云以更新可以提交的最大文件大小（一天不超过一次）。如果新的最大值小于当前值，当前值会更新为新的最大值，而且策略会标记为过期。

调整文件和恶意软件检测性能和存储

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁（文件控制）恶意软件 (AMP)	保护（文件控制）恶意软件 (AMP)	任何环境	任何环境	管理员/访问管理员/网络管理员

注意 在“文件和恶意软件设置”(Files and Malware Settings) 下更改值在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击 **Files and Malware Settings** 旁的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 设置文件和恶意软件检测性能和存储选项，第 775 页中所述的任何选项。

步骤 4 点击 **OK**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 XIV 部分

入侵检测和防御

第 47 章

网络分析和入侵策略概述

以下主题概述网络分析和入侵策略：

网络分析和入侵策略基础知识

网络分析和入侵策略共同用作Firepower系统的入侵检测和防御功能的一部分。术语入侵检测通常是指被动分析网络流量以查找潜在入侵，并存储攻击数据以进行安全分析的过程。术语入侵防御包括入侵检测的概念，但是添加了在恶意流量通过网络传播时对其进行阻止或修改的能力。

在入侵防御部署中，当系统检测数据包时：

- **网络分析策略**监管如何解码和预处理流量，以便可进一步对其进行评估，尤其适用于可能表明入侵尝试的异常流量。
- **入侵策略**使用入侵和预处理程序规则（有时统称为入侵规则）根据模式检测已解码数据包是否存在攻击。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。

网络分析和入侵策略均由父访问控制策略调用，但是在不同时间调用。在系统分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（其他预处理和入侵规则）阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

Firepower 系统随附若干以类似方式命名的网络分析和入侵策略（例如，“平衡安全性和连接”[Balanced Security and Connectivity]），这些策略是相辅相成的。通过使用系统提供的策略，您可以利用Cisco Talos 安全情报和研究小组 (Talos) 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，以及提供预处理器和其他高级设置的初始配置。

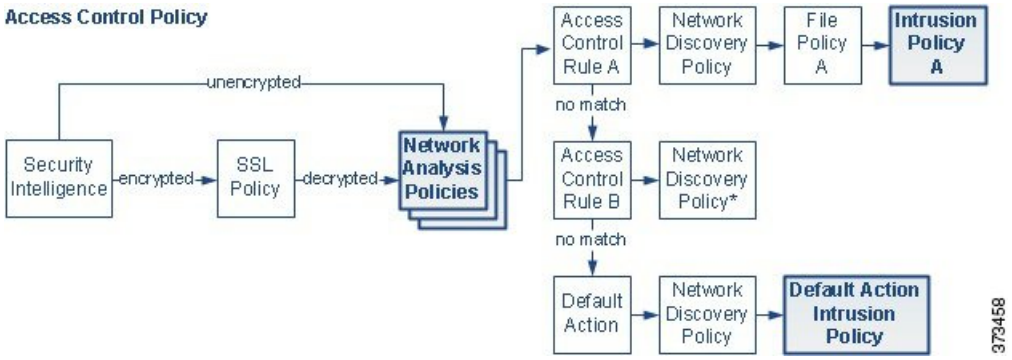
您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

您可在网络界面中使用相似的策略编辑器创建、编辑、保存和管理网络分析和入侵策略。在您编辑任一类型的策略时，导航面板显示在网络界面的左侧；右侧显示各种配置页面。

策略如何检查流量是否存在入侵

当系统在访问控制部署过程中分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（入侵规则和高级设置）阶段之前并与其分隔开来。

下图以简化方式显示内联、入侵防御和面向 Firepower 的 AMP 部署中的流量分析顺序。它说明访问控制策略如何调用其他策略来检测流量，以及这些策略的调用顺序。网络分析和入侵策略选择阶段突出显示。



在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），系统可以在图示过程中的几乎任何步骤阻止流量而不进行进一步检查。安全智能、SSL 策略、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。只有网络发现策略（被动检测数据包）无法影响流量的流动。

类似地，在该过程的每个步骤中，数据包都可能会导致系统生成事件。入侵和预处理程序事件（有时统称为入侵事件）指示数据包或其内容可能表示安全风险。

提示 当您的 SSL 配置允许已加密流量通过，或者您未配置 SSL 检查时，此图未反映访问控制规则处理已加密流量。默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略（如图所示），但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这不影响您在自定义网络分析策略中配置预处理的方式。

解码、规范化和预处理：网络分析策略

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。网络分析策略在以下时机监管这些流量处理任务：

- 在流量由安全智能过滤**之后**
- 在已加密会话由可选 SSL 策略解密**之后**
- 在流量可由文件或入侵策略检测**之前**

网络分析策略分阶段监管数据包处理。系统首先通过前三个 TCP/IP 层解码数据包，然后继续规范化、预处理和检测协议异常：

- 数据包解码器将数据包报头和负载转换为可由预处理程序并在以后由入侵规则轻松使用的格式。TCP/IP 堆栈的各层从数据链路层开始并持续到网络层和传输层依次解码。数据包解码器还会检测数据包报头中的各种异常行为。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他预处理程序和入侵规则进行检测，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。

注释 在被动部署中，思科建议您在访问控制策略级别配置自适应配置文件，而非在网络分析级别配置内联规范化。

- 各种网络层和传输层预处理器检测利用 IP 分段的攻击，执行校验和验证并执行 TCP 和 UDP 会话预处理。

  请注意，一些高级传输和网络预处理程序设置全局适用于由访问控制策略的目标设备处理的所有流量。您在访问控制策略中而不是在网络分析策略中配置这些高级设置。
- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。通过规范化应用层协议编码，系统可以将相同的内容相关的入侵规则有效地应用于以不同方式表示其数据的数据包，并且获取有意义的结果。
- Modbus 和 DNP3 SCADA 预处理程序检测异常流量并向入侵规则提供数据。监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。
- 通过若干预处理器，可以检测特定威胁，如 Back Orifice、端口扫描、SYN 泛洪和其他基于速率的攻击。

  请注意，您在入侵策略中配置敏感数据预处理器，该预处理器用于检测敏感数据（例如，ASCII 文本中的信用卡号和社会安全保障号）。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的所有入侵策略的所有流量的预处理。最初，系统使用 Balanced Security and Connectivity 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制流量预处理选项。

访问控制规则：入侵策略选择

在初始预处理后，访问控制规则（如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检查流量是否存在发现数据、恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检查是否存在发现数据和入侵。

注释 所有数据包（**无论**哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检测。

策略如何检查流量是否存在入侵，第 782 页中的图显示流经内联的入侵防御和面向 Firepower 的 AMP 部署中的设备的流量，如下所示：

- Access Control Rule A 允许匹配流量通过。然后该流量由网络发现策略检查是否存在发现数据，由 File Policy A 检查是否存在受禁文件和恶意软件，最后由 Intrusion Policy A 检查是否存在入侵。
- Access Control Rule B 也允许匹配流量通过。但是，在此情景中，未检查流量是否存在入侵（或文件或恶意软件），因此没有与规则关联的入侵或文件策略。请注意，默认情况下，您允许通过的流量将由网络发现策略进行检查；您不需要配置此检查。
- 在此情景中，访问控制策略的默认操作允许匹配流量。然后该流量将依次由网络发现策略和入侵策略进行检查。将入侵策略与访问控制规则或默认操作相关联时，可以（但不必）使用其他入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检测已阻止或信任的流量。

入侵检查：入侵策略、规则和变量集

在允许流量继续到达其目标之前，可以使用入侵防御作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则及其如何配置。

入侵和预处理程序规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则来分析网络流量，以检测其是否与规则中的条件匹配。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件都匹配，则触发此规则。

系统包含Cisco Talos 安全情报和研究小组 (Talos) 创建的以下类型的规则：

- 共享对象入侵规则，已编译且无法修改（规则标题信息除外，如源和目标端口及 IP 地址）
- 标准文本入侵规则，可以保存并修改为规则的新自定义实例。

- 预处理程序规则，是指与网络分析策略中的预处理程序和数据包解码器检测选项关联的规则。不能复制或编辑预处理程序规则。默认情况下，大多数预处理程序规则均已禁用；您必须将其启用才能使用预处理程序生成事件，并在内联部署中丢弃有问题的数据包。

当系统根据入侵策略处理数据包时，首先，规则优化器会根据传输层、应用协议、受保护网络的方向等条件对子集中所有已激活的规则进行分类。然后，入侵规则引擎选择要应用于每个数据包的相应规则子集。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。
- 数据包异常搜索查找没有包含特定内容而是违反既定协议的数据包报头和负载。

在自定义入侵策略中，您可以通过启用和禁用规则以及通过编写和添加自己的标准文本规则来调整检测。还可以遵从Firepower的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。

变量集

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标IP地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

系统提供单个由预定义默认变量组成的默认变量集。大多数系统提供的共享对象规则和标准文本规则均使用这些预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。

入侵事件生成

当系统识别可能的入侵时，它会生成入侵或预处理程序事件（有时统称为入侵事件）。受管设备将其事件传输到Firepower管理中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。在内联部署中，受管设备还可以丢弃或替换已知有害的数据包。

数据库中的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标IP地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还会记录一个或多个已触发事件的数据包的已解码数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎均会导致系统生成事件。例如：

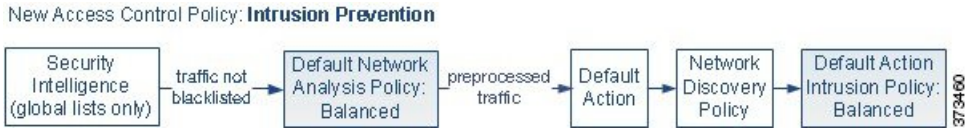
- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的IP数据包，解码器将此解释为异常流量。如果之后启用了用于检测数据包的入侵策略中的配套解码器规则，则系统会生成预处理程序事件。
- 如果 IP 分片重组预处理程序遇到一系列重叠的 IP 片段，则预处理程序会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成预处理程序事件。
- 在入侵规则引擎内，大多数标准文本规则和共享对象规则编写为在由数据包触发时会生成入侵事件。

随着数据库累计入侵事件，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

系统提供的与自定义的网络分析和入侵策略

创建新的访问控制策略是使用Firepower系统管理流量过程中的前几个步骤之一。默认情况下，新创建的访问控制策略调用系统提供的网络分析和入侵策略来检测流量。

下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请注意以下各种操作的方式：

- 默认网络分析策略监管由访问控制策略处理的所有流量的预处理。最初，系统提供的 *Balanced Security and Connectivity* 网络分析策略是默认策略。
- 访问控制策略的默认操作允许由系统提供的 *Balanced Security and Connectivity* 入侵策略确定的所有非恶意流量。由于默认操作允许流量通过，在入侵策略能够检查并可能阻止恶意流量之前，发现功能可以检查流量中的主机、应用和用户数据。
- 策略使用默认的安全情报选项（仅全局白名单和黑名单），不使用SSL解密已加密的流量，并且不使用访问控制规则对网络流量执行特殊处理和检查。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略为作为默认值。思科通过 Firepower 系统提供若干对策略。

或者，您可以通过创建和使用自定义策略来定制入侵防御部署。您可能会发现这些策略中配置的预处理程序选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检测其是否存在入侵。

系统提供的网络分析和入侵策略

思科通过 Firepower 系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用Cisco Talos 安全情报和研究小组 (Talos) 的经验。对于这些策略，Talos 会提供入侵和预处理器规则状态，以及预处理器和其他高级设置的初始配置。

没有哪一个系统提供的策略能够涵盖所有的网络配置文件、流量组合或防御安全状况。但每个此类策略都涵盖常见情况和网络设置，为提供精细调整的防御策略奠定基础。虽然您可以按原样使用系统提供的策略，但思科强烈建议您将其作为自定义策略的基础，对其进行调整以适合您的网络。

提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少应修改默认变量集中的关键默认变量。

随着新的漏洞被发现，Talos 会发布入侵规则更新。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理程序规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

如果规则更新影响您的部署，则网络界面将受影响的入侵和网络分析策略标记为已过期，并标记其父访问控制策略。您必须重新部署已更新的策略才能使其更改生效。

为方便起见，可以将规则更新配置为自动重新部署受影响的入侵策略（单独或与受影响的访问控制策略组合）。这使您能够轻松、自动保持部署为最新，以防范最近发现的漏洞和入侵。

为了确保获得最新的预处理设置，**必须**重新部署访问控制策略，该策略也会重新部署与当前运行的策略不同的所有关联的 SSL、网络分析和文件策略，同时还可以更新高级预处理和性能选项的默认值。

思科通过 Firepower 系统提供以下网络分析和入侵策略：

Balanced Security and Connectivity 网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织和部署类型的良好起点。系统在大多数情况下均使用 Balanced Security and Connectivity 策略和设置作为默认值。

Connectivity Over Security 网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于 Security over Connectivity 策略中启用的规则。仅会启用阻止流量的最重要规则。

Security Over Connectivity 网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略启用可能会提醒或丢弃合法流量的许多网络异常入侵规则。

“最大检测”(Maximum Detection) 网络分析和入侵策略

此类策略适用于网络基础设施安全性比在“安全性优先于连接”(Security Over Connectivity) 策略中还要重要，有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

No Rules Active 入侵策略

在 No Rules Active 入侵策略中，所有入侵规则和高级设置均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一中的已启用规则，可以尝试使用此策略。

自定义网络分析和入侵策略的优势

您可能会发现系统提供的网络分析和入侵策略中配置的预处理程序选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高环境中系统的性能，并且可以密切关注网络上发生的恶意流量和策略违例。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略（也称为基层），用于为策略中所有配置定义默认设置。层是可用于高效管理多个网络分析或入侵策略的构建块。

在大多数情况下，自定义策略基于系统提供的策略，但是可以使用其他自定义策略。不过，所有自定义策略在策略链中都以系统提供的策略作为最终基础。由于规则更新可能会修改系统提供的策略，因此导入规则更新可能会对您产生影响，即使使用自定义策略作为基础也如此。如果规则更新影响部署，则 Web 界面将受影响策略标记为过期。

除了您创建的自定义策略之外，系统还提供两种自定义入侵策略和两种自定义网络分析策略：初始内联策略和初始被动策略。这些策略使用相应的 Balanced Security and Connectivity 策略作为其基本策略。两种策略之间的唯一区别在于其 丢弃行为，该行为在内联策略中启用流量阻止和修改，在被动策略中禁用该功能。您可以编辑并使用系统提供的这些自定义策略。

自定义网络分析策略的优势

默认情况下，一个网络分析策略预处理访问控制策略处理的所有未加密流量。这意味着所有数据包都根据相同设置进行解码和预处理，无论后来使用哪种入侵策略（和因此使用的入侵规则集）对其进行检测。

最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。

可用的调整选项因预处理程序而异，但是可以调整预处理程序和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的预处理程序。例如，HTTP Inspect 预处理程序规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的预处理程序选项，从而减少系统处理开销。

注释 如果禁用自定义网络分析策略中的预处理器，但系统稍后需要使用该预处理器利用已启用的入侵或预处理器规则对数据包进行评估，系统会自动启用并使用预处理器，不过它在网络分析策略 Web 界面中保持禁用。

- 指定端口（如果适用）以关注某些预处理程序的活动。例如，可以确定要对 DNS 服务器响应或加密 SSL 会话进行监控的其他端口，或者确定解码 telnet、HTTP 和 RPC 流量所在的端口

对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。（请注意，ASA FirePOWER模块无法通过 VLAN 限制预处理。）

注释 使用自定义网络分析策略（尤其是多个网络分析策略）定制预处理是一个高级任务。由于预处理和入侵检测密切相关，因此，您**必须**注意，要确保允许检测单个数据包的网络分析和入侵策略能够互补。

自定义入侵策略的优势

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 Balanced Security and Connectivity 入侵策略对流量进行检测。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检查。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检测流量。然后，使用指定哪个策略检测哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 或用户。

入侵策略的主要功能是管理启用哪些入侵和预处理器规则及其如何配置，如下所示：

- 在每个入侵策略中，应该验证所有适用于环境的规则是否已启用，并且通过禁用不适用于环境的规则来提高性能。在内联部署中，可以指定哪些规则应该丢弃或修改恶意数据包。
- 如果遵从 Firepower 的建议，则可将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 您可以修改现有规则并根据需要编写新的标准文本规则，以捕获新的漏洞或强制实施安全策略。

您可能对入侵策略进行的其他自定义包括：

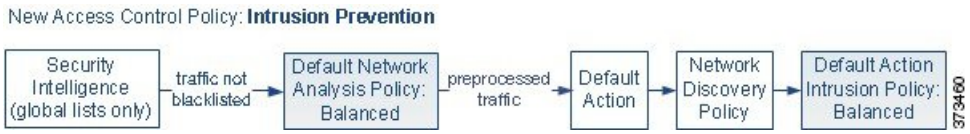
- 敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他预处理程序。
- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统被大量事件淹没。

- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。
- 除了网络界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志工具或者将事件数据发送到SNMP陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

自定义策略的限制

由于预处理和入侵检测如此密切相关，因此，您**必须**小心确保自己的配置允许网络网络分析和入侵策略处理和检测单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预处理由受管设备使用单个访问控制策略处理的所有流量。下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请留意默认网络分析策略如何监管访问控制策略处理的所有流量的预处理。最初，系统提供的Balanced Security and Connectivity 网络分析策略是默认策略。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。但是，如果在自定义网络分析策略中禁用预处理器，但系统需要根据已启用的入侵或预处理器规则评估预处理的数据包，则系统会自动启用并使用该预处理器，尽管其在网络分析策略 Web 界面中保持禁用。

注释 要获取禁用预处理程序的性能优势，您**必须**确保自己的入侵策略均未启用需要该预处理程序的规则。

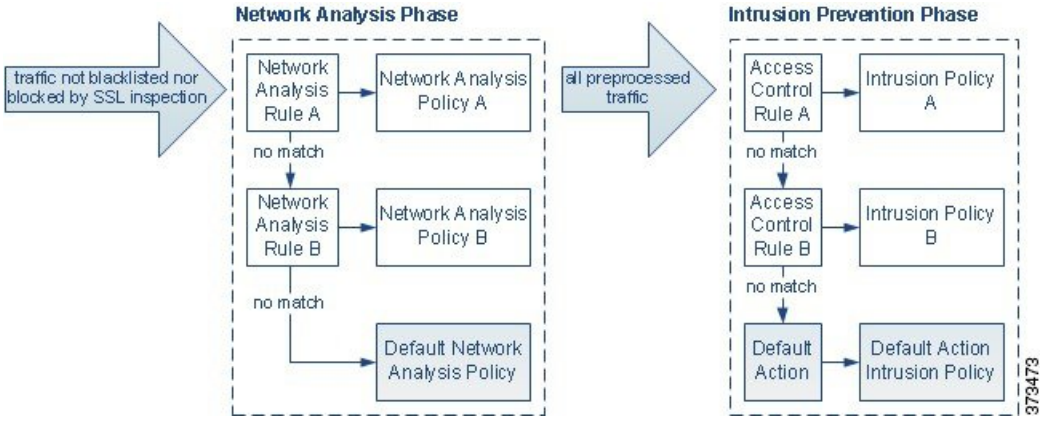
如果使用多个自定义网络分析策略，则会引起其他问题。对于使用复杂部署的高级用户，可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 自定义预处理。（请注意，ASA FirePOWER无法通过VLAN限制预处理。）为此，请向访问控制策略中添加自定义网络分析规则。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

提示 可以将网络分析规则配置为访问控制策略中的高级设置。与 Firepower 系统中其他类型的规则不同，网络分析规则调用网络分析策略，而不是由其包含在内。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包**无论**由哪个网络分析策略进行了预处理，后来都会在各自的进程中与访问控制规则匹配，从而可能会接受入侵策略的检查。换句话说，使用特定网络分析策略预处理数据包**不**保证将通过任

何特殊入侵策略检测该数据包。您**必须**仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图集中细解了网络分析策略（预处理）选择阶段如何在入侵防御（规则）阶段之前发生并与其分隔开来。为简单起见，此图省去了发现和文件/恶意软件检查阶段。它还突出显示默认网络分析和默认操作入侵策略。



在此情景中，访问控制策略配置有两条网络分析规则和一个默认网络分析策略：

- 网络分析规则 A 使用网络分析策略 A 预处理匹配流量。之后，您希望此流量由入侵策略 A 进行检测。
- 网络分析规则 B 使用网络分析策略 B 预处理匹配流量。之后，您希望此流量由入侵策略 B 进行检测。
- 所有剩余流量都使用默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检测。

系统在预处理流量之后，可以检测流量是否存在入侵。该图显示具有两条访问控制规则和一个默认操作的访问控制策略：

- 访问控制规则 A 允许匹配流量。然后，流量由入侵策略 A 进行检测。
- 访问控制规则 B 允许匹配流量。然后，流量由入侵策略 B 进行检测。
- 访问控制策略的默认操作允许匹配流量。然后，流量由默认操作的入侵策略进行检测。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项**高级**任务。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略，但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

导航面板：网络分析和入侵策略

网络分析和入侵策略使用类似的 Web 界面编辑和保存对其配置进行的更改。

编辑任一类型的策略时，导航面板会出现在网络界面左侧。下图显示网络分析策略（左）和入侵策略（右）的导航面板。

分隔线将导航面板分隔成指向策略设置的链接，可以通过（下方）或不通过（上方）与策略层的直接交互来配置这些设置。要导航到任何设置页面，请在导航面板中点击其名称。某项在导航面板中的浓阴影突出显示当前设置页面。例如，在上方的插图中，Policy Information 页面会显示到导航面板的右侧。

Policy Information

Policy Information 页面提供常用设置的配置选项。如以上网络分析策略面板的插图所示，当策略包含未保存的更改时，在导航面板中的 **Policy Information** 旁边会显示策略更改图标 ( )。保存更改后，该图标消失。

Rules（仅入侵策略）

通过入侵策略中的“规则”(Rules) 页面，您可以为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

Firepower 建议（仅入侵策略）

通过入侵策略中的“Firepower 建议”(Firepower Recommendations) 页面，您可以将在网络上检测到的操作系统、服务器和客户端应用协议与专门编写用于保护这些资产的入侵规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

Settings（网络分析策略）和 Advanced Settings（入侵策略）

网络分析策略中的 Settings 页面可供您启用或禁用预处理程序以及访问预处理程序配置页面。展开 **Settings** 链接会显示指向策略中所有已启用预处理程序的个别配置页面的子链接。

入侵策略中的Advanced Settings页面可供您启用或禁用高级设置以及访问这些高级设置的配置页面。展开 **Advanced Settings** 链接会显示指向策略中所有已启用高级设置的个别配置页面的子链接。

Policy Layers

Policy Layers 页面显示构成网络分析或入侵策略的各层的摘要。展开 Policy Layers 链接会显示指向策略中的各层的摘要页面的子链接。展开各层子链接会显示指向层中已启用的所有规则、预处理程序或高级设置的配置页面的进一步子链接。

冲突和更改：网络分析和入侵策略

在编辑网络分析或入侵策略时，策略更改图标 () 显示在导航面板中 **Policy Information** 的旁边以指示策略包含未保存的更改。必须首先保存（或提交）更改，然后系统才会认可这些更改。

注释 保存后，必须部署网络分析或入侵策略，更改才会生效。如果部署策略而不保存，则系统会使用最新保存的配置。

解决编辑冲突

“网络分析策略”(Network Analysis Policy) 页面（**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或 **策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**）以及“入侵策略”(Intrusion Policy) 页面（**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**）显示每个策略是否有未保存的更改，以及有关当前正在编辑策略的用户的信息。思科建议每次仅由一位人员编辑一个策略。如果执行同时编辑，则将产生以下后果：

- 如果在您编辑某条网络分析或入侵策略的同时另一用户也在编辑该策略，并且该用户保存对此策略的更改，则当您提交策略时系统将警告您会覆盖另一用户的更改。
- 如果以同一用户身份通过多个网络界面实例编辑同一网络分析或入侵策略，而且，您保存对一个实例的更改，则无法保存对其他实例的更改。

解析配置依赖关系

为了执行特殊分析，许多预处理程序和入侵规则均要求流量首先以某种方式得以解码或预处理，或者具有其他依存关系。保存网络分析或入侵策略时，系统会自动启用必需的设置，或者警告您已禁用的设置不会影响流量，如下所示：

- 如果已添加 SNMP 规则警报，但未配置 SNMP 告警，则无法保存入侵策略。必须配置 SNMP 告警或禁用规则警报，然后再次保存。
- 如果入侵策略包含已启用的敏感数据规则，但是您尚未启用敏感数据预处理程序，则无法保存该入侵策略。必须允许系统启用预处理程序并保存策略，或者禁用规则并再次保存。

- 如果在网络分析策略中禁用必需的预处理程序，则仍然可以保存该策略。但是，系统会通过已禁用预处理程序的当前设置使用该预处理程序，即使该预处理程序在网络界面中保持禁用亦如此。
- 如果在网络分析策略中禁用内联模式，但是启用内联规范化预处理程序，则仍然可以保存该策略。不过，系统会警告您将忽略规范化设置。禁用内联模式还会导致系统忽略允许预处理程序修改或阻止流量的其他设置，包括校验和验证和基于速率的攻击防御。

提交、丢弃和缓存策略更改

在编辑网络分析或入侵策略时，如果退出策略编辑器而不保存更改，则系统会缓存这些更改。即使注销系统或系统崩溃，仍然会缓存更改。系统缓存可以按照每个用户一个网络分析和一个入侵策略来存储未保存的更改；编辑同一类型的另一个策略之前，必须提交或放弃更改。编辑另一个策略而不保存对第一个策略的更改时，或者导入入侵规则更新时，系统会丢弃缓存的更改。

您可以在网络分析或入侵策略编辑器的“策略信息”(Policy Information) 页面上提交或丢弃策略更改。

在 Firepower 管理中心配置中，您可以控制：

- 是否提示（或要求）您在提交网络分析或入侵策略更改时对其添加注释
- 是否将更改和注释记录到审核日志中

退出网络分析或入侵策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

如果要退出网络分析或入侵策略高级编辑器，您有以下选择：

- 缓存 - 要退出策略和缓存更改，请选择任何菜单或指向另一个页面的其他路径。请在系统提示时点击**离开页面 (Leave page)** 退出，或者点击**停留在页面上 (Stay on page)** 停留在高级编辑器中。
- 放弃 - 要放弃未保存的更改，请点击“策略信息”(Policy Information) 页面上的**放弃更改 (Discard Changes)**，然后点击**确定 (OK)**。
- 保存 - 要保存对策略的更改，请点击“策略信息”(Policy Information) 页面上的**确认更改 (Commit Changes)**。如果出现提示，请输入注释，然后点击**确认 (OK)**。

第 48 章

入侵和网络分析策略中的层

以下主题介绍如何使用入侵和网络分析策略中的层：

层基础知识

拥有众多受管设备的大型组织可能具有许多入侵策略和网络分析策略来支持不同部门、业务单位或（某些情况下）不同公司的独特需求。两种策略类型中的配置均包含在构建块（称为层）中，可用于高效管理多个策略。

入侵和网络分析策略中的层基本以相同方式工作。您可以创建和编辑任一策略类型，而无需刻意使用层。您也可以修改策略配置；如果您没有向策略中添加用户层，系统会自动将您的更改纳入单个可配置的层（初始名称为 *My Changes*）。您还可以最多添加 200 个层，在其中可以配置设置的任意组合。可以复制、合并、移动和删除用户层，并且最重要的是，可与同一类型的其他策略共享个别用户层。

层堆栈

层堆栈由以下元素组成：

用户层

用户可配置层可以复制、合并、移动或删除任何用户可配置层，并将任何用户可配置层设置为由同一类型的其他策略共享。此层包括自动生成的层，其最初名为“我的更改”(My Changes)。

内置层

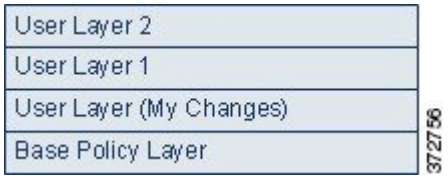
只读基本策略层。此层中的策略可以是系统提供的策略或您创建的自定义策略。

默认情况下，网络分析或入侵策略包括一个基本策略层和一个“我的更改”(My Changes) 层。可以根据需要添加用户层。

每个策略层均包含网络分析策略中所有预处理程序或入侵策略中所有入侵规则和高级设置的完整配置。最低基本策略层包含创建策略时选择的基本策略中的所有设置。较高层中的设置优先于较低层中的相同设置。在某一层中未明确设置的功能从对其进行了明确设置的下一最高层继承其设置。系统会将层平展，也就是说，它在处理网络流量时，仅应用所有设置的累积效果。

提示 可以仅根据基本策略中的默认设置创建入侵或网络分析策略。在创建入侵策略的情况下，如果要根据监控网络的特定需求定制入侵策略，您也可以使用 Firepower 规则陈述建议。

下图显示一个示例层堆栈，除基本策略层和初始My Changes层以外，还包括其他两个用户可配置层 *User Layer 1* 和 *User Layer 2*。请注意，图中添加的每个用户可配置层初始定位为堆栈中的最高层；因此，图中的 User Layer 2 最后添加并位于堆栈中的最高层。



无论是否允许规则更新修改策略，规则更新中的更改都绝不会覆盖您在层中所做的更改。这是因为规则更新中的更改是在基本策略中做出，基本策略会确定基本策略层中的默认设置；您的更改始终在更高层中做出，因此其会覆盖规则更新对基本策略所做出的任何更改。

基本层

入侵或网络分析策略的基本层（也称为基本策略）定义策略中所有配置的默认设置，并且是策略中的最低层。在不添加新层的情况下创建新策略以及更改设置，更改会存储在My Changes层中，并会覆盖（但不会更改）基本策略中的设置。

系统提供的基本策略

Firepower 系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用Cisco Talos 安全情报和研究小组 (Talos) 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，以及提供预处理器和其他高级设置的初始配置。可以按原样使用系统提供的这些策略，也可以将其用作自定义策略的基础。

如果使用系统提供的策略为基础，则导入规则更新可能会修改基本策略中的设置。但是，您可以配置自定义策略，以便系统不会自动对其系统提供的基本策略进行这些更改。这使您能够按照独立于规则更新的计划手动更新系统提供的基本策略。在任一情况下，规则更新对基本策略所做出的更改不会更改或覆盖 My Changes 或任何其他层中的设置。

系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，平衡安全性和连接网络分析策略和平衡安全性和连接入侵策略配合工作并可以在入侵规则更新中同时更新。

自定义基本策略

您可以使用自定义策略作为基本策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

如果更改用作其他策略的基础的自定义策略，则这些更改会自动用作使用该基础的策略的默认设置。

此外，即使使用自定义基本策略，规则更新也可能会影响您的策略，因为在策略链中，所有策略都将系统提供的策略作为最终基础。如果链中的第一个自定义策略（即使用系统提供的策略作为其基础的策略）允许规则更新修改其基本策略，则您的策略可能会受影响。

无论如何对基本策略进行更改（通过规则更新或在修改用作基本策略的自定义策略时做出更改），都不会更改或覆盖“我的更改”(My Changes) 或任何其他层中的设置。

规则更新对基本策略的影响

导入规则更新时，系统会修改系统提供的入侵策略、访问控制策略和网络分析策略。规则更新可能包括：

- 经过修改的网络分析预处理器设置
- 入侵和访问控制策略中经过修改的高级设置
- 新增和更新的入侵规则
- 经过修改的现有规则状态
- 新的规则类别和默认变量

规则更新还可从系统提供的策略中删除现有规则。

对默认变量和规则类别的更改在系统级别处理。

如果将系统提供的策略用作入侵或网络分析基本策略，您可以允许规则更新修改基本策略，在此情况下，基本策略是系统提供的策略的副本。如果允许规则更新更新基本策略，则新规则更新在基本策略中所做的更改与其对用作基本策略的系统提供的策略所做出的更改相同。如果您未曾对相应的设置进行过修改，则基本策略中的设置会决定策略中的设置。但是，规则更新不会覆盖您在策略中所做出的更改。

如果不允许规则更新修改基本策略，则可以在导入一个或多个规则更新后手动更新基本策略。

无论入侵策略中的规则状态如何或者是否允许规则更新修改基本入侵策略，规则更新始终会删除 Talos 删除的入侵规则。

在将更改重新部署到网络流量之前，当前部署的入侵策略中的规则行为如下：

- 已禁用的入侵规则保持禁用。
- 设置为**生成事件 (Generate Events)** 的规则在触发时继续生成事件。
- 设置为**丢弃并生成事件 (Drop and Generate Events)** 的规则在触发时继续生成事件并丢弃有问题的数据包。

除非同时满足以下两个条件，否则规则更新不会修改自定义基本策略：

- 允许规则更新修改父策略（即用于创建自定义基本策略的策略）的系统提供的基本策略。
- 在父策略中尚未进行覆盖父策略基本策略中相应设置的更改。

如果同时满足两个条件，保存父策略时，规则更新中的更改将传递给子策略（即使用自定义基本策略的策略）。

例如，如果规则更新启用以前禁用的入侵规则，并且您未曾修改该规则在父入侵策略中的状态，则在保存父策略时，已修改的规则状态会传递到基本策略。

同样，如果规则更新修改默认预处理程序设置，并且您未曾修改父网络分析策略中的设置，则在保存父策略时，已修改的设置会传递到基本策略。

更改基本策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以选择其他系统提供的策略或自定义策略作为基本策略。

可以链接最多五个自定义策略，这五个策略中有四个使用其余四个之一以前创建的策略作为其基本策略；第五个策略必须使用系统提供的策略作为其基础。

过程

步骤 1 编辑策略时，点击导航面板中的 **Policy Information**。

步骤 2 可以配置以下选项：

- 选择基本策略 - 从**基本策略 (Base Policy)** 下拉列表中进行选择。
- 允许规则更新修改基本策略 - 点击**管理基本策略 (Manage Base Policy)**，然后选中**在安装新的规则更新时更新 (Update when a new Rule Update is installed)** 复选框。

  提示 在清除此复选框的情况下保存策略然后导入规则更新时，Base Policy 摘要页面上会显示 **Update Now** 按钮，并且该页面上的状态消息会更新，通知此策略已过期。如果要使用最新导入的规则更新中的更改来更新基本策略，请点击**立即更新 (Update Now)**。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

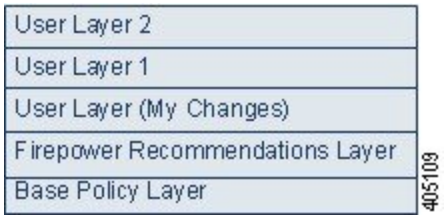
接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

Firepower 建议层

当在入侵策略中生成规则状态建议时，可以选择是否根据建议自动修改规则状态。

如下图所示，使用建议的规则状态会在紧挨基本层之上插入一个内置只读 Firepower 建议层。



请注意，此层对于入侵策略是唯一的。

如果您随后选择不使用建议的规则状态，则系统将移除 Firepower 建议层。您无法手动删除该层，但是，您可以通过选择使用或不使用建议的规则状态来添加和移除该层。

添加 Firepower 建议层会在导航面板中的“策略层”(Policy Layers) 下添加一个 Firepower 建议链接。此链接会引导您进入建议层页面的只读视图，在其中您可以只读模式访问“规则”(Rules) 页面的建议过滤视图。

使用建议的规则状态还会在导航面板中的 Firepower 建议链接之下添加“规则”(Rules) 子链接。借助于“规则”(Rules) 子链接，可访问 Firepower 建议层中“规则”(Rules) 页面的只读显示。注意此视图中的以下内容：

- 如果状态栏中没有规则状态图标，则从基本策略继承状态。
- 如果这个或其他“规则”(Rules) 页面视图的 Firepower 建议列中没有规则状态图标，则没有适合此规则的建议。

层管理

Policy Layers 页面提供网络分析或入侵策略的完整层堆栈的单页摘要。在此页面上，可以添加共享和非共享层，复制、合并、移动和删除层，访问每层的摘要页面，以及访问每层中已启用、禁用和覆盖的配置的配置页面。

对于每层，您均可查看以下信息：

- 层是内置层、共享用户层还是非共享用户层
- 哪些层包含最高（即最有效）预处理程序或高级设置配置（按功能名称）
- 在入侵策略中，在该层中设置了其状态的入侵规则的数量，以及设置为每个规则状态的规则的数量。

“策略层”(Policy Layers) 页面还提供所有已启用预处理器（网络分析）或高级设置（入侵）的实际效果的摘要，并为入侵策略提供入侵规则的实际效果的摘要。

每层的摘要中的功能名称指明在该层中已启用、禁用、覆盖或继承哪些配置，如下所示：

当功能...	功能名称…
层中已启用	以纯文本写入
层中已禁用	删除
被高级层中的配置覆盖	以斜体文本写入
从下层中继承	不存在

您最多可以向网络分析或入侵策略中添加 200 层。添加的层显示为策略中的最高层。初始状态对于所有功能都为 Inherit，并且在入侵策略中，未设置事件过滤、动态状态或警报规则操作。

在将用户可配置层添加到策略中时，可为该层提供唯一名称。之后，可以更改名称，或者可以在编辑层时添加或修改可视的说明。

您可以复制层，在“用户层”(User Layers) 页面区域中将层上移或下移，或删除用户层，包括初始“我的更改”(My Changes) 层。请注意以下考虑事项：

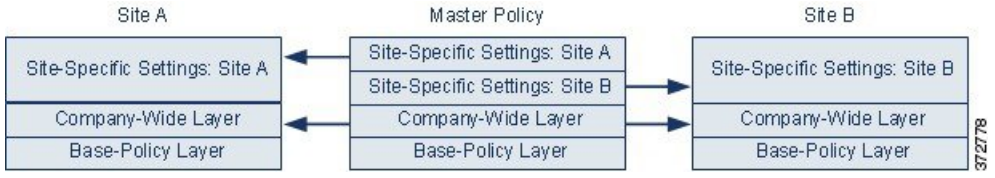
- 在复制层时，副本显示为最高层。
- 复制共享层会创建初始未共享且之后在选择时可共享的层。
- 不能删除共享层；已启用共享但未曾与其他策略共享的层不是共享层。

您可以将一个用户可配置层与其正下方的另一个用户可配置层合并。合并层保留任一层特有的所有设置，并且如果两层均包含同一预处理程序、入侵规则或高级设置的设置，则会接受更高层中的设置。合并层保留更低层的名称。如果在策略中创建的可共享层可以添加到其他策略，则可以将该可共享层正上方的非共享层与该可共享层合并，但是不能将该共享层与其下方的非共享层合并。如果在一个策略中添加的共享层在其他策略中已创建，则可以将该共享层合并到其正下方的非共享层中，所生成的层不再共享；不能将非共享层合并到其下方的共享层中。

共享层

当您在另一策略中创建层后，可以将该层添加到您的策略中并允许其共享，该层即为共享层。可共享的层是您允许共享的层。

下图显示一个主策略示例，您可在其中创建公司范围层，为站点 A 和 B 创建站点特定层，并允许进行共享。然后，将这些层作为共享层添加到站点 A 和 B 的策略中。



主策略中的公司范围层包含适用于站点 A 和 B 的设置。站点特定层包含特定于每个站点的设置。例如，如果使用网络分析策略，则 Site A 在受监控网络上可能没有 Web 服务器，并且不需要 HTTP

Inspect 预处理程序的保护或处理开销，但两个站点均可能需要 TCP 数据流预处理。可在与两个站点共享的公司范围层启用 TCP 数据流处理，在与站点 A 共享的站点特定层禁用 HTTP 检查预处理器，在与站点 B 共享的站点特定层启用 HTTP 检查预处理器。通过编辑站点特定策略中的较高层配置，如果需要任何配置调整，您还可以进一步微调每个站点的策略。

示例主策略中的扁平化网络设置不大可能对流量监控有用，但配置和更新站点特定策略所节省的时间使得它成为策略层的一种有用应用。

也可使用许多其他层配置。例如，您可以按公司、部门、网络甚至用户来界定策略层。如果使用入侵策略，则还可以在一层中包含高级设置，在另一层中包含规则设置。

可以将用户可配置层与同一类型（入侵或网络分析）的其他策略共享。在可共享层中修改配置，然后确认更改时，系统会更新共享层的所有策略，并为您提供所有受影响策略的列表。您只能在已创建该层的策略中修改功能配置。

不能对添加到另一个策略的层禁用共享；必须先从另一个策略中删除该层，或者删除另一个策略。

当基本策略是在其中已创建要共享的层的自定义策略时，不能向策略中添加共享层。这样将为策略提供循环依赖。

在多域部署中，可以将来自祖先策略的共享层添加到后代域中的策略。

管理层

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 编辑策略时，点击导航面板中的 **Policy Layers**。

步骤 2 可以在“策略层”(Policy Layers) 页面上执行下列任意管理操作：

- 添加其他策略中的共享层 - 点击“用户层”(User Layers) 旁边的添加共享层图标 ( )，从**添加共享层 (Add Shared Layer)** 下拉列表中选择层，然后点击**确定 (OK)**。
- 添加非共享层 - 点击“用户层”(User Layers) 旁边的添加层图标 ( )，输入**名称 (Name)**，然后点击**确定 (OK)**。
- 添加或更改层说明 - 点击层旁边的编辑图标 ( )，然后添加或更改**说明 (Description)**。
- 允许与其他策略共享层 - 点击层旁边的编辑图标 ( )，然后清除**共享 (Sharing)** 复选框。
- 更改层名称 - 点击层旁边的编辑图标 ( )，然后更改**名称 (Name)**。
- 复制层 - 点击该层的复制图标 ( )。
- 删除层 - 点击该层的删除图标 ( )，然后点击**确定 (OK)**。

- 合并两层 - 点击两层中上层的合并图标 ()，然后点击**确定 (OK)**。
- 移动层 - 点击层摘要中的任何开放区域并将其拖动，直至位置箭头 () 指向该层上方或下方要将该层移到的行。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

导航层

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 编辑策略时，点击导航面板中的 **Policy Layers**。

步骤 2 可以执行下列任意操作以在各层间导航：

- 访问预处理器或高级设置页面 - 如果要访问层级别的预处理器或高级设置配置页面，请点击该层对应的行中的功能名称。配置页面在基本策略和共享层中为只读。
- 访问规则页面 - 如果要访问按规则状态类型过滤的层级别的规则配置页面，请点击该层的摘要中的丢弃并生成事件图标 ()、生成事件图标 () 或已禁用图标 ()。如果该层不包含设置为所选规则状态的规则，则不会显示任何规则。
- 显示“策略信息”(Policy Information) 页面 - 如果要显示“策略信息”(Policy Information) 页面，请点击导航面板中的**策略摘要 (Policy Summary)**。
- 显示层摘要页面 - 如果要显示某层的摘要页面，请点击该层对应的行中的层名称，或者点击用户层旁边的编辑图标 ()。您也可以点击查看图标 () 来访问共享层的只读摘要页面。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

层中的入侵规则

可以在该层的 Rules 页面上查看个别层设置，也可以在 Rules 页面的策略视图中查看所有设置的实际效果。在 Rules 页面的策略视图中修改规则设置时，修改的是策略中的最高用户可配置层。可以在任何 Rules 页面上使用层下拉列表切换到另一层。

下表描述在多个层中配置相同类型设置的效果。

表 *82*: 层规则设置

您可设定.....	此设置类型.....	所需的操作…
一个	规则状态	覆盖为更低层中的规则设置的规则状态，并忽略在更低层中为该规则配置的所有阈值、抑制、基于速率的规则状态和警报。 如果希望规则从基本策略或更低层继承其状态，请将规则状态设置为 Inherit。请注意，在入侵策略“规则”(Rules) 页面上操作时，不能将规则状态设置为“继承”(Inherit)，因为入侵策略“规则”(Rules) 页面是所有规则设置的实际效果的综合视图。
一个	阈值 SNMP 警报	覆盖下层中规则的相同类型设置。请注意，设置阈值时会覆盖层中规则的任何现有阈值。
一个或多个	基于抑制率的规则状态	会将每个所选规则的相同类型设置累积合并至为该规则设定规则状态所在的第一层。设定规则状态所在层下的设置均被忽略。
一个或多个	注释	向规则添加注释。注释仅为规则特定，非策略或层特定。可将一条或多条注释添加至任何层中的规则。

例如，如在一层中将规则状态设置为 Drop and Generate Events，但在上层设置为 Disabled，则入侵策略的 Rules 页面将显示规则已被禁用。

再比如，如在一层中为规则将基于源的抑制设置为 192.168.1.1，同时也为该规则将基于目标的抑制设置为 192.168.1.2，则 Rules 页面显示：累积效应将为源地址 192.168.1.1 和目标地址 192.168.1.2 抑制事件。请注意，抑制和基于速率的规则状态设置会将每个所选规则的相同类型设置累积合并至为该规则设定规则状态所在的第一层。设定规则状态所在层下的设置均被忽略。

“规则”(Rules) 页面上特定层的颜色编码表示有效状态位于较高层、较低层还是当前层中，如下所示：

- 红色 - 有效状态位于较高层
- 黄色 - 有效状态位于较低层
- 无光度 - 有效状态位于当前层

由于入侵策略 Rules 页面是所有规则设置的实际效果的综合视图，因此规则状态在此页面上未进行颜色编码。

配置层中的入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在入侵策略中，可以为任何用户可配置层中的规则设置规则状态、事件过滤、动态状态、警报和规则注释。访问要更改的层后，可按照在入侵策略 Rules 页面上所用的相同方法在该层的 Rules 页面添加设置。

过程

步骤 1 编辑入侵策略时，展开导航面板中的**策略层 (Policy Layers)**。

步骤 2 展开要修改的策略层。

步骤 3 点击要修改的策略层正下方的 **Rules**。

步骤 4 修改使用规则调整入侵策略，第 817 页中所述的任意设置。

提示 要从可编辑层删除单项设置，请双击该层 Ruels 页面的规则消息，以显示规则详细信息。在要删除的设置旁，单击 **Delete**，然后双击 **OK**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

从多个层中删除规则设置

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以从入侵策略中的多个层同时删除特定类型的事件过滤器、动态状态或警报。系统移除所选设置并将规则的剩余设置复制到策略中的最高可编辑层。

系统将向下移除每层中设置的设置类型，直至移除所有设置或遇到为规则设置了规则状态的层。在后一种情况下，系统会从该层中删除设置并停止删除设置类型。

当系统在共享层或在基本策略中遇到该设置类型时，如果策略中的最高层可以编辑，则系统会将该规则的剩余设置和规则状态复制到该可编辑层。否则，如果策略中的最高层是共享层，系统会在该共享层上方创建新的可编辑层，并将该规则的剩余设置和规则状态复制到该可编辑层。

注释 移除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。

过程

步骤 1 编辑入侵策略时，点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

提示 也可为所有层在“规则”(Rules) 页面的层下拉列表中选择**策略 (Policy)**，或在“策略信息”(Policy Information) 页面选择**管理规则 (Manage Rules)**。

步骤 2 选择要从中删除多个设置的规则：

- 选择特定 - 如果要选择特定规则，请选中每条规则旁边的复选框。
- 选择全部 - 如果要选择当前列表中的所有规则，请选中列顶部的复选框。

步骤 3 选择以下选项之一：

- **事件过滤 (Event Filtering)** > **删除阈值 (Remove Thresholds)**
- **事件过滤 (Event Filtering)** > **删除抑制 (Remove Suppressions)**
- **动态状态 (Dynamic State)** > **删除基于速率的规则状态 (Remove Rate-Based Rule States)**
- **警报 (Alerting)** > **删除 SNMP 警报 (Remove SNMP Alerts)**

注释 移除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。

步骤 4 点击 **OK**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

接受来自自定义基本策略的规则更改

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

当未曾添加层的自定义网络分析或入侵策略使用另一个自定义策略作为其基本策略时，在以下情况下，必须将规则设置为继承其规则状态：

- 删除为基本策略中的规则设置的事件过滤器、动态状态或 SNMP 警报，以及
- 您希望规则接受在用作基本策略的另一个自定义策略中对其做出的后续更改

过程

步骤 1 编辑入侵策略时，展开导航面板中的**策略层 (Policy Layers)**。

步骤 2 展开**我的更改 (My Changes)**。

步骤 3 点击**我的更改 (My Changes)** 正下方的**规则 (Rules)** 链接。

步骤 4 选择要接受其设置的规则。有以下选项可供选择：

- 选择特定规则 - 如果要选择特定规则，请选中每条规则旁边的复选框。
- 选择所有规则 - 如果要选择当前列表中的所有规则，请选中列顶部的复选框。

步骤 5 从**规则状态 (Rule State)** 下拉列表选择**继承 (Inherit)**。

步骤 6 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

层中的预处理器和高级设置

您使用类似的机制在网络分析策略中配置预处理程序和在入侵策略中配置高级设置。您可以启用和禁用预处理程序（在网络分析 Settings 页面上）和入侵策略高级设置（在入侵策略 Advanced Settings 页面上）。这些页面还提供所有相关功能的有效状态的摘要。例如，如果网络分析 SSL 预处理程序在一层中已禁用但在更高层中已启用，则 Settings 页面将其显示为已启用。在这些页面上做出的更改显示在策略的顶层中。请注意，Back Orifice 预处理程序没有用户可配置选项。

您也可以在用户可配置层的摘要页面上启用或禁用预处理程序或高级设置并访问其配置页面。在此页面上，可以修改层名称和说明，并配置是否将该层与同一类型的其他策略共享。可以通过选择导航面板中 **Policy Layers** 下方的层名称来切换到另一层的摘要页面。

启用预处理程序或高级设置时，在导航面板中的层名称下方会显示指向该功能的配置页面的子链接，并且在层的摘要页面上的功能旁边会显示编辑图标 ()；在层中禁用该功能或将其设置为 Inherit 时，这些图标会消失。

设置预处理程序或高级设置的状态（已启用或已禁用）会覆盖更低层中该功能的状态和配置设置。如果希望预处理程序或高级设置从基本策略或更低层继承其状态和配置，请将其设置为 **Inherit**。请注意，当在 Settings 或 Advanced Settings 页面上操作时，无法选择 Inherit。另请注意，如果继承当前启用的功能，则导航面板中的功能子链接和配置页面上的编辑图标不再显示。

系统使用已启用该功能的最高层中的配置。除非明确修改配置，否则系统使用默认配置。例如，如果在一层中启用并修改网络分析 DCE/RPC 预处理程序，并且还在更高层中将其启用但不修改，则系统使用更高层中的默认配置。

每个层摘要页面上的颜色编码指示有效配置位于较高层、较低层还是当前层中，如下所示：

- 红色 - 有效配置位于较高层
- 黄色 - 有效配置位于较低层
- 无光度 - 有效配置位于当前层

由于 Settings 和 Advanced Settings 页面是所有相关设置的综合视图，因此，这些页面不使用颜色编码指明有效配置的位置。

配置层中的预处理器和高级设置

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 编辑策略时，请展开导航面板中的 **Policy Layers**，然后点击要修改的层的名称。

步骤 2 有以下选项可供选择：

- 更改层**名称 (Name)**。
- 添加或更改**说明 (Description)**。
- 选中或清除**共享 (Sharing)** 复选框以指定层是否可以与其他策略共享。
- 要访问已启用的预处理器/高级设置的配置页面，请点击编辑图标 () 或功能子链接。
- 要禁用当前层中的预处理器/高级设置，请点击功能旁边的**已禁用 (Disabled)**。
- 要启用当前层中的预处理器/高级设置，请点击功能旁边的**已启用 (Enabled)**。

- 要从当前层下方的最高层中的设置继承预处理器/高级设置，请点击**继承 (Inherit)**。

步骤 3 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

第 49 章

入侵策略使用入门

以下主题介绍如何开始使用入侵策略：

入侵策略基础知识

入侵策略是已定义的几组入侵检测和防护配置，用于检查流量是否存在安全违规，以及在内联部署中阻止或修改恶意流量。入侵策略供访问控制策略调用，是系统在允许流量到达目标之前的最后一道防线。

每个入侵策略的中心是入侵规则。启用的规则导致系统为匹配规则的流量生成入侵事件（或阻止该流量）。禁用规则将停止该规则的处理。

Firepower 系统提供几种基本入侵策略，使您可以利用Cisco Talos 安全情报和研究小组 (Talos) 的经验。对于这些策略，Talos 可设置入侵和预处理器规则状态（启用或禁用），以及提供其他高级设置的初始配置。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，平衡安全性和连接网络分析策略和平衡安全性和连接入侵策略配合工作并可以在入侵规则更新中同时更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。

如果创建自定义入侵策略，您可以：

- 通过启用和禁用规则，以及撰写和添加您自己的规则来调整检测。
- 遵从 Firepower 的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 配置各种高级设置，例如，外部警告，敏感数据预处理和全局规则阈值。
- 使用分层作为构建块，以有效地管理多个入侵策略。

在内联部署中，入侵策略可以阻止和修改流量：

- 丢弃规则可以丢弃匹配的数据包和生成入侵事件。要配置入侵或预处理器丢弃规则，请将其状态设置为“丢弃并生成事件”(Drop and Generate Events)。
- 入侵规则可使用 `replace` 关键字来替换恶意内容。

要使入侵规则影响流量，必须正确配置丢弃规则和内容替换规则，以及正确部署内联受管设备，也就是与内联接口集内联。最后，必须启用入侵策略的丢弃行为或 **Drop when Inline** 设置。

当定制入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式对流量进行解码或预处理。在入侵策略检查数据包之前，数据包根据网络分析策略中配置对其进行预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

注意 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

在配置自定义入侵策略后，可以在访问控制配置过程中通过以下方式使用该策略：将入侵策略与一个或多个访问控制规则或访问控制策略的默认操作相关联。这会强制系统在某个允许的流量到达最终目的地之前使用入侵策略检查该流量。与入侵策略共同使用的变量集，用于准确地反映您的家庭和外部网络以及网络上的服务器（如果适当）。

请注意，默认情况下，系统禁用加密负载的入侵检查。当加密连接与已配置入侵检查的访问控制规则匹配时，这有助于减少误报和提高性能。

管理入侵策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在“入侵策略”(Intrusion Policy) 页面 (**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**) 上，可以查看当前自定义入侵策略以及下列信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及执行此修改的用户。
- 是否已启用 **Drop when Inline** 设置，该设置允许您在内联部署中丢弃和修改流量

- 哪些访问控制策略和设备在使用入侵策略检查流量
- 策略是否有未保存的更改，以及有关何人（如果有任何人）当前正在编辑该策略的信息
- 在多域部署中，创建了策略的域

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 管理入侵策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 261 页。
- 创建 - 点击**创建策略 (Create Policy)**；请参阅创建自定义入侵策略，第 812 页。
- 删除 - 点击要删除的策略旁边的删除图标 ()。如果另一用户在策略中有未保存的更改，则系统会提示您确认并进行通知。点击 **OK** 确认。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 编辑 - 点击要编辑的策略旁边的编辑图标 ()；请参阅编辑入侵策略，第 812 页。

  如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。
- 导出 - 如果要导出入侵策略以在其他 Firepower 管理中心上进行导入，请点击导出图标 ()；请参阅导出配置，第 151 页。
- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改，第 254 页。
- 报告 - 点击报告图标 ()；请参阅生成当前策略报告，第 262 页。

自定义入侵策略创建

当您创建新的入侵策略时，必须为其提供唯一的名称，指定基本策略并指定丢弃行为。

基本策略定义入侵策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。

入侵策略的丢包行为或 **Drop when Inline** 设置确定系统如何处理丢弃规则（规则状态设置为 Drop and Generate Events 的入侵或预处理器规则）和影响流量的其他入侵策略配置。当想要放弃或替换恶意数据包时，应该在内联部署中启用丢弃行为。请注意，在被动部署中，系统无法影响流量传输，无论丢包行为如何设置。

创建自定义入侵策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击 **Create Policy**。如果您在另一策略中有未保存的更改，当系统提示您返回 Intrusion Policy 页面时请点击 **Cancel**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 指定初始**基本策略**。
您可以使用系统提供的策略或其他自定义策略作为您的基本策略。

步骤 5 设置内联部署中的系统丢弃行为，如设置内联部署中的丢弃行为，第 814 页中所述。

步骤 6 创建策略：

- 点击 **Create Policy** 创建新策略并返回到 Intrusion Policy 页面。新策略的设置与其基本策略相同。
- 点击 **Create and Edit Policy** 创建策略并在高级入侵策略编辑器中打开该策略进行编辑；请参阅入侵策略更改，第 813 页。

编辑入侵策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击想要配置的入侵策略旁边的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑策略：

- 更改基本策略 - 从**基本策略 (Base Policy)** 下拉列表中选择基本策略；请参阅更改基本策略，第 798 页。
- 配置高级设置 - 点击导航面板中的**高级设置 (Advanced Settings)**；请参阅入侵策略高级设置，第 814 页。
- 配置 Firepower 建议的入侵规则 - 点击导航面板中的 **Firepower 建议 (Firepower Recommendations)**；请参阅生成和应用 Firepower 建议，第 848 页。
- 丢弃内联部署中的行为 - 选中或取消选中**内联时丢弃 (Drop when Inline)**；请参阅设置内联部署中的丢弃行为，第 814 页。
- 按建议的规则状态过滤规则 - 生成建议后，点击每个建议类型旁边的**查看 (View)**。点击**查看建议的更改 (View Recommended Changes)** 以查看所有建议。
- 按当前规则状态过滤规则 - 点击每个规则状态类型（生成事件、丢弃和生成事件）旁边的**查看 (View)**；请参阅入侵策略中的入侵规则过滤器，第 825 页。
- 管理策略层 - 点击导航面板中的**策略层 (Policy Layers)**；请参阅层管理，第 799 页。
- 管理入侵规则 - 点击**管理规则 (Manage Rules)**；请参阅查看入侵策略中的入侵规则，第 818 页。
- 查看基本策略中的设置 - 点击**管理基本策略 (Manage Base Policy)**；请参阅基本层，第 796 页。

步骤 4 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

入侵策略更改

当创建新的入侵策略时，它具有与其基本策略相同的入侵规则和高级设置。

系统为每个用户缓存一个入侵策略。在编辑入侵策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。

内联部署中的丢弃行为

如果要评估配置如何在内联部署中起作用（即，使用路由式、交换式或透明接口或内联接口对将相关配置部署到设备），而实际上不影响流量，则可以禁用丢弃行为。在这种情况下，系统生成入侵事件，但不会丢弃触发丢弃规则的数据包。当对结果满意时，可以启用丢弃行为。

请注意，在分路模式下，在被动部署或内联部署中，无论丢弃行为如何，系统都无法影响流量。换句话说，在被动部署中，设置为 Drop and Generate Events 的规则与设置为 Generate Events 的规则行为相同 - 系统生成入侵事件，但不会丢弃数据包。

注释 要阻止恶意软件通过 FTP 传输，不仅必须正确配置面向 Firepower 的 AMP，还必须在访问控制策略的默认入侵策略中启用**内联时丢弃 (Drop when Inline)**。

当您查看入侵事件时，工作流可以包括内联结果，以指示流量是否确实已丢弃，或者它是否仅仅应该已丢失。

设置内联部署中的丢弃行为

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 设置策略的丢弃行为：

- 选中**内联时丢弃 (Drop when Inline)** 复选框，以允许入侵规则影响流量并生成事件。
- 清除**内联时丢弃 (Drop when Inline)** 复选框，以防止入侵规则在生成事件时影响流量。

步骤 4 点击**确认更改 (Commit Changes)** 以保存自上次策略确认后在此策略中做出的更改。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

入侵策略高级设置

配置入侵策略的高级设置需要特定专业知识。入侵策略的基本策略决定了默认情况下启用哪些高级设置及各自的默认配置。

在入侵策略的导航面板中选择**高级设置 (Advanced Settings)** 时，策略将按类型列出其高级设置。在 Advanced Settings 页面中，您可以启用或禁用入侵策略中的高级设置，以及访问高级设置配置页面。高级设置必须在启用后才能配置。

当禁用高级设置时，子链接和 **Edit** 链接将不显示，但会保留您的配置。请注意，某些入侵策略配置（敏感数据规则、入侵规则的 SNMP 警报）需要启用和正确配置高级设置。您无法保存通过这种方式误配置的入侵策略。

修改高级设置的配置要求了解正在进行的修改及其对网络的潜在影响。

具体威胁检测

敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。

请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他预处理程序。

入侵规则阈值

全局规则阈值允许使用阈值来限制系统记录和显示的入侵事件数量，从而可以防止您的系统由于无法应付大量事件而崩溃。

外部响应

除了网络界面中的各种入侵事件视图之外，您还可以启用记录到系统日志 (syslog) 工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。

请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

优化入侵检测和防御的性能

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员（访问控制）；管理员/发现管理员（网络发现）

如果要让Firepower系统执行入侵检测和防御，但不需要利用发现数据，则可以通过禁用新发现来优化性能，如下所述。

过程

步骤 1 修改或删除与部署在目标设备的访问控制策略关联的规则。与该设备关联的任何访问控制规则均没有用户、应用或 URL 条件；请参阅创建和编辑访问控制规则，第 630 页。

步骤 2 从目标设备的网络发现策略中删除所有规则；请参阅配置网络发现规则，第 1209 页。

步骤 3 将已更改的配置部署到目标设备；请参阅部署配置更改，第 254 页。

第 50 章

使用规则调整入侵策略

以下主题介绍如何使用规则调整入侵策略：

入侵规则调整基础知识

您可以使用入侵策略中的“规则”(Rules) 页面为共享对象规则、标准文本规则和预处理器规则配置规则状态和其他设置。

将规则的状态设置为 Generate Events 或 Drop and Generate Events 即可启用该规则。启用规则后，系统将对匹配该规则的流量生成事件。禁用规则将停止该规则的处理。您还可以设置入侵策略，以便在内联部署中设置为“丢弃并生成事件”(Drop and Generate Events) 的规则在匹配流量时生成事件并丢弃该匹配流量。在被动部署中，设置为 Drop and Generate Events 的规则仅对匹配的流量生成事件。

您可以对规则进行过滤来显示规则的一个子集，这样就能选择要更改其规则状态或规则设置的确切规则集。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

入侵规则类型

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

入侵策略包含：

- 入侵规则，可细分为共享对象规则和标准文本规则
- 预处理器规则，与数据包解码器的检测选项或与 Firepower 系统随附的预处理器相关联

下表总结了这些规则类型的属性：

表 *83*：入侵规则类型

Type	生成器 ID (GID)	Snort ID (SID)	来源	可以复制？	可以编辑？
共享对象规则	3	低于 1000000	Cisco Talos 安全情报和研究小组 (Talos)	yes	有限
标准文本规则	1	低于 1000000	Talos	yes	有限
		1000000 或更高	由用户创建或导入	是	是
预处理器规则	特定于解码器或预处理器	低于 1000000	Talos	否	否
		1000000 或更高	由系统在选项配置期间生成	否	否

无法保存对 Talos 所创建的任何规则的更新，但是可以将已修改的规则的副本另存为自定义规则。可以修改在规则或规则报头信息中使用的变量（例如源和目标端口及 IP 地址）。在多域部署中，Talos 所创建的规则属于全局域。后代域中的管理员可以保存随后可编辑的规则的本地副本。

对于其创建的规则，Talos 在每个默认入侵策略中分配默认规则状态。大多数预处理器规则在默认情况下已禁用，如果希望系统为预处理器规则生成事件并在内联部署中丢弃违规的数据包，则必须启用这些规则。

在多域部署中，系统会在后代域中创建或导入的任何自定义规则的 SID 之前添加一个域编号。例如，在全局域中添加的规则的 SID 可能为 1000000，而在后代域中添加的规则的 SID 可能为 11000000 和 21000000。

查看入侵策略中的入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以调整规则在入侵策略中的显示方式，并且可按多个条件将规则排序。也可以显示特定规则的详细信息，以便查看规则设置、规则文档和其他规则详情。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 下的**规则 (Rules)**。

步骤 4 查看规则时，您可以执行以下操作：

- 过滤规则，如在入侵策略中设置规则过滤器，第 831 页中所述。
- 通过点击要按其排序的列顶部的标题或图标对规则进行排序。
- 查看入侵规则的详细信息，如查看入侵规则详细信息，第 821 页中所述。
- 通过从**策略 (Policy)** 下拉列表中选择一个层来查看不同策略层中的规则。

“入侵规则”(Intrusion Rules) 页面列

“入侵规则”(Intrusion Rules) 页面在其菜单栏和列标题中使用相同的图标。例如，“规则状态”(Rule State) 菜单使用与“规则状态”(Rule State) 列相同的图标 ( ) 列出规则。

表 *84*: “规则”*(Rules)* 页面列

标题	说明
GID	该整数表示规则的生成器 ID (GID)。
SID	该整数表示充当规则唯一标识符的 Snort ID (SID)。 对于自定义规则， SID 为 1000000 或更大值。 在多域部署中，系统会在后代域中创建或导入的任何自定义规则的 SID 之前添加一个域编号。例如，在全局域中添加的规则的 SID 可能为 1000000，而在后代域中添加的规则的 SID 可能为 11000000 和 21000000。
消息	此规则生成的事件中包含的消息，亦充当该规则的名称。

标题	说明
	规则的规则状态： • 丢弃并生成事件 () • 生成事件 () • 禁用 () 请注意，与为生成事件而不丢弃流量设置的规则的图标相比，已禁用规则的图标只是暗一些而已。此外，您还可以通过点击规则的规则状态图标来更改规则状态。
	Firepower 为规则建议的规则状态。
	事件过滤器，包括应用于该规则的事件阈值和事件抑制。
	该规则的动态规则状态，如果发生指定的速率异常则会生效。
	为规则配置的警报（当前仅限 SNMP 警报）。
	向规则添加的注释。

也可以使用层下拉列表切换到策略中其他层的 Rules 页面。请注意，除非向策略中添加层，否则下拉列表中列出的唯一可编辑视图是策略的 Rules 页面和最初命名为 `My Changes` 的策略层的 Rules 页面；另请注意，在这些视图其中之一进行更改与在其他视图中进行更改相同。该下拉列表中还会列出只读基本策略的 Rules 页面。

入侵规则详细信息

您可以从“规则详细信息”(Rule Detail) 视图查看规则文档、Firepower 建议和规则开销。还可以查看和添加特定于规则的功能。

表 *85*：规则详细信息

项目	说明
摘要	规则摘要。对基于规则的事件，此行将在规则文档包含摘要信息时显示。
Rule State	规则的当前规则状态。也表示设置规则状态所在的层。
Firepower 建议	如果已生成 FirePOWER 建议，则图标表示建议的规则状态；请参阅“入侵规则”(Intrusion Rules) 页面列，第 819 页。如果建议是启用规则，系统还会指出触发该建议的网络资产或配置。

项目	说明
Rule Overhead	规则对系统性能的潜在影响以及规则产生误报的可能性。本地规则没有分配的开销，除非被映射到漏洞。
阈值	当前为此规则设置的阈值，以及用于为该规则添加阈值的工具。
Suppressions	当前为此规则设置的抑制设置，以及用于为该规则添加抑制的工具。
Dynamic State	当前为此规则设置的基于速率的规则状态，以及用于为该规则添加动态规则状态的工具。
风险通告	为此规则设置的 SNMP 警报，以及用于为此规则添加警报的工具。
备注	向此规则添加的注释，以及用于为该规则添加注释的工具。
文档	当前规则的规则文档，由Cisco Talos 安全情报和研究小组 (Talos) 提供。

查看入侵规则详细信息

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 在导航窗格中，点击**规则 (Rules)**。

步骤 4 点击要查看其规则详细信息的规则，然后点击页面底部的**显示详细信息 (Show Details)**。屏幕上将显示规则详细信息，如入侵规则详细信息，第 820 页中所述。

步骤 5 从规则详细信息中，您可以配置：

- 警报 - 请参阅为入侵规则设置 SNMP 警报，第 824 页。
- 注释 - 请参阅将注释添加到入侵规则，第 824 页。
- 动态规则状态 - 请参阅从规则详细信息页面设置动态规则状态，第 823 页。
- 阈值 - 请参阅为入侵规则设置阈值，第 822 页。

- 抑制 - 请参阅为入侵规则设置抑制，第 822 页。

为入侵规则设置阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以在 Rule Detail 页面中为规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

请注意，当输入无效值时，在字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**阈值 (Thresholds)** 旁边的**添加 (Add)**。

步骤 2 从**类型 (Type)** 下拉列表中，选择要设置的阈值的类型：

- 选择**限制 (Limit)** 以将通知限于每个时间段的指定数量的事件实例。
- 选择**阀值 (Threshold)** 以在每个时间段内每次事件实例数达到指定数量时提供通知
- 选择**两者 (Both)** 以在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 3 从**跟踪方式 (Track By)** 下拉列表中，选择**源 (Source)** 或**目标 (Destination)** 以指示希望按源 IP 地址还是目标 IP 地址跟踪事件实例。

步骤 4 在**计数 (Count)** 字段中，输入要用作阈值的事件实例数。

步骤 5 在**秒 (Seconds)** 字段中，输入用于指定跟踪事件实例的时间段的数字（以秒为单位）。

步骤 6 点击 **OK**。

提示 系统在“事件过滤”(Event Filtering) 列中的规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，系统将在图标上注明事件过滤器的数量。

为入侵规则设置抑制

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以为入侵策略中的规则设置一个或多个抑制。

请注意，当键入的值无效时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**抑制 (Suppressions)** 旁边的**添加 (Add)**。

步骤 2 从**抑制类型 (Suppression Type)** 下拉列表中，选择下列选项之一：

- 选择**规则 (Rule)** 将完全抑制所选规则的事件。
- 选择**源 (Source)** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择**目标 (Destination)** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 3 如果为抑制类型选择**源 (Source)** 或**目标 (Destination)**，则在**网络 (Network)** 字段中输入 IP 地址、地址块或由这些值的任意组合组成并以逗号分隔的列表。
如果入侵策略与某个访问控制策略的默认操作相关联，则还可以在默认操作变量集中指定或列出网络变量。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 点击 **OK**。

提示 系统将在被抑制规则旁边的“事件过滤”(Event Filtering) 列中的规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，图标上的数字表示过滤器的数量。

从规则详细信息页面设置动态规则状态

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。当两个动态规则状态相冲突时，将执行第一个状态的操作。

动态规则状态为策略特定的。

请注意，当输入无效值时，在字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 从入侵规则的详细信息中，点击**动态状态 (Dynamic State)** 旁边的**添加 (Add)**。

步骤 2 从**跟踪方式 (Track By)** 下拉列表中，选择用于指示要如何跟踪规则匹配项的选项：

- 选择**源 (Source)** 将跟踪由特定的一个或一组源地址发出的该规则匹配项的数量。
- 选择**目标 (Destination)** 将跟踪发往特定的一个或一组目标地址的该规则匹配项的数量。
- 选择**规则 (Rule)** 将跟踪该规则的所有匹配项。

步骤 3 如果将**跟踪方式 (Track By)** 设置为**源 (Source)** 或**目标 (Destination)**，请在**网络 (Network)** 字段中输入要跟踪的每台主机的 IP 地址。
系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 在**速率 (Rate)** 旁边，指定每个时间段的规则匹配项数，以设置攻击速率：

- 在**计数 (Count)** 字段中，指定要用作阈值的规则匹配数。
- 在**秒数 (Seconds)** 字段中，指定跟踪攻击的时间段的秒数。

步骤 5 从**新状态 (New State)** 状态下拉列表中，选择满足条件时要采取的新操作。

步骤 6 在**超时 (Timeout)** 字段中输入值。
在超时后，规则将恢复到其原始状态。输入 0 可防止新操作超时。

步骤 7 点击 **OK**。

提示 系统将在“动态状态”(Dynamic State) 列中的规则旁边显示动态状态图标 ( )。如果向规则中添加多个动态规则状态过滤器，图标上的数字表示过滤器的数量。

为入侵规则设置 SNMP 警报

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以从 Rule Detail 页面为规则设置 SNMP 警报。

过程

从入侵规则的详细信息中，点击**警报 (Alerts)** 旁边的**添加 SNMP 警报 (Add SNMP Alert)**。

提示 系统将在“警报”(Alerting) 列中的规则旁边显示警报图标 ( )。如果向规则中添加多个警报，则系统将在图标上指示警报的数量。

将注释添加到入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 从入侵规则的详细信息中，点击**注释 (Comments)** 旁边的**添加 (Add)**。

步骤 2 在**注释 (Comment)** 字段中，输入规则注释。

步骤 3 点击 **OK**。

提示 系统将并在“注释”(Comments) 列中的规则旁显示注释图标 ( )。如果将多个注释添加到规则，图标上的数字表示注释的数量。

步骤 4 要删除规则注释，请点击规则注释部分的 **Delete**。仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

入侵策略中的入侵规则过滤器

可以按单一条件或按一个或多个条件的组合来过滤 Rules 页面中显示的规则。

规则过滤器关键字可帮助您找到要对其应用规则状态或事件过滤器等规则设置的规则。您可以按关键字进行过滤，同时从 Rules 页面的过滤器面板选择所需参数作为关键字的参数。

入侵规则过滤器说明

您所构造的过滤器显示于 Filter 文本框中。点击过滤器面板中的关键字和关键字参数可以构造过滤器。当选择多个关键字时，系统会使用 AND 逻辑将其组合以创建复合搜索过滤器。例如，如果选择**类别 (Category)** 下的**预处理器 (preprocessor)**，然后选择**规则内容 (Rule Content)** > **GID** 并输入 `116`，则会获得过滤器 `Category: “preprocessor” GID:”116”`，用于检索属于预处理器规则**并且** GID 为 116 的所有规则。

通过 Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor 和 Priority 过滤器组，可以为一个关键字提交多个参数（以逗号分隔）。例如，可以从**类别 (Category)** 中选择 **os-linux** 和 **os-windows** 以生成过滤器 `Category:"os-windows,os-linux"`，用于检索 `os-linux` 类别或 `os-windows` 类别中的任意规则。

要显示过滤器面板，请点击显示图标 ( )。

要隐藏过滤器面板，请点击隐藏图标 ( )。

入侵策略规则过滤器构建准则

在大多数情况下，当构建过滤器时，可以使用入侵策略中“规则”(Rules) 页面左侧的过滤器面板选择要使用的关键字/参数。

规则过滤器在过滤器面板中分为不同的规则过滤器组。许多规则过滤器组包含子条件，因此可以更轻松地找到所需的特定规则。有些规则过滤器有多个级别，可展开以向下钻取到各个规则。

过滤器面板中的项有时表示过滤器类型组，有时表示关键字，还有时表示关键字的参数。请注意以下提示：

- 当选择不是关键字的过滤器类型组标题（“规则配置”[Rule Configuration]、“规则内容”[Rule Content]、“平台特定”[Platform Specific] 和“优先级”[Priority]）时，该标题会展开以列出可用关键字。

  通过点击条件列表中的节点来选择关键字时，将显示一个弹出窗口，其中提供要作为过滤条件的参数。

  如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

  例如，如果点击过滤器面板中**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**丢弃并生成事件 (Drop and Generate Events)**，则会将 `Recommendation:"Drop and Generate Events"` 添加到过滤器文本框中。如果随后点击**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**生成事件 (Generate Events)**，则过滤器会更改为 `Recommendation:"Generate Events"`。

- 当选择属于关键字的过滤器类型组标题（“类别”[Category]、“分类”[Classifications]、“Microsoft 漏洞”[Microsoft Vulnerabilities]、“Microsoft 蠕虫”[Microsoft Worms]、“优先级”[Priority] 和“规则更新”[Rule Update]）时，该标题会列出可用参数。

  从此类型的组中选择项目时，该参数及其应用到的关键字会立即添加到过滤器中。如果该关键字已经在过滤器中，它将替换与该组对应的关键字的现有参数。

  例如，如果点击过滤器面板中 **Category** 下的 **os-linux**，则会将 `Category:"os-linux"` 添加到过滤器文本框中。如果随后点击 **Category** 下的 **os-windows**，过滤器将更改为 `Category:"os-windows"`。

- Rule Content 下的 Reference 是关键字，其下方列出的特定引用 ID 类型同样如此。选择任何引用关键字时，会显示一个弹出窗口，其中提供添加到现有过滤器的参数和关键字。如果过滤器中已在使用该关键字，则提供的新参数将替换现有参数。

  例如，如果依次点击过滤器面板中的**规则内容 (Rule Content)** > **引用 (Reference)** > **CVE ID**，系统将显示弹出窗口，提示您提供 CVE ID。如果输入 `2007`，则会将 `CVE:”2007”` 添加到过滤器文本框中。又例如，如果依次点击过滤器面板中的**规则内容 (Rule Content)** > **引用 (Reference)**，系统将显示弹出窗口，提示您提供该引用。如果输入 `2007`，则会将 `Reference:”2007”` 添加到过滤器文本框中。

- 从不同的组中选择规则过滤器关键字时，会将每个过滤器关键字都添加到过滤器中并保留所有现有关键字（除非被同一关键字的新值覆盖）。

  例如，如果点击过滤器面板中 **Category** 下的 **os-linux**，则会将 `Category:"os-linux"` 添加到过滤器文本框中。如果随后点击 **Microsoft Vulnerabilities** 下的 **MS00-006**，过滤器将更改为 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`。

- 当选择多个关键字时，系统会使用 AND 逻辑将其组合以创建复合搜索过滤器。例如，如果选择**类别 (Category)** 下的**预处理器 (preprocessor)**，然后选择**规则内容 (Rule Content)** > **GID** 并输入 `116`，则会获得过滤器 `Category: “preprocessor” GID:”116”`，用于检索属于预处理器规则**并且** GID 为 116 的所有规则。
- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific 和 Priority 过滤器组可以为一个关键字提交多个参数（以逗号分隔）。例如，可以从**类别 (Category)** 中选择 **os-linux** 和 **os-windows** 以生成过滤器 `Category:"os-windows,app-detect"`，用于检索 `os-linux` 类别或 `os-windows` 类别中的任意规则。

同一规则可以按多个过滤器关键字/参数对进行检索。例如，如果按类别 **dos** 来过滤规则，系统将显示 DOS Cisco 尝试规则 (SID 1545)，按优先级 **High** 进行过滤亦如此。

注释 Cisco Talos 安全情报和研究小组 (Talos) 可能会使用规则更新机制添加和删除规则过滤器。

请注意，“规则”(Rules) 页面上的规则可以是共享对象规则（生成器 ID 为 3），也可以是标准文本规则（生成器 ID 为 1）。下表介绍不同的规则过滤器。

表 *86*: 规则过滤器组

过滤器组	说明	是否支持多个参数?	标题为……	列表中的项目为……
Rule Configuration	根据规则的配置查找规则。	否	组	关键词
Rule Content	根据规则的内容查找规则。	否	组	关键词
类别	根据规则编辑器使用的规则类别来查找规则。请注意，本地规则显示于本地子组中。	是	关键字	参数
Classifications	根据规则生成的事件的数据包显示中所显示的攻击分类来查找规则。	否	关键字	参数
Microsoft Vulnerabilities	根据 Microsoft 公告号查找规则。	是	关键字	参数
Microsoft Worms	根据影响 Microsoft Windows 主机的特定蠕虫查找规则。	是	关键字	参数
Platform Specific	根据规则与特定操作系统版本的相关性来查找规则。 请注意，规则可能会影响多个操作系统或某个操作系统的多个版本。例如，启用 SID 2260 会影响多个版本的 Mac OS X、IBM AIX 以及其他操作系统。	是	关键字	参数 请注意，如果从子列表中选择一个项目，则会将一个修饰符添加到参数。

过滤器组	说明	是否支持多个参数?	标题为……	列表中的项目为……
预处理程序	查找各个预处理器的规则。 请注意，在启用预处理器时，必须启用与预处理器选项相关联的预处理器规则才能生成该选项的事件。	是	组	子组
优先级	根据高、中和低优先级查找规则。 分配给规则的分类将确定该规则的优先级。这些组进一步分为不同的规则类别。请注意，本地规则（即您创建的规则）不会显示于优先级组中。	是	关键字	参数 请注意，如果从子列表中选择一个项目，则会将一个修饰符添加到参数。
Rule Update	查找通过特定规则更新添加或修改的规则。对于每个规则更新，可以查看该更新中的所有规则、仅查看更新中导入的新规则或仅查看更新所更改的现有规则。	否	关键字	参数

入侵规则配置过滤器

您可以按多个规则配置设置来过滤 Rules 页面中列出的规则。例如，如果要查看规则状态与建议的规则状态不匹配的一组规则，可以选择 **Does not match recommendation** 来根据规则状态进行过滤。

通过点击条件列表中的节点来选择关键字时，可以提供要作为过滤条件的参数。如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**丢弃并生成事件 (Drop and Generate Events)**，则会将 `Recommendation:"Drop and Generate Events"` 添加到过滤器文本框中。如果随后点击**规则配置 (Rule Configuration)** > **建议 (Recommendation)** 下的**生成事件 (Generate Events)**，则过滤器会更改为 `Recommendation:"Generate Events"`。

入侵规则内容过滤器

您可以按多个规则内容项来过滤 Rules 页面中列出的规则。例如，通过搜索规则的 SID 可以快速检索该规则。也可以查找用于检测发往特定目标端口的流量的所有规则。

通过点击条件列表中的节点来选择关键字时，可以提供要作为过滤条件的参数。如果过滤器中已在使用该关键字，则提供的参数将替换该关键字的现有参数。

例如，如果点击过滤器面板中 **Rule Content** 下的 **SID**，系统将显示弹出窗口，提示您提供 SID。如果键入 `1045`，则 `SID:”1045”` 会被添加到过滤器文本框中。如果随即再次点击 **SID** 并将 SID 过滤器更改为 `1044`，过滤器将更改为 `SID:”1044”`。

表 *87*：规则内容过滤器

以下过滤器	查找符合以下条件的规则
消息	在消息字段中包含所提供的字符串。
SID	具有指定的 SID。
GID	具有指定的 GID。
参考	在引用字段中包含所提供的字符串。您也可以按特定类型的引用和所提供字符串进行过滤。
操作	首先执行 `alert` 或 `pass`。
协议	包含所选协议。
Direction	基于规则是否包含指示的方向设置。
源 IP	使用指定的地址或变量作为规则中的源 IP 地址指定。可以按有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。
目标 IP	使用指定的地址或变量作为规则中的源 IP 地址指定。可以按有效 IP 地址、CIDR 块/前缀长度或者使用 `$HOME_NET` 或 `$EXTERNAL_NET` 等变量进行过滤。
源端口	包括指定的源端口。端口值必须为 1 到 65535 之间的整数或端口变量。
目的端口	包括指定的目标端口。端口值必须为 1 到 65535 之间的整数或端口变量。
Rule Overhead	具有所选规则开销。
元数据	具有包含匹配的键值对的元数据。例如，键入`metadata:”service http”`可查找元数据与HTTP应用协议相关的规则。

入侵规则类别

Firepower 系统根据规则检测的流量类型对规则分类。在 Rules 页面中，可以按规则类别过滤，从而可为某个类别中的所有规则设置规则属性。例如，如果网络中没有 Linux 主机，则可以按 **os-linux** 类别过滤，然后禁用表明将禁用整个 **os-linux** 类别的所有规则。

可以将鼠标指针悬停在类别名称上方来显示该类别中的规则数。

注释 Cisco Talos 安全情报和研究小组 (Talos) 可能会使用规则更新机制添加和删除规则类别。

入侵规则过滤器组件

通过编辑过滤器可以修改您在过滤器面板中点击过滤器时所提供的特定关键字及其参数。Rules 页面中的自定义过滤器的功能与规则编辑器中使用的过滤器类似，但除此之外，您还可以使用在 Rules 页面过滤器中提供的任何关键字，使用在过滤器面板中选择过滤器时显示的语法。要确定供今后使用的关键字，请点击右侧过滤器面板中的相应参数。过滤器关键字和参数语法显示于过滤器文本框中。请记住，只有 Category 和 Priority 过滤器类型支持关键字有多个以逗号分隔的参数。

您可以使用关键字和参数、字符串及带引号的原义字符串，以空格分隔多个过滤条件。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

keyword:*" argument"*

其中，keyword 是入侵规则过滤器组中的关键字之一，argument 是要在与该关键字相关的一个或多个特定字段中搜索的字母数字字符串，用双引号引起来且不区分大小写。请注意，键入的关键字应该首字母大写。

除 `gid` 和 `sid` 之外的所有关键字的参数都会被视为部分字符串。例如，参数 `123` 将返回 `"12345"`、`"41235"`、`"45123"` 等结果。`gid` 和 `sid` 的参数只会返回完全匹配项；例如，`sid:3080` 只会返回结果 `SID 3080`。

每个规则过滤器还可以包含一个或多个字母数字字符串。字符串将搜索规则的“消息”(Message) 字段、Snort ID (SID) 和生成器 ID (GID)。例如，字符串 `123` 会返回规则消息中的 `"Lotus123"`、`"123mania"` 等字符串，也会返回 `SID 6123`、`SID 12375` 等。使用一个或多个字符串来进行过滤可以搜索部分 SID。

所有字符串都不区分大小写并被视为部分字符串。例如，`ADMIN`、`admin` 或 `Admin` 等字符串中任意一个都会返回 `"admin"`、`"CFADMIN"`、`"Administrator"` 等结果。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 `"overflow attempt"` 只会返回完全匹配的该字符串，而由 `overflow` 和 `attempt` 这两个字符串组成的未加引号的过滤器则会返回 `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` 等结果。

输入关键字、文字字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

入侵规则过滤器的使用

可以从入侵策略中 Rules 页面左侧的过滤器面板中选择预定义的过滤器关键字。选择过滤器时，该页面会显示所有匹配的规则，或者指出没有匹配的规则。

您可以对过滤器添加关键字来进一步对其进行限制。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤条件，页面将清空，转而返回新过滤器的结果。

您也可以使用在选择过滤器时提供的相同关键字和参数语法来键入过滤条件，或者在选择过滤器后修改其中的参数值。当键入的搜索条件没有关键字、关键字的首字母没有大写或者没有用引号将参数引起来时，该搜索将被视为字符串搜索，并搜索类别、消息和 SID 字段中有无指定条件。

在入侵策略中设置规则过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以对 Rules 页面中的规则进行过滤来显示其中一组规则。然后，可以使用任何页面功能，包括选择情景菜单中可用的任何功能。例如，当您需要为某个特定类别的所有规则设置阈值时，此功能会非常有用。您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，您可以将新的规则状态应用到已过滤或未过滤列表中的规则。

所有过滤器关键字、关键字参数和字符串都不区分大小写。如果点击过滤器中已存在的关键字的参数，则该参数将替换现有的参数。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击**规则 (Rules)**。

步骤 4 使用以下任一方法单独或以组合形式构建过滤器：

- 在**过滤器 (Filter)** 文本框中输入值，然后按 Enter 键。
- 展开任何预定义的关键字。例如，点击**规则配置 (Rule Configuration)**。
- 点击一个关键字，并指定参数值（如果提示）。例如：

  在**规则配置 (Rule Configuration)** 下，可以点击**规则状态 (Rule State)**，从下拉列表中选择 `生成事件 (Generate Events)`，然后点击**确定 (OK)**。

  在**规则配置 (Rule Configuration)** 下，可以点击**注释 (Comment)**，输入要筛选的注释文本字符串过滤，然后点击**确定 (OK)**。

在**类别 (Category)** 下，可以点击**应用检测 (app-detect)**，系统将其用作参数值。

- 展开关键字，然后点击一个参数值。例如，展开**规则状态 (Rule State)**，然后点击**生成事件 (Generate Events)**。

入侵规则状态

通过入侵规则状态，您可在个别入侵策略中启用或禁用规则，以及指定受监控条件触发该规则时系统采取的操作。

Cisco Talos 安全情报和研究小组 (Talos)为每个默认策略中的每条入侵规则和预处理器规则设置默认状态。例如，一条规则可能会在 Security over Connectivity 默认策略中启用而在 Connectivity over Security 默认策略中禁用。Talos 有时会使用规则更新来更改默认策略中一条或多条规则的默认状态。如果允许规则更新对基本策略进行更新，则意味着当用于创建策略的默认策略中的默认状态发生更改时，也允许规则更新更改策略中的规则默认状态。但请注意，如果您已经更改了规则状态，规则更新不会覆盖您的更改。

创建入侵规则时，它会继承用于创建策略的默认策略中相应规则的默认状态。

入侵规则状态选项

在入侵策略中，可以将规则的状态设置为以下值：

Generate Events

您希望系统检测特定入侵企图，并在其发现匹配流量时生成入侵事件。当恶意数据包通过网络并触发该规则时，数据包被发送到其目标，系统生成入侵事件。该恶意数据包到达其目标，但是您通过事件日志记录收到通知。

Drop and Generate Events

您希望系统检测特定入侵企图，丢弃包含攻击的数据包，并在其发现匹配流量时生成入侵事件。该恶意数据包永远不会到达其目标，并且您通过事件日志记录收到通知。

请注意，设置为此规则状态的规则在被动部署中生成事件但不丢弃数据包，包括 7000 或 8000 系列设备内联接口集处于分路模式下的部署。为使系统丢弃数据包，还必须在入侵策略中启用**内联时丢弃 (Drop when Inline)** 并部署设备内联。

Disable

您不希望系统评估匹配流量。

注释 选择**生成事件 (Generate Events)** 或**丢弃并生成事件 (Drop and Generate Events)** 选项可启用规则。选择**禁用 (Disable)** 会禁用规则。

思科**强烈**建议**不要**启用入侵策略中的所有入侵规则。如果启用所有规则，受管设备的性能可能会下降。相反，应调整规则集，使之与网络环境尽可能相符。

设置入侵规则状态

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

入侵规则状态为策略特定的。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

提示 此页面指示已启用规则的总数、设置为“生成事件”(Generate Events) 的已启用规则的总数，以及设置为“丢弃并生成事件”(Drop and Generate Events) 的总数。另请注意，在被动部署中，设置为 Drop and Generate Events 的规则仅生成事件。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中设置规则状态的一条或多条规则。

步骤 5 选择以下其中一个选项：

- **规则状态 (Rule State)** > **生成事件 (Generate Events)**
- **规则状态 (Rule State)** > **丢弃并生成事件 (Drop and Generate Events)**
- **规则状态 (Rule State)** > **禁用 (Disable)**

步骤 6 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

入侵策略中的入侵事件通知过滤器

入侵事件的重要性可根据发生频率或者源或目标IP地址而定。在某些情况下，您可能并不在意发生不到一定次数的事件。例如，如果有人企图登录服务器，在其失败达到一定次数之前，您可能不会关心。但在其他情况下，也许只需要发生几次，就能让您知道存在普遍性问题。例如，如果有人对网络服务器发动DoS攻击，可能只需要发生区区数次入侵事件，您就会明白需要解决这种情况。发生数百次相同事件只会让系统不堪重负。

入侵事件阈值

您可以逐个入侵策略为各条规则设置阈值，根据事件在指定时间段内生成的次数来限制系统记录和显示入侵事件的次数。这可以防止因相同事件数量过多而使系统不堪重负。您可以根据共享对象规则、标准文本规则或预处理器规则设置阈值。

入侵事件阈值配置

要设置阈值，请先指定阈值类型。

表 *88*：阈值选项

选项	说明
Limit	为指定时间段内触发规则的指定数量的数据包（由Count参数指定）记录并显示事件。例如，如果将类型设置为 **Limit**，将 **Count** 设置为 `10`，并将 **Seconds** 设置为 `60`，而同一分钟内有14个数据包触发规则，则系统在显示发生的前10个违反该规则的事件后将停止记录违反该规则的事件。
阈值	在指定时间段内，当指定数量的数据包（由Count参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为 **Threshold**，将 **Count** 设置为 `10`，并将 **Seconds** 设置为 `60` 时，如果到33秒时规则触发10次，则系统将生成一个事件，然后将Seconds和Count计数器重置为0。其后，该规则在接下来25秒内又触发10次。由于计数器在第33秒时已重置为0，因此系统此时会再记录一个事件。
两者	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。例如，如果将类型设置为 **Both**，将 **Count** 设置为2，并将 **Seconds** 设置为 `10`，则事件计数结果如下： • 如果10秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果10秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果10秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

接下来，指定跟踪，从而确定事件阈值是按源IP地址计算还是按目标IP地址计算。

表 *89*：阈值 *IP* 选项

选项	说明
来源	按源 IP 地址计算事件实例计数。
目标	按目标 IP 地址计算事件实例计数。

最后，指定用于定义阈值的实例数和时间段。

表 *90*：阈值实例/时间选项

选项	说明
计数	每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数量。
秒	计数重置之前经过的秒数。如果将阈值类型设置为 **limit**，将跟踪设置为 **Source IP**，将 **count** 设置为 `10`，并将 **seconds** 设置为 `10`，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在 10 秒过后重新开始计数。

请注意，入侵事件阈值可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件抑制的任意组合配合使用。

提示 也可以在入侵事件的数据包视图中添加阈值。

添加和修改入侵事件阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以为入侵策略中的一条或多条特定规则设置阈值。也可以单独或同时修改现有阈值设置。可以为每条规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

还可以修改默认应用到与入侵策略关联的所有规则和预处理器生成的事件的全局阈值。

当输入无效值时，字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

提示 在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中设置阈值的一条或多条规则。

步骤 5 选择**事件过滤 (Event Filtering)** > **阈值 (Threshold)**。

步骤 6 从**类型 (Type)** 下拉列表中选择阈值类型。

步骤 7 从**跟踪方式 (Track By)** 下拉列表中，选择要按**源 (Source)** 还是**目标 (Destination)** IP 地址跟踪事件实例。

步骤 8 在**计数 (Count)** 字段中输入值。

步骤 9 在**秒数 (Seconds)** 字段中输入值。

步骤 10 点击 **OK**。

提示 系统在“事件过滤”(Event Filtering) 列中的规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，图标上的数字表示事件过滤器的数量。

步骤 11 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

查看和删除入侵事件阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可能需要查看或删除一个规则的现有阈值设置。可以使用 Rules Details 视图显示为阈值配置的设置，看其是否适合系统。如果不适合，可以添加新的阈值来覆盖现有值。

请注意，还可以修改全局阈值，它默认应用到入侵策略所记录的所有规则和预处理器生成的事件。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择配置了要查看或删除的阈值的一条或多条规则。

步骤 5 要删除每条所选规则的阈值，请依次选择**事件过滤器 (Event Filtering)** > **删除阀值 (Remove Thresholds)**。

步骤 6 点击 **OK**。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

入侵策略抑制配置

您可以在特定 IP 地址或 IP 地址范围触发特定规则或预处理器时抑制入侵事件通知。这对杜绝误报十分有用。例如，如果邮件服务器传输的数据包看起来像某种特定的漏洞，则可能会在邮件服务器触发该事件时抑制对其发出的事件通知。所有数据包都会触发该规则，但您只会看到真正的攻击事件。

入侵策略抑制类型

请注意，入侵事件抑制可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件阈值的任意组合配合使用。

提示 可以在入侵事件的数据包视图中添加抑制。在入侵规则编辑器页面（**对象 (Objects)** > **入侵规则 (Intrusion Rules)**）和任何入侵事件页面（如果该事件由入侵规则触发）上，也可以使用右键点击情景菜单访问抑制设置。

抑制特定规则的入侵事件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以在入侵策略中抑制一个或多个规则的入侵事件通知。当某条规则的通知被抑制时，规则会触发，但不会生成事件。您可以为规则设置一个或多个抑制。列出的第一个抑制的优先级最高。当两个抑制发生冲突时，将执行第一个抑制的操作。

请注意，当输入无效值时，在字段中会显示恢复图标 ( )；点击该图标可恢复为该字段的上一个有效值，如果没有先前值，则会清除该字段。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要为其配置抑制条件的一个或多个规则。

步骤 5 依次选择**事件过滤 (Event Filtering)** > **抑制 (Suppression)**。

步骤 6 选择**抑制类型 (Suppression Type)**。

步骤 7 如果为抑制类型选择了**源 (Source)** 或**目标 (Destination)**，请在**网络 (Network)** 字段中输入要指定为源或目标 IP 地址的 IP 地址、地址块或变量，或者输入由这些值的任意组合组成的逗号分隔列表。系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 8 点击 **OK**。

提示 系统将在被抑制规则旁边的“事件过滤”(Event Filtering) 列中的规则旁边显示事件过滤器图标 ( )。如果向规则中添加多个事件过滤器，图标上的数字表示事件过滤器的数量。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

查看和删除抑制条件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可能需要查看或删除现有抑制条件。例如，由于某个邮件服务器通常会传输看起来像漏洞的数据包，因此可以抑制由该邮件服务器 IP 地址发出的数据包的事件通知。如果以后停用该邮件服务器并将此 IP 地址重新分配给其他主机，应删除对该源 IP 地址的抑制条件。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要查看或删除其抑制的一个或多个规则。

步骤 5 有以下选项可供选择：

- 要删除规则的所有抑制，请依次选择**事件过滤 (Event Filtering)** > **删除抑制 (Remove Suppressions)**。
- 要删除特定抑制设置，请点击规则，然后点击**显示详细信息 (Show details)**。展开抑制设置，然后点击要删除的抑制设置旁边的 **Delete**。

步骤 6 点击 **OK**。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

动态入侵规则状态

基于速率的攻击通过向网络或主机发送过大的流量，企图让网络或主机不堪重负，导致其速度下降或拒绝合法请求。为了应对特定规则出现过多规则匹配项的情况，可以使用基于速率的防御来更改规则的操作。

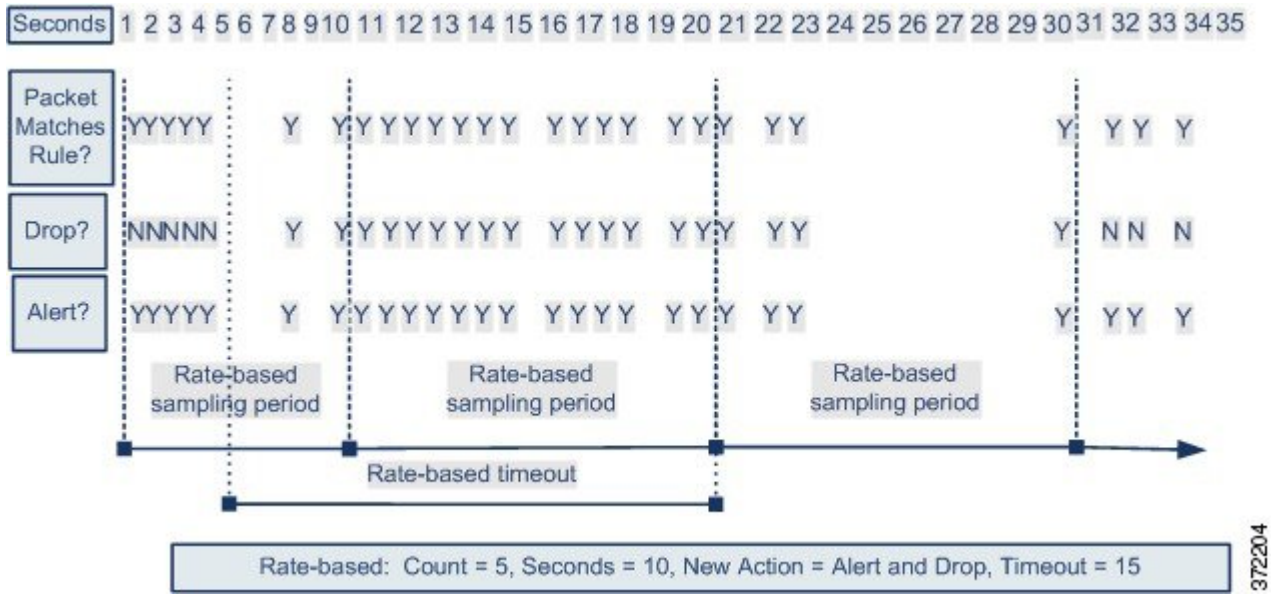
您可以配置入侵策略，使其包含基于速率的过滤器，在指定时间段内出现某条规则的太多匹配项时进行检测。此功能可以用于内联部署的受管设备上，先在指定时间内拦截基于速率的攻击，然后恢复为规则匹配项仅生成事件而不丢弃流量的规则状态。

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。您可以识别出发往一个或多个特定目标 IP 地址或者由一个或多个特定源 IP 地址发出的流量中存在的过多规则匹配项。也可以对检测的所有流量中符合特定规则的过多匹配项作出反应。

在某些情况下，您可能不希望将某规则设置为 Drop and Generate Events 状态，因为您不想丢弃与该规则匹配的每个数据包，但同时您又确实希望在指定事件内出现特定频率的匹配项时丢弃与该规则匹配的数据包。动态规则状态可用于配置应该触发规则操作更改的速率、达到该速率时应该改而执行的操作以及新操作应该持续的时间。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为 Drop and Generate Events。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为 Generate Events。



动态入侵规则状态配置

在入侵策略中，可以为任何入侵规则或预处理器规则配置基于速率的过滤器。基于速率的过滤器包含三个组成部分：

- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过速率时要执行的新操作，可用的操作有三项：Generate Events、Drop and Generate Events 和 Disable
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。达到超时后，如果速率低于阈值，则规则的操作会恢复到为该规则最初配置的操作。

在内联部署中，可以将基于速率的攻击防御临时或永久配置为拦截攻击。如果没有基于速率的配置，设置为 Generate Events 的规则确实会生成事件，但系统不会丢弃这些规则的数据包。但是，如果攻

击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为 Drop and Generate Events。

注释 基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器的操作相冲突时，将执行第一个基于速率的过滤器的操作。

从规则页面设置动态规则状态

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以为规则设置一个或多个动态规则状态。列出的第一个动态规则状态具有最高优先级。当两个动态规则状态相冲突时，将执行第一个状态的操作。

动态规则状态为策略特定的。

当输入无效值时，字段中会显示恢复图标 ()；点击该图标可恢复为该字段的上一个有效值，如果没有上一个值，则会清除该字段。

注释 动态规则状态无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中添加动态规则状态的一条或多条规则。

步骤 5 依次选择**动态状态 (Dynamic State)** > **添加基于速率的规则状态 (Add Rate-Based Rule State)**。

步骤 6 从**跟踪方式 (Track By)** 下拉列表中选择一个值。

步骤 7 如果将 **Track By** 设置为 **Source** 或 **Destination** 时，请在 **Network** 字段中输入要跟踪的每台主机的地址。可以指定单个 IP 地址、地址块、变量或由这些值的任意组合组成并以逗号分隔的列表。
系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 8 在**速率 (Rate)** 旁边，指定每个时间段的规则匹配项数，以设置攻击速率：

- 在**计数 (Count)** 字段中输入值。

- 在**秒数 (Seconds)** 字段中输入值。

步骤 9 从**新状态 (New State)** 状态下拉列表中，指定满足条件时要采取的新操作。

步骤 10 在**超时 (Timeout)** 字段中输入值。
在超时后，规则将恢复到原始状态。指定 0 或将 **Timeout** 字段留空可防止新操作超时。

步骤 11 点击 **OK**。

提示 系统将在“动态状态”(Dynamic State) 列中的规则旁边显示动态状态图标 ( )。如果向规则中添加多个动态规则状态过滤器，图标上的数字表示过滤器的数量。

提示 要删除一组规则的所有动态规则设置，请在“规则”(Rules) 页面中选择这些规则，然后依次选择**动态状态 (Dynamic State)** > **删除基于速率的状态 (Remove Rate-Based States)**。也可以从规则的规则详细信息中删除个别基于速率的规则状态过滤器，方法是选择该规则后点击**显示详细信息 (Show details)**，然后点击要删除的基于速率的过滤器旁边的**删除 (Delete)**。

步骤 12 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置入侵规则的 SNMP 警报

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

开始之前

- 在相应的入侵策略中启用 SNMP 警报；请参阅配置 SNMP 响应，第 1381 页。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击**规则 (Rules)**。

步骤 2 选择要在其中设置 SNMP 警报的规则。

步骤 3 依次选择**警报 (Alerting)** > **添加 SNMP 警报 (Add SNMP Alert)**。

步骤 4 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加入侵规则注释

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以向入侵策略中的规则添加注释。按这种方式添加的注释是策略特定的；即添加到一个入侵策略的规则中的注释在其他入侵策略中不可见。添加的任何注释都将显示在该入侵策略的“规则”(Rules) 页面的“规则详细信息”(Rule Details) 视图中。

提交包含注释的入侵策略更改后，点击该规则 Edit 页面中的 **Rule Comment** 也可查看该注释。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

步骤 4 选择要在其中添加注释的一条或多条规则。

步骤 5 依次选择**注释 (Comments)** > **添加规则注释 (Add Rule Comment)**。

步骤 6 在**注释 (Comment)** 字段中，输入规则注释。

步骤 7 点击 **OK**。

提示 系统将并在“注释”(Comments) 列中的规则旁显示注释图标 ( )。如果向规则中添加多个注释，图标上的数字表示注释的数量。

步骤 8 或者，通过点击注释旁边的**删除 (Delete)** 以删除规则注释。

仅当缓存的注释具有未提交的入侵策略更改时，才能删除该注释。提交入侵策略更改之后，规则注释即是永久性的。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 51 章

根据网络资产定制入侵防护

以下主题介绍如何使用 Firepower 建议规则：

Firepower 建议的规则基础知识

可以遵从Firepower入侵规则建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

系统为每个入侵策略制定一组单独的建议。它通常会建议标准文本规则和共享对象规则的规则状态更改。但是，它也可建议预处理器和解码器规则的更改。

当生成规则状态建议时，可以使用默认设置或配置高级设置。通过高级设置，可以执行以下操作：

- 重新定义系统监控网络上的哪些主机以查找漏洞
- 影响系统根据规则开销建议哪些规则
- 指定是否生成建议以禁用规则

您还可以选择是要立即使用建议还是在接受之前审核建议（和受影响规则）。

选择使用建议规则状态会向入侵策略中添加只读Firepower建议层，并且随后选择不使用建议规则状态会删除该层。

您可以安排任务来根据入侵策略中最近保存的配置设置自动生成建议。

系统不会更改手动设置的规则状态：

- 在生成建议之前手动设置指定规则的状态可防止系统将来修改这些规则的状态。

- 在生成建议之后手动设置指定规则的状态可覆盖这些规则的建议状态。

提示 入侵策略报告可能包含具有与建议状态不同的规则状态的规则列表。

在显示对建议过滤后的 Rules 页面时，或者从导航面板或 Policy Information 页面直接访问 Rules 页面后，可以手动设置规则状态、对规则排序并执行 Rules 页面中的任何其他可用操作，例如抑制规则、设置规则阈值等。

注释 Cisco Talos 安全情报和研究小组 (Talos)确定系统提供的策略中的各规则的相应状态。如果使用系统提供的策略作为基本策略，并且允许系统将规则设置为 Firepower 建议规则状态，则入侵策略中的规则与思科为网络资产建议的设置相匹配。

建议规则和多租户

系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

Firepower 建议的默认设置

当生成Firepower建议时，系统会搜索基本策略以查找防范与网络资产关联的漏洞的规则，并识别基本策略中的规则的当前状态。然后，系统会建议规则状态，如果选择如此，则会将规则设置为建议状态。

系统执行以下基本分析来生成建议：

表 *91*：基于漏洞的 *Firepower* 规则状态建议

基本策略规则状态	规则是否保护发现的资产？	建议的规则状态
“生成事件”(Generate Events) 或“禁用”(Disable)	yes	Generate Events
Drop and Generate Events	yes	Drop and Generate Events
any	否	Disable

当生成建议而不更改Firepower建议规则的高级设置时，系统会建议更改所发现的整个网络中所有主机的规则状态。

默认情况下，系统仅为低开销或中等开销的规则生成建议，并生成禁用规则的建议。

系统不会为基于使用“影响限定条件”(Impact Qualification) 功能禁用的漏洞的入侵规则建议规则状态。

系统始终建议启用与映射到主机的第三方漏洞相关联的本地规则。

对于未映射的本地规则，系统不会给出状态建议。

Firepower 建议的高级设置

在策略报告中包括建议和规则状态之间的所有差异

默认情况下，入侵策略报告列出策略中已启用的规则，即设置为“生成事件”(Generate Events) 或“丢弃并生成事件”(Drop and Generate Events) 的规则。启用**包括所有差异 (Include all differences)** 选项还会列出其建议状态与已保存状态不同的规则。有关策略报告的信息，请参阅策略报告，第 262 页。

要检查的网络

指定为给出建议而要检查的受监控网络或单独主机。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

指定主机中的地址列表与一个逻辑或运算关联，但逻辑非除外，逻辑非在所有逻辑或运算计算完之后与一个逻辑与运算关联。

如果要根据主机信息动态调整对特定数据包的主动规则处理，也可以启用自适应配置文件。

建议阈值（就规则开销而言）

防止系统推荐或自动启用开销高于您选择的阈值的入侵规则。

开销基于规则对系统性能的潜在影响以及规则产生误报的可能性。允许开销较高的规则通常会得到更多的建议，但会影响系统性能。在“入侵规则”(Intrusion Rules) 页面的规则详细信息视图中，可以查看规则的开销级别。

请注意，系统在给出禁用规则的建议时，不会将规则开销作为一项考虑因素。此外，本地规则没有开销，除非被映射到第三方漏洞。

为开销级别为特定设置的规则生成建议并不会妨碍您使用不同的开销生成建议后再重新为原来的开销设置生成建议。每次为同一规则集生成建议时，无论生成多少次建议或者生成多少不同的开销设置，为每个开销设置获得的规则状态建议都相同。例如，您可以将开销依次设置为中、高，并最终设置为中来生成建议，如果网络中的主机和应用尚未更改，对于该规则集给出的开销设置为中的两组建议均相同。

接受禁用规则的建议

指定系统是否根据 Firepower 建议禁用入侵规则。

接受禁用规则的建议会限制规则的覆盖范围。忽略禁用规则的建议会扩大规则的覆盖范围。

生成和应用 Firepower 建议

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

开始或停止使用 Firepower 建议可能需要几分钟的时间，具体取决于网络和入侵规则集的大小。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

过程

步骤 1 在入侵策略编辑器的导航窗格中，点击 **Firepower 建议 (Firepower Recommendations)**。

步骤 2 （可选）配置高级设置；请参阅Firepower 建议的高级设置，第 847 页。

步骤 3 生成并应用建议。

- 生成并使用建议 - 生成建议并更改规则状态以使其匹配。仅在您从未生成过建议时可用。
- 生成建议 - 无论您是否在使用建议，生成新的建议，但不更改规则状态使其匹配。
- 更新建议 - 如果您正在使用建议，生成建议并更改规则状态以使其匹配。否则，生成新的建议，但不更改规则状态。
- 使用建议 - 更改规则状态以匹配任何未实施的建议。
- 不使用建议 - 停止使用建议。如果您在应用建议前手动更改了规则状态，则规则状态会恢复为您为其指定的值。否则，规则状态会恢复为其默认值。

在您生成建议时，系统会显示建议更改的摘要。要查看系统建议更改状态的规则列表，请点击最近建议的规则状态旁边的**查看 (View)**。

步骤 4 评估并调整您实施的建议。
即使您接受大多数 Firepower 建议，也可以通过手动设置规则状态覆盖个别建议；请参阅设置入侵规则状态，第 833 页。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 52 章

敏感数据检测

以下主题介绍敏感数据检测及其配置方式：

敏感数据检测基础知识

敏感数据（如社会保障号码、信用卡号码、驾驶证号码等）可能会被有意或无意地在互联网上泄露。系统提供的敏感数据预处理程序能够检测 ASCII 文本中的敏感数据并为之生成事件，此功能对于检测意外数据泄露特别有用。

全局敏感数据检测选项用于控制预处理器的工作方式。可以修改指定以下内容的全局选项：

- 预处理器是否在触发数据包中替换信用卡号或社会保障号的最后四位数
- 网络上的哪些目标主机监控敏感数据
- 单个会话中所有数据类型总共出现多少次会产生事件

具体数据类型确定了在指定目标网络流量中可以针对其进行检测并生成事件的敏感数据。可以为指定以下内容的数据类型选项修改默认设置：

- 某种检测到的数据类型必须达到才能生成单个会话事件的阈值

- 每种数据类型要监控的目标端口
- 每种数据类型要监控的应用协议

可以创建和修改自定义数据类型以检测指定的数据模式。例如，医院可以创建一种数据类型来保护患者编号；再如，大学可以创建一种数据类型来检测具有唯一编号模式的学号。

系统通过将各个数据类型与流量进行比对来检测每个 TCP 会话中的敏感数据。可以为每种数据类型和适用于入侵策略中所有数据类型的全局选项修改默认设置。Firepower 系统提供了常用的预定义数据类型。您也可以创建自定义数据类型。

敏感数据预处理程序规则与每种数据类型相关联。可通过为数据类型启用相应的预处理器，为每种数据类型启用敏感数据检测和事件生成。配置页面上的链接会将您指向 Rules 页面上的敏感数据规则的过滤视图，可以在其中启用和禁用规则以及配置其他规则属性。

保存对入侵策略所做的更改时，如果与数据类型关联的规则已启用且敏感数据检测已禁用，可以选择自动启用敏感数据预处理器。

提示 敏感数据预处理器可以检测使用 FTP 或 HTTP 上传和下载的未加密 Microsoft Word 文件中的敏感数据；之所以可以这样，大概是因为 Word 文件单独分组 ASCII 文本和格式命令的方式。

系统不会检测经过加密的或模糊的敏感数据，也不会检测压缩或编码格式（例如 Base64 编码邮件附件）的敏感数据。例如，系统会检测电话号码 (555)123-4567，但不会检测该号码经过模糊处理的版本（即，每个数字用空格分开，例如 (5 5 5) 1 2 3 - 4 5 6 7，或者通过 HTML 代码介入，例如 (555)-123-4567）。但是，系统会检测采用 HTML 代码的号码 (555)-123-4567，在该号码中，没有介入代码中断编号模式。

全局敏感数据检测选项

全局敏感数据选项是特定于策略的并适用于所有数据类型。

掩码

在触发数据包中用 X 替换信用卡号或社会保障号的最后四位数。掩码数字显示在网络界面中的入侵事件数据包视图中和下载的数据包中。

网络

指定监控敏感数据的目标主机。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。系统会将空白字段解读为 `any`，意指任何目标 IP 地址。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

Global Threshold

指定在生成全局阈值事件之前预处理器必须在任何组合中检测的单个会话中所有数据类型出现的总次数。可以指定 1 至 65535 之间的任意数字。

思科建议将此选项的值设置为大于在策略中启用的任何单个数据类型的最高阈值。

关于全局阈值，请注意：

- 必须启用预处理器规则 139:1 才能检测和生成关于数据类型出现次数的事件。
- 在每个会话中，预处理器最多生成一个全局阈值事件。
- 全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到全局阈值时生成事件，而不管任何具体数据类型的事件阈值是否达到，反之亦然。

单个敏感数据类型选项

每种自定义数据类型至少必须指定一个事件阈值和至少一个要监控的端口或应用协议。

每种系统提供的预定义数据类型使用一种其他方法无法访问的 `sd_pattern` 关键字来定义用于在流量中进行检测的内置数据模式。您还可以创建自定义数据类型，然后可以使用简单的正则表达式为这些数据类型指定自己的数据模式。

敏感数据类型显示在“敏感数据检测”(Sensitive Data Detection) 功能已启用的所有入侵策略中。系统提供的数据类型显示为只读。对于自定义数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

在多域部署中，系统会显示在当前域中创建的敏感数据类型，您可以对其进行编辑。系统还会显示在祖先域中创建的数据类型，您可以通过有限的方式对其进行编辑。对于祖先数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

表 *92*: 单个数据类型选项

选项	说明
Data Type	指定数据类型的唯一名称。
阈值	指定系统生成事件时数据类型出现的次数。可以指定 1 至 255 之间的数字。 请注意，在每个会话中，预处理器为检测到的数据类型生成一个事件。另请注意，全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到数据类型事件阈值时生成事件，而不管全局事件阈值是否达到，反之亦然。
Destination Ports	为数据类型指定要监控的目标端口。可以指定单个端口、端口的逗号分隔列表或 `any`（表示任何目标端口）。
应用协议	最多可以为数据类型指定八个要监控的应用协议。必须激活应用检测器来识别要监控的应用协议。 请注意，对于典型设备，此功能需要控制许可证。
Pattern	指定要检测的模式。此字段仅为自定义数据类型提供。

系统提供的敏感数据类型

每个入侵策略包括用于检测常用数据模式的系统提供的数据类型，例如，信用卡号、邮箱地址、美国电话号码以及带有和不带破折号的美国社会保障号。

每种系统提供的数据类型都与一个生成器 ID (GID) 为 138 的敏感数据预处理器规则相关联。必须启用入侵策略中的关联敏感数据规则才能为要用于策略中的每种数据类型启用检测和事件生成。

下表介绍了每种数据类型，并列出了必须启用才能为数据类型启用检测和事件生成的对应预处理器规则。

表 *93*：系统提供的敏感数据类型

Data Type	说明	预处理器规则 GID:SID
信用卡号	匹配 15 位和 16 位数字的 Visa®、MasterCard®、Discover® 和 American Express® 信用卡号（无论是否带正常分隔破折号或空格）；也可以使用 Luhn 算法来验证信用卡校验位。	138:2
邮件地址	匹配邮件地址。	138:5
美国电话号码	匹配符合 `(\d{3}) ?\d{3}-\d{4}` 模式的美国电话号码。	138:6
不带破折号的美国社会保障号	匹配包含有效的 3 位数区域号码、有效的 2 位数群组号码且不带破折号的 9 位数美国社会保障号。	138:4
带破折号的美国社会保障号	匹配包含有效的 3 位数区域号码、有效的 2 位数群组号码且带破折号的 9 位数美国社会保障号。	138:3

为了减少对社会保障号以外的 9 位数号码的误报，预处理器使用一种算法来验证 3 位数区域号码和 2 位数群组号码；在每个社会保障号中，这两组号码位于 4 位数序列号的前面。预处理器可验证 2009 年 11 月之前的社会保障号中的群组号码。

配置敏感数据检测

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护或控制	任何环境	任何环境	管理员/入侵管理员

由于敏感数据检测对 Firepower 系统的性能可能具有重大影响，思科建议遵循以下准则：

- 选择“无活动规则”(No Rules Active) 默认策略作为基本入侵策略。

- 确保在相应的网络分析策略中已启用以下设置：

  Application Layer Preprocessors 下的 **FTP and Telnet Configuration**

  Transport/Network Layer Preprocessors 下的 **IP Defragmentation** 和 **TCP Stream Configuration**。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的编辑图标 ( )。

步骤 6 有以下选项可供选择：

- 修改全局设置，如全局敏感数据检测选项，第 850 页中所述。
- 在**目标 (Targets)** 部分中选择数据类型，然后修改数据类型配置，如单个敏感数据类型选项，第 851 页中所述。
- 如果要检查自定义敏感数据，请创建自定义数据类型；请参阅自定义敏感数据类型，第 856 页。

步骤 7 为数据类型添加或删除要监控的应用协议；请参阅受监控应用协议和敏感数据，第 854 页。

注释 要检测 FTP 流量中的敏感数据，必须添加 `Ftp data` 应用协议。

步骤 8 或者，要显示敏感数据预处理器规则，请点击**配置敏感数据检测的规则 (Configure Rules for Sensitive Data Detection)**。

可以启用或禁用所列的任何规则。还可以为 Rules 页面上可用的任何其他操作（例如规则抑制、基于速率的攻击防御，等等）配置敏感数据规则；有关详细信息，请参阅入侵规则类型，第 818 页。

步骤 9 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在策略中启用敏感数据预处理器规则而未启用敏感数据检测，在保存策略更改时，系统会提示启用敏感数据检测。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 如果要生成入侵事件，请启用敏感数据检测规则 138:2、138:3、138:4、138:5、138:6、138:>999999 或 139:1。有关详细信息，请参阅入侵规则状态，第 832 页、全局敏感数据检测选项，第 850 页、系统提供的敏感数据类型，第 852 页和自定义敏感数据类型，第 856 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

受监控应用协议和敏感数据

最多可以为每种数据类型指定八个应用协议进行监控。必须为选择的每个应用协议至少启用一个检测器。默认情况下，系统提供的所有检测器均已激活。如果没有为应用协议启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。

必须为每种数据类型至少指定一个要监控的应用协议或端口。但是，除了要检测 FTP 流量中的敏感数据的情况之外，思科建议在指定应用协议时指定相应的端口，以便实现最全面覆盖。例如，如果指定 HTTP，还可以配置通用的 HTTP 端口 80。如果网络上的新主机实施 HTTP，系统会在其发现新 HTTP 应用协议的时间间隔内监控端口 80。

如果要检测 FTP 流量中的敏感数据，必须指定 `FTP data` 应用协议；在这种情况下，指定端口号没什么好处。

选择要监控的应用协议

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	可控性	任何环境	任何环境	管理员/入侵管理员

可以指定要在系统提供的和自定义的敏感数据类型中监控的应用协议。选择的应用协议为策略特定的。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的编辑图标 ( )。

步骤 6 点击**数据类型 (Data Types)** 下的数据类型名称。

步骤 7 点击**应用协议 (Application Protocol)** 字段旁边的编辑图标 ( )。

步骤 8 有以下选项可供选择：

- 要添加用于监控的应用协议，请从**可用 (Available)** 列表中选择一个或多个应用协议，然后点击右箭头 (>) 按钮。最多可以添加八个应用协议用于监控。
- 要删除进行监控的应用协议，请从**已启用 (Enabled)** 列表中选择，然后点击左箭头 (<) 按钮。

步骤 9 点击 **OK**。

步骤 10 要保存自上次策略提交以来在此策略中进行的更改，请点击导航窗格中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

特殊情况：FTP 流量中的敏感数据检测

通常，可通过指定要监控的端口或在部署中指定应用协议来确定要监控敏感数据的流量。

但是，对于检测 FTP 流量中的敏感数据来说，指定端口或应用协议并不足够。在 FTP 应用协议的流量中找到 FTP 流量中的敏感数据，这种情况间歇出现并使用临时端口号，因此难以检测。要检测 FTP 流量中的敏感数据，**必须**在配置中包括以下几项：

- 指定 `FTP 数据 (FTP data)` 应用协议以启用 FTP 流量中的敏感数据检测。

  对于检测 FTP 流量中的敏感数据这种特殊情况，指定 `FTP data` 应用协议不会调用检测功能；而是会调用 FTP/Telnet 预处理器的快速处理功能来检测 FTP 流量中的敏感数据。

- 确保 FTP Data 检测器已启用（默认情况下已启用）。
- 确保配置包括至少一个要监控敏感数据的端口。

请注意，不需要指定 FTP 端口（只要检测 FTP 流量中的敏感数据这种罕见情况除外）。大多数敏感数据配置将包括其他端口（例如 HTTP 或邮件端口）。如果只要指定一个 FTP 端口进行监控，思科建议指定 FTP 命令端口 `23`。

自定义敏感数据类型

创建的每种自定义数据类型还会创建一个敏感数据预处理器规则，该规则的生成器ID (GID) 为 138，Snort ID (SID) 为大于或等于 1000000（也就是本地规则的 SID）。 在多域部署中，系统会在后代域中创建或导入的任何自定义规则的 SID 之前添加一个域编号。例如，在全局域中添加的规则的 SID 可能为 1000000，而在后代域中添加的规则的 SID 可能为 11000000 和 21000000。

必须启用关联的敏感数据规则才能为要用于策略中的每种自定义数据类型启用检测和事件生成。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向入侵策略“规则”(Rules) 页面的过滤视图，其中显示所有系统提供和自定义的敏感数据规则。您还可以通过在入侵策略“规则”(Rules) 页面上选择本地过滤类别，使自定义敏感数据规则与任何自定义本地规则一起显示。请注意，自定义敏感数据规则不会列于入侵规则编辑器页面 (**对象 (Objects)** > **入侵规则 (Intrusion Rules)**)。

创建自定义数据类型后，您可以在系统中的任何入侵策略或多域部署中的当前域中启用该自定义数据类型。要启用自定义数据类型，必须在要用于检测和生成该自定义数据类型事件的任何策略中启用关联敏感数据规则。

自定义敏感数据类型中的数据模式

可使用一组由以下部分组成的正则表达式来定义自定义数据类型的数据模式：

- 三个元字符
- 允许将元字符用作原义字符的转义字符
- 六个字符类

元字符是在正则表达式中具有特殊含义的原义字符。

表 *94*：敏感数据模式元字符

元字符	描述	示例
`?`	匹配前面的字符或转义序列零次或一次；也就是说，前面的字符或转义序列是可选的。	`colou?r` 匹配 `color` 或 `colour`
`{n}`	匹配前面的字符或转义序列 n 次。	例如，`\d{2}` 匹配 `55`、`12` 等；`\l{3}` 匹配 `AbC`、`www` 等；`\w{3}` 匹配 `a1B`、25C 等；`x{5}` 匹配 `xxxxx`
`\`	元字符可用作实际字符，还可用于指定预定义的字符类。	`\?` 匹配问号，`\\` 匹配反斜杠，`\d` 匹配数字字符等

必须将反斜杠用于转义某些字符，这样敏感数据预处理器才能将它们正确解释为原义字符。

表 *95*：转义敏感数据模式字符

使用的转义字符	代表的原义字符
\?	?
\{	{
\}	}
\\	\

在定义自定义敏感数据模式时，可以使用字符类。

表 *96*：敏感数据模式字符类

字符类	说明	字符类定义
\d	匹配任何 ASCII 数字字符 0-9	0-9
\D	匹配任何不是 ASCII 数字字符的字节	不是 0-9
\l（小写“ell”）	匹配任何 ASCII 字母	a-zA-Z
\L	匹配任何不是 ASCII 字母的字节	不是 a-zA-Z
\w	匹配任何 ASCII 字母数字字符 请注意，与 PCRE 正则表达式不同，这不包括下划线 (_)。	a-zA-Z0-9
\W	匹配任何不是 ASCII 字母数字字符的字节	不是 a-zA-Z0-9

预处理器将直接输入（而不是作为正则表达式的一部分输入）的字符视为原义字符。例如，数据模式 1234 匹配 `1234`。

以下数据模式示例（用于系统提供的敏感数据规则138:4）使用转义的数字字符类、乘数和选项说明符元字符、文字破折号 (-) 和左右括号 () 字符来检测美国电话号码：

```
(\d{3}) ?\d{3}-\d{4}
```

创建自定义数据模式时务必谨慎。考虑将下列备选数据模式用于检测电话号码，尽管使用的是有效语法，但可能会导致许多误报：

```
(?\d{3})? ?\d{3}-?\d{4}
```

由于第二个示例结合了可选括号、可选空格和可选破折号，它会在下列所需模式中检测电话号码及其他方面：

- `(555)123-4567`

- 555123-4567
- 5551234567

但是，第二个示例模式也会检测以下可能无效的模式及其他方面，从而造成误报：

- (555 1234567
- 555)123-4567
- 555) 123-4567

最后举一个极端的例子（仅作说明用途）：创建一种数据模式，用以在小型企业网络上的所有目标流量中使用一个低事件阈值来检测小写字母 a。这种数据模式能够在短短几分钟内生成数百万的事件，从而可能令系统不胜负荷。

配置自定义敏感数据类型

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的敏感数据类型，您可以对其进行编辑。系统还会显示在祖先域中创建的数据类型，您可以通过有限的方式对其进行编辑。对于祖先数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

如果在任何入侵策略中启用某个数据类型的敏感数据规则，则不能删除该数据类型。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的编辑图标 ( )。

步骤 6 点击**数据类型 (Data Types)** 旁边的添加图标 ( )。

步骤 7 输入数据类型的名称。

步骤 8 输入要使用此数据类型检测的模式；请参阅自定义敏感数据类型中的数据模式，第 856 页。

步骤 9 点击 **OK**。

步骤 10 或者，点击数据类型名称，并修改单个敏感数据类型选项，第 851 页中所述的选项。

步骤 11 或者，通过点击删除图标 ( ) 删除自定义数据类型，然后点击**确定 (OK)** 以确认。

注释　如果在任何入侵规则中启用该数据类型的敏感数据规则，则系统会发出警告，表明不能删除该数据类型。再次尝试删除之前，必须禁用受影响策略中的敏感数据规则；请参阅设置入侵规则状态，第 833 页。

步骤 12 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 在要使用该数据类型的每个策略中启用关联的自定义敏感数据预处理规则；请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

编辑自定义敏感数据类型

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以编辑自定义敏感数据类型中的所有字段。但请注意，当修改名称或模式字段时，这些设置在系统上的所有入侵策略中都会更改。可以将其他选项设置为策略特定值。

在多域部署中，系统会显示在当前域中创建的敏感数据类型，您可以对其进行编辑。系统还会显示在祖先域中创建的数据类型，您可以通过有限的方式对其进行编辑。对于祖先数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的**编辑 (Edit)**。

步骤 6 在**目标 (Targets)** 部分中，点击自定义数据类型的名称。

步骤 7 点击**编辑数据类型名称和模式 (Edit Data Type Name and Pattern)**。

步骤 8 修改数据类型名称和模式；请参阅自定义敏感数据类型中的数据模式，第 856 页。

步骤 9 点击 **OK**。

步骤 10 将其余选项设置为策略特定值；请参阅单个敏感数据类型选项，第 851 页。

步骤 11 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 53 章

全局限制入侵事件日志记录

以下主题介绍如何全局限制入侵事件日志记录：

全局规则阈值基础知识

全局规则阈值为入侵策略记录的事件设置了限制。您可以跨所有流量设置全局规则阈值，用于限制策略在每个指定时间段记录和显示来自特定源地址或目标地址的事件的频率。您还可以根据策略中的共享对象规则、标准文本规则或预处理器规则设置阈值。设置全局阈值后，该阈值将应用于策略中没有特定阈值可覆盖该阈值的每条规则。阈值可以防止因事件数量过多而使系统不堪重负。

每个入侵策略包含一个默认应用于所有入侵规则和预处理器规则的默认全局规则阈值。此默认阈值将发往目标地址的流量的事件数限制为每 60 秒一个事件。

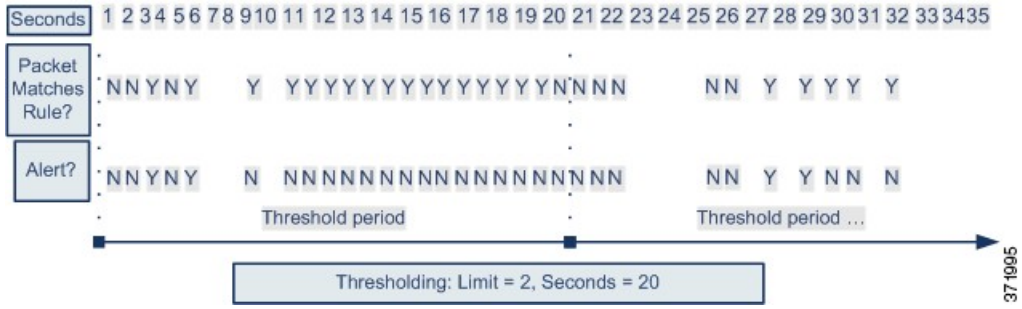
您可以执行以下操作：

- 更改全局阈值。
- 禁用全局阈值。
- 通过为特定规则设置单独的阈值来覆盖全局阈值。

  例如，可将全局限值阈值设置为每 60 秒生成五个事件，然后为 SID 1315 设置每 60 秒生成十个事件的特定阈值。所有其他规则每 60 秒生成的事件不超过五个，但是系统每 60 秒可为 SID 1315 生成多达十个事件。

提示 在有多个 CPU 的受管设备上，全局阈值或单独的阈值可能会导致事件数量高于预期。

下图展示了全局规则阈值的工作方式。在此示例中，系统正受到违反特定规则的攻击。全局限值阈值设置为将每条规则的事件生成频率限制为每 20 秒生成两个事件。请注意，该时间段在 1 秒时开始，在21秒时结束。该时间段结束后，时间周期重新开始，接下来两次规则匹配生成了事件，随后系统在这一时间段内不再生成事件。



全局规则阈值选项

默认阈值将每条规则的事件生成频率限制为对发往同一个目标地址的流量每60秒生成一个事件。全局规则阈值选项的默认值如下：

- **Type** - Limit
- **Track By** - Destination
- **Count** - 1
- **Seconds** - 60

您可以如下修改这些默认值：

表 *97*：阈值类型

选项	说明
Limit	为指定时间段内触发规则的指定数量的数据包（由计数参数指定）记录并显示事件。 例如，如果将类型设置为 **Limit**，将 **Count** 设置为 `10`，并将 **Seconds** 设置为 `60`，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
阈值	在指定时间段内，当指定数量的数据包（由计数参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。 例如，将类型设置为 **Threshold**，将 **Count** 设置为 `10`，并将 **Seconds** 设置为 `60` 时，如果到 33 秒时规则触发 10 次，系统将生成一个事件，然后将 Seconds 和 Count 计数器重置为 `0`。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 `0`，因此，系统此时会记录另一个事件。

选项	说明
两者	每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。 例如，如将类型设置为 **Both**，将 **Count** 设置为 2，将 **Seconds** 设置为 10，则事件计数结果如下： • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

跟踪依据 (Track By) 选项确定事件实例计数是按源 IP 地址计算还是按目标 IP 地址计算。

您还可以如下指定用于定义阈值的实例数和时间段：

表 *98*：阈值实例/时间选项

选项	说明
计数	对于**限制 (Limit)** 阈值，是指每个跟踪 IP 地址或地址范围在每个指定时间段内达到阈值所需的事件实例数。 对于**阀值 (Threshold)** 阈值，是指要用作阈值的规则匹配项的数量。
秒	对于**限制 (Limit)** 阈值，是指组成跟踪攻击的时间段的秒数。 对于**阀值 (Threshold)** 阈值，是指计数重置之前经过的秒数。如果将阈值类型设置为 **Limit**，将跟踪设置为 **Source**，将 **Count** 设置为 10，并将 **Seconds** 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了七个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。

配置全局阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**入侵规则阈值 (Intrusion Rule Thresholds)** 下的**全局规则阈值** （**Global Rule Thresholding**） 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**全局规则阈值 (Global Rule Thresholding)** 旁边的编辑图标 ( )。

步骤 6 使用**类型 (Type)** 单选按钮，指定在**秒数 (Seconds)** 字段中指定的时间内将应用的阈值类型。

步骤 7 使用**跟踪方式 (Track By)** 单选按钮，指定跟踪方式。

步骤 8 在**计数 (Count)** 字段中输入值。

步骤 9 在**秒数 (Seconds)** 字段中输入值。

步骤 10 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

禁用全局阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

如果要为特定规则的事件设置阈值而不是将阈值默认应用于每条规则，则可以在最高策略层禁用全局阈值。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 点击**入侵规则阈值 (Intrusion Rule Thresholds)** 下的**全局规则阈值 (Global Rule Thresholding)** 旁边的**已禁用 (Disabled)**。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 54 章

入侵规则编辑器

以下主题介绍如何使用入侵规则编辑器：

入侵规则编辑简介

入侵规则是系统用于检测利用网络漏洞企图的一组关键字和参数。当系统分析网络流量时，它会将数据包与每条规则中指定的条件进行比较。如果数据包数据与规则中指定的所有条件都匹配，则会触发此规则。如果规则是警报规则，将生成入侵事件。如果是通过规则，将忽略流量。对于内联部署中的丢弃规则，系统将丢弃数据包并生成事件。可以通过Firepower管理中心或网络界面查看和评估入侵事件。

Firepower 系统提供两种入侵规则：共享对象规则和标准文本规则。Cisco Talos 安全情报和研究小组(Talos)可以使用共享对象规则来检测传统的标准文本规则无法检测到的漏洞攻击。您无法创建共享对象规则。在自行编写入侵规则时，您可以创建标准文本规则。

您可以编写自定义标准文本规则，以调整可能出现的事件类型。请注意，虽然本文档有时讨论以检测特定漏洞为目标的规则，但最成功的规则是以检测可能试图利用已知漏洞的流量为目标，而不是以检测特定已知漏洞为目标。通过编写规则和指定规则的事件消息，可以更轻松地识别可能存在攻击和策略逃避行为的流量。

当在自定义入侵策略中启用自定义标准文本规则时，请记住，某些规则关键字和参数要求首先以特定方式对流量进行解码或预处理。本章说明在用于管理预处理的网络分析策略中必须配置的选项。请注意，如果禁用所需的预处理器，系统会自动采用其当前设置使用该预处理器，尽管该预处理器在网络分析策略网络界面中保持禁用状态。

注意 将编写的入侵规则用于生产环境之前，请务必使用受控网络环境测试这些规则。编写错误的入侵规则可能会严重影响系统性能。

在多域部署中，系统会显示在当前域中创建的规则，您可以对其进行编辑。系统还会显示在祖先域中创建的规则，您不可以对其进行编辑。要查看和编辑在较低域中创建的规则，请切换至该域。系统提供的入侵规则属于全局域。后代域中的管理员可以创建这些系统规则的本地可编辑副本。

规则剖析

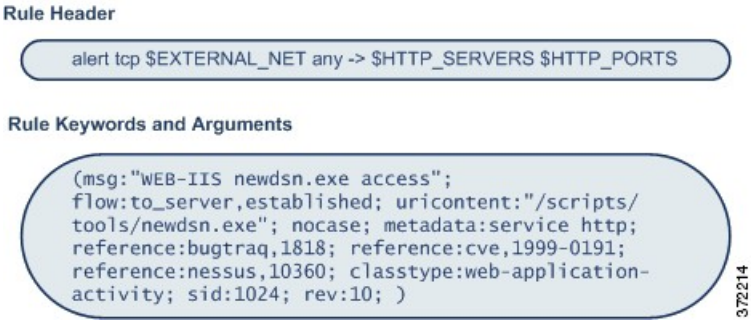
所有标准文本规则均包含两个逻辑部分：规则报头和规则选项。规则报头包含：

- 规则的操作或类型
- 协议
- 源 IP 地址、目标 IP 地址和子网掩码
- 方向指示符（显示从源到目标的流量流动方向）
- 源端口和目标端口

规则选项部分包含：

- 事件消息
- 关键字及其参数
- 模式（数据包负载必须与之匹配才能触发规则）
- 规范（规定规则引擎应检查数据包的哪些部分）

下图说明规则的组成部分：



请注意，括号里的是规则选项部分。入侵规则编辑器提供了一个易于使用的界面来帮助您构建标准文本规则。

入侵规则报头

每个标准文本规则和共享对象规则都有一个包含参数的规则报头。下面说明规则报头的组成部分：

下表介绍了规则报头的上述各个部分。

表 *99*：规则报头值

规则报头组成部分	示例值	示例值的作用
操作	`alert`	如果触发，将会生成事件。
协议	`tcp`	仅测试 TCP 流量。
源 IP 地址	`$EXTERNAL_NET`	测试来自不在内部网络上的任何主机的流量。
源端口	`any`	测试来自发起主机上任何端口的流量。
Operator	`->`	测试外部流量（流向网络上的网络服务器）。
目标 IP 地址：	`$HTTP_SERVERS`	测试将要传送到内部网络上被指定为网络服务器的任何主机的流量
目标端口	`$HTTP_PORTS`	测试传送到内部网络上 HTTP 端口的流量。

注释 与大多数入侵规则一样，以上示例使用默认变量。

入侵规则报头操作

每个规则报头都包含一个用于指定数据包触发规则时系统应采取的操作的参数。操作设置为 *alert* 的规则将会针对触发规则的数据包生成入侵事件并记录该数据包的详细信息。操作设置为 *pass* 的规则不会针对触发规则的数据包生成入侵事件，也不会记录该数据包的详细信息。

注释 在内联部署中，规则状态设置为“丢弃并生成事件”*(Drop and Generate Events)* 的规则会针对触发规则的数据包生成入侵事件。此外，如果在被动部署中应用丢弃规则，该规则将会充当警报规则。

默认情况下，通过规则会覆盖警报规则。可以创建通过规则来防止符合通过规则中定义的条件的数据包在特定情况下触发警报规则，而无需禁用预警报则。例如，您可能希望使检测尝试作为“匿名”

用户登录 FTP 服务器这种情况的规则保持活动状态。但是，如果网络有一个或多个合法的匿名 FTP 服务器，您可以编写并激活一个通过规则，在其中指明匿名用户不会对那些特定服务器触发原始规则。

在入侵规则编辑器中，可以从**操作 (Action)** 列表中选择规则类型。

入侵规则报头协议

在每个规则报头中，必须指定规则检查的流量的协议。可以指定以下网络协议用于分析：

- ICMP（互联网控制消息协议）
- IP（Internet 协议）

注释 如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。

- TCP（传输控制协议）
- UDP（用户数据报协议）

如果使用 **IP** 作为协议类型，将会检查 IANA 分配的所有协议（包括 TCP、UDP、ICMP、IGMP 等等）。

注释 目前不能编写与 IP 负载中下一个报头（例如 TCP 报头）模式匹配的规则。相反，内容匹配从上一个解码的协议开始。要解决这个问题，可以使用规则选项来匹配 TCP 报头中的模式。

在“入侵规则”(Intrusion Rules) 编辑器中，可以从**协议 (Protocol)** 列表中选择协议类型。

入侵规则报头方向

在规则报头中，可以指定数据包为使规则对其进行检查而必须传播的方向。下表介绍了这些选项。

表 *100*：规则报头中的方向选项

使用.....	以测试.....
Directional	仅测试从指定源 IP 地址流向指定目标 IP 地址的流量
双向	测试指定的源 IP 地址和目标 IP 地址之间的所有流量

入侵规则报头源和目标 IP 地址

通过将数据包检查限制为仅针对来自或发往特定 IP 地址的数据包，可以减少系统必须执行的数据包检查工作量。这样做还可以令规则更加具体，并消除规则针对源和目标 IP 地址未指示可疑行为的数据包进行触发的可能性，从而减少误报。

提示 系统只能识别 IP 地址，不接受源或目标 IP 地址的主机名。

在入侵规则编辑器中，可以在**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 字段中指定源 IP 地址和目标 IP 地址。

编写标准文本规则时，可以根据自身需求以多种方法指定 IPv4 和 IPv6 地址。可以指定单个 IP 地址、`any`、IP 地址列表、CIDR 记法、前缀长度、网络变量、网络对象或网络对象组。此外，还可以指明要排除的特定 IP 地址或 IP 地址集。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在多域部署中，在此配置中使用文字 IP 地址可能会出现意外结果。例如，可使用文字源 IP 地址 (192.0.2.2) 在全局域中创建入侵规则，并在后代域使用的入侵策略中启用该规则。在此情况下，您可能会看到后代域 A（其中 192.0.2.2 代表设备 A）和后代域 B（其中 192.0.2.2 代表设备 B）中的事件，但只有一组事件是入侵漏洞的可靠指标。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

入侵规则中的 *IP* 地址语法

下表总结了可用于指定源 IP 地址和目标 IP 地址的各种方法。

表 *101*：源/目标 *IP* 地址语法

要指定.....	使用.....	示例
任何 IP 地址	`any`	`any`
特定 IP 地址	IP 地址 请注意，不能在同一规则中混合使用 IPv4 和 IPv6 源地址和目标地址。	`192.168.1.1` `2001:db8::abcd`
IP 地址列表	使用方括号 (`[]`) 将地址括起来，并使用逗号分隔各个 IP 地址	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP 地址块	IPv4 CIDR 块或 IPv6 地址前缀记法	`192.168.1.0/24` `2001:db8::/32`
除特定 IP 地址或地址集以外的任何项	`!` 字符，后接要否定的 IP 地址	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
IP 地址块中除一个或多个特定 IP 地址以外的任何 IP 地址	在地址块后加上被否定地址或地址块的列表	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
网络变量定义的 IP 地址	前面带有 `$` 的大写字母形式的变量名称 请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。	`$HOME_NET`

要指定.....	使用.....	示例
除 IP 地址变量定义的地址以外的所有 IP 地址	前面带有 `!$` 的大写字母形式的变量名称	`!$HOME_NET`
网络对象或网络对象组定义的 IP 地址	采用 `!{object_name}` 这种格式的对象或对象组名称。	`${192.168sub16}`
除网络对象或网络对象组定义的地址以外的所有 IP 地址	对象或对象组名称用花括号 (`{}`) 括起来，前面带有 `!$`。	`!${192.168sub16}`

以下描述提供了有关某些 IP 地址输入方法的其他信息。

任意 IP 地址

可以指定 `any` 这个词作为规则的源或目标 IP 地址，以指示 IPv4 或 IPv6 地址。

例如，以下规则在**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 字段中使用参数 any 来评估具有任意 IPv4 或 IPv6 源地址或目标地址的数据包：

```
alert tcp any any -> any any
```

还可以指定 `::` 以指示 IPv6 地址。

多个 IP 地址

可以列出多个 IP 地址，地址之间用逗号分隔，如有需要，还可以用方括号将非否定地址列表括起来，如以下示例所示：

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

可以单独或以任意组合列出 IPv4 和 IPv6 地址，如以下示例所示：

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

请注意，现在不再要求用方括号将 IP 地址列表括起来（旧版软件要求这样做）。另请注意，输入列表时，可以在每个逗号前后添加一个空格。

注释 必须用方括号将否定列表括起来。

也可以使用 IPv4 无类别域际路由选择 (CIDR) 记法或 IPv6 前缀长度来指定地址块。例如：

- 192.168.1.0/24 指定子网掩码为 255.255.255.0 的 192.168.1.0 网络中的 IPv4 地址，即，192.168.1.0 至 192.168.1.255。
- 2001:db8::/32 指定前缀长度为 32 位的 2001:db8:: 网络中的 IPv6 地址，即，2001:db8:: 至 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff。

提示 如果需要指定 IP 地址块，但仅以 CIDR 或前缀长度记法无法表示出该地址块，可以在 IP 地址列表中使用 CIDR 块和前缀长度。

网络对象

可以使用以下语法指定网络对象或网络对象组：

```
${object_name | group_name}
```

其中：

- object_name 是网络对象的名称
- group_name 是网络对象组的名称

假设已创建一个名为 `192.168sub16` 的网络对象和一个名为 `all_subnets` 的网络对象组，那么，可以指定以下语法以识别使用该网络对象的 IP 地址：

```
${192.168sub16}
```

并且可以指定以下语法以使用该网络对象组：

```
${all_subnets}
```

还可以对网络对象和网络对象组进行否定。例如：

```
!${192.168sub16}
```

IP 地址否定

可以使用感叹号 (`!`) 否定指定 IP 地址。也就是说，可以匹配除指定 IP 地址以外的所有 IP 地址。例如，`!192.168.1.1` 指定除 192.168.1.1 以外的任何 IP 地址，`!2001:db8:ca2e::fa4c` 指定除 2001:db8:ca2e::fa4c 以外的任何 IP 地址。

要否定某个 IP 地址列表，请用方括号将该 IP 地址列表括起来，并在其前面加上 `!`。例如，`![192.168.1.1,192.168.1.5]` 将定义除 192.168.1.1 和 192.168.1.5 以外的任何 IP 地址。

注释 要否定 IP 地址列表，必须使用方括号。

对 IP 地址列表使用否定字符时务必要小心。例如，如果使用 `[!192.168.1.1,!192.168.1.5]` 匹配不是 192.168.1.1 和 192.168.1.5 的任何地址，系统会将此语法解释为“非 192.168.1.1 的任何地址，**或**非 192.168.1.5 的任何地址”。

由于 192.168.1.5 不是 192.168.1.1，且 192.168.1.1 不是 192.168.1.5，因此，这两个 IP 地址都与 `[!192.168.1.1,!192.168.1.5]` 的 IP 地址值匹配；此语法实质上与使用“`any`”相同。

应该使用 `![192.168.1.1,192.168.1.5]`。系统会将此语法为“**非** 192.168.1.1 **且非** 192.168.1.5”，这意味着，与方括号中所列地址以外的任何 IP 地址匹配。

请注意，从逻辑上讲，不能对 `any` 进行否定（如果它被否定，将表示无地址）。

入侵规则报头源和目标端口

在入侵规则编辑器中，可以在**源端口 (Source Port)** 和**目标端口 (Destination Port)** 字段中指定源端口和目标端口。

入侵规则中的端口语法

Firepower 系统使用特定类型的语法来定义规则报头中使用的端口号。

注释 如果协议设置为 `ip`，系统将忽略入侵规则报头中的端口定义。

可以列出多个端口，端口之间用逗号分隔，如以下示例所示：

```
80, 8080, 8138, 8600-9000, !8650-8675
```

或者，以下示例显示如何用方括号将端口列表括起来（先前软件版本中要求如此，但现在不再有此要求）：

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

请注意，**必须**用方括号将求反端口列表括起来，如以下示例所示：

```
![20, 22, 23]
```

下表总结了可使用的语法：

表 *102*: 源/目标端口语法

要指定.....	使用	示例
任意端口	`any`	`any`
特定端口	端口号	`80`
端口范围	范围内第一个和最后一个端口号之间使用破折号	`80-443`
所有小于或等于指定端口号的端口	在端口号前面加上破折号	`-21`
所有大于或等于指定端口号的端口	在端口号后面加上破折号	`80-`
除特定端口或端口范围以外的所有端口	要求反的端口、端口列表或端口范围前面的 `!` 字符 请注意，在逻辑上可以对除 any（如果求反，将指示无端口）以外的所有端口指定使用求反。	`!20`
端口变量定义的所有端口	前面带有 `$` 的大写字母形式的变量名称	`$HTTP_PORTS`
除端口变量定义的端口以外的所有端口	前面带有 `!$` 的大写字母形式的变量名称	`!$HTTP_PORTS`

入侵事件详细信息

构建标准文本规则时，可以包含说明规则在攻击尝试中检测到的漏洞的情景信息。也可以在其中纳入对漏洞数据库的外部参考，以及定义入侵事件在贵公司中具有的优先级。这样，如果分析师发现入侵事件，他们可随时获取有关优先级、漏洞和已知缓解措施的信息。

消息

可以指定规则触发时以消息形式显示的有意义的文本。这类消息使您可以即时了解规则检测的漏洞的性质。可以使用除花括号 ({}) 以外的所有可打印标准 ASCII 字符。系统将移除将消息完全引起来的引号。

提示 必须指定规则消息。此外，消息不能只包含空白字符、一个或多个引号、一个或多个撇号或者仅由空白字符、引号或撇号组成的任意组合。

要在入侵规则编辑器中定义事件消息，请在**消息 (Message)** 字段中输入事件消息。

分类

对于每个规则，可以指定事件数据包显示中出现的攻击分类。下表列出了每种分类的名称和编号。

表 *103*：规则分类

编号	分类名称	说明
1	not-suspicious	非可疑流量
2	unknown	未知流量
3	bad-unknown	潜在不良流量
4	attempted-recon	尝试信息泄露
5	successful-recon-limited	信息泄露
6	successful-recon-largescale	大规模信息泄露
7	attempted-dos	尝试拒绝服务
8	successful-dos	拒绝服务
9	attempted-user	尝试获取用户权限
10	unsuccessful-user	未成功获取用户权限
11	successful-user	成功获取用户权限

编号	分类名称	说明
12	attempted-admin	尝试获取管理员权限
13	successful-admin	成功获取管理员权限
14	rpc-portmap-decode	解码 RPC 查询
15	shellcode-detect	检测到可执行代码
16	string-detect	检测到可疑字符串
17	suspicious-filename-detect	检测到可疑文件名
18	suspicious-login	检测到尝试使用可疑用户名的登录
19	system-call-detect	检测到系统调用
20	tcp-connection	检测到 TCP 连接
21	trojan-activity	检测到网络木马
22	unusual-client-port-connection	客户端使用异常端口
23	network-scan	检测网络扫描
24	denial-of-service	检测拒绝服务攻击
25	non-standard-protocol	检测非标准协议或事件
26	protocol-command-decode	通用协议命令解码
27	web-application-activity	访问可能易受攻击的网络应用
28	web-application-attack	网络应用攻击
29	misc-activity	其他活动
30	misc-attack	其他攻击
31	icmp-event	一般 ICMP 事件
32	inappropriate-content	检测到不当内容
33	policy-violation	可能违反公司隐私策略
34	default-login-attempt	尝试使用默认用户名和密码登录

编号	分类名称	说明
35	sdf	敏感数据
36	malware-cnc	已知恶意软件命令和控制流量
37	client-side-exploit	已知客户端攻击尝试
38	file-format	已知的恶意文件或基于文件的攻击

自定义分类

如果您希望事件的数据包显示说明的更多自定义内容由您定义的规则生成，则可以创建自定义分类。

参数	说明
分类名称	分类的名称。如果使用超过40个字符，则页面难以读取。不支持以下字符：`<>()\'"&$;` 以及空格字符。
分类说明 (Classification Description)	分类的说明。可使用字母数字字符和空格。不支持以下字符：`<>()\'"&$;`
优先级	高、中或低。

自定义优先级

默认情况下，规则的优先级来源于其事件分类。但是，可以通过向规则中添加 `priority` 关键字并选择高、中或低优先级来覆盖规则的分类优先级。例如，要为检测 Web 应用攻击的规则分配高优先级，请向该规则中添加 `priority` 关键字，并选择**高 (high)** 作为优先级。

自定义参考

可以使用 `reference` 关键字添加对外部网站以及对关于事件的其他信息的参考。添加参考使分析师可以随时获得所需的资源，从而帮助他们确定数据包触发规则的原因。下表列出了一些可提供关于已知漏洞和攻击的数据的外部系统。

表 *104*：外部攻击识别系统

系统 ID	说明	示例 ID
bugtraq	Bugtraq 页面	8550
cve	通用漏洞与风险页面	CAN-2003-0702
mcafee	McAfee 页面	98574
url	网站参考	www.example.com?exploit=14
msb	Microsoft 安全公告	MS11-082
nessus	Nessus 页面	10039
secure-url	安全网站参考 (https://...)	intranet/exploits/exploit=14 请注意，可以对任何安全网站使用 secure-url。

通过输入参考值指定参考，如下所示：

```
id_system,id
```

其中，id_system 是用作前缀的系统，id 是 Bugtraq ID、CVE 编号、Arachnids ID 或 URL（不包含 http://）。

例如，要指定 Bugtraq ID 17134 中记录的 Microsoft Commerce Server 2002 服务器上的身份验证绕行漏洞，请输入以下值：

```
bugtraq,17134
```

向规则添加参考时应注意以下几点：

- 逗号后不能有空格。
- 系统 ID 不能是大写字母。

添加自定义分类

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域创建的自定义分类，您可以设置这些分类的优先级。系统还会显示在祖先域创建的自定义分类，但您无法设置这些分类的优先级。要查看和编辑在较低域中创建的自定义分类，请切换至该域。

过程

步骤 1 当创建或编辑规则时，请从**分类 (Classification)** 下拉列表中选择**编辑分类 (Edit Classifications)**。如果系统显示**查看分类 (View Classifications)**，则配置属于祖先域，或者您没有修改配置的权限。

步骤 2 输入**分类名称 (Classification Name)** 和**分类说明 (Classification Description)**，如入侵事件详细信息，第 875 页中所述。

步骤 3 从**优先级 (Priority)** 下拉列表中为分类选择优先级。

步骤 4 点击 **Add**。

步骤 5 点击 **Done**。

接下来的操作

- 继续创建或编辑规则。有关详细信息，请参阅编写新规则，第 881 页或修改现有规则，第 882 页。

定义事件优先级

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 当创建或编辑规则时，从**检测选项 (Detection Options)** 下拉列表中选择优先级 (priority)。

步骤 2 点击**添加选项 (Add Option)**。

步骤 3 从**优先级 (priority)** 下拉列表中选择值。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 继续创建或编辑规则。有关详细信息，请参阅编写新规则，第 881 页或修改现有规则，第 882 页。

定义事件引用

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 在创建或编辑规则时，从**检测选项 (Detection Options)** 下拉列表中选择 `reference`。

步骤 2 点击**添加选项 (Add Option)**。

步骤 3 在 **reference** 字段中输入值，如入侵事件详细信息，第 875 页中所述。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 继续创建或编辑规则。有关详细信息，请参阅编写新规则，第 881 页或修改现有规则，第 882 页。

自定义规则创建

您可以通过以下方式创建自定义入侵规则：

- 创建您自己的标准文本规则
- 将现有标准文本规则保存为新规则
- 将系统提供的共享对象规则保存为新规则
- 在多域名部署中，将祖先规则保存为后代域中的新规则
- 导入本地规则文件

无论您使用哪种创建方法，系统都会将自定义规则保存在本地规则类别中。

当您创建自定义入侵规则时，系统会为它分配唯一的规则编号（其格式为 `GID:SID:Rev`）。此编号的元素如下：

GID

生成器 ID。对于所有标准文本规则，此值为 1。对于您保存为新规则的所有共享对象规则，此值为 3。

SID

Snort ID。指示规则是否为系统规则的本地规则。当您创建新规则时，系统会为本地规则分配下一个可用 SID。

本地规则的 Snort ID 号从 1000000 开始，且每个本地新规则的 SID 号以 1 递增。 在多域部署中，系统会在后代域中创建或导入的任何自定义规则的 SID 之前添加一个域编号。例如，在全局域中添加的规则的 SID 可能为 1000000，而在后代域中添加的规则的 SID 可能为 11000000 和 21000000。

Rev

修订号。对于新规则，修订号为 1。每修改一次自定义规则，修订号就增加 1。

在自定义标准文本规则中，可以设置规则报头设置、规则关键字和规则参数。您可以通过规则报头设置将规则设置为仅匹配使用特定协议以及发往或来自特定 IP 地址或端口的流量。

在系统提供的自定义标准文本规则或共享对象规则中，您只能修改规则报头信息，例如，源端口、目标端口、源 IP 地址和目标 IP 地址。您无法修改规则关键字或规则参数。

为共享对象规则修改报头信息并保存更改将会为该规则创建生成器 ID (GID) 为 3 的新实例，并会为自定义规则创建下一个可用 SID。系统将共享对象规则的新实例链接到保留的 `soid` 关键字，该关键字会将创建的规则映射到Cisco Talos 安全情报和研究小组 (Talos)所创建的规则。您可以删除您创建的共享对象规则的实例，但无法删除 Talos 创建的共享对象规则。

编写新规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**入侵规则 (Intrusion Rules)**。
- 选择**对象 (Objects)** > **入侵规则 (Intrusion Rules)**。

步骤 2 点击 **Create Rule**。

步骤 3 在**消息 (Message)** 字段中输入值。

步骤 4 从以下每个下拉列表中选择值：

- **分类**
- **操作**
- **协议**
- **Direction**

步骤 5 在以下字段中输入值：

- **源 IP (Source IPs)**
- **目标 IP**
- **源端口**

- 目标端口

如果没有为这些字段指定值，请系统会使用值 any。

注释　系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 6　从**检测选项 (Detection Options)** 下拉列表中选择值。

步骤 7　点击**添加选项 (Add Option)**。

步骤 8　输入所添加的关键字的任何参数。

步骤 9　或者，重复步骤 6 至步骤 8。

步骤 10　如果添加了多个关键字，则可以执行以下操作：

- 对关键字重新排序 - 点击要移动的关键字旁边的向上或向下箭头。
- 删除关键字 - 点击该关键字旁边的 **X**。

步骤 11　点击**另存为新 (Save as New)**。

接下来的操作

- 在相应的入侵策略中启用新的或已更改的规则；请参阅查看入侵策略中的入侵规则，第818页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

修改现有规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以修改自定义入侵规则。在多域部署中，只能修改属于当前域的自定义入侵规则。

可以将系统提供的规则以及属于祖先域的规则另存为本地规则类别中的新自定义规则，随后可对这些新规则进行修改。

过程

步骤 1　使用以下任一方法访问入侵规则：

- 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**入侵规则 (Intrusion Rules)**。
- 选择**对象 (Objects)** > **入侵规则 (Intrusion Rules)**。

步骤 2　找到要修改的规则。有以下选项可供选择：

- 浏览文件夹以查找规则。
- 搜索规则；请参阅搜索规则，第 885 页。
- 过滤规则所属的组；请参阅过滤规则，第 889 页。

步骤 3 点击规则旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 针对规则类型相应地修改规则。

注释 请勿修改共享对象规则的协议；此修改将会致使规则无效。

步骤 5 有以下选项可供选择：

- 如果编辑的是自定义规则并要覆盖该规则的当前版本，请点击**保存 (Save)**。
- 如果编辑的是系统提供的规则或属于祖先域的任何规则，或者如果编辑的是自定义规则并要将更改另存为新规则，请点击**另存为新项目 (Save As New)**。

接下来的操作

- 如果要使用规则的本地修改而不是系统提供的规则，请通过使用入侵规则状态，第 832 页中的程序停用系统提供的规则并激活本地规则。
- 部署配置更改；请参阅部署配置更改，第 254 页。

将注释添加到入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以向任何入侵规则添加注释。这种注释可有助于提供有关规则及其识别出的漏洞或策略违规的额外情景和信息。

在多域部署中，系统会显示在当前域中创建的注释，您可以对其进行删除。系统还会显示在祖先域中创建的注释，您不可以对其进行删除。要查看在较低域中创建的注释，请切换至该域。

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**入侵规则 (Intrusion Rules)**。

- 选择**对象 (Objects)** > **入侵规则 (Intrusion Rules)**。

步骤 2 找到要添加注释的规则。有以下选项可供选择：

- 浏览文件夹以查找规则。
- 搜索规则；请参阅搜索规则，第 885 页。
- 过滤规则所属的组；请参阅过滤规则，第 889 页。

步骤 3 点击规则旁边的编辑图标 ( )。

如果规则旁边改为显示查看图标 ( )，则表明规则属于祖先策略，或者您没有修改配置的权限。

步骤 4 点击 **Rule Comment**。

步骤 5 在文本框中输入注释。

步骤 6 点击**添加注释 (Add Comment)**。

提示 也可以在入侵事件的数据包视图中添加和查看规则注释。

接下来的操作

- 继续创建或编辑规则。有关详细信息，请参阅编写新规则，第 881 页或修改现有规则，第 882 页。

删除自定义规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以删除当前未在入侵策略中启用的自定义规则。无法删除系统提供的标准文本规则或共享对象规则。在多域部署中，只能删除在当前域中创建的本地规则。

系统将删除的规则存储在删除的类别中，您可以使用删除的规则作为新规则的依据。入侵策略中的 Rules 页面不显示删除的类别，因此您不能启用删除的自定义规则。

提示 自定义规则包括与修改后的报头信息一起保存的共享对象规则。系统还会将这些规则保存在本地规则类别中，并以 3 作为 GID 将它们列出来。您可以删除修改后的共享对象规则版本，但无法删除原始共享对象规则。

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**入侵规则 (Intrusion Rules)**。
- 选择**对象 (Objects)** > **入侵规则 (Intrusion Rules)**。

步骤 2 您有两种选择：

- 删除所有本地规则 - 点击**删除本地规则 (Delete Local Rules)**，然后点击**确定 (OK)**。
- 删除单条规则 - 从**规则分组方法 (Group Rules By)** 下拉列表中选择 `Local Rules`，点击要删除的规则旁边的删除图标 ( )，然后点击**确定 (OK)** 以确认删除。

搜索规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

Firepower 系统提供数千个标准文本规则，并且Cisco Talos 安全情报和研究小组 (Talos) 会在发现新漏洞和攻击时继续添加规则。您可以轻松搜索您想要激活、禁用或编辑的特定规则。

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**入侵规则 (Intrusion Rules)**。
- 选择**对象 (Objects)** > **入侵规则 (Intrusion Rules)**。

步骤 2 点击工具栏上的 **Search**。

步骤 3 添加搜索条件。

步骤 4 点击 **Search**。

接下来的操作

- 如果要查看或编辑找到的规则（或系统规则的副本），请点击超链接规则消息。有关详细信息，请参阅编写新规则，第 881 页或修改现有规则，第 882 页。

入侵规则的搜索条件

下表介绍了可用的搜索选项：

表 *105*：规则搜索条件

选项	说明
Signature ID	要根据 Snort ID (SID) 搜索单个规则，请输入一个 SID 号。要搜索多个规则，请输入以逗号分隔的 SID 号列表。此字段中最多可输入 80 个字符。
Generator ID	要搜索标准文本规则，请选择 **1**。要搜索共享对象规则，请选择 **3**。
消息	要搜索带有特殊消息的规则，请在 **Message** 字段中输入规则消息中的一个字。例如，要搜索 DNS 攻击，可输入 `DNS`；要搜索缓冲区溢出攻击，可输入 `overflow`。
协议	要搜索评估特定协议的流量的规则，请选择该协议。如果不选择协议，搜索结果将包含适用于所有协议的规则。
源端口	要搜索检查来自指定端口的数据包的规则，请输入源端口号或端口相关变量。
目标端口	要搜索检查发往特定端口的数据包的规则，请输入目标端口号或端口相关变量。
源 IP	要搜索检查来自指定 IP 地址的数据包的规则，请输入源 IP 地址或 IP 地址相关变量。
目标 IP	要搜索检查发往指定 IP 地址的数据包的规则，请输入目标 IP 地址或 IP 地址相关变量。
关键字	要搜索特定关键字，可以使用关键字搜索选项。可以选择要搜索的关键字并输入关键字值。也可以在关键字值前面加上感叹号 (!) 以匹配任何未指定的值。
类别	要搜索特定类别中的规则，请从 **Category** 列表中选择该类别。
分类	要搜索具有特定分类的规则，请从 **Classification** 列表中选择该分类名称。
Rule State	要在特定策略和特定规则状态中搜索规则，请从第一个 **Rule State** 列表中选择策略，并从第二个列表中选择状态，以搜索状态设置为 **Generate Events**、**Drop and Generate Events** 或 **Disabled** 的规则。

入侵规则编辑器页面上的规则过滤

您可以对入侵规则编辑器页面上的规则进行过滤以显示其中一组规则。例如，如果想要修改某个规则或更改其状态，但是难以在成千上万个可用规则中找到该规则，这个过滤功能可能很有用。

当您输入过滤器时，页面将显示至少包含一条匹配规则或消息（如果没有匹配规则）的文件夹。

过滤准则

过滤器可以包含特殊关键字及其参数、字符串和用引号引起来的文字字符串，多个过滤器条件之间用空格隔开。过滤器不能包含正则表达式、通配符或任何特殊运算符，例如取反字符 (!)、大于号 (>) 和小于号 (<) 等。

所有关键字、关键字参数和字符串都不区分大小写。除关键字 `gid` 和 `sid` 之外，所有参数和字符串都被视为部分字符串。`gid` 和 `sid` 的参数只会返回完全匹配项。

您可以在未经过滤的原始页面上展开某个文件夹，如果后续过滤器返回该文件夹中的匹配项，该文件夹将会保持展开。这对于在包含大量规则的文件夹中搜索规则可能有用。

不能使用后续过滤器限制任何过滤器。输入的任何过滤器都会搜索整个规则数据库并返回所有匹配的规则。当您在页面仍显示上一过滤器的结果时输入过滤条件，页面将清空，转而返回新过滤器的结果。

您可以对已过滤或未过滤列表中的规则使用相同的功能。例如，可以编辑入侵规则编辑器页面上经过过滤或未经过滤的列表中的规则。您也可以使用该页面上下文菜单中的任何选项。

提示 如果所有子组中的总规则数量很大，过滤所需的时间可能大大增加，因为规则显示在多个类别中，即使唯一规则的总数少很多也是如此。

关键字过滤

每个规则过滤器都可以包含一个或多个关键字，其格式如下：

```
keyword:argument
```

其中，关键字是下表中的其中一个关键字，参数是要在与该关键字相关的一个或多个指定字段中搜索的一个字母数字字符串，不区分大小写。

除 `gid` 和 `sid` 之外的所有关键字的参数都会被视为部分字符串。例如，参数 `123` 将返回 `"12345"`、`"41235"`、`"45123"` 等结果。`gid` 和 `sid` 的参数只会返回完全匹配项；例如，`sid:3080` 只会返回结果 SID 3080。

提示 使用一个或多个字符串来进行过滤可以搜索部分 SID。

下表介绍了可以用于过滤规则的特定过滤关键字和参数。

表 *106*：规则过滤器关键字

关键字	描述	示例
arachnids	根据规则引用中的完整或部分 Arachnids ID 返回一个或多个规则。	arachnids:181
bugtraq	根据规则引用中的完整或部分 Bugtraq ID 返回一个或多个规则。	bugtraq:2120
cve	根据规则引用中的完整或部分 CVE 编号返回一个或多个规则。	cve:2003-0109
gid	参数 1 将返回标准文本规则。参数 3 将返回共享对象规则。	gid:3
mcafee	根据规则引用中的完整或部分 McAfee ID 返回一个或多个规则。	mcafee:10566
msg	根据规则的完整或部分 Message 字段（又称为事件消息）返回一个或多个规则。	msg:chat
nessus	根据规则引用中的完整或部分 Nessus ID 返回一个或多个规则。	nessus:10737
ref	根据规则引用或规则 Message 字段中一个完整的字母数字字符串或其一部分返回一个或多个规则。	ref:MS03-039
sid	返回带有完全匹配的 Snort ID 的规则。	sid:235
url	根据规则引用中的完整或部分 URL 返回一个或多个规则。	url:faqs.org

字符串过滤

每个规则过滤器可以包含一个或多个字母数字字符串。字符串将搜索规则的**消息 (Message)** 字段、Snort ID (SID) 和生成器 ID (GID)。例如，字符串 `123` 会返回规则消息中的 `"Lotus123"`、`"123mania"` 等字符串，也会返回 SID 6123、SID 12375 等。

所有字符串都不区分大小写并被视为部分字符串。例如，`ADMIN`、`admin` 或 `Admin` 等字符串中任意一个都会返回 `"admin"`、`"CFADMIN"`、`"Administrator"` 等结果。

用引号将字符串引起来可以返回完全匹配项。例如，用引号引起来的原义字符串 `"overflow attempt"` 只会返回完全匹配的该字符串，而由 `overflow` 和 `attempt` 这两个字符串组成的未加引号的过滤器则会返回 `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` 等结果。

组合关键字和字符串过滤

输入关键字、文字字符串或这二者的任意组合并以空格分隔可以缩小过滤结果的范围。结果包括符合所有过滤条件的任意规则。

可以按照任意顺序输入多个过滤条件。例如，以下每个过滤器返回的规则相同：

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

过滤规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在“入侵规则”(Intrusion Rules) 页面上，可以将规则过滤为子集，以便可以更轻松地查找特定规则。然后，可以使用任何页面功能，包括选择情景菜单中可用的任何功能。

规则过滤尤其适用于查找要编辑的特定规则。

过程

步骤 1 使用以下任一方法访问入侵规则：

- 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**入侵规则 (Intrusion Rules)**。
- 选择**对象 (Objects)** > **入侵规则 (Intrusion Rules)**。

步骤 2 在过滤之前，您有以下选择：

- 展开要展开的任何规则组。某些规则组还具有可展开的子组。
  如果您预计规则可能在某个组中，则在未经过滤的原始页面上展开该组可能有用。如果后续过滤器返回该文件夹中的匹配项，当您点击过滤器清除图标 ( ) 返回到未经过滤的原始页面时，该组将会保持展开。
- 从**规则分组方法 (Group Rules By)** 下拉列表中选择其他分组方法。

步骤 3 在**规则分组方法 (Group Rules By)** 列表下的过滤器图标 ( ) 旁边的文本框中输入过滤器限制。

步骤 4 按下 Enter 键。

注释 通过点击过滤器清除图标 ( ) 清除当前已过滤的列表。

入侵规则中的关键字和参数

借助规则语言，可以通过组合关键字来指定规则行为。关键字及其相关值（称为参数）规定系统如何评估规则引擎测试的数据包和数据包相关值。Firepower 系统当前支持允许您执行检查功能（例如内容匹配、协议特定模式匹配和状态特定匹配）的关键字。在每个关键字中最多可以定义 100 个参数，还可以组合任意数量的兼容关键字来创建非常具体的规则。这有助于降低出现误报和漏报的可能性，使您可以重点关注接收到的入侵信息。

请注意，您也可以在被动部署中使用自适应配置文件，以根据规则元数据和主机信息动态调整对特定数据包的主动规则处理。

本节所述的关键字列于规则编辑器中的“检测选项”(Detection Options) 下。

content 和 protected_content 关键字

使用 `content` 关键字或 `protected_content` 关键字可以指定要在数据包中检测的内容。

大多数情况下，应始终在 `content` 或 `protected_content` 关键字后面加上修饰符，指示对内容进行搜索的位置、搜索是否区分大小写及其他选项。

请注意，要使规则触发事件，所有内容匹配必须为真，也就是说，每项内容匹配与其他匹配之间都存在 AND 关系。

另请注意，在内联部署中，可以将规则设置为匹配恶意内容并将其更换为您自定义的等长文本字符串。

content

当使用 `content` 关键字时，规则引擎在数据包负载或数据流中搜索该字符串。例如，如果输入 `/bin/sh` 作为其中一个 `content` 关键字的值，则规则引擎会在数据包负载中搜索字符串 `/bin/sh`。

可以使用 ASCII 字符串、十六进制内容（二进制字节代码）或这两者的组合来匹配内容。可以在关键字值中将十六进制内容放在两条竖线 (|) 之间。例如，可以混合使用十六进制内容和 ASCII 内容，例如，`|90C8 C0FF FFFF|/bin/sh`。

可以在一个规则中指定多项内容匹配。要这样做，请使用 `content` 关键字的其他实例。对于各项内容匹配，可以指明必须在数据包负载或数据流中发现内容匹配才可触发规则。

注意 如果创建的规则只包含一个 `content` 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。

protected_content

`protected_content` 关键字使您可以在配置规则参数前对搜索内容字符串进行编码。原始规则作者在配置关键字前使用哈希函数（SHA-512、SHA-256 或 MD5）对字符串进行编码。

如果使用 protected_content 关键字而不使用 content 关键字，规则引擎在数据包负载或数据流中搜索字符串的方式并不会改变，且大多数关键字选项将起到预期作用。下表总结了 protected_content 关键字选项与 content 关键字选项存在差异的例外情况。

表 *107*：*protected_content* 选项例外

选项	说明
Hash Type	protected_content 规则关键字的新增选项。
区分大小写	不支持
Within	不支持
深度	不支持
长度	protected_content 规则关键字的新增选项。
Use Fast Pattern Matcher	不支持
Fast Pattern Matcher Only	不支持
Fast Pattern Matcher Offset and Length	不支持

思科建议在包含 protected_content 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。在规则中，content 关键字应置于 protected_content 关键字之前。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 Use Fast Pattern Matcher 参数，规则引擎都会使用快速模式匹配程序。

注意 如果创建的规则只包含一个 protected_content 关键字，但没有为该关键字选择 **Not** 选项，可能会使入侵策略无效。

基本 content 和 protected_content 关键字参数

可以通过修饰 content 或 protected_content 关键字的参数来限制内容搜索的位置以及大小写。配置用于修饰 content 或 protected_content 关键字的选项可以指定要搜索的内容。

区分大小写

注释 配置 protected_content 关键字时**不**支持此选项。

可以指示规则引擎在搜索 ASCII 字符串内容匹配时忽略大小写。要使搜索不区分大小写，请在指定内容搜索时选择 **Case Insensitive**。

Hash Type

注释 此选项仅对于 protected_content 关键字可配置。

使用 **Hash Type** 下拉列表确定用于编码搜索字符串的哈希函数。系统支持对 protected_content 搜索字符串进行 SHA-512、SHA-256 和 MD5 哈希处理。如果哈希内容的长度与所选的哈希类型不匹配，系统将不会保存规则。

系统自动选择思科设置的默认值。如果选择了 **Default**，将不会向规则写入特定哈希函数，且系统将假设 SHA-512 为哈希函数。

Raw Data

Raw Data 选项指示规则引擎在分析规范化负载数据（由网络分析策略解码）之前分析原始数据包负载，并且此选项不使用参数值。进行规范化之前，可以在分析 telnet 流量时使用此关键字在负载中检查 telnet 协商选项。

不能在同一 content 或 protected_content 关键字中同时使用**原始数据 (Raw Data)** 选项和任何 HTTP 内容选项。

提示 可以配置 HTTP 检查预处理器 **Client Flow Depth** 和 **Server Flow Depth** 选项，以确定是否在 HTTP 流量中检查原始数据以及检查的原始数据量。

不

选择 **Not** 选项可搜索与指定内容不匹配的内容。如果创建包含选择了**不匹配 (Not)** 选项的 content 或 protected_content 关键字的规则，还必须在该规则中至少包含一个未选择**不匹配 (Not)** 选项的其他 content 或 protected_content 关键字。

注意 请勿创建仅包含一个 content 或 protected_content 关键字的规则（如果该关键字已选择**不匹配 [Not]** 选项）。否则，可能会使入侵策略无效。

例如，SMTP 规则 1:2541:9 包含三个 content 关键字，其中一个选择了 **Not** 选项。如果移除除选择了 **Not** 选项的关键字以外的其他 content 关键字，基于该规则的自定义规则将无效。将该规则添加到入侵策略将导致策略失效。

提示 不能对同一个 content 关键字同时选择 **Not** 复选框和 **Use Fast Pattern Matcher** 复选框。

content 和 protected_content 关键字搜索位置

可以使用搜索位置选项指定开始搜索指定内容的位置以及继续搜索的深度。

允许的组合：*content* 搜索位置参数

可以使用两个 `content` 位置对指定开始搜索指定内容的位置以及继续搜索的深度，如下所述：

- 同时使用 **Offset** 和 **Depth** 选项可相对于数据包负载起点进行搜索。
- 同时使用 **Distance** 和 **Within** 可相对于当前搜索位置进行搜索。

如果仅指定选项对中的其中一个选项，系统将会假设另一个选项使用默认值。

不能将**偏移量 (Offset)** 和**深度 (Depth)** 选项与**距离 (Distance)** 和**范围内 (Within)** 选项混合使用。例如，不能将 **Offset** 和 **Within** 这两个选项配对。可以在规则中使用任意数量的位置选项。

如果未指定位置，系统将假设 **Offset** 和 **Depth** 选项为默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 `byte_extract` 变量指定位置选项的值。

提示 可以在规则中使用任意数量的位置选项。

允许的组合：*protected_content* 搜索位置参数

将必填的**长度 (Length)**`protected_content` 位置选项与**偏移 (Offset)** 或**距离 (Distance)** 位置选项结合使用，可指定开始搜索指定内容的位置以及继续搜索的深度，如下所示：

- 同时使用 **Length** 和 **Offset** 选项可相对于数据包负载起点搜索受保护字符串。
- 同时使用 **Length** 和 **Distance** 选项可相对于当前搜索位置搜索受保护字符串。

提示 不能在单个关键字配置中同时使用 **Offset** 和 **Distance** 选项，但可以在规则内使用任意数量的位置选项。

如果未指定位置，系统将假设使用默认值；也就是说，将从数据包负载起点开始进行内容搜索，直至数据包终点。

还可以使用现有 `byte_extract` 变量指定位置选项的值。

content 和 *protected_content* 搜索位置参数

深度

注释 此选项**仅**在配置 `content` 关键字时可用。

指定最大内容搜索深度（以字节为单位），从偏移量值起点开始计算，如果没有配置偏移量，则从数据包负载起点开始计算。

例如，如果规则的内容值为 `cgi-bin/phf`，`offset` 值为 `3`，`depth` 值为 `22`，规则将从字节 3 开始搜索 `cgi-bin/phf` 字符串内容匹配，并在处理完符合规则报头指定参数的数据包中的 22 个字节（字节 25）后停止。

必须指定一个大于或等于指定内容长度的数值，最多 65535 字节。不能指定值 0。

默认深度是搜索至数据包终点。

距离

指示规则引擎识别在上一次成功内容匹配后出现指定数量字节的后续内容匹配。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从上一次成功内容匹配开始继续搜索。例如，如果指定 4，搜索将从第五个字节开始。

可指定 -65535 到 65535 字节之间的值。如果在 `Distance` 中指定负值，开始搜索的字节可能位于数据包开头以外。所有计算都会将数据包以外的字节考虑在内，尽管搜索实际上从数据包的第一个字节开始。例如，如果数据包当前位置是第五个字节，下一个内容规则选项指定 `Distance` 值为 -10，`Within` 值为20，搜索将从负载起点开始，且 `Within` 选项将调整为 15。

默认距离是 0，表示继上一次内容匹配之后数据包中的当前位置。

长度

注释 此选项**仅**在配置 `protected_content` 关键字时可用。

长度 (Length)`protected_content` 关键字选项表示非散列搜索字符串的长度（以字节为单位）。

例如，如果使用了内容 `Sample1` 生成安全哈希，请将 **Length** 值设置为 `7`。**必须**在该字段中输入一个值。

Offset

指定数据包负载中开始内容搜索的位置与数据包负载起点之间的距离（以字节为单位）。可指定 65535 到 65535 字节之间的值。

由于偏移量计数器从字节 0 开始计算，因此，应指定比所需字节数小 1 的值，以便从数据包负载起点开始继续搜索。例如，如果指定 7，搜索将从第八个字节开始。

默认偏移量是 0，表示数据包起点。

Within

注释 此选项**仅**在配置 `content` 关键字时可用。

Within 选项指明，要触发规则，下一次内容匹配必须发生在上一次成功内容匹配结束之后指定数量的字节内。例如，如果将 **Within** 值指定为 `8`，下一次内容匹配必须出现在数据包负载中接下来的八个字节之内，否则将无法满足触发规则的条件。

可以指定一个大于或等于指定内容长度的数值，最多 65535 字节。

Within 的默认设置是搜索至数据包终点。

概述：HTTP content 和 protected_content 关键字参数

通过 HTTP `content` 或 `protected_content` 关键字选项，可以在 HTTP 检查预处理器解码的 HTTP 消息中指定搜索内容匹配项的位置。

以下两个选项搜索 HTTP 响应中的状态字段：

- **HTTP Status Code**
- **HTTP Status Message**

请注意，尽管规则引擎搜索未规范化的原始状态字段，但这里分别列出这些选项，以方便在下文解释将其他原始 HTTP 字段与规范化 HTTP 字段结合使用时应考虑的限制。

以下五个选项根据情况搜索 HTTP 请求和/或响应中的规范化字段：

- **HTTP URI**
- **HTTP 方法**
- **HTTP Header**
- **HTTP Cookie**
- **HTTP Client Body**

以下三个选项根据情况搜索 HTTP 请求和/或响应中的原始（未规范化）非状态字段：

- **HTTP Raw URI**
- **HTTP Raw Header**
- **HTTP Raw Cookie**

选择 HTTP `content` 选项时，请遵循以下准则：

- HTTP `content` 选项仅适用于 TCP 流量。
- 为避免对性能造成负面影响，应只选择消息中那些可能出现指定内容的部分。

  例如，如果流量可能包含大型 cookie（例如，购物车消息中的 cookie），可以在 HTTP 报头中搜索指定内容，而不是在 HTTP cookie 中搜索。

- 为利用 HTTP 检查预处理器规范化以及提高性能，所创建的任何 HTTP 相关规则应包含至少一个已选择 **HTTP URI**、**HTTP Method**、**HTTP Header** 或 **HTTP Client Body** 选项的 `content` 或 `protected_content` 关键字。
- 不能将 `replace` 关键字与 HTTP `content` 或 `protected_content` 关键字选项配合使用。

可以指定单个规范化 HTTP 选项或状态字段，或者使用规范化 HTTP 选项与状态字段的任意组合，以指向要匹配的内容区域。但在使用 HTTP 字段选项时，请注意以下限制：

- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用 **Raw Data** 选项和任何 HTTP 选项。

- 不能在同一个 `content` 或 `protected_content` 关键字中同时使用原始 HTTP 字段选项（**HTTP Raw URI**、**HTTP Raw Header** 或 **HTTP Raw Cookie**）及其对应的规范化选项（分别是 **HTTP URI**、**HTTP Header** 或 **HTTP Cookie**）。
- 不同同时选择 **Use Fast Pattern Matcher** 和以下一个或多个 HTTP 字段选项：

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message** 或 **HTTP Status Code**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 `content` 或 `protected_content` 关键字中包含上述选项：

  HTTP URI、**HTTP Header** 或 **HTTP Client Body**

  例如，如果选择 **HTTP Cookie**、**HTTP Header** 和 **Use Fast Pattern Matcher**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。

- 将受限选项和不受限选项结合使用时，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将规则传递到入侵规则编辑器来完成评估，包括受限字段的评估。

HTTP content 和 *protected_content* 关键字参数

HTTP URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。

注释 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，则规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP Raw URI

选择此选项将会在规范化的请求 URI 字段中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP URI (U) 选项结合使用来搜索相同的内容。

注释 管道化 HTTP 请求数据包包含多个 URI。如果选择了 **HTTP URI**，且规则引擎检测到管道化 HTTP 请求数据包，规则引擎将会搜索数据包中的所有 URI 以进行内容匹配。

HTTP 方法

选择此选项将会在请求方法字段中搜索内容匹配，该字段确定要对 URI 中识别出的资源执行的操作（例如 GET 和 POST）。

HTTP Header

选择此选项将会在 HTTP 请求内的规范化报头字段（cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 报头 (H) 选项结合使用来搜索相同的内容。

HTTP Raw Header

选择此选项将会在 HTTP 请求内的原始报头字段（cookie 除外）中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应中搜索内容匹配。

请注意，不能将此选项与 `pcre` 关键字 HTTP 原始报头 (D) 选项结合使用来搜索相同的内容。

HTTP Cookie

选择此选项将会在规范化 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配。请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。

请注意：

- 不能将此选项与 `pcre` 关键字 HTTP cookie (C) 选项结合使用来搜索相同的内容。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Raw Cookie

选择此选项将会在原始 HTTP 客户端请求报头内识别出的任何 cookie 中搜索内容匹配；如果 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项已启用，还会在响应 set-cookie 数据中搜索内容匹配；请注意，系统将消息正文中包含的 cookie 看作正文内容。

若要仅对 cookie 进行内容匹配搜索，必须启用 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项；否则，规则引擎将搜索包括 cookie 在内的整个报头。

请注意：

- 不能将此选项与 `pcre` 关键字 HTTP 原始 cookie (K) 选项结合使用来搜索相同的内容。
- `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

HTTP Client Body

选择此选项将会在 HTTP 客户端请求消息正文中搜索内容匹配。

请注意，要使此选项起作用，必须为 HTTP 检查预处理器的 **HTTP Client Body Extraction Depth** 选项指定一个 0 到 65535 之间的值。

HTTP Status Code

选择此选项将会在 HTTP 响应的三位数状态代码中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项。

HTTP Status Message

选择此选项将会在 HTTP 响应中状态代码随附的文字描述中搜索内容匹配。

要使此选项能够返回匹配，必须启用 HTTP 检查预处理器的 **Inspect HTTP Responses** 选项。

概述：content 关键字快速模式匹配程序

注释 配置 `protected_content` 关键字时，这些选项不可用。

快速模式匹配程序快速确定在将数据包传递到规则引擎之前要对哪些规则进行评估。这项初步工作可大大减少用于数据包评估的规则数量，从而提高性能。

默认情况下，快速模式匹配程序会在数据包内搜索规则中指定的最长内容；这样可最大程度地消除不必要的规则评估。以如下规则片段为例：

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

几乎所有 HTTP 客户端请求都包含内容 `GET`，但是很少会包含内容 `/exploit.cgi`。使用 `GET` 作为快速模式内容将会导致规则引擎在大多数情况下评估此规则，但极少会产生匹配。但是，对于大多数客户端 `GET` 请求，将不会使用 `/exploit.cgi` 对其进行评估，从而提高性能。

规则引擎仅在快速模式匹配程序检测到指定内容时根据规则评估数据包。例如，如果某个规则中的三个 `content` 关键字分别指定内容 `short`、`longer` 和 `longest`，快速模式匹配程序将使用内容 `longest`，并且仅在规则引擎在负载中找到 `longest` 的情况下对该规则进行评估。

content 关键字快速模式匹配程序参数

Use Fast Pattern Matcher

使用此选项可指定较短的搜索模式以供快速模式匹配程序使用。理想情况下，指定的模式在数据包中被找到的可能性低于最长模式，因此，因此能够更具体地识别所针对的漏洞。

在同一个 `content` 关键字中选择 **Use Fast Pattern Matcher** 和其他选项时，请注意以下限制：

- 只能为每个规则指定一次 **Use Fast Pattern Matcher**。
- 如果同时选择 **Use Fast Pattern Matcher** 和 **Not**，将不能使用 **Distance**、**Within**、**Offset** 和 **Depth**。
- 不同同时选择 Use Fast Pattern Matcher 和以下任何 HTTP 字段选项：

  HTTP Raw URI、**HTTP Raw Header**、**HTTP Raw Cookie**、**HTTP Cookie**、**HTTP Method**、**HTTP Status Message** 或 **HTTP Status Code**

  但是，可以在也使用快速模式匹配程序搜索以下其中一个规范化字段的 `content` 关键字中包含上述选项：

  HTTP URI、**HTTP Header** 或 **HTTP Client Body**

例如，如果选择 **HTTP Cookie**、**HTTP Header** 和 **Use Fast Pattern Matcher**，规则引擎将会在 HTTP cookie 和 HTTP 报头中搜索内容，但快速模式匹配程序仅适用于 HTTP 报头，而不适用于 HTTP cookie。

请注意，不能在同一个 `content` 关键字中同时使用原始 HTTP 字段选项（**HTTP Raw URI**、**HTTP Raw Header** 或 **HTTP Raw Cookie**）和对应的规范化选项（分别是 **HTTP URI**、**HTTP Header** 或 **HTTP Cookie**）。

如果将受限选项和不受限选项结合使用，快速模式匹配程序将仅搜索您指定的不受限字段，以测试是否要将数据包传递到规则引擎以完成评估（包括受限字段的评估）。

- 或者，如果选择 **Use Fast Pattern Matcher**，还可以选择 **Fast Pattern Matcher Only** 或 **Fast Pattern Matcher Offset and Length** 选项，但不能同时选择这两个选项。
- 检测 Base64 数据时，不能使用快速模式匹配程序。

Fast Pattern Matcher Only

通过此选项，您可以将 `content` 关键字仅用作快速模式匹配程序选项，而不用作规则选项。如果无需规则引擎评估指定的内容，可以使用此选项来节省资源。例如，假设规则仅要求内容 `12345` 位于负载中的任何位置。如果快速模式匹配程序检测到该模式，可根据规则中的其他关键字对数据包进行评估。规则引擎无需重新评估数据包来确定其是否包含模式 `12345`。

如果规则包含其他与指定内容相关的状况，无需使用此选项。例如，如果另一个规则条件尝试确定 `abcd` 是否出现在 `1234` 之前，将无需使用此项选项搜索内容 `1234`。在这种情况下，规则引擎无法确定相对位置，因为选择 **Fast Pattern Matcher Only** 将会指示规则引擎不搜索指定内容。

使用此选项时请注意：

- 指定的内容与位置无关，也就是说，该内容可出现在负载中的任何位置；因此，不能使用位置选项（**Distance**、**Within**、**Offset**、**Depth** 或 **Fast Pattern Matcher Offset and Length**）。
- 不能将此选项与 **Not** 结合使用。
- 不能将此选项与 **Fast Pattern Matcher Offset and Length** 结合使用。
- 指定的内容将被视为不区分大小写，因为所有模式均以不区分大小写的方式插入到快速模式匹配程序中；系统会自动处理这种情况，因此您无需在选择此选项时选择 **Case Insensitive**。
- 不应在使用**仅快速模式匹配程序 (Fast Pattern Matcher Only)** 选项的 `content` 关键字后紧跟以下关键字（这些关键字设置相对于当前搜索位置的搜索位置）：

  `isdataat`

  `pcre`

  `content`（在选择了 **Distance** 或 **Within** 的情况下）

  `content`（在选择了 **HTTP URI** 的情况下）

  `asn1`

  `byte_jump`

  `byte_test`

byte_extract

base64_decode

Fast Pattern Matcher Offset and Length

使用 **Fast Pattern Matcher Offset and Length** 选项可指定要搜索的部分内容。如果模式很长，且只需模式的一部分即足以识别出可能是匹配的规则，使用此选项可减少内存消耗。如果快速模式匹配程序选择了某个规则，将会根据该规则评估整个模式。

可以确定快速模式匹配程序要使用的部分，方法是，使用以下语法以字节为单位指定搜索的开始位置（偏移量）以及搜索内容的深入度（长度）：

```
offset,length
```

例如，对于以下内容：

```
1234567
```

如果如下指定偏移量和长度字节数：

```
1,5
```

快速模式匹配程序仅搜索内容 `23456`。

请注意，不能将此选项与 **Fast Pattern Matcher Only** 结合使用。

replace 关键字

可以在内嵌部署中使用 `replace` 关键字替换指定内容。

注释 不能使用 `replace` 关键字替换思科 SSL 设备检测到的 SSL 流量中的内容。将会传输原始加密数据而非替代数据。有关详细信息，请参阅《思科 *SSL* 设备管理和部署指南》。

要使用 `replace` 关键字，请构建一个使用 `content` 关键字来查找特定字符串的自定义标准文本规则。然后使用 `replace` 关键字指定一个字符串，以替换该内容。替代值和内容值必须是相同长度的字符串。

注释 不能使用 `replace` 关键字替换 `protected_content` 关键字中的哈希内容。

或者，可以用引号将替代字符串引起来，以便向后兼容以前的 Firepower 系统 软件版本。如果不加引号，替代字符串将被自动添加到规则，以使规则在语法上正确。要将前引号或后引号纳入为替代文本的一部分，必须使用反斜杠对引号进行转义，如以下示例所示：

```
"replacement text plus \"quotation\" marks""
```

每个规则可包含多个 `replace` 关键字，但只能包含一个 `content` 关键字。只会替换规则找到的内容中的第一个实例。

下面介绍 `replace` 关键字的使用示例：

- 如果系统检测到传入数据包包含漏洞，您可以使用一个无害字符串来替换该恶意字符串。有时，这种方法比单纯地丢弃违规数据包更有效。在某些攻击场景中，攻击者只需重新发送被丢弃的数据包，直至该数据包绕过网络防御或对网络造成泛洪攻击。通过将一个字符串替换为另一个字符串（而非丢弃数据包），可以令攻击者相信其攻击的目标并非易受攻击。
- 如果您担心侦察攻击，这类攻击试图了解是您否正在运行易受攻击版本的设备（例如，网络服务器），则您可以检测传出数据包，并将横幅替换为自己的文本。

注释 请确保在要其中使用替换规则的内联入侵规则中将规则状态设置为 Generate Events；如果将规则设置为 Drop and Generate events，将会导致数据包被丢弃，进而造成无法替换内容。

在字符串替换过程中，该系统会自动更新数据包校验和，以使目标主机可以毫无差错地接收数据包。

请注意，不能将 `replace` 关键字与 HTTP 请求消息的 `content` 关键字选项结合使用。

byte_jump 关键字

`byte_jump` 关键字首先计算指定字节段中定义的字节数，然后在数据包中跳过该数量的字节 - 可以从指定字节段的末尾向前跳，也可以从数据包负载起点向前跳，还可以从与上一次内容匹配有关的点向前跳，具体取决于指定的选项。这对于具有如下特点的数据包很有用：数据包中的特定字节段描述数据包所包含的变量数据。

下表介绍了 `byte_jump` 关键字所需的参数。

表 *108*：所需的 *byte_jump* 参数

参数	说明
字节	要从数据包采集的字节数量。 如果不与 DCE/RPC 一起使用，则允许的值为 1 - 10 ，具有以下限制： • • 如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。） 如果与 DCE/RPC 一起使用，则允许的值为 1、2 和 4。
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 `offset` 值：用从数据包负载起点或上一次成功内容匹配起向前跳所需的字节数减去 1。 可指定 -65535 到 65535 字节。 您也可以使用现有 `byte_extract` 变量指定此参数的值。

下表介绍了可用于定义系统如何解释您为必需参数指定的值的选项。

表 *109*：其他可选 *byte_jump* 参数

参数	说明
Relative	使偏移量相对于上一次成功内容匹配中找到的上一个模式。
Align	将转换的字节数四舍五入为下一个 32 位边界。
倍数	指明规则引擎应将其与从数据包获取的 `byte_jump` 值相乘的值，以获得最终的 `byte_jump` 值。 也就是说，规则引擎跳过一个与您通过 Multiplier 参数指定的整数相乘的字节数，而不是跳过指定字节段中定义的字节数。
Post Jump Offset	应用其他 `byte_jump` 参数后要向前跳或向后跳的字节数（-65535 到 65535）。选择正值将会向前跳，选择负值将会向后跳。将此字段留空或输入 `0` 将会禁用此字段。 请注意，选择 **DCE/RPC** 参数时，一些 `byte_jump` 参数不适用。
From Beginning	指明规则引擎应从数据包负载起点开始跳过负载中指定的字节数，而不是从数据包的当前位置开始跳。

只能指定 **DCE/RPC**、**Endian** 或 **Number Type**。

如果要定义 `byte_jump` 关键字如何计算字节数，则可以选择下表中介绍的参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *110*：字节排序 *byte_jump* 参数

参数	说明
Big Endian	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 `byte_jump` 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 `byte_jump` 与其他特定 DCE/RPC 关键字结合使用。

使用下表所列的其中一个参数来定义系统如何查看数据包中的字符串。

表 *111*：数字类型参数

参数	说明
Hexadecimal String	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下设置 `byte_jump` 的值：

- Bytes = 4
- Offset = 12
- Relative 已启用
- Align 已启用

规则引擎将会计算自上一次成功内容匹配后显示的 13 个字节当中 4 个字节中描述的数量，并向前跳过数据包中该数量的字节。例如，如果特定数据包中计算出的 4 个字节是 `00 00 00 1F`，规则引擎会将它转换为 31。由于指定了 `align`（指示引擎移到下一个 32 位边界），因此，规则引擎将在数据包中向前跳过 32 个字节。

或者，如果如下设置 `byte_jump` 的值：

- Bytes = 4
- Offset = 12
- From Beginning 已启用
- Multiplier = 2

规则引擎将会计算在数据包起点后显示的 13 个字节当中 4 个字节中描述的数值。然后，引擎会将该数值乘以 2，以获得将要跳过的字节总数。例如，如果特定数据包中计算出的 4 个字节是 `00 00 00 1F`，规则引擎会将它转换为 31，然后再乘以 2 以得到 62。由于启用了 From Beginning，因此，规则引擎会跳过数据包中的前 63 个字节。

byte_test 关键字

`byte_test` 关键字根据 Value 参数及其运算符测试指定的字节段。

下表介绍了 `byte_test` 关键字所需的参数。

表 *112*：所需的 *byte_test* 参数

参数	说明
字节	从数据包进行计算的字节数。 如果不与 DCE/RPC 配合使用，则允许的值为 1 到 10。但是，如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。） 如果与 DCE/RPC 一起使用，则允许的值为 1、2 和 4。
值	要测试的值，包括其运算符。 支持的运算符：<、>、=、!、&、^、!>、!<、!=、!& 或 !^。 例如，如果指定 `!1024`，`byte_test` 将会转换该指定数字，且如果该数字不等于 1024，则会生成事件（如果其他所有关键字参数都匹配）。 请注意，! 和 != 等效。 您也可以使用现有 `byte_extract` 变量指定此参数的值。
Offset	从负载开头到开始进行处理之间的字节数。偏移量计数器从字节 0 开始计数，因此，应该如下计算 `offset` 值：用从数据包负载起点或上一次成功内容匹配起向前计算所需的字节数减去 1。 可以使用现有 `byte_extract` 变量指定此参数的值。

可以用下表中所述的参数进一步定义系统如何使用 `byte_test` 参数。

表 *113*：其他可选 *byte_test* 参数

参数	说明
Relative	使偏移量相对于上一次成功模式匹配。

只能指定 **DCE/RPC**、**Endian** 或 **Number Type**。

要定义 `byte_test` 关键字如何计算其测试的字节，请从下表中选择参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *114*：字节排序 *byte_test* 参数

参数	说明
Big Endian	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据

参数	说明
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 `byte_test` 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 `byte_test` 与其他特定 DCE/RPC 关键字结合使用。

可以使用下表所列的其中一个参数来定义系统如何在数据包中查看字符串。

表 *115*：数字类型 *byte-test* 参数

参数	说明
Hexadecimal String	使用十六进制格式表示转换的字符串数据。
Decimal String	使用十进制格式表示转换的字符串数据。
Octal String	使用八进制格式表示转换的字符串数据。

例如，如果如下指定 `byte_test` 的值：

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative 已启用

规则引擎计算距离（相对于）上一个成功的内容匹配项 9 个字节的 4 个字节中描述的数值，如果计算的数值大于 128 字节，则会触发规则。

byte_extract 关键字

可以使用 `byte_extract` 关键字将数据包中指定数量的字节读取到某个变量中。然后，可以在同一规则中使用该变量作为某些其他检测关键字中特定参数的值。

此参数很有用，例如，可用于从其中的特定字节段描述数据包数据所包含的字节数的数据包提取数据大小。例如，特定字节段可能指出后续数据是由 4 个字节组成；您可以提取 4 个字节的数据大小来作为变量值。

可以使用 `byte_extract` 在规则中最多同时创建两个独立的变量。可以任意多次地重新定义 `byte_extract` 变量；如果输入变量名称相同但变量定义不同的新的 `byte_extract` 关键字，将会覆盖该变量的上一个定义。

下表介绍了 `byte_extract` 关键字所需的参数。

表 *116*：所需的 *byte_extract* 参数

参数	说明
Bytes to Extract	要从数据包采集的字节数量。 如果指定除 1、2 或 4 以外的字节数，则必须指定数字类型（十六进制、八进制或十进制。）
Offset	从负载开头到开始提取数据之间的字节数。可指定 -65535 到 65535 字节。偏移量计数器从字节 0 开始计数，因此，计算偏移量值时，应该用向前计算所需的字节数减去 1。例如，指定 7 将会从 8 字节开始向前计算。规则引擎会从数据包负载起点开始向前计算；如果还指定了 **Relative**，规则引擎会从上一次成功内容匹配起向前计算。请注意，如果还指定了 **Relative**，则只能指定负数。
Variable Name	用于其他检测关键字的参数中的变量名称。可以指定以字母开头的字母数字字符串。

要进一步定义系统如何查找要提取的数据，可以使用下表中所述的参数。

表 *117*：其他可选的 *byte_extract* 参数

参数	说明
倍数	从数据包提取的值的乘数。可指定 0 到 65535 之间的任意数字。如果未指定乘数，将会默认设置为 1。
Align	将提取的数值四舍五入为最接近的 2 字节或 4 字节边界。如果选择了 **Multiplier**，系统会在进行舍入之前应用该乘数。
Relative	使**偏移量**相对于上一次成功内容匹配的结尾而不是负载起点。

只能指定 **DCE/RPC**、**Endian** 或 **Number Type**。

要定义 `byte_extract` 关键字如何计算其测试的字节，可以从下表中选择参数。如果未选择字节排序参数，规则引擎使用大端字节顺序。

表 *118*：字节排序 *byte_extract* 参数

参数	说明
Big Endian	按大端字节顺序处理数据（大端字节顺序是默认的网络字节顺序）。
Little Endian	按小端字节顺序处理数据

参数	说明
DCE/RPC	指定 DCE/RPC 预处理器处理的流量的 `byte_extract` 关键字。 由 DCE/RPC 预处理器确定大端字节顺序或小端字节顺序，**Number Type** 和 **Endian** 参数不适用。 如果启用此参数，还可以将 `byte_extract` 与其他特定 DCE/RPC 关键字结合使用。

可以指定数字类型来将数据读取为 ASCII 字符串。要定义系统如何在数据包中查看字符串，可选择下表中所述的其中一个参数。

表 *119*：数字类型 *byte_extract* 参数

参数	说明
Hexadecimal String	以十六进制格式读取提取的字符串数据。
Decimal String	以十进制格式读取提取的字符串数据。
Octal String	以八进制格式读取提取的字符串数据。

例如，如果如下指定 `byte_extract` 的值：

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative 已启用

那么，规则引擎将会距离（相对于）上一次成功内容匹配 9 字节的四个字节中描述的数字读取到名为 `var` 的变量中（然后，您可以将该数字指定为某些关键字参数的值）。

下表列出了可以在其中指定 `byte_extract` 关键字中定义的变量的关键字参数。

表 *120*：接受 *byte_extract* 变量的参数

关键字	参数
content	Depth、Offset、Distance、Within
byte_jump	Offset
byte_test	Offset、Value
isdataat	Offset

概述：pcre 关键字

pcre 关键字使您可以使用兼容 Perl 的正则表达式 (PCRE) 为指定的内容检查数据包负载。使用 PCRE 可避免编写以匹配相同内容的细微变化为目的的多个规则。

搜索可以多种方式显示的内容时，正则表达式很有用。内容可能有不同的属性；在尝试从数据包负载中查找内容时，您会需要考虑其属性。

请注意，入侵规则使用的正则表达式语法是完整正则表达式库的一个子集，并该库中所用命令的语法在某些方面存在不同之处。使用入侵规则编辑器添加 pcre 关键字时，请按以下格式输入完整值：

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

其中：

- ! 是可选求反（如果要匹配与正则表达式**不**匹配的模式，请使用此求反）。
- /pcre/ 是兼容 Perl 的正则表达式。
- ismxAEGRBUIPHDMCKSY 是修饰符选项的任意组合。

另请注意，在 PCRE 中使用下表所列字符在数据包负载中搜索特定内容时，必须对这些字符进行转义，以使规则引擎能正确地解释这些字符。

表 *121*：转义的 *PCRE* 字符

必须转义的字符.....	使用反斜杠.....	或使用十六进制代码.....
#（哈希标记）	\#	\x23
;（分号）	\;	\x3B
|（竖线）	\\|	\x7C
:（冒号）	\:	\x3A

您还可以使用 m?regex?，其中 ? 是除 / 以外的分隔符。如果需要在正则表达式中匹配一个正斜杠，但不想用一个反斜杠来进行转义，可能需要使用此分隔符。例如，您可能使用 m?regex? ismxAEGRBUIPHDMCKSY，其中 regex 是兼容 Perl 的正则表达式，ismxAEGRBUIPHDMCKSY 是修饰符选项的任意组合。

提示 或者，可以用引号将兼容 Perl 的正则表达式引起来，例如，pcre_expression 或 “pcre_expression”。选择使用引号适合习惯使用先前版本（其中引号为必需而非可选）的有经验的用户。在保存规则后显示该规则时，入侵规则编辑器不显示引号。

pcre 语法

pcre 关键字接受兼容 Perl 的正则表达式 (PCRE) 标准语法。以下各节介绍这种语法。

提示 尽管本节介绍可用于 PCRE 的基本语法，但您可能想要参阅专门关于 Perl 和 PCRE 的网上参考资料或书籍，以获取更多高级信息。

元字符

元字符是在正则表达式中具有特殊含义的原义字符。在正则表达式中使用元字符时，必须通过在元字符前添加一个反斜杠来对其进行“转义”。

下表举例说明可用于 PCRE 的元字符。

表 *122*：*PCRE* 元字符

元字符	描述	示例
.	匹配除换行符以外的任何字符。如果将 s 用作修饰选项，还将匹配换行符。	abc. 匹配 abcd、abc1、abc# 等等。
*	匹配字符或表达式的零次或多次出现次数。	abc* 匹配 abc、abcc、abccc、abcccc 等等。
?	匹配字符或表达式的零次或一次出现次数。	abc? 匹配 abc。
+	匹配字符或表达式的一次或多次出现次数。	abc+ 匹配 abc、abcc、abccc、abcccc 等等。
()	组表达。	(abc)+ 匹配 abc、abcabc、abcabcabc 等等。
{}	为字符或表达式指定匹配项数限制。如果要设置下限和上限，请用逗号将下限和上限隔开。	a{4,6} 匹配 aaaa、aaaaa 或 aaaaaa。 (ab){2} 匹配 abab。
[]	允许定义字符类，并匹配字符集中包含的任意字符或字符组合。	[abc123] 匹配 a、b 或 c 等等。
^	匹配字符串开头的内容。如果在字符类中使用，也可用于否定。	^in 匹配 info 中的“in”，但不匹配 bin 中的“in”。 [^a] 匹配不包含 a 的任何内容。
$	匹配字符串结尾的内容。	ce$ 匹配 announce 中的“ce”，但不匹配 cent 中的“ce”。
|	指示 OR 表达式。	(MAILTO|HELP) 匹配 MAILTO 或 HELP。

元字符	描述	示例
\	元字符可用作实际字符，还可用于指定预定义的字符类。	\. 匹配句号，* 匹配星号，\\ 匹配反斜线，依此类推。\d匹配数字字符，\w匹配字母数字字符，依此类推。

字符类

字符类包括字母字符、数字字符、字母数字字符和空白字符。可以用方括号创建自己的字符类，也可以使用预定义类作为不同字符类型的快捷方式。如果不与其他限定符配合使用，一个字符类通常匹配一个数字或字符。

下表举例说明 PCRE 接受的预定义字符类。

表 *123*: *PCRE* 字符类

字符类	说明	字符类定义
\d	匹配数字字符（“数字”）。	[0-9]
\D	对应不是数字字符的任何字符。	[^0-9]
\w	匹配字母数字字符（“单词”）。	[a-zA-Z0-9_]
\W	匹配不是字母数字字符的任何字符。	[^a-zA-Z0-9_]
\s	匹配空白字符，包括空格、回车符、制表符、换行符和换页符。	[\r\t\n\f]
\S	匹配不是空白字符的任何字符。	[^ \r\t\n\f]

pcre 修饰符选项

指定pcre关键字值中的正则表达式语法后，可以使用修饰选项。这些修饰符执行特定于Perl、PCRE和Snort 的处理功能。修饰符始终按以下格式显示在 PCRE 值的末尾：

```
/pcre/ismxAEGRBUIPHDMCKSY
```

其中，ismxAEGRBUPHMC 可以包括下表中的任何修饰选项。

提示 或者，可以用引号将正则表达式和任何修饰选项引起来，例如，“/pcre/ismxAEGRBUIPHDMCKSY”。这一做法适合习惯使用旧版本的有经验的用户（旧版本要求必须用引号将正则表达式引起来）。在保存规则后显示该规则时，入侵规则编辑器不显示引号。

下表介绍了可用于执行 Perl 处理功能的选项。

表 *124*：*Perl* 相关的后正则表达式选项

选项	说明
i	使正则表达式不区分大小写。
s	点字符 (.) 匹配除换行符和 \n 字符以外的所有字符。可使用 "s" 选项覆盖此选项，这样，点字符将匹配所有字符（包括换行符）。
m	默认情况下，一个字符串被视为单行字符，^ 和 $ 分别匹配特定字符串的开头和结尾。如果使用 "m" 代替选项，^ 和 $ 将匹配紧接在缓冲区内所有换行符之前或之后的内容，以及位于缓冲区开头或结尾的内容。
x	忽略可能在这一模式中出现的空白数据字符，除非其为转义字符（前面加有反斜杠）或包含在字符类中。

下表介绍了可用于正则表达式后的 PCRE 修饰符。

表 *125*：*PCRE* 相关的后正则表达式选项

选项	说明
A	模式必须在字符串开头进行匹配（与在正则表达式中使用 ^ 具有相同的效果）。
E	将 $ 设置为只在目标字符串结尾进行匹配。（如果最后一个字符是换行符，即使没有 E，$ 也会匹配紧接在该字符之前的内容，但不会匹配任何其他换行符之前的内容）。
G	默认情况下，* + 和 ? 是“贪婪”的，这意味着，如果找到两个或更多匹配项，将会选择最长的匹配项。使用 G 字符可使这些字符在后面无问号字符 (?) 的情况下总是选择第一个匹配项。例如，在使用 G 修饰符的构造中，*? +? 和 ?? 将是贪婪字符，而 *、+ 或 ? 在不附带问号的情况下不是贪婪字符。

下表介绍了可用于正则表达式后的 Snort 特定修饰符。

.

表 *126*：特定于 *Snort* 的后正则表达式修饰符

选项	说明
R	相对于规则引擎上一次找到的匹配项的结尾搜索匹配的内容。
B	在未被预处理器解码的数据中搜索内容（此选项类似于使用带有 content 或 protected_content 关键字的 Raw Data 参数）。

选项	说明
U	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 `content` 或 `protected_content` 关键字的 **HTTP URI** 选项结合使用来搜索相同的内容。 请注意，管道化 HTTP 请求数据包包含多个 URI。包含 U 选项的 PCRE 表达式使规则引擎仅在管道化 HTTP 请求数据包的第一个 URI 中搜索内容匹配。要搜索数据包中的所有 URI，请使用已选择 **HTTP URI** 的 `content` 或 `protected_content` 关键字（可随附或不随附使用 U 选项的 PCRE 表达式）。
I	在已由 HTTP 检查预处理器解码的原始 HTTP 请求消息的 URI 中搜索内容。请注意，不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP 原始 URI (HTTP Raw URI)** 选项结合使用来搜索相同的内容
P	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的正文中搜索内容。
H	在已由 HTTP 检查预处理器解码的 HTTP 请求或响应消息的报头（不包括 cookie）中搜索内容。请注意，不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Header** 选项结合使用来搜索相同的内容。
D	在已由 HTTP 检查预处理器解码的原始 HTTP 请求或响应消息的报头（不包括 cookie）中搜索内容。请注意，不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Raw Header** 选项结合使用来搜索相同的内容。
M	在已由 HTTP 检查预处理器解码的规范化 HTTP 请求消息的方法字段中搜索内容；该方法字段确定要对URI中识别出的资源执行的操作（例如，GET、PUT、CONNECT 等）。
选	如果 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索规范化内容；如果该预处理器的 **Inspect HTTP Responses** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索规范化内容。当**检查HTTP Cookies** 的选项不可用时，搜索整个消息头，包括 cookies 或set-cookie中的数据。 请注意： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Cookie** 选项结合使用来搜索相同的内容。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

选项	说明
K	如果 HTTP 检查预处理器的 **Inspect HTTP Cookies** 选项已启用，将会在 HTTP 请求报头的任何 cookie 中搜索原始内容；如果该预处理器的 **Inspect HTTP Responses** 选项已启用，还会在 HTTP 响应报头的任何 set-cookie 中搜索原始内容。如果未启用 **Inspect HTTP Cookies** 选项，将会搜索包括 cookie 或 set-cookie 数据在内的整个报头。 请注意： • 消息正文中包含的 cookie 将被视为正文内容。 • 不能将此选项与 `content` 或 `protected_content` 关键字 **HTTP Raw Cookie** 选项结合使用来搜索相同的内容。 • `Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。
S	搜索 HTTP 响应中的三位数状态代码。
支持	搜索 HTTP 响应中状态代码随附的文字描述。

注释 请勿将 U 选项与 R 选项结合使用，否则可能会导致性能问题。此外，请勿将 U 选项与任何其他 HTTP 内容选项（I、P、H、D、M、C、K、S 或 Y）结合使用。

pcre 示例关键字值

以下示例显示可为 `pcre` 输入的值，并说明每个示例将会匹配的内容。

- /feedback[(\d{0,1})]?\.cgi/U

此示例搜索 `feedback` 的数据包负载，feedback 后面紧跟着零个或一个数字字符，再紧跟着 `.cgi`，且仅在 URI 数据中进行搜索。

此示例将匹配：

- `feedback.cgi`
- `feedback1.cgi`
- `feedback2.cgi`
- `feedback3.cgi`

此示例不匹配：

- `feedbacka.cgi`
- `feedback11.cgi`

- `feedback21.cgi`
- `feedbackzb.cgi`
- /^ez(\w{3,5})\.cgi/iU

此示例在字符串开头搜索 `ez` 的数据包负载，ez 后面跟有一个包含 3 到 5 个字母的单词，该单词后面跟着 `.cgi`。此搜索不区分大小写，且仅搜索 URI 数据。

此示例将匹配：

- `EZBoard.cgi`
- `ezman.cgi`
- `ezadmin.cgi`
- `EZAdmin.cgi`

此示例**不**匹配：

- `ezez.cgi`
- `fez.cgi`
- `abcezboard.cgi`
- `ezboardman.cgi`
- /mail(file|seek)\.cgi/U

此示例在 URI 数据中搜索后面跟有 `file` 或 `seek` 的 `mail` 的数据包负载。

此示例将匹配：

- `mailfile.cgi`
- `mailseek.cgi`

此示例**不**匹配：

- `MailFile.cgi`
- `mailfilefile.cgi`
- m?http\\x3a\x2f\x2f.*(\n|\t)+?U

此示例跟在任意数量字符后面的 HTTP 请求中为制表符或换行符搜索 URI 内容的数据包负载。此示例使用 `m?`regex`?` 以避免在表达式中使用 `http\:\/\/`。请注意，冒号前面有一个反斜杠。

此示例将匹配：

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

此示例**不**匹配：

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- m?http\\x3a\x2f\x2f.*=\|.*\|+?sU

此示例为带有任意数量字符（包括换行符）的URL搜索数据包负载，后面跟有一个等号以及包含任意数量字符或空白字符的竖线。此示例使用 `m?`regex`?` 以避免在表达式中使用 `http\:\/\/`。

此示例将匹配：

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

此示例**不**匹配：

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- /[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i

此示例为任何 MAC 地址搜索数据包负载。请注意，此示例使用反斜杠对冒号进行转义。

metadata 关键字

您可以使用 `metadata` 关键字向规则中添加自己的描述性信息。您还可以使用具有 `service` 参数的 `metadata` 关键字识别网络流量中的应用和端口。可以使用所添加的信息通过适合需求的方式组织或识别规则，并且可以搜索规则中所添加的信息和有关 `service` 参数的信息。

系统根据参数格式验证元数据：

keyvalue

其中，*key* 和 *value* 提供以空格分隔的组合描述。这是Cisco Talos 安全情报和研究小组 (Talos) 用于向思科提供的规则添加元数据的格式。

也可以使用其他格式：

key=value

例如，通过按如下方式使用类别和子类别，可以使用 *key value* 格式按作者和日期识别规则：

```
author SnortGuru_20050406
```

可以在规则中使用多个 `metadata` 关键字。还可以使用逗号分隔单个 `metadata` 关键字中的多个 *key value* 参数，如以下示例所示：

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,

revised_by SnortUser1_20070123
```

并非只能使用 *key value* 或 *key=value* 格式；但是，应了解根据这些格式进行验证产生的局限性。

要避免的受限字符

请注意以下字符限制：

- 请勿使用分号 (;) 或冒号 (:)。
- 系统将逗号解释为多个 *key value* 或 *key=value* 参数的分隔符。例如：

  keyvalue,keyvalue,keyvalue
- 系统将等于 (=) 字符或空格字符解释为 *key* 和 *value* 之间的分隔符。例如：

  keyvalue

  key=value

允许使用所有其他字。

要避免的保留元数据

请避免在 `metadata` 关键字中使用以下单词作为单个参数或作为 *key value* 参数中的 *key*；这些单词保留供 Talos 使用：

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

注释 如需有关将受限元数据添加到可能不具有预期作用的本地规则方面的帮助，请联系支持部门。

影响级别 1

可以在 `metadata` 关键字中使用以下保留的 *key value* 参数：

```
impact_flag red
```

此 *key value* 参数针对导入的本地规则或使用入侵规则编辑器创建的自定义规则将影响标志设置为红色（级别 1）。

请注意，当 Talos 在思科提供的规则中包含 `impact_flag red` 参数时，Talos 已确定触发该规则的数据包指示源主机或目标主机可能受病毒、特洛伊木马或其他恶意软件的损害。

服务元数据

系统检测在网络中的主机上运行的应用，并将应用协议信息插入网络流量中；无论如何配置发现策略，它都会执行此操作。您可以在 TCP 或 UDP 规则中使用 `metadata` 关键字 `service` 参数来匹配网络流量中的应用协议和端口。您可以在某个规则中组合一个或多个 `service` 应用参数与单个端口参数。

服务应用

可以使用带 `service` 的 `metadata` 关键字作为 *key*，并使用应用作为 *value*，以匹配具备已识别应用协议的数据包。例如，`metadata` 关键字中的以下 *key value* 参数会将规则与 HTTP 流量关联：

```
service http
```

可以识别多个以逗号分隔的应用。例如：

```
service http, service smtp, service ftp
```

下表介绍与 `service` 关键字配合使用的最常见应用值。

注释 如需有关识别表中未列出的应用方面的帮助，请联系支持部门。

表 *127*：*service* 值

值	说明
`cvs`	当前版本系统
`dcerpc`	分布式计算环境/远程过程调用系统
`dns`	域名系统
`finger`	Finger 用户信息协议
`ftp`	文件传输协议
`ftp-data`	文件传输协议（数据通道）
`http`	超文本传输协议
`imap`	Internet 消息访问协议
`isakmp`	互联网安全关联和密钥管理协议
`mysql`	我的结构化查询语言
`netbios-dgm`	NetBIOS 数据报服务
`netbios-ns`	NetBIOS 名称服务
`netbios-ssn`	NetBios 会话服务
`nntp`	网络新闻传输协议
`oracle`	Oracle 网络服务
`外壳`	操作系统外壳

值	说明
pop2	邮局协议第 2 版
pop3	邮局协议第 3 版
smtp	简单邮件传输协议
snmp	简单网络管理协议
ssh	安全外壳网络协议
sunrpc	Sun 远程过程调用协议
telnet	Telnet 网络协议
tftp	简单文件传输协议
x11	X Window 系统

服务端口

可以使用带 service 的 metadata 关键字作为 *key*，并使用指定端口参数作为 *value*，以定义规则如何与应用结合来匹配端口。

可以指定下表中的任何一个端口值，每条规则一个值。

表 *128*：*service* 端口值

值	说明
else-ports 或 unknown	如果符合以下任一条件，则系统将应用规则： • 数据包应用已知，且匹配规则应用。 • 数据包应用未知，且数据包端口匹配规则端口。 当 service 指定一个不含端口修饰符的应用协议时，else-ports 和 unknown 将产生系统使用的默认行为。
and-ports	如果数据包应用已知且匹配规则应用，则系统应用规则，并且数据包端口匹配规则报头中的端口。您无法在未指定应用的规则中使用 and-ports。

值	说明
or-ports	如果符合以下任何条件，则系统将应用规则： • 数据包应用已知，且匹配规则应用。 • 数据包应用未知，且数据包端口匹配规则端口。 • 数据包应用不匹配规则应用，且数据包端口匹配规则端口。 • 规则未指定应用，且数据包端口匹配规则端口。

请注意以下提示：

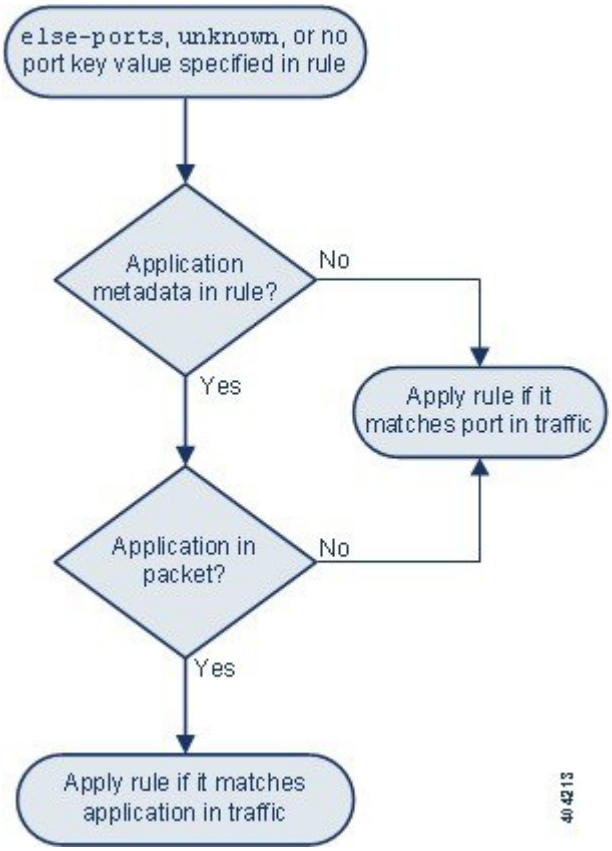
- 必须包含带 service and-ports 参数的 service 应用参数。
- 如果某个规则指定上表中的多个值，则系统将应用该规则中最后出现的一个值。
- 端口和应用参数可以为任何顺序。

除了 and-ports 值，可以包含带或不带一个或多个 service 应用参数的 service 端口参数。例如：service or-ports, service http, service smtp

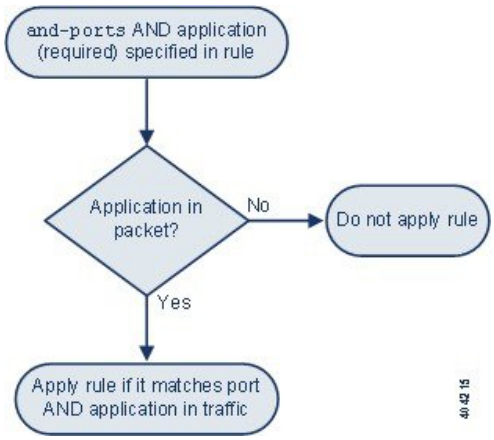
流量中的应用和端口

下图展示了入侵规则支持的应用和端口组合，以及将这些规则限制应用到数据包数据的结果。

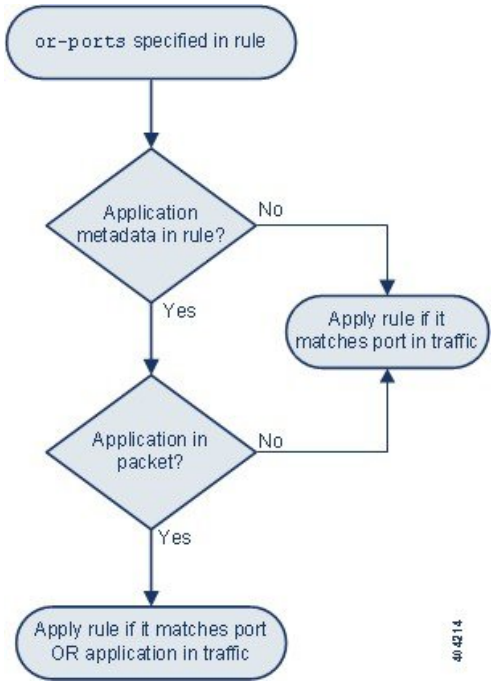
主机应用协议的其他源/目标端口：



主机应用协议和源/目标端口：



主机应用协议或源/目标端口：



示例匹配

以下规则示例使用带 `service` 参数的 `metadata` 关键字，与其匹配和不匹配的数据示例一同显示：

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

示例匹配	不匹配示例
• TCP 端口 80 上的 HTTP 流量 • TCP 端口 8080 上的 HTTP 流量 • TCP 端口 80 上的 SMTP 流量 • TCP 端口 8080 上的 SMTP 流量	• 端口 80 或 8080 的 POP3 流量 • 端口 80 或 8080 上的未知应用流量 • 端口 9999 上的 HTTP 流量

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

示例匹配	不匹配示例
• 任意端口上的 HTTP 流量 • 端口 80 上的 SMTP 流量 • 端口 8080 上的 SMTP 流量 • 端口 80 和 8080 上的未知应用流量	• 除 80 或 8080 外的端口上的非 HTTP 和非 SMTP 流量

• 以下任何一规则：

```
alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)
alert tcp any any -> any [80,8080] metadata:service unknown, service http;)
alert tcp any any -> any [80,8080] metadata:service http;)
```

示例匹配	不匹配示例
• 任意端口上的 HTTP 流量 • 如果数据包应用未知，则为端口80 • 如果数据包应用未知，则为端口8080	• 端口 80 或 8080 的 SMTP 流量 • 端口 80 或 8080 的 POP3 流量

元数据搜索准则

要搜索使用`metadata`关键字的规则，请在规则搜索页面上选择`metadata`关键字，或者键入元数据的任何部分。例如，可以键入：

- `search`，以显示在其中对 *key* 使用了 `search` 的所有规则。
- `search http`，以显示在其中对 *key* 使用了 `search` 并对 *value* 使用了 `http` 的所有规则。
- `author snortguru`，以显示在其中对 *key* 使用了 `author` 并对 *value* 使用了 `SnortGuru` 的所有规则。
- `author s`，以显示在其中为 *key* 使用了 `author` 并对 *value* 使用了任何词条（例如 `SnortGuru`、`SnortUser1` 或 `SnortUser2`）的所有规则。

提示 如果同时搜索 *key* 和 *value*，应在搜索中使用与规则的 *key value* 参数中使用的相同连接运算符（等号 [=] 或空格字符）；搜索将返回不同的结果，具体取决于 *key* 后面跟的是等号 (=) 还是空格字符。

请注意，无论使用何种格式添加元数据，系统都会将元数据搜索词解释为 *key value* 或 *key=value* 参数的全部或一部分。例如，以下是没有遵循 *key value* 或 *key=value* 格式的有效元数据：

```
ab cd ef gh
```

但是，系统会将此示例中的每个空格解释为 *key* 和 *value* 之间的分隔符。因此，对于并列和单个术语，可以使用以下任何搜索成功查找到包含元数据示例的规则：

```
cd ef
ef gh
ef
```

但是，使用以下搜索不会找到该规则（系统会将其解释为单个 *key value* 参数）：

```
ab ef
```

IP 报头值

可以使用关键字来识别数据包 IP 报头中可能存在的攻击或安全策略违规。

fragbits

`fragbits` 关键字检查 IP 报头中的分片和保留位。可以检查每个数据包的 Reserved 位、More Fragments 位和 Don't Fragment 位的任意组合。

表 *129*：*Fragbits* 参数值

参数	说明
R	Reserved 位
M	More Fragments 位
D	Don’t Fragment 位

为进一步改进使用 `fragbits` 关键字的规则，可以在规则的参数值后指定下表中所述的任何运算符。

表 *130*：*Fragbit* 运算符

Operator	说明
加号 (+)	数据包必须匹配所有指定的位。
星号 (*)	数据包可以匹配任何指定的位。
感叹号 (!)	如果未设置任何指定的位，数据包将符合条件。

例如，要生成有关设置了 Reserved 位（还可能设置了任何其他位）的数据包的事件，请使用 `R+` 作为 `fragbits` 值。

id

id关键字根据您在此关键字的参数中指定的值测试IP报头分片标识字段。某些拒绝服务工具和扫描仪将此字段设置为容易检测的特定数字。例如，在 SID630（检测 Synscan 端口扫描）中，id 设置为 39426，这是在扫描仪传输的数据包中用作 ID 号的静态值。

注释 id 参数值必须为数字。

ipopts

使用 IPopts 关键字可在数据包中搜索指定的 IP 报头选项。下表列出了可用的参数值。

表 *131*：*IPoption* 参数

参数	说明
rr	记录路由
eol	列表结束
nop	无操作
ts	时间戳
秒	IP 安全选项
lsrr	松散源路由
ssrr	严格源路由
satid	数据流标识符

分析师最经常监视严格和松散源路由，因为这两个选项可能指出欺骗性源 IP 地址。

ip_proto

使用 ip_proto 关键字可识别使用指定为关键字值的 IP 协议的数据包。可以为 IP 协议指定 0 到 255 之间的数字。可以将这些协议号与以下运算符结合使用：<、> 或 !。例如，要检查使用非 ICMP 的任何协议的流量，请使用 !1 作为 ip_proto 关键字的值。也可以在一个规则中多次使用 ip_proto 关键字；但请注意，规则引擎会将此关键字的多个实例解释为具有布尔 AND 关系。例如，如果创建一个包含 ip_proto:!3; ip_proto:!6 的规则，该规则将忽略使用 GGP 协议和 TCP 协议的流量。

tos

有些网络使用服务类型 (ToS) 值设置在网络上传输的数据包的优先级。使用 `tos` 关键字可根据指定为该关键字的参数的值测试数据包的 IP 报头 ToS 值。对于其 ToS 已设置为指定值且符合规则中规定的其他条件的数据包，使用 `tos` 关键字的规则将会触发。

注释 `tos` 参数值必须为数字。

ToS 字段已在 IP 报头协议中弃用，取而代之的是 Differentiated Services Code Point (DSCP) 字段。

ttl

数据包的生存时间 (ttl) 值指明数据包在被丢弃之前可以跳多少次。可以使用 `ttl` 关键字根据指定为关键字参数的值或值范围测试数据包的 IP 报头 ttl 值。将 `ttl` 关键字参数设置为较小的值（例如 0 或 1）可能会有帮助，因为小的生存时间值有时表示跟踪路由或入侵逃避行为。（但请注意，此关键字的相应值取决于受管设备的位置和网络拓扑。）使用以下语法：

- 将 TTL 值设置为 0 到 255 之间的整数。也可以该值前面加上一个等号 (=)（例如，可以指定 `5` 或 `=5`）。
- 使用连字符 (-) 指定 TTL 值的范围（例如，`0-2` 指定 0 到 2 之间的所有值，`-5` 指定 0 到 5 之间的所有值，`5-` 指定 5 到 255 之间的所有值）。
- 使用大于号 (>)指定 TTL 值大于一个特定值（例如，`>3` 指定大于 3 的所有值）。
- 使用大于或等于号 (>=) 指定 TTL 值大于或等于一个特定值（例如，`>=3` 指定大于或等于 3 的所有值）。
- 使用小于号 (<)指定 TTL 值小于一个特定值（例如，`<3` 指定小于 3 的所有值）。
- 使用小于或等于号 (<=) 指定 TTL 值小于或等于一个特定值（例如，`<=3` 指定小于或等于 3 的所有值）。

ICMP 报头值

Firepower 系统支持可用于识别 ICMP 数据包报头中的攻击和安全策略违规的关键字。但请注意，存在的预定义规则检测大多数 ICMP 类型和代码。可考虑启用现有规则或者根据现有规则创建本地规则；如果您从头开始构建 ICMP 规则，可能会更快找到符合您需求的规则。

icmp_id 和 icmp_seq

ICMP 标别号和序列号有助于将 ICMP 响应与 ICMP 请求关联起来。在正常流量中，这些值动态地分配给数据包。有些隐蔽通道和分布式拒绝服务 (DDoS) 程序使用静态 ICMP ID 和序列值。使用以下关键字可识别具有静态值的 ICMP 数据包。

关键字	Definition
icmp_id	检查 ICMP 回应请求或应答数据包的 ICMP ID 号。应使用对应于 ICMP ID 号的数值作为 `icmp_id` 关键字的参数。

关键字	Definition
icmp_seq	`icmp_seq` 关键字检查 ICMP 回应请求或应答数据包的 ICMP 序列。应使用对应于 ICMP 序列号的数值作为 `icmp_seq` 关键字的参数。

itype

使用 `itype` 关键字可查找具有特定 ICMP 消息类型值的数据包。您可以指定有效的 ICMP 类型值或无效的 ICMP 类型值来测试不同类型的流量。例如，攻击者可以将 ICMP 类型值设置为超出范围，从而导致拒绝服务和泛洪攻击。

可以使用小于号 (<) 和大于号 (>) 指定 `itype` 参数值的范围。

例如：

- <35
- >36
- 3<>55

icode

ICMP 消息有时包含代码值，用于在目标不可达的情况下提供有关详细信息。

您可以使用 `icode` 关键字来识别具有特定 ICMP 代码值的数据包。可以指定有效的 ICMP 代码值或无效的 ICMP 代码值来测试不同类型的流量。

可以使用小于号 (<) 和大于号 (>) 指定 `icode` 参数值的范围。

例如：

- 要查找小于 35 的值，请指定 `<35`。
- 要查找大于 36 的值，请指定 `>36`。
- 要查找 3 到 55 之间的值，请指定 `3<>55`。

提示 可以同时使用 `icode` 和 `itype` 关键字来识别与这两者都匹配的流量。例如，要识别包含 ICMP Destination Unreachable 代码类型和 ICMP Port Unreachable 代码类型的 ICMP 流量，请指定 3 作为 `itype` 关键字的值（用于 Destination Unreachable 类型），并指定 3 作为 `icode` 关键字的值（用于 Port Unreachable 类型）。

TCP 报头值和数据流大小

Firepower 系统支持专门用于使用数据包 TCP 报头和 TCP 数据流大小来识别尝试的攻击的关键字。

ack

可以使用 `ack` 关键字将某个值与数据包的 TCP 确认号进行比较。如果数据包的 TCP 确认号与为 `ack` 关键字指定的值相匹配，则会触发规则。

`ack` 参数值必须为数字。

标志

可以使用 `flags` 关键字指定 TCP 标志的任意组合，如果在已检查的数据包中设置此关键字，将触发规则。

注释 在使用 `A+` 作为 `flags` 的值的一般情况下，应转为使用具有 `established` 值的 `flow` 关键字。通常，如果使用标志以确保标志的所有组合均已检测到，应使用具有 `stateless` 值的 `flow` 关键字。

可以检查或忽略下表中所述的 `flag` 关键字的值。

表 *132*：*flag* 参数

参数	TCP 标志
Ack	确认数据。
Psh	数据应该在此数据包中发送。
Syn	新的连接。
Urg	包含紧急数据的数据包。
Fin	关闭的连接。
Rst	中止的连接。
CWR	ECN 堵塞窗口已减少。这以前是 R1 参数，仍支持向后兼容。
ECE	ECN 响应。这以前是 R2 参数，仍支持向后兼容。

使用 `flags` 关键字时，可以使用运算符来指示系统如何匹配多个标志。下表介绍了这些运算符。

表 *133*：与 *flags* 配合使用的运算符

Operator	描述	示例
all	数据包必须包含所有指定的标志。	选择 `Urg` 和 `all` 可规定数据包必须包含紧急标志，且可以包含任何其他标志。

Operator	描述	示例
any	数据包可包含任何指定的标志。	选择 Ack、Psh 和 any 可规定必须设置 Ack 和/或 Psh 标志才能触发规则，且也可以对数据包设置其他标志。
要	数据包**不得**包含指定的标志集。	选择 Urg 和 not 可规定**不**对会触发此规则的数据包进行设置紧急标志。

流

可以使用 flow 关键字选择由规则根据会话特征进行的检查的数据包。flow 关键字允许您指定规则应用的流量的方向，从而将规则应用于客户端流量或服务器流量。要指定 flow 关键字如何检查数据包，可以设置要分析的流量的方向、已检查的数据包的状态以及这些数据包是否是重建数据流的一部分。

数据包状态检测发生在规则处理之后。如果要使某个 TCP 规则忽略无状态流量（尚未建立会话上下文的流量），必须将 flow 关键字添加到该规则，并为该关键字选择 **Established** 参数。如果要使某个 UDP 规则忽略无状态流量，必须将 flow 关键字添加到该规则，并选择 **Established** 参数和/或方向参数。这样，TCP 或 UDP 规则就会执行数据包状态检查。

如果添加方向参数，规则引擎将只检查具有已建立状态且流向与指定方向匹配的数据包。例如，如果将具有 established 参数和 From Client 参数的 flow 关键字添加到某个规则，且该规则会在检测到 TCP 或 UDP 连接的情况下触发，那么规则引擎将只检查从特定客户端发送的数据包。

提示 为了获得最佳性能，应始终在 TCP 规则或 UDP 会话规则中包含 flow 关键字。

下表介绍了可为 flow 关键字指定的数据流相关参数：

表 *134*：状态相关的 *flow* 参数

参数	说明
建立	在已建立连接的情况下触发。
无状态	无论数据流处理器的状态如何，都会触发。

下表介绍了可为 flow 关键字指定的方向选项：

表 *135*：*flow* 方向参数

参数	说明
To Client	服务器响应时触发。
到服务器	客户端响应时触发。

参数	说明
From Client	客户端响应时触发。
From Server	服务器响应时触发。

请注意，`From Server` 和 `To Client` 执行相同的功能，`To Server` 和 `From Client` 执行相同的功能。这些选项是为了是规则具有上下文和可读性。例如，如果要创建用于检测从服务器向客户端发起的木马攻击的规则，应使用 `From Server`。但是，如果要创建用于检测从客户端向服务器发出的木马攻击的规则，应使用 `From Client`。

下表介绍了可为 `flow` 关键字指定的数据流相关参数：

表 *136*：数据流相关的 *flow* 参数

参数	说明
Ignore Stream Traffic	重建流数据包时不触发。
Only Stream Traffic	仅在重建流数据包时触发。

例如，可以使用 `To Server, Established, Only Stream Traffic` 作为 `flow` 关键字的值，这样将会检测在建立的会话中从客户端流向服务器并且由数据流预处理器重组的流量。

seq

使用 `seq` 关键字可指定静态序列号值。序列号与指定参数相匹配的数据包将会触发包含此关键字的规则。虽然此关键字很少使用，但它有助于识别使用生成的具有静态序列号的数据包的攻击和网络扫描。

window

可以使用 `window` 关键字指定感兴趣的 TCP 窗口大小。包含此关键字的规则在遇到具有指定 TCP 窗口大小的数据包时，都会触发。虽然此关键字很少使用，但它有助于识别使用生成的具有静态 TCP 窗口大小的数据包的攻击和网络扫描。

stream_size

可以将 `stream_size` 关键字与数据流预处理器配合使用，以确定 TCP 数据流的大小（以字节为单位），具体格式如下：

```
direction,operator,bytes
```

其中，bytes 是字节数。必须以逗号 (,) 分隔参数中的每个选项。

下表介绍了可为 `stream_size` 关键字指定的不区分大小写的方向选项：

表 *137*：*stream_size* 关键字定向参数

参数	说明
客户端	当来自客户端的数据流与指定数据流大小相匹配时触发。
server	当来自服务器的数据流与指定数据流大小相匹配时触发。
both	当来自客户端和服务器的流量都与指定数据流大小相匹配时触发。 例如，如果来自客户端的流量大于 200 字节，且来自服务器的流量也大于 200 字节，参数 `both, >, 200` 将会触发。
either	当来自客户端或服务器流量与指定数据流大小相匹配时触发（无论哪一种情况先发生）。 例如，如果来自客户端的流量大于 200 字节，或来自服务器的流量大于 200 字节，参数 `either, >, 200` 将会触发。

下表介绍了可与 `stream_size` 关键字配合使用的运算符：

表 *138*：*stream_size* 关键字参数运算符

Operator	说明
=	等于
!=	不等于
>	大于
<	小于
>=	大于或等于
<=	小于或等于

例如，可以使用 `client, >=, 5001216` 作为 `stream_size` 关键字的参数，以检测从客户端发往服务器的且大于或等于 5001216 字节的 TCP 数据流。

stream_reassembly 关键字

如果单个连接上的已检测流量与规则条件相匹配，则可以使用 `stream_reassemble` 关键字为该连接启用或禁用 TCP 流重组。或者，可以在规则中多次使用此关键字。

可使用以下语法启用或禁用数据流重组：

```
enable|disable, server|client|both, option, option
```

下表介绍可与 `stream_reassemble` 关键字配合使用的可选参数。

表 *139*：*stream_reassemble* 可选参数

参数	说明
noalert	无论规则中是否指定任何其他检测选项，都不生成事件。
fastpath	当有匹配时，忽略连接流量的其余部分。

例如，以下示例禁用 TCP 客户端数据流重组，而且不针对在 HTTP 响应中检测到 200 OK 状态代码的连接生成事件：

```
alert tcp any 80 -> any any (flow:to_client, established; content: “200 OK”;
stream_reassemble:disable, client, noalert
```

SSL 关键字

可以使用 SSL 规则关键字调用安全套接字层 (SSL) 预处理器，并从加密会话中的数据包提取有关 SSL 版本和会话状态的信息。

客户机和服务器进行通信以使用 SSL 或安全传输层 (TLS) 建立加密会话时，它们之间会交换握手消息。虽然在会话中传输的数据是加密的，但握手消息没有加密。

SSL 预处理器从特定握手字段提取状态和版本信息。握手中的两个字段分别指明用于加密会话的 SSL 或 TLS 版本以及握手的阶段。

ssl_state

`ssl_state` 关键字可用于匹配加密会话的状态信息。要同时检查所用的两个或更多 SSL 版本，请在规则中使用多个 `ssl_version` 关键字。

如果规则使用 `ssl_state` 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 状态信息。

例如，要检测是否有攻击者试图通过发送具有超长长度和过量数据的 `ClientHello` 消息来造成服务器缓冲区溢出，可以使用带有 `client_hello` 参数的 `ssl_state` 关键字，然后检查异常大的数据包。

可使用逗号分隔列表为 SSL 状态指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果指定 `client_hello` 和 `server_hello` 作为参数，系统将会根据带有 `client_hello` 或 `server_hello` 的流量对规则进行评估。

还可以否定任何参数；例如：

```
!client_hello, !unknown
```

要确保连接已达到状态集中的每个状态，应使用具有 ssl_state 规则选项的多个规则。`ssl_state` 关键字将以下标识符作为参数：

表 *140*：*ssl_state* 参数

参数	目的
client_hello	当客户端请求加密会话时，匹配消息类型为 ClientHello 的握手消息。
server_hello	当服务器响应客户端的加密会话请求时，匹配消息类型为 ServerHello 的握手消息。
client_keyx	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 ClientKeyExchange 的握手消息。
server_keyx	当客户端向服务器发出密钥以确认收到来自服务器的密钥时，匹配消息类型为 ServerKeyExchange 的握手消息。
unknown	匹配任何握手消息类型。

ssl_version

ssl_version 关键字可用于匹配加密会话的版本信息。如果规则使用 ssl_version 关键字，规则引擎将调用 SSL 预处理器来检查流量的 SSL 版本信息。

例如，如果知道 SSL 2 版本中存在缓冲区溢出漏洞，可以使用带有 sslv2 参数的 ssl_version 关键字来识别使用该 SSL 版本的流量。

可使用逗号分隔列表为 SSL 版本指定多个参数。如果列出多个参数，系统将使用 OR 运算符对这些参数进行评估。例如，如果要识别任何未使用 SSLv2 的加密流量，可以向规则添加 ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2。这样，规则将会评估任何使用 SSL 3 版本、TLS 1.0 版本、TLS 1.1 版本或 TLS 1.2 版本的流量。

ssl_version 关键字将以下 SSL/TLS 版本标识符作为参数：

表 *141*：*ssl_version* 参数

参数	目的
sslv2	匹配使用安全套接字层 (SSL) 2 版本编码的流量。
sslv3	匹配使用安全套接字层 (SSL) 3 版本编码的流量。
tls1.0	匹配使用传输层安全 (TLS) 1.0 版本编码的流量。
tls1.1	匹配使用传输层安全 (TLS) 1.1 版本编码的流量。
tls1.2	匹配使用传输层安全 (TLS) 1.2 版本编码的流量。

appid 关键字

可以使用 `appid` 关键字识别数据包中的应用协议、客户端应用或 Web 应用。例如，可以针对据知易受特定漏洞影响的特定应用。

在入侵规则的 `appid` 关键字中，点击**配置 AppID (Configure AppID)** 以选择一个或多个要检测的应用。

浏览可用应用

首次开始构建条件时，**可用应用 (Available Applications)** 列表不受限制，并且显示系统检测的每个应用（每页 100 个）：

- 要翻页浏览应用，请点击列表下方的箭头。
- 要打开弹出窗口，显示有关应用特性的摘要信息以及可点选的互联网搜索链接，请点击应用旁边的信息图标 ()。

使用应用过滤器

为帮助查找要匹配的应用，您可以通过以下方式限制 **Available Applications** 列表：

- 要搜索应用，请点击列表上方的 **Search by name** 提示，然后键入名称。列表会在您键入内容时进行更新，以显示匹配的应用。
- 要通过应用过滤器来限制应用，请使用**应用过滤器 (Application Filters)** 列表。**Available Applications** 列表在您应用过滤器时进行更新。为方便起见，系统使用解锁图标 () 标记系统只能在解密流量中识别（在加密或未加密流量中无法识别）的应用。

注释 如果您在 Application Filters 列表中选择一个或多个过滤器，并在这种状态下搜索 **Available Applications** 列表，系统会使用 AND 运算将您的选择与搜索过滤出的 **Available Applications** 列表进行组合。

选择应用

要选择单个应用，请选择该应用并点击**添加到规则 (Add to Rule)**。要选择当前受限制视图中的所有应用，请右键点击并选择**全选 (Select All)**。

应用层协议值

虽然预处理器执行应用层协议值的大部分检查和规范化工作，但您仍可以使用各种预处理器选项来检查应用层值。

RPC 关键字

rpc 关键字识别 TCP 或 UDP 数据包中的开放网络计算远程过程调用 (ONC RPC) 服务。这使您可以检测尝试识别主机上 RPC 程序的行为。入侵者可以使用 RPC 端口映射程序来确定网络上是否运行着可以利用的任何 RPC 服务。他们还可能尝试访问不使用端口映射程序运行 RPC 的其他端口。下表列出了 rpc 关键字接受的参数。

表 *142*：*rpc* 关键字参数

参数	说明
application	RPC 应用编号
procedure	调用的 RPC 程序
版本	RPC 版本

要为 rpc 关键字指定参数，请使用以下语法：

```
application,procedure,version
```

其中，application 是 RPC 应用编号，procedure 是 RPC 过程编号，version 是 RPC 版本号。必须指定 rpc 关键字的所有参数 - 如果无法指定其中一个参数，请将其替换为星号 (*)。

例如，要搜索具有任意程序或版本的 RPC 端口映射程序（以数字 100000 表示的 RPC 应用），可使用 `100000,*,*` 作为参数。

ASN.1 关键字

asn1 关键字使您可以解码整个或部分数据包，以查找各种恶意编码。

下表介绍了 asn1 关键字的参数。

表 *143*：*asn.1* 关键字参数

参数	说明
Bitstring Overflow	检测可远程攻击的无效位串编码。
Double Overflow	检测大于标准缓冲区的双 ASCII 编码。这是 Microsoft Windows 中的一个已知漏洞，但目前不知道哪些服务可能会被利用。
Oversize Length	检测长度大于提供的参数的 ASN.1 类型。例如，如果将 Oversize Length 设置为 500，任何大于 500 的 ASN.1 类型都会触发规则。
Absolute Offset	设置从数据包负载起点算起的绝对偏移量。（请记住，offset 计数器从字节 0 开始计算。）例如，如果要解码 SNMP 数据包，请将 Absolute Offset 设置为 0，但不设置 Relative Offset。Absolute Offset 可以是正数或负数。

参数	说明
Relative Offset	从上一次成功内容匹配、pcre 或 byte_jump 算起的相对偏移量。要解码紧接在内容“foo”后的 ASN.1 序列，请将 Relative Offset 设置为 0，但不设置 Absolute Offset。Relative Offset 可以是正数或负数。（请记住，偏移量计数器从字节 0 开始计算。）

例如，Microsoft ASN.1 库中存在一个会造成缓冲区溢出的已知漏洞，使得攻击者能够利用包含特制的身份验证数据包的条件。当系统解码 ASN.1 数据时，数据包中的攻击代码可以在具有系统级别权限的主机上执行，或可能导致 DoS 条件。以下规则使用 asn1 关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用端口 445 的任何 IP 地址，上述规则将会生成事件。此外，它仅对与服务器之间建立的 TCP 连接执行规则。然后，该规则在特定位置对特定内容进行测试。最后，该规则使用 asn1 关键字检测位串编码和双 ASCII 编码，以及确定自上一次成功内容匹配结束以来从 55 字节开始算起超过 100 字节的 asn.1 长度类型。（请记住，offset 计数器从字节 0 开始计算。）

urilen 关键字

可以将 urilen 关键字和 HTTP 检查预处理器结合使用，以检查 HTTP 流量中特定长度、小于最大长度、大于最小长度或在指定范围内的 URI。

在 HTTP 检查预处理器对数据包进行规范化和检查后，规则引擎将根据规则评估数据包，并确定 URI 是否与 urilen 关键字指定的长度条件相匹配。可以使用此关键字来检测试图利用 URI 长度漏洞的攻击，例如，创建缓冲区溢出，以使攻击者可以在具有系统级别权限的主机上形成 DoS 条件或执行代码。

在规则中使用 urilen 关键字时，请注意：

- 实际上，urilen 关键字总是与 flow:established 关键字以及一个或多个其他关键字结合使用。
- 规则协议始终是 TCP。
- 目标端口始终是 HTTP 端口。

可以使用十进制字节数、小于号 (<) 和大于号 (>) 指定 URI 长度。

例如：

- 指定 5 将会检测长度为 5 字节的 URI。
- 指定 < 5（用一个空格字符隔开）将会检测长度小于 5 字节的 URI。
- 指定 > 5（用一个空格字符隔开）将会检测长度大于 5 字节的 URI。
- 指定 3 <> 5（<> 前后各有一个空格字符）将会检测长度为 3 到 5 字节的 URI。

例如，Novell服务器的监控和诊断实用程序iMonitor 2.4版中存在一个已知漏洞，该漏洞来自eDirectory 8.8 版。包含过长 URI 的一个数据包造成缓冲区溢出，使得攻击者者能够利用包含特制数据包的条件，该数据包可以在具有系统级别权限的主机上执行或可能导致DoS条件。以下规则使用urilen关键字检测试图利用此漏洞的行为：

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

当有 TCP 流量从 $EXTERNAL_NET 变量中定义的使用任何端口的任何 IP 地址流向 $HOME_NET 变量中定义的使用 $HTTP_PORTS 变量中定义的端口的任何 IP 地址，上述规则将会生成事件。此外，仅针对与服务器之间建立的 TCP 连接根据该规则评估数据包。该规则使用 urilen 关键字检测长度超过 8192 字节的任何 URI。最后，该规则在 URI 中搜索不区分大小写的特定内容 /nds/。

DCE/RPC 关键字

下表中描述的三个 DCE/RPC 关键字可用于监控 DCE/RPC 会话流量的漏洞。当系统处理带有这些关键字的规则时，会调用 DCE/RPC 预处理器。

表 *144*: *DCE/RPC* 关键字

使用.....	使用方式	要检测的内容
dce_iface	独立	识别特定 DCE/RPC 服务的数据包
dce_opnum	在前面加上 dce_iface	识别特定 DCE/RPC 服务操作的数据包
dce_stub_data	在前面加上 dce_iface+ dce_opnum	定义特定操作请求或响应的存根数据

请注意，在上表中，应始终在 dce_iface 前面加上 dce_iface，在 dce_stub_data 前面加上 dce_iface 和 dce_opnum。

也可以将这些 DCE/RPC 关键字与其他规则关键字结合连用。请注意，对于 DCE/RPC 规则，应使用选择了 **DCE/RPC** 参数的 byte_jump、byte_test 和 byte_extract 关键字。

思科建议在包含 DCE/RPC 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 content 关键字，无论您是否启用 content 关键字的 **Use Fast Pattern Matcher** 参数，规则引擎都会使用快速模式匹配程序。

在以下情况下，可以将 DCE/RPC 版本及相邻报头信息用作匹配的内容：

- 规则不包括其他 content 关键字
- 规则包含另一个 content 关键字，但 DCE/RPC 版本及相邻信息代表比其他内容更独特的模式

  例如，DCE/RPC 版本及相邻信息更有可能比内容的单个字节更加独特。

应使用以下其中一个版本及相邻信息内容匹配来终止限定规则：

- 对于面向连接的 DCE/RPC 规则，使用内容 `|05 00 00|`（用于 05 主要版本、00 次要版本和请求 PDU [协议数据单元]类型 00）。
- 对于无连接的 DCE/RPC 规则，使用内容 `|04 00|`（用于 04 版本和请求 PDU 类型 00）。

在这两种情况下，都应将版本及相邻信息的 `content` 关键字放在规则末尾，以调用快速模式匹配程序而不重复 DCE/RPC 预处理器已完成的处理。请注意：将 `content` 关键字放在规则末尾这种做法适用于被用作调用快速模式匹配程序的手段的版本内容，对于规则中的其他内容匹配无需这样做。

dce_iface

可以使用 `dce_iface` 关键字识别特定 DCE/RPC 服务。

或者，还可以将 `dce_iface` 与 `dce_opnum` 和 `dce_stub_data` 关键字结合使用，以进一步限制要检查的 DCE/RPC 流量。

固定的 16 字节通用唯一标识符 (UUID) 用于识别分配给每个 DCE/RPC 服务的应用接口。例如，UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 识别 DCE/RPC lanmanserver 服务（又称为 srvsvc 服务），该服务提供大量用于共享对等网络打印机、文件和 SMB 命名管道的管理功能。DCE/RPC 预处理器使用 UUID 及相关报头值来跟踪 DCE/RPC 会话。

接口 UUID 是由 5 个十六进制字符串（字符串之间用连字符分隔）组成：

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

可以通过输入整个 UUID（包括连字符）来指定接口，如以下用于 netlogon 接口的 UUID 中所示：

```
12345678-1234-abcd-ef00-01234567cffb
```

请注意，必须以大端字节顺序指定 UUID 中的前三个字符串。尽管发布的接口列表和协议分析工具通常以正确的字节顺序显示 UUID，但您可能需要在输入前重新排列 UUID 字节顺序。考虑以下所示的信使服务 UUID，在原始 ASCII 文本中，该 UUID 的前三个字符串有时可能会以小端字节顺序显示：

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

可以为 `dce_iface` 关键字指定这个相同的 UUID，方法是先插入连字符，然后以大端字节顺序放置前三个字符串，如下所示：

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

尽管一个 DCE/RPC 会话可能包含发向多个接口的请求，但在一个规则中只能包含一个 `dce_iface` 关键字。可创建其他规则来检测其他接口。

DCE/RPC 应用接口也有接口版本号。或者，可以指定带有运算符的接口版本，用该操作符指明版本是等于、不等于、小于还是大于指定值。

除了 TCP 分段或 IP 分片外，还可以对面向连接和无连接的 DCE/RPC 进行分片。通常，将任何 DCE/RPC 分片（第一个除外）与指定接口相关联没有任何作用，而且这样做可能导致大量误报。但是，为了提高灵活性，可以根据指定接口对所有分片进行评估。

下表总结了 `dce_iface` 关键字参数。

表 145：dce_iface 参数

参数	说明
Interface UUID	UUID（包括连字符），用于识别要在DCE/RPC流量中检测的特定服务的应用接口。与指定接口相关的任何请求将匹配接口 UUID。
版本	或者，可以选择应用接口版本号 0 到 65535 和一个操作符，以指明是否检测大于 (>)、小于 (<)、等于 (=) 或不等于 (!) 指定值的版本。
All Fragments	或者，可以选择匹配与 DCE/RPC 分片相关的所有接口和（如有指定）接口版本。默认情况下，此参数被禁用，表示关键字仅在第一个分片或整个未分片数据包与指定接口相关时才进行匹配。请注意，启用此参数可能会导致误报。

dce_opnum 关键字

可以将 dce_opnum 关键字和 DCE/RPC 预处理器结合使用，以检测识别 DCE/RPC 服务提供的一个或多个特定操作的数据包。

客户端功能调用请求特定服务函数（这些函数在DCE/RPC规范中称为操作）。操作编号 (opnum) 用于识别 DCE/RPC 报头中的特定操作。漏洞可能会针对特定操作。

例如，UUID 12345678-1234-ABCD-ef00-01234567cffb 识别用于 netlogon 服务的接口；该服务提供几十个不同的操作，其中之一是操作 6，NetrServerPasswordSet 操作。

应该在 dce_opnum 关键字前面加上 dce_iface 关键字，以识别操作的服务。

可以为特定操作指定一个 0 到 65535 之间的十进制值，可以指定一系列由连字符分隔的操作，或者指定逗号分隔的操作和范围列表，其中的操作和范围可按任何顺序排列。

以下任何示例都将指定有效的 netlogon 操作编号：

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data 关键字

可以将 dce_stub_data 关键字与 DCE/RPC 预处理器结合使用，以指定无论任何其他规则选项如何，规则引擎都应从存根数据的开头开始检查。紧跟在 dce_stub_data 关键字后面的数据包负载规则选项相对于存根数据缓冲区适用。

DCE/RPC 存根数据提供客户端程序调用和 DCE/RPC 运行时系统之间的接口，这种机制可提供对于 DCE/RPC 至关重要的例程和服务。DCE/RPC 漏洞在 DCE/RPC 数据包的存根数据部分中识别出。由于存根数据与特定的操作或函数调用相关，因此，应始终在 dce_stub_data 前面加上 dce_iface 和 dce_opnum，以识别相关的服务和操作。

dce_stub_data 关键字没有参数。

SIP 关键字

有四个 SIP 关键字可用于监控 SIP 会话流量的漏洞。

请注意，SIP 协议容易受到拒绝服务 (DoS) 攻击。基于速率的攻击防御可能对解决这类攻击的规则有利。

sip_header 关键字

可以使用 `sip_header` 关键字从提取的 SIP 请求或响应报头开头开始检查，并将检查限制为仅针对报头字段。

`sip_header` 关键字没有参数。

以下示例规则分片指向 SIP 报头并匹配 CSeq 报头字段：

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body 关键字

可以使用 `sip_body` 关键字在提取的 SIP 请求或响应消息正文开头开始检查，并将检查限制为仅针对消息正文。

`sip_body` 关键字没有参数。

以下示例规则分片指向 SIP 消息正文，并匹配所提取 SDP 数据的 c（连接信息）字段中的特定 IP 地址：

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

请注意，规则不仅限于搜索 SDP 内容。 SIP 预处理器将提取整个消息正文并使其可供规则引擎使用。

sip_method 关键字

每个 SIP 请求中的“方法”(*method)* 字段识别请求的目的。可以使用 `sip_method` 关键字测试特定方法的 SIP 请求。使用逗号隔开多种方法。

可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。可以使用逗号分隔多个方法。

由于将来可能会定义新的 SIP 方法，因此也可以指定自定义方法（即，当前未定义的 SIP 方法）。RFC 2616 中定义了接受的字段值，该规范允许除控制字符和分隔符（例如 `=`、`(` 和 `}`）以外的所有字符。有关排除的分隔符的完整列表，请参阅 RFC 2616。当系统在流量中遇到指定的自定义方法时，它将检查数据包报头，但不检查消息。

系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。请注意，总共有 32 种方法，包括使用 **Methods to Check** SIP 预处理器选项指定的方法。

如果使用否定形式，只能指定一种方法。例如：

```
!invite
```

但请注意，规则中的多个 `sip_method` 关键字与 **AND** 运算相关联。例如，为测试除 `invite` 和 `cancel` 以外的所有提取的方法，将会使用两个否定形式的 `sip_method` 关键字：

```
sip_method: !invite
sip_method: !cancel
```

思科建议在包含 sip_method 关键字的规则中至少包含一个 content 关键字，以确保规则引擎使用快速模式匹配程序，从而加快处理速度和提高性能。请注意，如果规则包含至少一个 content 关键字，无论是否启用 content 关键字的**使用快速模式匹配程序 (Use Fast Pattern Matcher)** 参数，规则引擎都会使用快速模式匹配程序。

sip_stat_code 关键字

每个SIP响应中的三位数状态代码指明请求操作的结果。您可以使用 sip_stat_code 关键字测试特定状态代码的 SIP 响应。

可以指定一个一位响应型数字（1 到 9）、一个特定的三位数（100 到 999）或者包含这两项的任意组合的逗号分隔列表。如果列表中的任何一个数字与 SIP 响应中的代码相匹配，则列表匹配。

下表介绍了可指定的 SIP 状态代码值。

表 *146*: *sip_stat_code* 值

要检测的内容	可指定的内容	示例	会检测的内容
特定状态代码	三位数状态代码	189	189
任何以指定一位数开始的三位数代码	一位数	1	1xx；即，100、101、102 等
值列表	以逗号分隔的特定代码与一位数的组合	222, 3	222 以及 300、301、302 等

另请注意，规则引擎不使用快速模式匹配程序搜索用 sip_stat_code 关键字指定的值，无论规则是否包含 content 关键字。

GTP 关键字

有三个 GSRP 隧道协议 (GTP) 关键字可用于检查 GTP 命令通道的 GTP 版本、消息类型和信息元素。GTP 关键字不可与其他入侵规则关键字（例如 content 或 byte_jump 关键字）结合使用。**必须**在使用 gtp_info 或 gtp_type 关键字的每个规则中使用 gtp_version 关键字。

gtp_version 关键字

可以使用 gtp_version 关键字检查 GTP 控制信息以确定 GTP 版本为 0、1 还是 2。

由于不同的 GTP 版本定义不同的信息类型和信息元素，因此，使用 gtp_type 或 gtp_info 关键字时必须同时使用 gtp_version。可以将值指定为 0、1 或 2。

gtp_type 关键字

每条 GTP 消息由一种消息类型标识，消息类型由一个数值和一个字符串组成。可以使用 gtp_type 关键字检查特定 GTP 消息类型的流量。由于不同的 GTP 版本定义不同的信息类型和信息元素，因此在使用 gtp_type 或 gtp_info 关键字时必须同时使用 gtp_version。

可以为消息类型指定定义的十进制值，可以指定定义的字符串，或者指定包含这两项的任意组合的逗号分隔列表，如以下示例所示：

```
10, 11, echo_request
```

系统使用 OR 操作来匹配列出的每个值或字符串。值和字符串的列出顺序并不重要。 列表中的任何一个值或字符串均与此关键字匹配。如果尝试保存包含无法识别的字符串或超出范围的值的规则，将会出现错误消息。

请注意，下表中不同的GTP版本有时会对同一种消息类型使用不同的值。例如，`sgsn_context_request` 这一消息类型在 GTPv0 和 GTPv1 中值是 50，但在 GTPv2 中值是 130。

`gtp_type` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在GTPv0或GTPv1数据包中，此关键字匹配消息类型值 50，在 GTPv2 数据包中，则匹配值 130。如果数据包中的消息类型值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为消息类型指定一个整数，则当关键字中的消息类型与GTP数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的为每种 GTP 消息类型定义的值和字符串。

表 *147*: *GTP* 消息类型

值	版本 0	版本 1	版本 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	不适用
5	node_alive_response	node_alive_response	不适用
6	redirection_request	redirection_request	不适用
7	redirection_response	redirection_response	不适用
16	create_pdp_context_request	create_pdp_context_request	不适用
17	create_pdp_context_response	create_pdp_context_response	不适用
18	update_pdp_context_request	update_pdp_context_request	不适用
19	update_pdp_context_response	update_pdp_context_response	不适用
20	delete_pdp_context_request	delete_pdp_context_request	不适用
21	delete_pdp_context_response	delete_pdp_context_response	不适用

值	版本 0	版本 1	版本 2
22	create_aa_pdp_context_request	init_pdp_context_activation_request	不适用
23	create_aa_pdp_context_response	init_pdp_context_activation_response	不适用
24	delete_aa_pdp_context_request	不适用	不适用
25	delete_aa_pdp_context_response	不适用	不适用
26	error_indication	error_indication	不适用
27	pdu_notification_request	pdu_notification_request	不适用
28	pdu_notification_response	pdu_notification_response	不适用
29	pdu_notification_reject_request	pdu_notification_reject_request	不适用
30	pdu_notification_reject_response	pdu_notification_reject_response	不适用
31	不适用	supported_ext_header_notification	不适用
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	不适用	不适用	change_notification_request
39	不适用	不适用	change_notification_response
48	identification_request	identification_request	不适用
49	identification_response	identification_response	不适用
50	sgsn_context_request	sgsn_context_request	不适用
51	sgsn_context_response	sgsn_context_response	不适用
52	sgsn_context_ack	sgsn_context_ack	不适用

值	版本 0	版本 1	版本 2
53	不适用	forward_relocation_request	不适用
54	不适用	forward_relocation_response	不适用
55	不适用	forward_relocation_complete	不适用
56	不适用	relocation_cancel_request	不适用
57	不适用	relocation_cancel_response	不适用
58	不适用	forward_srns_contex	不适用
59	不适用	forward_relocation_complete_ack	不适用
60	不适用	forward_srns_contex_ack	不适用
64	不适用	不适用	modify_bearer_command
65	不适用	不适用	modify_bearer_failure_indication
66	不适用	不适用	delete_bearer_command
67	不适用	不适用	delete_bearer_failure_indication
68	不适用	不适用	bearer_resource_command
69	不适用	不适用	bearer_resource_failure_indication
70	不适用	ran_info_relay	downlink_failure_indication
71	不适用	不适用	trace_session_activation
72	不适用	不适用	trace_session_deactivation
73	不适用	不适用	stop_paging_indication
95	不适用	不适用	create_bearer_request
96	不适用	mbms_notification_request	create_bearer_response
97	不适用	mbms_notification_response	update_bearer_request
98	不适用	mbms_notification_reject_request	update_bearer_response
99	不适用	mbms_notification_reject_response	delete_bearer_request

值	版本 0	版本 1	版本 2
100	不适用	create_mbms_context_request	delete_bearer_response
101	不适用	create_mbms_context_response	delete_pdn_request
102	不适用	update_mbms_context_request	delete_pdn_response
103	N/A	update_mbms_context_response	不适用
104	不适用	delete_mbms_context_request	不适用
105	N/A	delete_mbms_context_response	不适用
112	不适用	mbms_register_request	不适用
113	不适用	mbms_register_response	不适用
114	不适用	mbms_deregister_request	不适用
115	不适用	mbms_deregister_response	不适用
116	不适用	mbms_session_start_request	不适用
117	不适用	mbms_session_start_response	不适用
118	不适用	mbms_session_stop_request	不适用
119	不适用	mbms_session_stop_response	不适用
120	不适用	mbms_session_update_request	不适用
121	不适用	mbms_session_update_response	不适用
128	不适用	ms_info_change_request	identification_request
129	不适用	ms_info_change_response	identification_response
130	不适用	不适用	sgsn_context_request
131	不适用	不适用	sgsn_context_response
132	不适用	不适用	sgsn_context_ack
133	不适用	不适用	forward_relocation_request
134	不适用	不适用	forward_relocation_response

值	版本 0	版本 1	版本 2
135	不适用	不适用	forward_relocation_complete
136	不适用	不适用	forward_relocation_complete_ack
137	不适用	不适用	forward_access
138	不适用	不适用	forward_access_ack
139	不适用	不适用	relocation_cancel_request
140	不适用	不适用	relocation_cancel_response
141	不适用	不适用	configuration_transfer_tunnel
149	不适用	不适用	detach
150	不适用	不适用	detach_ack
151	不适用	不适用	cs_paging
152	不适用	不适用	ran_info_relay
153	不适用	不适用	alert_mme
154	不适用	不适用	alert_mme_ack
155	不适用	不适用	ue_activity
156	不适用	不适用	ue_activity_ack
160	不适用	不适用	create_forward_tunnel_request
161	不适用	不适用	create_forward_tunnel_response
162	不适用	不适用	suspend
163	不适用	不适用	suspend_ack
164	不适用	不适用	在如图所示的
165	不适用	不适用	resume_ack
166	不适用	不适用	create_indirect_forward_tunnel_request
167	不适用	不适用	create_indirect_forward_tunnel_response

值	版本 0	版本 1	版本 2
168	不适用	不适用	delete_indirect_forward_tunnel_request
169	不适用	不适用	delete_indirect_forward_tunnel_response
170	不适用	不适用	release_access_bearer_request
171	不适用	不适用	release_access_bearer_response
176	不适用	不适用	downlink_data
177	不适用	不适用	downlink_data_ack
179	不适用	不适用	pgw_restart
180	不适用	不适用	pgw_restart_ack
200	不适用	不适用	update_pdn_request
201	不适用	不适用	update_pdn_response
211	不适用	不适用	modify_access_bearer_request
212	不适用	不适用	modify_access_bearer_response
231	不适用	不适用	mbms_session_start_request
232	不适用	不适用	mbms_session_start_response
233	不适用	不适用	mbms_session_update_request
234	不适用	不适用	mbms_session_update_response
235	不适用	不适用	mbms_session_stop_request
236	不适用	不适用	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	不适用
241	data_record_transfer_response	data_record_transfer_response	不适用
254	不适用	end_marker	不适用
255	pdu	pdu	不适用

gtp_info 关键字

一条GTP消息可以包含多个信息元素，其中的每一个元素均由已定义的一个数值和一个字符串来识别。可以使用 `gtp_info` 关键字在指定的信息元素开头开始检查，并将检查限于指定的信息元素。由于不同的GTP版本定义不同的消息类型和信息元素，因此在使用此关键字时还必须使用 `gtp_version`。

可以为信息元素指定已定义的十进制值或字符串。可以指定一个值或字符串，也可以在一个规则中使用多个 `gtp_info` 关键字来检查多个信息元素。

如果一条消息包含相同类型的多个信息元素，将会全部检查这些元素来进行匹配。如果信息元素按无效顺序出现，将仅检查最后一个实例。

请注意，不同的GTP版本有时对同一个信息元素使用不同的值。例如，`cause` 信息元素在GTPv0和GTPv1中值为1，但在GTPv2中值为2。

`gtp_info` 关键字匹配不同的值，具体取决于数据包中的版本号。在上述示例中，在GTPv0或GTPv1数据包中，此关键字匹配信息元素值1，在GTPv2数据包中，则匹配值2。如果数据包中的信息元素值不是在数据包中指定的版本的已知值，此关键字不会匹配数据包。

如果为信息元素指定一个整数，则当关键字中的消息类型与GTP数据包中的该值匹配时，关键字将会匹配，无论数据包中指定的版本如何。

下表列出了系统识别出的每个GTP信息元素的值和字符串。

表 *148*: *GTP* 信息元素

值	版本 0	版本 1	版本 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	恢复
4	tlli	tlli	不适用
5	p_tmsi	p_tmsi	不适用
6	qos	不适用	不适用
8	recording_required	recording_required	不适用
9	authentication	authentication	不适用
11	map_cause	map_cause	不适用
12	p_tmsi_sig	p_tmsi_sig	不适用
13	ms_validated	ms_validated	不适用
14	恢复	恢复	不适用

值	版本 0	版本 1	版本 2
15	selection_mode	selection_mode	不适用
16	flow_label_data_1	teid_1	不适用
17	flow_label_signalling	teid_control	不适用
18	flow_label_data_2	teid_2	不适用
19	ms_unreachable	teardown_ind	不适用
20	不适用	nsapi	不适用
21	不适用	ranap	不适用
22	不适用	rab_context	不适用
23	不适用	radio_priority_sms	不适用
24	不适用	radio_priority	不适用
25	不适用	packet_flow_id	不适用
26	不适用	charging_char	不适用
27	不适用	trace_ref	不适用
28	不适用	trace_type	不适用
29	不适用	ms_unreachable	不适用
71	不适用	不适用	apn
72	不适用	不适用	ambr
73	不适用	不适用	ebi
74	不适用	不适用	ip_addr
75	不适用	不适用	mei
76	不适用	不适用	msisdn
77	不适用	不适用	indication
78	不适用	不适用	pco

值	版本 0	版本 1	版本 2
79	不适用	不适用	paa
80	不适用	不适用	bearer_qos
80	不适用	不适用	flow_qos
82	不适用	不适用	rat_type
83	不适用	不适用	serving_network
84	不适用	不适用	bearer_tft
85	不适用	不适用	tad
86	不适用	不适用	uli
87	不适用	不适用	f_teid
88	不适用	不适用	tmsi
89	不适用	不适用	cn_id
90	不适用	不适用	s103pdf
91	不适用	不适用	s1udf
92	不适用	不适用	delay_value
93	不适用	不适用	bearer_context
94	不适用	不适用	charging_id
95	不适用	不适用	charging_char
96	不适用	不适用	trace_info
97	不适用	不适用	bearer_flag
99	不适用	不适用	pdn_type
100	不适用	不适用	pti
101	不适用	不适用	drx_parameter
103	不适用	不适用	gsm_key_tri

值	版本 0	版本 1	版本 2
104	不适用	不适用	umts_key_cipher_quin
105	不适用	不适用	gsm_key_cipher_quin
106	不适用	不适用	umts_key_quin
107	不适用	不适用	eps_quad
108	不适用	不适用	umts_key_quad_quin
109	不适用	不适用	pdn_connection
110	不适用	不适用	pdn_number
111	不适用	不适用	p_tmsi
112	不适用	不适用	p_tmsi_sig
113	不适用	不适用	hop_counter
114	不适用	不适用	ue_time_zone
115	不适用	不适用	trace_ref
116	不适用	不适用	complete_request_msg
117	不适用	不适用	guti
118	不适用	不适用	f_container
119	不适用	不适用	f_cause
120	不适用	不适用	plmn_id
121	不适用	不适用	target_id
123	不适用	不适用	packet_flow_id
124	不适用	不适用	rab_contex
125	不适用	不适用	src_rnc_pdcp
126	不适用	不适用	udp_src_port
127	charge_id	charge_id	apn_restriction

值	版本 0	版本 1	版本 2
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	不适用
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	信道
134	msisdn	msisdn	emlpp_pri
135	不适用	qos	node_type
136	不适用	authentication_qu	fqdn
137	不适用	tft	ti
138	不适用	target_id	mbms_session_duration
139	不适用	utran_trans	mbms_service_area
140	不适用	rab_setup	mbms_session_id
141	不适用	ext_header	mbms_flow_id
142	不适用	trigger_id	mbms_ip_multicast
143	不适用	omc_id	mbms_distribution_ack
144	不适用	ran_trans	rfsp_index
145	不适用	pdp_context_pri	uci
146	不适用	addi_rab_setup	csg_info
147	不适用	sgsn_number	csg_id
148	不适用	common_flag	cmi
149	不适用	apn_restriction	service_indicator
150	不适用	radio_priority_lcs	detach_type

值	版本 0	版本 1	版本 2
151	不适用	rat_type	ldn
152	不适用	user_loc_info	node_feature
153	不适用	ms_time_zone	mbms_time_to_transfer
154	不适用	imei_sv	throttling
155	不适用	camel	ARP
156	不适用	mbms_ue_context	epc_timer
157	不适用	tmp_mobile_group_id	signalling_priority_indication
158	不适用	rim_routing_addr	tmgi
159	不适用	mbms_config	mm_srvcc
160	不适用	mbms_service_area	flags_srvcc
161	不适用	src_rnc_pdcp	nmbr
162	不适用	addi_trace_info	不适用
163	不适用	hop_counter	不适用
164	不适用	plmn_id	不适用
165	不适用	mbms_session_id	不适用
166	不适用	mbms_2g3g_indicator	不适用
167	不适用	enhanced_nsapi	不适用
168	不适用	mbms_session_duration	不适用
169	不适用	addi_mbms_trace_info	不适用
170	不适用	mbms_session_repetition_num	不适用
171	不适用	mbms_time_to_data	不适用
173	不适用	bss	不适用
174	不适用	cell_id	不适用

值	版本 0	版本 1	版本 2
175	不适用	pdu_num	不适用
177	不适用	mbms_bearer_capab	不适用
178	不适用	rim_routing_disc	不适用
179	不适用	list_pfc	不适用
180	不适用	ps_xid	不适用
181	不适用	ms_info_change_report	不适用
182	不适用	direct_tunnel_flags	不适用
183	不适用	correlation_id	不适用
184	不适用	bearer_control_mode	不适用
185	不适用	mbms_flow_id	不适用
186	不适用	mbms_ip_multicast	不适用
187	不适用	mbms_distribution_ack	不适用
188	不适用	reliable_inter_rat_handover	不适用
189	不适用	rfsp_index	不适用
190	不适用	fqdn	不适用
191	不适用	evolved_allocation1	不适用
192	不适用	evolved_allocation2	不适用
193	不适用	extended_flags	不适用
194	不适用	uci	不适用
195	不适用	csg_info	不适用
196	不适用	csg_id	不适用
197	不适用	cmi	不适用
198	不适用	apn_ambr	不适用

值	版本 0	版本 1	版本 2
199	不适用	ue_network	不适用
200	不适用	ue_ambr	不适用
201	不适用	apn_ambr_nsapi	不适用
202	不适用	ggsn_backoff_timer	不适用
203	不适用	signalling_priority_indication	不适用
204	不适用	signalling_priority_indication_nsapi	不适用
205	不适用	high_bitrate	不适用
206	不适用	max_mbr	不适用
251	charging_gateway_addr	charging_gateway_addr	不适用
255	private_extension	private_extension	private_extension

SCADA 关键字

规则引擎使用 Modbus 和 DNP3 规则访问某些协议字段。

Modbus 关键字

可以单独使用 Modbus 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

modbus_data

可以使用 `modbus_data` 关键字指向 Modbus 请求或响应中 Data 字段的开头。

modbus_func

可以使用 `modbus_func` 关键字来匹配 Modbus 应用层请求或响应报头中的“函数代码”(Function Code) 字段。可以为 Modbus 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 Modbus 函数代码定义的值和字符串。

表 *149*: *Modbus* 函数代码

值	字符串
1	read_coils

值	字符串
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

modbus_unit

可以使用 `modbus_unit` 关键字来匹配 Modbus 请求或响应报头中的 Unit ID 字段。

DNP3 关键字

可以单独使用 DNP3 关键字，也可以将它与其他关键字（例如 `content` 和 `byte_jump` 关键字）结合使用。

dnp3_data

可以使用 `dnp3_data` 关键字指向重组 DNP3 应用层分片的开头。

DNP3 预处理器将链路层帧重组到应用层分片中。`dnp3_data` 关键字指向每个应用层分片的开头；其他规则选项可匹配分片中的重组数据，而无需每 16 个字节分隔数据并添加校验和。

dnp3_func

可以使用 `dnp3_func` 关键字来匹配 DNP3 应用层请求或响应报头中的 Function Code 字段。可以为 DNP3 函数代码指定一个已定义的十进制值或一个已定义的字符串。

下表列出了系统识别出的为 DNP3 函数代码定义的值和字符串。

表 *150*: *DNP3* 函数代码

值	字符串
0	confirm
1	read
2	write
3	选择
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl

值	字符串
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	效率低下
130	unsolicited_response
131	authenticate_resp

dnp3_ind

可以使用 `dnp3_ind` 关键字来匹配 DNP3 应用层响应报头中 Internal Indications 字段中的标志。可以为一个已知标志指定一个字符串，也可以指定以逗号分隔的标志列表，如以下示例所示：

```
class_1_events, class_2_events
```

如果指定多个标志，此关键字将会匹配列表中的任意标志。要检测标志组合，可在一个规则中多次使用 dnp3_ind 关键字。

以下列表提供了系统识别出的用于已定义的 DNP3 内部指示标志的字符串语法。

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

可以使用 dnp3_obj 关键字来匹配请求或响应中的 DNP3 对象报头。

DNP3 数据由一系列不同类型的 DNP3 对象组成，例如模拟输入、二进制输入，等等。每种类型均以组进行识别，例如模拟输入组、二进制输入组等，每个组均可由一个十进制值进行识别。每个组中的对象均以对象变体进一步识别，例如 16 位整数、32 位整数、短浮点等，每个这些变体均指定对象的数据格式。每种类型的对象变体也可以十进制值进行识别。

可以通过为对象报头组和类型和对象变体类型分别指定一个十进制数值来识别对象报头。这两种类型的组合可定义特定类型的 DNP3 对象。

数据包特征

可以编写只针对具有特定特征的数据包生成事件的规则。

dsize

dsize 关键字测试数据包负载大小。使用此关键字时，可以用大于号和小于号（< 和 >）指定值的范围。可以使用以下语法来指定范围：

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

例如，要表示大于 400 字节的数据包大小，请使用 >400 作为 dtype 值。要表示小于 500 字节的数据包大小，请使用 <500。要指定规则针对介于 400 到 500 字节（包括 400 和 500 字节）的任何数据包触发，请使用 400<>500。

注意 dsize 关键字测试未经任何预处理器解码的数据包。

isdataat

isdataat 关键字指示规则引擎验证数据是否驻留在负载中的特定位置。

下表列出了可与 isdataat 关键字配合使用的参数。

表 151：*isdataat* 参数

参数	类型	说明
Offset	必要	负载中的特定位置。例如，要测试显示在数据包负载中第 50 个字节处的数据，需要指定 50 作为偏移值。! 修饰符对 isdataat 测试的结果进行求反；如果负载中不存在一定的数据量，则会发出警报。 您也可以使用现有 byte_extract 变量指定此参数的值。
Relative	可选	使位置相对于上一次成功内容匹配。指定相对位置时请注意，计数器从字节 0 开始计算，因此，应该如下计算相对位置：用从上一次成功内容匹配起向前计算所需的字节数减去 1。例如，要指定数据必须显示在上一次成功内容匹配后的第九个字节处，需要将相对偏移量指定为 8。
Raw Data	可选	指定数据在由任何 Firepower 系统预处理器进行解码或应用层规范化之前位于原始数据包负载中。如果上一次内容匹配出现在原始数据包数据中，可以将此参数与 **Relative** 结合使用。

例如，在查找内容 foo 的规则搜索中，如果如下指定 isdataat 的值：

- Offset = !10
- Relative 已启用

那么，如果规则引擎在负载结束前未能在 foo 之后检测到 10 字节，系统将会发出警报。

sameip

sameip 关键字测试数据包的源 IP 地址和目标 IP 地址是否相同。此关键字没有参数。

fragoffset

fragoffset 关键字测试分片数据包的偏移量。由于某些漏洞（例如，WinNuke 拒绝服务攻击）使用手动生成的具有特定偏移量的数据包分片，因此，此关键字很有用。

例如，要测试分片数据包的偏移量是否为 31337 字节，应指定 31337 作为 fragoffset 的值。

为 fragoffset 关键字指定参数时，可以使用以下运算符。

表 152：*fragoffset* 关键字参数运算符

Operator	说明
!	要
>	大于

Operator	说明
<	小于

请注意，不能将 not (!) 运算符与 < 或 > 结合使用。

cvs

cvs 关键字测试并发版本系统 (CVS) 流量中是否存在格式不正确的 CVS 条目。攻击者可以使用格式不正确的条目来强制堆溢出，并且在CVS服务器上执行恶意代码。此关键字可用于识别针对两种已知 CVS 漏洞的攻击：CVE-2004-0396（CVS1.11.x 至 1.11.15，以及 CVS1.12.x 至 1.12.7）和 CVS-2004-0414（CVS1.12.x 至 1.12.8，以及 CVS1.11.x 至 1.11.16）。cvs 关键字检查格式正确的记录，如果检测到格式不正确的条目，将会发出警报。

规则应包含 CVS 运行所在的端口。此外，应将任何可能出现流量的端口添加到 TCP 策略的数据流重组端口列表，以便为 CVS 会话维护状态。TCP 端口 2401 (pserver) 和 514 (rsh) 包含在出现数据流重组的客户端端口列表中。但请注意，如果服务器作为 xinetd 服务器（即，pserver）运行，它可以在任何 TCP 端口上运行。应将任何非标准端口添加到数据流重组 **Client Ports** 列表中。

活动响应关键字

系统可以发起活动响应，以在响应触发的 TCP 规则时关闭 TCP连接，或者在响应触发的 UDP 规则时关闭UDP会话。有两个关键字提供了两种不同的活动响应发起方法。如果数据包触发包含这两个关键字当中的任何一个，系统将发起单一活动响应。您还可以使用 config response 命令配置活动响应接口以及要在被动部署中尝试的 TCP 重置次数。

活动响应在内联部署中最有效，因为重置更有可能及时到达以影响连接或会话。例如，在内联部署中对 react 关键字作出响应时，系统会为连接的两端将 TCP 重置 (RST) 数据包直接插入到流量中（正常情况下，这样应该会关闭连接）。

出于一些原因，活动响应并不用于取代防火墙；这些原因包括：系统不能在被动部署中插入数据包；攻击者可能已选择忽略或绕过活动响应。

由于活动响应可以回送，因此，系统不允许TCP重置发起TCP重置；这样可防止活动响应出现无穷尽的顺序。此外，为了符合标准做法，系统也不允许ICMP不可达数据包发起ICMP不可达数据包。

可以配置 TCP 数据流预处理器，使它在入侵规则触发了活动响应后检测连接或会话的其他流量。如果预处理器检测到其他流量，它会将指定最大数量的其他活动响应发送到连接或会话的两端。

resp 关键字

可以使用 resp 关键字来主动响应 TCP 连接或 UDP 会话，具体取决于在规则报头中指定的是 TCP 还是 UDP 协议。

使用关键字参数可指定数据包方向，以及指定是使用 TCP 重置 (RST) 数据包还是 ICMP 不可达数据包作为活动响应。

可以使用任何 TCP 重置或 ICMP 不可达参数来关闭 TCP 连接。只能使用 ICMP 不可达参数来关闭 UDP 会话。

此外，不同的TCP重置参数使得可以将数据包源和/或目标作为活动响应的目标。所有ICMP不可达参数都将数据包源作为目标，并且允许指定是使用ICMP网络、主机还是端口的不可达数据包，还是同时使用这三者的不可达数据包。

下表列出可与`resp`关键字结合使用以明确指定希望Firepower系统在规则触发时采取的操作的参数。

表 153：*resp* 参数

参数	说明
reset_source	将TCP重置数据包引至发送触发规则的数据包的终端。此外，可以指定`rst_snd`（为了获得向后兼容性，仍支持使用此参数）。
reset_dest	将TCP重置数据包引至触发规则的数据包的预期目标终端。此外，可以指定`rst_rcv`（为了获得向后兼容性，仍支持使用此参数）。
reset_both	将TCP重置数据包引至发送终端和接收终端。此外，可以指定`rst_all`（为了获得向后兼容性，仍支持使用此参数）。
icmp_net	将ICMP网络不可达消息引至发送方。
icmp_host	将ICMP主机不可达消息引至发送方。
icmp_port	将ICMP端口不可达消息引至发送方。此参数用于终止UDP流量。
icmp_all	将以下ICMP消息引至发送方： • 网络不可达消息 • 主机不可达消息 • 端口不可达消息

例如，要将规则配置为会在规则触发时重置连接的两端，可使用`reset_both`作为`resp`关键字的值。

可以使用逗号分隔列表指定多个参数，如下所示：

```
argument,argument,argument
```

可以使用`config response`命令配置要使用的活动响应接口以及要在被动部署中尝试的TCP重置次数。

react 关键字

如果数据包触发规则，您可以使用`react`关键字将默认HTML页面发送到TCP连接客户端；发送HTML页面后，系统将使用TCP重置数据包来发起对连接两端的活动响应`react`关键字不会对UDP流量触发活动响应。

或者，可以指定以下参数：

`msg`
如果数据包触发使用 `msg` 参数的 `react` 规则，HTML 页面将包含规则事件消息。

如果未指定 `msg` 参数，HTML 页面将包含以下消息：

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

注释 由于活动响应可以回送，因此，请确保 HTML 响应页面不会触发 `react` 规则；否则，可能会导致活动响应出现无穷尽的顺序。思科建议在生产环境中激活 `react` 规则之前先对其进行广泛测试。

可以使用 `config response` 命令配置要使用的活动响应接口以及要在被动部署中尝试的 TCP 重置次数。

config response 命令

可以使用 **config response** 命令进一步配置由 `resp` 和 `react` 规则发起的 TCP 重置的行为。此命令还会影响丢弃规则发起的活动响应的行为。

要使用 **config response** 命令，可以在 USER_CONF 高级变量中的单独一行插入此命令。

在 USER_CONF 高级变量中的单独一行插入 `config response` 命令的一种形式，如下所示：

- 要仅指定活动响应重置尝试次数，请插入以下命令：

  `config response: attempts`att

  例如：`config response: attempts 10`

- 要仅指定活动响应界面，请插入以下命令：

  `config response: device`dev

  例如：`config response: device eth0`

- 要指定活动响应重置尝试次数和活动响应界面，请插入以下命令：

  `config response: attempts`att, `device`dev

  其中：

  att 是尝试次数（1 到 20），每个 TCP 重置数据包在达到指定的尝试次数后，就会停留在当前连接窗口，以使接收主机接受该数据包。这种扫射式序列仅对被动部署有用；在内联部署中，系统会将重置数据包直接插入到数据流中，而不是触发数据包。系统只会发送 1 个 ICMP 可达活动响应。

  dev 为备用接口，您希望系统在被动部署中使用该接口发送活动响应，或者在内联部署中在该接口处插入活动响应。

  例如：`config response: attempts 10, device eth0`

注意 请**勿**使用高级变量 `USER_CONF` 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

detection_filter 关键字

可以使用 `detection_filter` 关键字来防止某个规则生成事件，除非在指定时间内有指定数量的数据包触发该规则。这样可防止规则过早生成事件。例如，在几秒钟内登录失败两三次可能是预期行为，但在同一时间内出现大量登录尝试可能表示存在蛮力攻击。

`detection_filter` 关键字需要使用参数来定义系统是否跟踪源或目标 IP 地址、满足检测条件多少次后才会触发事件以及持续计数多长时间。

可使用以下语法延迟事件触发：

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 参数指定在计算符合规则检测条件的数据包数量时，是否使用数据包的源或目标 IP 地址。可选择下表中所述的参数值来指定系统如何跟踪事件实例。

表 *154*：*detection_filter* 跟踪参数

参数	说明
by_src	按源 IP 地址计算检测条件。
by_dst	按目标 IP 地址计算检测条件。

`count` 参数指定要使某个规则生成事件，在指定时间内必须有多少数据包为指定 IP 地址触发该规则。

`seconds` 参数指定要使某个规则生成事件，必须在多少秒内有指定数量的数据包触发该规则。

假设某个规则在数据包中搜索内容 `foo`，并将以下参数与 `detection_filter` 关键字配合使用：

```
track by_src, count 10, seconds 20
```

在此示例中，规则在 20 秒内从来自给定 IP 地址的 10 个数据包中检测到 `foo` 后才会生成事件。如果系统在头 20 秒内仅检测到有 7 个数据包包含 `foo`，将不会生成事件。 但是，如果在头 20 秒内 `foo` 出现 40 次，规则将会生成 30 个事件，并在 20 秒后再次进行计数。

比较 threshold 和 detection_filter 关键字

`detection_filter` 关键字取代已被弃用的 `threshold` 关键字。但是，为了获得向后兼容性，仍支持使用 `threshold` 关键字，其作用与您在入侵策略中设置的阈值相同。

`detection_filter` 关键字是一种检测功能，适合在数据包触发规则前使用。在达到指定的数据包数量之前，规则不会针对触发检测到的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，在达到指定的数据包数量之前，规则不会丢弃数据包。相反，规则会针对会触发规则且在达到指定数据包数量后出现的数据包生成事件；在内联部署中，如果规则设置为丢弃数据包，规则将会丢弃数据包。

阈值是一种事件通知功能，不会造成检测操作。此功能适合在数据包触发事件后使用。在内联部署中，被设置为丢弃数据包的规则将会丢弃触发其本身的所有数据包，无论规则阈值如何。

请注意，可以在入侵策略中使用使用 `detection_filter` 关键字与入侵事件阈值、入侵事件抑制和基于速率的攻击防御等功能的任意组合。另请注意，如果启用某个导入的本地规则，而该规则将弃用的 `threshold` 关键字与某个入侵策略中的入侵事件阈值功能结合起来使用，策略验证将会失败。

tag 关键字

使用 `tag` 关键字可指示系统记录主机或会话的其他流量。使用 `tag` 关键字指定要捕获的流量的类型和数量时，可使用以下语法：

```
tagging_type, count, metric, optional_direction
```

以下三个表介绍了其他可用参数。

有两种标记类型可供选择。下表介绍这两种标记类型。请注意，如果在入侵规则中仅配置规则报头选项，则会话标签参数类型会使系统像记录来自不同会话的数据包一样记录来自同一会话的数据包。要将来自同一会话的数据包分组在一起，请在同一入侵规则中配置一个或多个规则选项（例如，`flag` 关键字或 `content` 关键字）。

表 *155*：标记参数

参数	说明
session	记录触发规则的会话中的数据包。
host	记录来自发送触发规则的数据包的主机的数据包。可以添加方向修饰符，以仅记录来自主机 (`src`) 或发送到主机 (`dst`) 的流量。

要指明想要记录的流量数量，请使用以下参数：

表 *156*：计数参数

参数	说明
count	您想在规则触发后记录的数据包数量或秒数。 此度量单位用指标参数指定（该参数跟在计数参数后面）。

选择下表中所述的其中一个指标，以指明是要按时间还是流量数量进行记录。

注意 高带宽网络可以每秒查看成千上万个数据包，而且对大量数据包进行标记可能会严重影响性能，因此，请务必根据网络环境调整设置。

表 *157*：日志记录指标参数

参数	说明
数据包	在规则触发后记录计数指定的数量的数据包。
seconds	在规则触发后在计数指定的秒数内记录流量。

例如，如果带有以下 `tag` 关键字值的规则触发：

```
host, 30, seconds, dst
```

将会记录在接下来的 30 秒内从客户端传输到主机的所有数据包。

flowbits 关键字

可以使用 `flowbits` 关键字为会话分配状态名称。通过根据之前命名的状态分析会话中的后续数据包，系统可以检测在一个会话中跨越多个数据包的攻击，并发出有关警报。

`flowbits` 状态名称是用户定义的标签，将被分配给会话特定部分中的数据包。可以根据数据包内容给数据包分配状态名称标签，以帮助将恶意数据包和那些您不想对其发出警报的数据包区分开。最多可以为每个受管设备定义1024个状态名称。例如，如果要对您知道仅在成功登录后才会出现的恶意数据包发出警报，可以使用 `flowbits` 关键字过滤掉构成初始登录尝试的数据包，这样就能够重点关注恶意数据包。要这样做，首先要创建一个会给具有状态为 `logged_in` 的已建立登录的会话中的所有数据包分配标签的规则，然后创建另一个包含 `flowbits` 的规则，用以检查具有您在第一个规则中设置的状态的数据包，并且只对这些数据包采取操作。

可选的组名称用于向状态组添加状态名称。一个状态名称可以属于若干个组。未与组关联的状态并不相互排斥，因此，触发和设置未与组关联的状态的规则不会影响其他同时设置的状态。

flowbits 关键字选项

下表介绍了可用于 `flowbits` 关键字的运算符、状态和组的各种组合。请注意，状态名称可以包含字母数字字符、句号 (.)、下划线 (_) 和破折号 (-)。

表 *158*：*flowbits* 选项

Operator	状态选项	Group	说明
set	state_name	可选	为数据包设置某个指定状态。如果定义了某个组，则在该指定的组中设置该状态。
set	state_name&state_name	可选	为数据包设置多个指定状态。如果定义了某个组，则在该指定的组中设置这些状态。
setx	state_name	必需	为数据包在指定组中设置某个指定状态，并取消设置该组中的所有其他状态。
setx	state_name&state_name	必需	为数据包在指定组中设置多个指定状态，并取消设置该组中的所有其他状态。
unset	state_name	没有组	为数据包取消设置某个指定状态。
unset	state_name&state_name	没有组	为数据包取消设置多个指定状态。
unset	all	必需	取消设置指定组中的所有状态。
toggle	state_name	没有组	取消设置某个指定状态（如果已设置），以及设置某个指定状态（如果未设置）。
toggle	state_name&state_name	没有组	取消设置多个指定状态（如果已设置），以及设置多个指定状态（如果未设置）。
toggle	all	必需	取消设置指定组中已设置的所有状态，以及设置指定组中未设置的所有状态。
isset	state_name	没有组	确定是否已在数据包中设置了某个指定状态。
isset	state_name&state_name	没有组	确定是否已在数据包中设置了多个指定状态。
isset	state_name|state_name	没有组	确定是否已在数据包中设置了任何指定状态。
isset	any	必需	确定是否已在指定组中设置了任何状态。
isset	all	必需	确定是否已在指定组中设置了所有状态。
isnotset	state_name	没有组	确定是否未在数据包中设置某个指定状态。
isnotset	state_name&state_name	没有组	确定是否未在数据包中设置多个指定状态。
isnotset	state_name|state_name	没有组	确定是否未在数据包中设置任何指定状态。

Operator	状态选项	Group	说明
isnotset	any	必需	确定是否未在数据包中设置任何状态。
isnotset	all	必需	确定是否未在数据包中设置所有状态。
reset	（无状态）	可选	为所有数据包取消设置所有状态。取消设置某个组中的所有状态（如果已指定该组）。
noalert	（无状态）	没有组	可将此运算符与任何其他运算符结合使用，以抑制事件生成。

flowbits 关键字使用准则

使用 flowbits 关键字时，请注意：

- 使用 setx 运算符时，指定的状态只能属于指定的组，而不能属于任何其他组。
- 可以多次定义 setx 操作符，每次用一个实例指定不同的状态和同一个组。
- 如果使用 setx 运算符并指定了某个组，则不能对该指定的组使用 set、toggle 或 unset 运算符。
- isset 和 isnotset 运算符会对指定状态进行评定，无论该状态是否在组中。
- 保存入侵策略、重新应用入侵策略以及应用访问控制策略时（不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果您启用包含**未**指定组的 isset 或 isnotset 运算符的一个规则，而且您不会为对应的状态名称和协议启用至少一个会影响 flowbits 分配的规则（set、setx、set、toggle），那么，将会启用会影响对应状态名称的 flowbits 分配的所有规则。
- 保存入侵策略、重新应用入侵策略以及应用访问控制策略时（不管访问控制策略是引用一个入侵策略还是多个入侵策略），如果您启用包含**已**指定组的 isset 或 isnotset 运算符的一个规则，系统还将会启用会影响 flowbits 分配（set、setx、unset、toggle）且定义对应组名称的所有规则。

flowbits 关键字示例

本节提供三个使用 flowbits 关键字的示例。

flowbits 关键字示例：使用 *state_name* 的配置

这是使用 state_name 的 flowbits 配置的示例。

以 Bugtraq ID #1110 中所述的 IMAP 漏洞为例。该漏洞存在于 IMAP 的实现中，尤其是在 LIST、LSUB、RENAME、FIND 和 COPY 命令中。但是，要想利用该漏洞，攻击者必须登录到 IMAP 服务器。由于来自 IMAP 服务器的登录确认及紧随着而来的漏洞必定存在于不同的数据包中，因此，难以构建非基于流量的规则来捕获该漏洞。通过使用 flowbits 关键字，可以构建一系列规则来跟踪用

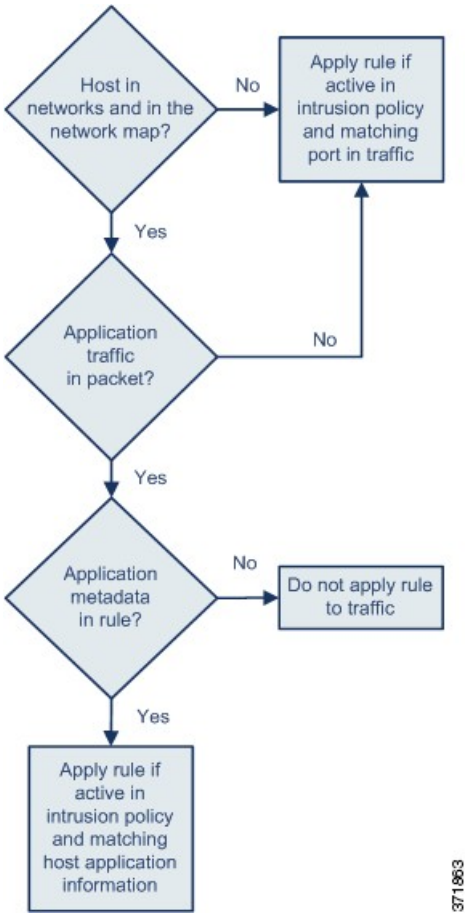
户是否登录 IMAP 服务器；如果已登录，则在检测到其中一项攻击时生成事件。如果用户未登录，则攻击不能利用该漏洞，且不会生成事件。

以下两个规则分片说明了此示例。第一个规则分片查找来自 IMAP 服务器的 IMAP 登录确认：

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：



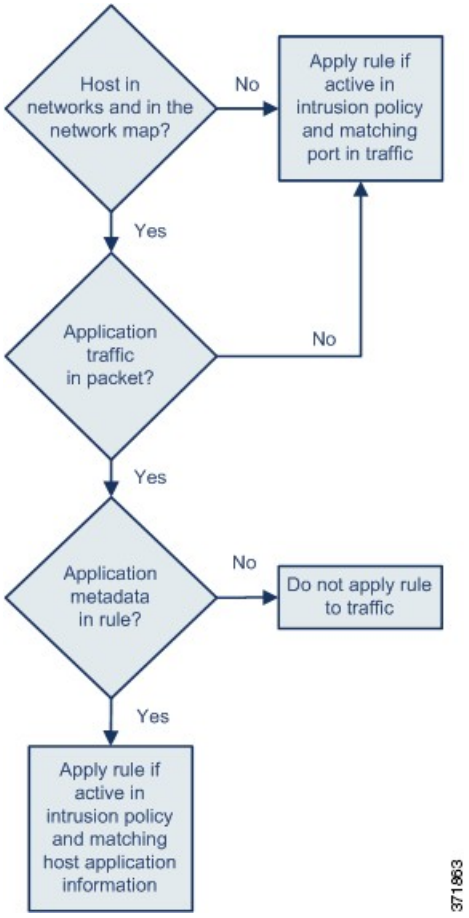
请注意，`flowbits:set` 设置 `logged_in` 状态，`flowbits:noalert` 则抑制警报，因为 IMAP 服务器上可能会出现许多无恶意的登录会话。

以下规则分片查找LIST字符串，但不生成事件，除非由于会话中某个之前的数据包而设置了logged_in状态：

```
alert tcp any any -> any 143 (msg:"IMAP LIST";

content:"LIST"; flowbits:isset,logged_in;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：



在这种情况下，如果之前的数据包已促使包含第一个分片的规则触发，则包含第二个分片的规则将会触发并生成事件。

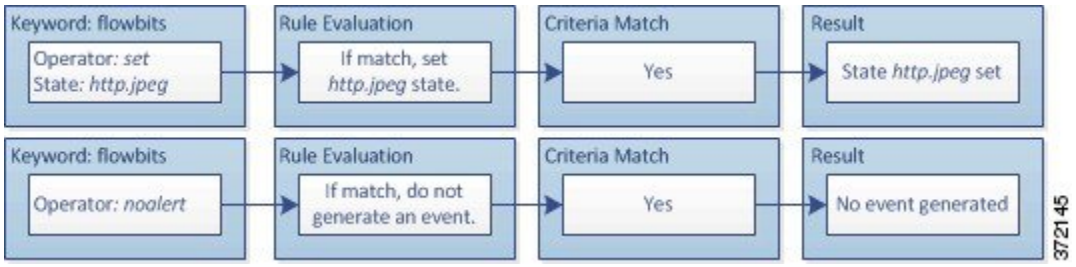
flowbits 关键字示例：导致误报事件的配置

在一个组中包含在不同规则中设置的不同状态名称可防止误报事件；如果后续数据包中的内容与状态不再有效的规则相匹配，就会出现误报事件。以下示例说明不在一个组中包含多个状态名称如何会导致误报。

假设以下三个规则分片在一个会话中按所示的顺序触发：

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：

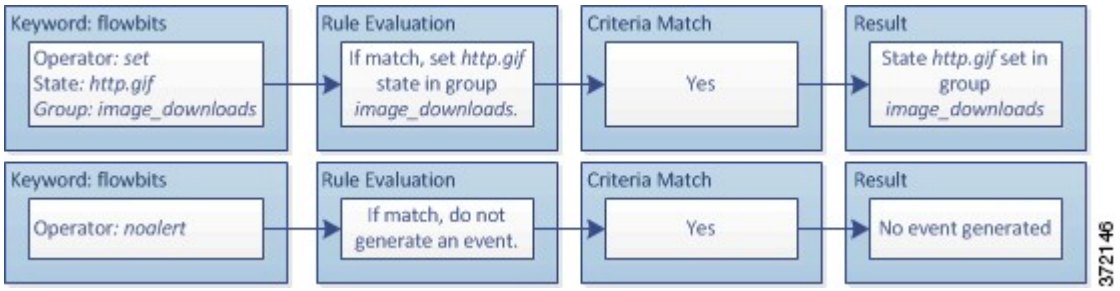


第一个规则分片中的 content 和 pcre 关键字与 JPEG 文件下载相匹配，flowbits:set,http.jpeg 设置 http.jpeg flowbits 状态，flowbits:noalert 阻止规则生成事件。将不会生成事件，因为该规则的目的是检测文件下载并设置 flowbits 状态；为此，一个或多个伴随规则可以测试状态名称和恶意内容，如果检测到恶意内容，将会生成事件。

以下规则分片检测在上述 JPEG 文件下载之后发生的 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

下图展示前述规则分片中 flowbits 关键字的影响：

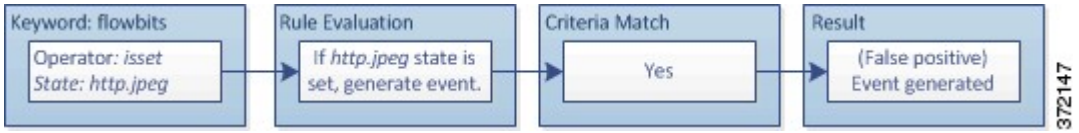


第二个规则中的 content 和 pcre 关键字与 GIF 文件下载相匹配，flowbits:set,http.jpg 设置 http.jpg flowbit 状态，flowbits:noalert 阻止规则生成事件。请注意，仍会设置由第一个规则分片设置的 http.jpeg 状态，即使不再需要使用它；这是因为如果检测到后续 GIF 下载，JPEG 下载必须终止。

第三个规则分片伴随第一个规则分片出现：

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图展示前述规则分片中 flowbits 关键字的影响：



在第三个规则分片中，flowbits:isset,http.jpeg 确定是否已设置现在不相关的 http.jpeg 状态，content 和 pcre 则匹配在 JPEG 文件中是恶意的但在 GIF 文件中并非恶意的内容。第三个规则分片会针对 JPEG 文件中不存在漏洞生成误报事件。

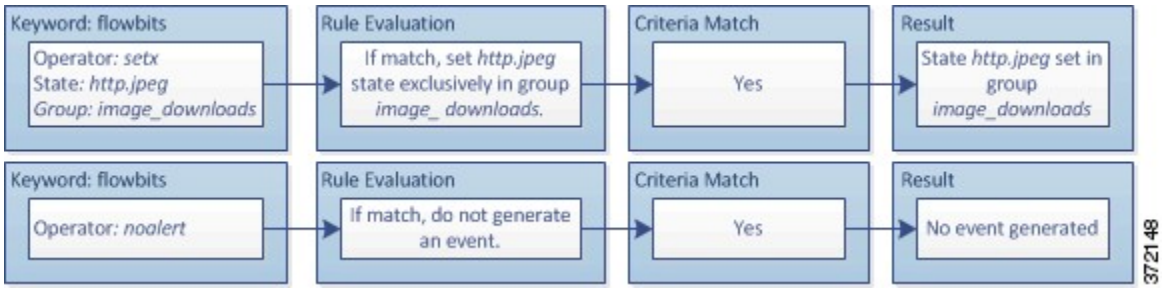
flowbits 关键字示例：防止误报事件的配置

以下示例说明在一个组中包含多个状态名称并使用 setx 运算符如何能防止误报。

以下规则分片与上一个规则分片示例大致相同，不同之处是，以下示例的前两个规则将两个不同的状态名称包含在同一个状态组中。

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

下图展示前述规则分片中 flowbits 关键字的影响：

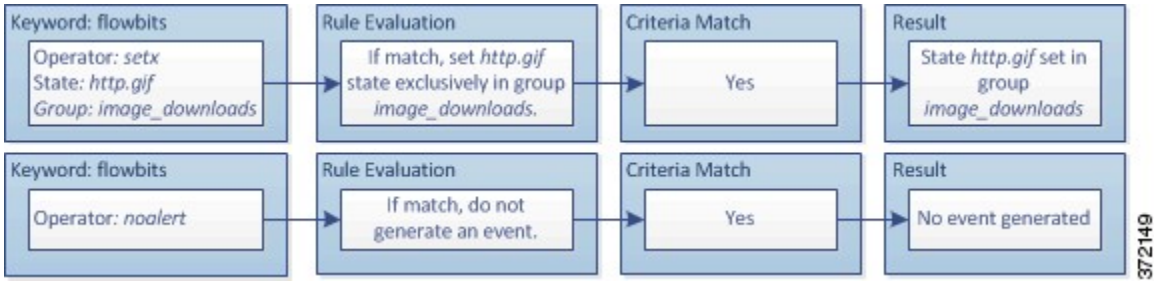


如果第一个规则分片检测到 JPEG 文件下载，`flowbits:setx,http.jpeg,image_downloads` 关键字会将 `flowbits` 状态设置为 `http.jpeg`，并将该状态包含在 `image_downloads` 组中。

然后，下一个规则会后续 GIF 文件下载：

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：

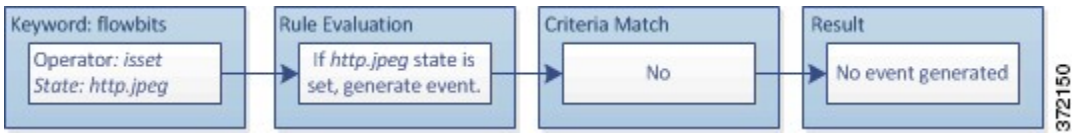


如果第二个规则分片与 GIF 下载相匹配，`flowbits:setx,http.jpg,image_downloads` 关键字将会设置 `http.jpg flowbits` 状态，并取消设置组中的另一个状态 `http.jpeg`。

第三个规则分片不会导致误报：

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

下图展示前述规则分片中 `flowbits` 关键字的影响：



由于 `flowbits:isset,http.jpeg` 为假，因此，规则引擎会停止处理规则，且不会生成事件，从而避免误报（即使 GIF 文件中的内容与 JPEG 文件的漏洞内容相匹配）。

http_encode 关键字

您可以使用 `http_encode` 关键字在未经规范化的 HTTP 请求或响应中生成关于编码类型的事件 - 可以是在 HTTP URI 中，在 HTTP 报头的非 cookie 数据中，在 HTTP 请求报头的 cookie 中，或者在 HTTP 响应的 set-cookie 数据中。

必须配置 HTTP 检查预处理器以检查 HTTP 响应和 HTTP cookie，从而使用 `http_encode` 关键字返回规则的匹配项。

此外，您必须在 HTTP 检查预处理器配置中为每个特定编码类型启用解码和警报选项，以使入侵规则中的 `http_encode` 关键字可以触发关于该编码类型的事件。

下表介绍了此选项可在 HTTP URI、报头、cookie 和 set-cookie 中为其生成事件的编码类型。

表 *159*：*HTTP_encode* 编码类型

编码类型	说明
utf8	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 UTF-8 编码。
double_encode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测双编码。
non_ascii	当检测到非 ASCII 字符但未启用检测到的编码类型时，在指定位置检测非 ASCII 字符。
uencode	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测 Microsoft %u 编码。
bare_byte	如果此编码类型已启用，并可供 HTTP 检查预处理器进行解码，将会在指定位置检测裸字节编码。

http_encode 关键字语法

编码位置

指定是要在 HTTP URI、报头还是 cookie（包括 set-cookie）中搜索指定的编码类型。

编码类型

使用以下格式之一指定一个或多个编码类型：

```
encode_type
encode_type|encode_type|encode_type...
```

其中，`encode_type` 是以下其中一项：

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

请注意，不能同时使用求反 (!) 和 OR (|) 运算符。

http_encode 关键字示例：使用两个 http_endcode 关键字搜索两种编码

以下示例使用同一规则中的两个 `http_encode` 关键字在 HTTP URI 中搜索 UTF-8 AND Microsoft IIS %u 编码：

第一个，`http_encode` 关键字：

- **Encoding Location**：`HTTP URI`
- **Encoding Type**：`utf8`

然后，另一个 `http_encode` 关键字：

- **Encoding Location**：`HTTP URI`
- **Encoding Type**：`uencode`

概述：file_type 和 file_group 关键字

`file_type` 和 `file_group` 关键字允许根据文件的类型和版本检测通过 FTP、HTTP、SMTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传输的文件。请**勿**在单个入侵规则中使用多个 `file_type` 或 `file_group` 关键字。

提示 更新漏洞数据库 (VDB) 可以使入侵规则编辑器获得最新的文件类型、版本和组。

注释 系统不会自动启用预处理器以适应 `file_type` 和 `file_group` 关键字。

如果要为匹配 `file_type` 或 `file_group` 关键字的流量生成入侵事件，**必须**启用特定预处理器。

表 *160*：*file_type* 和 *file_group* 入侵事件生成

协议	所需的预处理器或预处理器选项
FTP	FTP/Telnet 预处理器和**规范化 TCP 负载 (Normalize TCP Payload)** 内联规范化预处理器选项
HTTP	在 HTTP 流量中生成入侵事件的 HTTP 检查预处理器
SMTP	在 HTTP 流量中生成入侵事件的 SMTP 预处理器
IMAP	IMAP 预处理器
POP3	POP 预处理器

协议	所需的预处理器或预处理器选项
Netbios-ssn (SMB)	DCE/RPC 预处理器和 **SMB 文件检查 (SMB File Inspection)** DCE/RPC 预处理器选项

file_type 和 file_group 关键字

file_type

使用 `file_type` 关键字可指定在流量中检测到的文件的类型和版本。文件类型参数（例如 **JPEG** 和 **PDF**）用于识别要在流量中查找的文件格式。

注释 请**勿**在同一入侵规则中将 `file_type` 关键字与另一个 `file_type` 或 `file_group` 关键字配合使用。

系统默认选择 **Any Version**，但某些文件类型允许选择版本选项（例如 PDF 版本 **1.7**）来确定要在流量中查找的特定文件类型版本。

file_group

使用 `file_group` 关键字可选择思科定义的、包含在流量中找到的类似文件类型（例如**多媒体**或**音频**）的组。文件组还包含思科为组中的每种文件类型定义的版本。

注释 请**勿**在同一入侵规则中将 `file_group` 关键字与另一个 `file_group` 或 `file_type` 关键字配合使用。

file_data 关键字

`file_data` 关键字提供一个指针，该指针作为可用于其他关键字（例如 `content`、`byte_jump`、`byte_test` 和 `pcre`）的位置参数参考。检测到的流量确定 `file_data` 关键字指向的数据类型。您可以使用 `file_data` 关键字来指向以下负载类型的开头：

- HTTP 响应正文

  要检查 HTTP 响应数据包，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应。如果 HTTP 检查预处理器检测到 HTTP 响应正文数据，`file_data` 关键字将会进行匹配。

- 未压缩的 gzip 文件数据

  要检查 HTTP 响应正文中未压缩的 gzip 文件，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为会检查 HTTP 响应以及会解压缩 HTTP 响应正文中的 gzip 压缩文件。有关详细信息，请参阅**检测 HTTP 响应 (Inspect HTTP Responses)** 和**检测压缩数据 (Inspect Compressed Data)** 服务器级别 HTTP 规范化选项。如果 HTTP 检查预处理器在 HTTP 响应正文中检测到未压缩的 gzip 数据，`file_data` 关键字将会进行匹配。

- 规范化的 JavaScript

  要检查规范化的 JavaScript 数据，必须启用 HTTP 检查预处理器，还必须将该预处理器配置为检查 HTTP 响应。如果 HTTP 检查预处理器在响应主体数据中检测到 JavaScript，`file_data` 关键字将会进行匹配。

- SMTP 负载

  要检查 SMTP 负载，必须启用 SMTP 预处理器。如果 SMTP 预处理器检测到 SMTP 数据，`file_data` 关键字将会进行匹配。

- SMTP、POP 或 IMAP 流量中的编码邮件附件

  要检查 SMTP、POP 或 IMAP 流量中的邮件附件，必须分别启用 SMTP、POP 或 IMAP 预处理器或者启用它们的任意组合。然后，必须确保将已启用的每个预处理器配置为会对您想要解码的每种附件编码类型进行解码。可以为每个预处理器配置的附件解码选项是：**Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth** 和 **Unix-to-Unix Decoding Depth**。

  可以在一个规则中使用多个 `file_data` 关键字。

pkt_data 关键字

`pkt_data` 关键字提供一个指针，该指针作为可用于其他关键字（例如 `content`、`byte_jump`、`byte_test` 和 `pcre`）的位置参数参考。

如果检测到规范化的 FTP、telnet 或 SMTP 流量，`pkt_data` 关键字将指向规范化数据包负载的开头。如果检测到其他流量，`pkt_data` 关键字将指向原始 TCP 或 UDP 负载的开头。

必须启用以下规范化选项，系统才会对相应流量进行规范化以供入侵规则进行检测：

- 启用 FTP 和 Telnet 预处理器的**检测 FTP 命令内的 Telnet 转义代码 (Detect Telnet Escape Codes within FTP Commands)** 选项可规范化 FTP 流量以进行检查。
- 启用 FTP 和 Telnet 预处理器的**规范化 (Normalize)** Telnet 选项可规范化 Telnet 流量以进行检查。
- 启用 SMTP 预处理器的**规范化 (Normalize)** 选项可规范化 SMTP 流量以进行检查。

可以在一个规则中使用多个 `pkt_data` 关键字。

base64_decode 和 base64_data 关键字

可以结合使用 `base64_decode` 和 `base64_data` 关键字，以指示规则引擎将指定数据作为 Base64 数据进行解码和检查。这可能很有用，例如，对于检查 Base64 编码 HTTP 身份验证请求报头，以及对于检查 HTTP PUT 和 POST 请求中的 Base64 编码数据。

这两个关键字对于编码和检查 HTTP 请求中的 Base64 数据尤其有用。但是，也可以将这两个关键字与像 HTTP 一样使用空格和制表符的任何协议（例如 SMTP）结合使用，以将长的报头行展开为跨越多行。如果协议中不存在这样的行展开（即为“折叠”），检查将在后面不跟有空格或制表符的任何回车符或换行符处结束。

base64_decode

base64_decode 关键字指示规则引擎将数据包数据解码为 Base64 数据。使用可选参数可指定要解码的字节数量以及在数据中的哪个位置开始解码。

可以在一个规则中使用 base64_decode 关键字一次；此关键字必须位于至少一个 base64_data 关键字实例前面。

解码 Base64 数据之前，规则引擎会将跨越多行的已折叠的长报头展开。当规则引擎遇到以下任何情况时，解码将会结束：

- 报头行结尾
- 要解码的指定字节数
- 数据包结尾

下表介绍了可与 base64_decode 关键字配合使用的参数。

表 *161*：可选 *base64_decode* 参数

参数	说明
字节	指定要解码的字节数。如果未指定，解码将持续到报头行结尾或数据包负载结尾（以先到者为准）。可以指定非零的正值。
Offset	确定相对于数据包负载开头的偏移量，如果还指定了 **Relative**，则确定相对于当前检查位置的偏移量。可以指定非零的正值。
Relative	指定相对于当前检查位置的检查。

base64_data

base64_data 关键字提供用于检查使用 base64_decode 关键字进行解码的 Base64 数据的参考。base64_data 关键字将检查设置在解码的 Base64 数据开头开始。或者，可以随后使用可用于其他关键字的位置参数（例如 content 或 byte_test）进一步指定要检查的位置。

使用 base64_decode 关键字之后，必须至少使用一次 base64_data 关键字；或者，可以多次使用 base64_data 以返回到解码的 Base64 数据的开头。

检查 Base64 数据时，请注意：

- 不能使用快速模式匹配程序。
- 如果在规则中使用干预性 HTTP 内容参数中断 Base64 检查，则必须在该规则中插入另一个 base64_data 关键字，然后再进一步检查 Base64 数据。

第 55 章

入侵防御性能调整

以下主题介绍如何优化入侵防御性能：

概述：入侵防御性能调整

思科提供多项功能，用于提高系统在分析流量中的入侵企图时的性能。您可以执行以下操作：

- 指定事件队列中允许的数据包数量。您还可以在数据流重组前后，启用或禁用对将重建到更大数据流中的数据包进行的检测。
- 覆盖入侵规则中使用的 PCRE 默认匹配和递归限制以检查数据包负载内容。
- 选择使规则引擎在生成多个事件时为每个数据包或数据包流记录多个事件，使您可以收集报告事件之外的信息。
- 在安全和通过数据包及规则延迟阈值将设备延迟保持在可接受水平的需求之间保持平衡。
- 配置设备如何监控和报告其自身性能的基本参数。这样，您可以指定系统更新设备上的性能统计信息的间隔。

可以基于每个访问控制策略配置这些性能设置，他们可应用于该父访问控制策略调用的所有入侵策略。

限制入侵的模式匹配

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**模式匹配限制 (Pattern Matching Limits)** 选项卡。

步骤 4 在**每个数据包要分析的最大模式状态数 (Maximum Pattern States to Analyze Per Packet)** 字段中输入要加入队列的最大事件数的值。

步骤 5 要禁用在数据流重组前后将重建为更大数据流的数据包的检查，请选中**对有待未来重组的流量禁用内容检查 (Disable Content Checks on Traffic Subject to Future Reassembly)** 复选框。重组前后的检测需要更多的处理开销，可能会导致性能下降。

步骤 6 点击 **OK**。

步骤 7 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

入侵规则的正则表达式限制覆盖

默认正则表达式限制可确保最低性能级别。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

注意 除非在撰写入侵规则方面很有经验，并且了解衰减模式的影响，否则，不要覆盖默认的PCRE限制。

表 *162*：正则表达式限制选项

选项	说明
Match Limit State	指定是否覆盖 **Match Limit**。您有以下选择： • 选择 **Default**，以使用为 **Match Limit** 配置的值 • 选择 **Unlimited**，以允许不限次数的尝试 • 选择 **Custom**，为 **Match Limit** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 匹配评估
Match Limit	指定在与 PCRE 正则表达式中定义的模式进行匹配时的尝试次数。
Match Recursion Limit State	指定是否覆盖 **Match Recursion Limit**。您有以下选择： • 选择 **Default**，以使用为 **Match Recursion Limit** 配置的值 • 选择 **Unlimited**，以允许进行次数不限的递归 • 选择 **Custom**，为 **Match Recursion Limit** 指定 1 或更大的值，或指定 0 以彻底禁用 PCRE 递归 注意：为使 **Match Recursion Limit** 具有意义，其值必须小于 **Match Limit**。
Match Recursion Limit	指定在根据数据包静载荷对 PCRE 正则表达式进行评估时的递归次数。

覆盖入侵规则的正则表达式限制

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**正则表达式限制 (Regular Expression Limits)** 选项卡。

步骤 4 可以修改入侵规则的正则表达式限制覆盖，第 978 页中的任何选项。

步骤 5 点击 **OK**。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

每个数据包的入侵事件生成限制

当入侵规则引擎根据规则评估流量时，它会将针对给定数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。配置入侵事件日志记录限制时，可指定队列中可放置的事件数量及要记录的事件数量，并可选择确定队列中事件顺序的条件。

表 *163*：入侵事件日志记录限制选项

选项	说明
Maximum Events Stored Per Packet	为给定数据包或数据包流可存储的最多事件数量。
Maximum Events Logged Per Packet	为给定数据包或数据包流记录的事件数量。这不能超过 **Maximum Events Stored Per Packet** 的值。
Prioritize Event Logging By	该值用于确定事件队列中事件排序方法。排序最高的事件通过用户界面进行报告。有以下选项可供选择： • `priority`，按事件的优先级对队列中的事件进行排序。 • `content_length`，按识别出的最长匹配内容对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。

限制每个数据包生成的入侵事件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击**性能设置 (Performance Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 点击**性能设置 (Performance Settings)** 弹出窗口中的**入侵事件日志记录限制 (Intrusion Event Logging Limits)** 选项卡。

步骤 4 可以修改每个数据包的入侵事件生成限制，第 980 页中的任何选项。

步骤 5 点击 **OK**。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

数据包和入侵规则延迟阈值配置

每个访问控制策略都具有基于延迟的设置，这些设置使用阈值来管理数据包和规则处理性能。

数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检测。

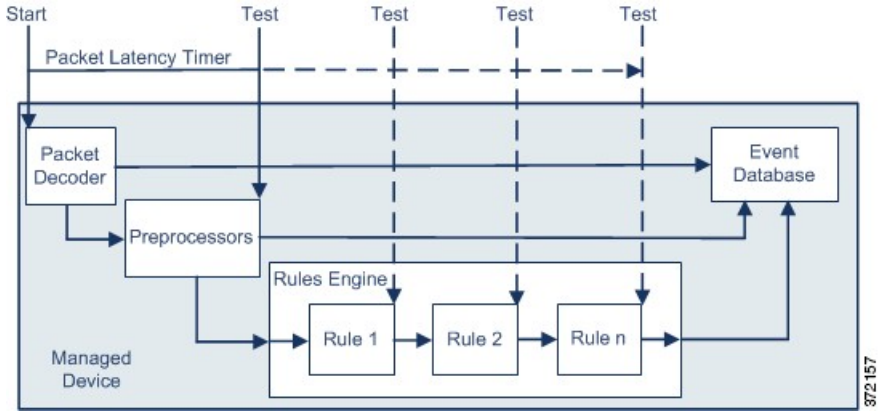
规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。

数据包延迟阈值

数据包延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

延迟阈值的得失分别为：实现性能和延迟优势的同时，也会导致未经检查的数据包可能包含攻击。但是，数据包延迟阈值提供的工具可用于平衡安全性与连接性。

解码器处理开始时，每个数据包的计时器开始计时。计时器会持续计时，直到数据包的所有处理工作结束或处理时间在计时测试点超过阈值。



如上图所示，数据包延迟计时在以下测试点测试：

- 在所有解码器和预处理程序的处理完成之后且在规则处理开始之前
- 在每条规则的处理之后

如果处理时间在任何测试点超出阈值，数据包检测将停止。

提示 总的数据包处理时间不包括常规的 TCP 数据流或 IP 分片重组时间。

对于由处理数据包的解码器、预处理程序或规则所触发的事件，数据包延迟阈值不会对其产生影响。只有当数据包已完全处理完毕，或当数据包处理因超过了延迟阈值而终止时（以先出现者为准），任何适用的解码器、预处理程序或规则才会触发事件。如果丢弃规则在内联部署中检测到入侵，则丢弃规则将触发事件并将数据包丢弃。

注释 只有当数据包的处理因超出数据包延迟阈值而停止后，才会根据规则评估数据包。本可触发事件的规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

数据包延迟阈值功能对被动式部署和内嵌式部署的性能均有提升作用，并且可以停止检测需要大量处理时间的数据包，从而降低延迟。例如，这些性能优势可以在以下情形中发挥出来：

- 对于被动和内联式部署，多个规则依序检查一个数据包需要过长的时间
- 对于内联式部署，网络性能不佳（例如，当有人下载超大文件时）期间，数据包处理变慢。

在被动式部署中，停止数据包的处理可能无助于恢复网络性能，这是因为，只不过转至处理下一数据包而已。

数据包延迟阈值说明

表 *164*：数据包延迟阈值选项

选项	说明
Threshold (microseconds)	指定数据包检测停止的时间，以微秒为单位。

很多因素影响系统性能和数据包延迟，如CPU速度、数据速率、数据包大小和协议类型。因此，思科建议您使用下表中的阈值设置，直到您计算出了适合自己的网络环境的设置。

表 *165*：最小数据包延迟阈值设置

针对此数据速率...	将阈值（微秒）设置为至少...
1 Gbps	100
100 Mbps	250
5 Mbps	1000

计算设置时请确定：

- 每秒的平均数据包数
- 每个数据包所需的平均微秒数

将网络中每个数据包所需的平均微秒数乘以一个较大的安全因子，以确保不必要地中止数据包检查。

例如，思科建议千兆环境中的最小数据包延迟阈值应为 100 微秒。此建议的最小阈值所依据的测试数据为每秒平均 250,000 个数据包，即每微秒 0.25 个数据包，或每个数据包用时 4 微秒。乘以因子 25 即得出建议的最小阈值 100 微秒。

配置数据包延迟阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**数据包处理 (Packet Handling)** 选项卡。

步骤 4 有关所建议的最小**阈值 (Threshold)** 设置，请参阅数据包延迟阈值说明，第 983 页。

步骤 5 点击 **OK**。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

规则延迟阈值

规则延迟阈值度量所需时间，而不仅是处理时间，目的是为了更准确地反映规则在处理数据包时实际所需的时间。然而，延迟阈值功能是基于软件实现的延迟管理功能，并不能实施严格的定时功能。

延迟阈值的得失分别为：实现性能和延迟优势的同时，也会导致未经检查的数据包可能包含攻击。但是，规则延迟阈值提供的工具可用于平衡安全性与连接性。

计时器测量每次根据一组规则处理数据包所用的处理时间。任何时候，只要规则处理时间超出指定的规则延迟阈值，系统就会递增计数器的计数。如果连续超出阈值的次数达到了指定的数值，系统就会执行下列操作：

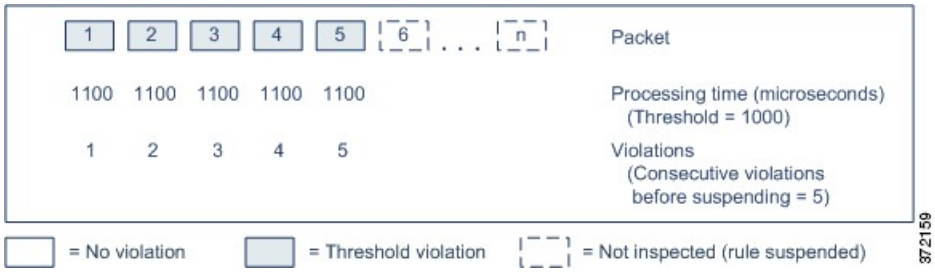
- 按指定的期限暂停规则
- 触发事件以指明规则已暂停
- 暂停时间到期时重新启用规则
- 触发事件以指明规则已重新启用

当该组规则已暂停时，或当规则违规次数非连续时，系统会将计数器清零。如在暂停规则前允许一定次数的连续违规，则将忽略对性能的影响无足轻重的偶发性违规，转而专注于反复超出规则延迟阈值的规则所造成的更大影响。

以下示例显示了未导致规则暂停的 5 次连续规则处理时间。

在以上示例中，处理前三个数据包中各个数据包的所需时间超出1000微秒的规则延迟阈值，每次违规时违规计数器均将递增 1 次计数。第四个数据包的处理时间未超出阈值，因此违规计数器重置为 0。第五个数据包的处理时间超出阈值，因此违规计数器从 1 开始重新计数。

以下示例显示了导致规则暂停的 5 次连续规则处理时间。



在第二个示例中，处理五个数据包中每个数据包所需的时间均超出1000微秒的规则延迟阈值。由于每个数据包的规则处理时间是 1100 微秒，超出 1000 微秒阈值的次数到达指定的连续 5 次，因此该组规则被暂停。在暂停时间到期前，任何后续的数据包（在图中表示为数据包 6 至 n）均不会根据暂停的规则得以检查。如果重新启用规则后收到了更多的数据包，违规计数器从 0 开始重新计数。

规则延迟阈值对数据包处理规则所触发的入侵事件无影响。无论规则处理时间是否超出阈值，规则都会因数据包中检测到的任何入侵而触发事件。如果检测到入侵的规则是内联部署中的丢弃规则，则将丢弃数据包。当丢弃规则检测到数据包中存在将导致暂停规则的入侵时，丢弃规则将触发入侵事件，数据包将被丢弃，该规则和所有相关规则均被暂停。

注释 系统不会根据已暂停的规则对数据包进行评估。本可触发事件的已暂停规则无法触发该事件，同时，丢弃规则无法丢弃该数据包。

通过暂停在处理数据包时耗时最长的规则，规则延迟阈值可提高被动和内联部署模式下的系统性能，并缩短内联部署中的延迟。在可配置的时间到期之前，系统不会根据被暂停的规则对数据包再次进行评估，从而留出时间让过载设备进行恢复。例如，这些性能优势可以在以下情形中发挥出来：

- 匆忙写就、大量未经测试的规则需要过长的处理时间
- 网络性能不佳期间（例如，当有人下载超大文件时），数据包检查变慢。

规则延迟阈值说明

可修改规则延迟阈值、已暂停规则的暂停时间以及暂停规则前必须连续超出阈值的次数。

如果规则处理数据包时所用时间超过 **Consecutive Threshold Violations Before Suspending Rule** 所指定的连续次数的**阈值**，则规则延迟阈值就会按 **Suspension Time** 指定的时间暂停规则。

可启用规则 134:1，当规则已暂停时生成事件；并启用规则 134:2，在启用已暂停规则时生成事件。

表 *166*：规则延迟阈值选项

选项	说明
阈值	指定规则在检查数据包时不应超出的时间，单位为微秒。
暂停规则前连续超出阈值的次数	指定在暂停规则之前，规则可按超过为 **Threshold** 设置的时间检查数据包的连续次数。
Suspension Time	指定暂停一组规则前需经过的秒数。

许多因素影响系统性能，如CPU速度、数据速率、数据包大小和协议类型。因此，思科建议您使用下表中的阈值设置，直到您计算出了适合自己的网络环境的设置。

表 *167*：最小规则延迟阈值设置

针对此数据速率...	将阈值（微秒）设置为至少...
1 Gbps	500
100 Mbps	1250
5 Mbps	5000

计算设置时请确定：

- 每秒的平均数据包数
- 每个数据包所需的平均微秒数

将网络中每个数据包所需的平均微秒数乘以一个较大的安全因子，以确保不必要地中断规则检查。

配置规则延迟阈值

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击**基于延迟的性能设置 (Latency-Based Performance Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 在**基于延迟的性能设置 (Latency-Based Performance Settings)** 弹出窗口中，点击**规则处理 (Rule Handling)** 选项卡。

步骤 4 可以按规则延迟阈值说明，第 986 页中所述配置任何选项。

步骤 5 点击 **OK**。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 如果要生成入侵事件，请启用规则延迟规则 134:1 和 134:2。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

入侵性能统计信息日志记录配置

Sample time (seconds) and Minimum number of packets

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

Troubleshooting Options: Log Session/Protocol Distribution

支持部门可能要求您在故障排除调用期间记录协议分布、数据包长度和端口统计信息。

注意 请勿启用“记录会话/协议分发”(Log Session/Protocol Distribution)，除非支持人员指示执行此操作。

Troubleshooting Options: Summary

支持部门可能要求您在故障排除调用期间将系统配置为仅在 Snort 进程关闭或重新启动时计算性能统计数据。要启用此选项，也必须启用 **Log Session/Protocol Distribution** 故障排除选项。

注意 请勿启用“摘要”(Summary)，除非支持人员指示执行此操作。

配置入侵性能统计信息日志记录

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，然后点击**性能设置 (Performance Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 点击出现的弹出窗口中的**性能统计信息 (Performance Statistics)** 选项卡。

步骤 3 如上所述修改 **Sample time** 或 **Minimum number of packets**。

步骤 4 或者，展开 **Troubleshoot Options** 部分并修改这些选项（仅当支持部门要求这样做时）

步骤 5 点击 **OK**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 XV 部分

高级网络分析和预处理

第 56 章

网络分析和入侵策略的高级访问控制设置

以下主题介绍如何配置网络分析和入侵策略的高级访问控制设置：

概述：网络分析和入侵策略的高级访问控制设置

访问控制策略中的多项高级设置可监管需要特定专门技术才能做出的入侵检测和防御配置。高级设置通常几乎不需要修改，并非在每个部署中都出现。

默认入侵策略

每个访问控制策略使用其默认入侵策略初始检测流量，然后系统才能准确确定如何检测该流量。之所以这样做，是因为有时系统必须处理连接中的前几个数据包，**允许其通过**，然后它才能确定哪条访问控制规则（如有）将处理流量。因此，这些数据包不会未经检测就到达其目的地，然而，您可以使用称为默认入侵策略的入侵策略对其进行检测并生成入侵事件。默认情况下，默认入侵策略使用默认变量集。

默认入侵策略在执行应用控制和URL过滤时尤为有用，因为系统无法在客户端与服务器之间完全建立连接之前识别应用或过滤 URL。例如，如果一个数据包与具有应用或 URL 条件的访问控制规则中的所有其他条件相匹配，则将允许该数据包及其后续数据包通过，直到建立连接且完成应用或 URL 识别，通常为 3 到 5 个数据包。

系统使用默认入侵策略检测允许的这些数据包，他们可以生成事件，内联时还可阻止恶意流量。系统识别应处理连接的访问控制规则或默认操作后，相应地处理和检测连接中剩余的数据包。

在创建访问控制策略时，其默认入侵策略取决于您**首先**选择的默认操作。用于访问控制的初始默认入侵策略如下：

- Balanced Security and Connectivity（系统提供的策略）是在您首先选择 **Intrusion Prevention** 默认操作时访问控制策略的默认入侵策略。
- No Rules Active 是在您首先选择 **Block all traffic** 或 **Network Discovery** 默认操作时访问控制策略的默认入侵策略。尽管选择此选项会禁用对上述已允许数据包的入侵检测，但是，如果您对入侵数据不感兴趣，它可提高性能。

注释 如果未在执行入侵检查（例如，在仅发现部署中），请保持“无活动规则”(No Rules Active) 策略作为默认入侵策略。

如果在创建访问控制策略后更改默认操作，则默认入侵策略**不**自动更改。要手动更改，请使用访问控制策略的高级选项。

您可以选择系统或用户创建的策略。

注释 与第一个匹配网络分析规则关联的网络分析策略预处理默认入侵策略的流量。如果没有网络分析规则，或者无任何网络分析规则匹配，则使用默认网络分析策略。

设置默认入侵策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

注意 更改访问控制策略使用的入侵策略总数在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。通过以下方式更改入侵策略总数：将策略当前未使用的入侵策略与访问控制规则、默认操作或默认入侵策略关联；或者从其中任意一个中删除访问控制策略使用的最后一个入侵策略实例。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**选项卡，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 从**确定访问控制规则之前使用的入侵策略 (Intrusion Policy used before Access Control rule is determined)** 下拉列表中选择入侵策略。

如果选择用户创建的策略，则可以点击编辑图标 () 在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 3 或者，从**入侵策略变量集 (Intrusion Policy Variable Set)** 下拉列表中选择其他变量集。您还可以点击变量集旁边的编辑图标 () 以创建和编辑变量集。如果您未更改变量集，系统会使用默认的变量集。

步骤 4 点击 **OK**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

网络分析策略的高级设置

网络分析策略监管如何解码和预处理流量，以便进一步对其进行评估，特别适用于可能表明入侵尝试的异常流量。此流量预处理发生在安全情报黑名单和流量解密之后，但是，发生在入侵策略对数据包进行详细检查之前。默认情况下，系统提供的“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略是默认网络分析策略。

提示 系统提供的 Balanced Security and Connectivity 网络分析策略和 Balanced Security and Connectivity 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。

为此，请向访问控制策略中添加自定义网络分析规则。网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

每条规则均有：

- 一组规则条件，用于识别想要预处理的特定流量
- 一条关联的网络分析策略，想要用来预处理符合所有规则条件的流量

在系统预处理流量时，其将数据包按照规则编号自上而下的顺序与网络分析规则相匹配。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

设置默认网络分析策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

您可以选择系统或用户创建的策略。

注释 如果禁用预处理器，但是系统需要根据已启用的入侵或预处理器规则评估预处理的数据包，则系统将自动启用和使用预处理器，尽管它在网络分析策略 Web 界面中保持禁用。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。由于预处理和入侵检测如此密切相关，因此，请**务必**小心确保允许网络和入侵策略检测每个数据包，以实现互补。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 从**默认网络分析策略 (Default Network Analysis Policy)** 下拉列表中，选择一个默认网络分析策略。

如果选择用户创建的策略，则可以点击编辑图标 ( ) 在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 3 点击 **OK**。

步骤 4 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改 ， 第 254 页。

网络分析规则

在访问控制策略的高级设置中，您可以使用网络分析规则定制网络流量的预处理配置。

网络分析规则从 1 开始进行编号。在系统预处理流量时，它将数据包按照升序规则编号自上而下的顺序与网络分析规则相匹配，然后根据所有条件都匹配的第一个规则预处理流量。

您可以向规则中添加区域、网络和 VLAN 标记条件。如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，一条包含网络条件但不含区域条件的规则根据其源 IP 地址或目标 IP 地址评估流量，不管其进出接口如何。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

配置网络分析规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**选项卡，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

提示 点击**网络分析策略列表 (Network Analysis Policy List)** 以查看和编辑现有自定义网络分析策略。

步骤 2 在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

步骤 3 点击 **Add Rule**（添加规则）。

步骤 4 通过点击与要添加的条件对应的选项卡来配置规则条件；请参阅规则条件类型，第 268 页。

步骤 5 点击**网络分析 (Network Analysis)** 选项卡，并选择要用于预处理匹配此规则的流量的**网络分析策略 (Network Analysis Policy)**。

点击编辑图标 ( )，在新窗口中编辑自定义策略。无法编辑系统提供的策略。

步骤 6 点击 **Add**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

管理网络分析规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，然后点击“入侵和网络分析策略”(Intrusion and Network Analysis Policies) 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

步骤 3 编辑您的自定义规则。您有以下选择：

- 要编辑某条规则的条件或更改该规则调用的网络分析策略，请点击该规则旁的编辑图标( )。
- 要更改某条规则的评估顺序，请点击该规则并将其拖至正确的位置。要选择多条规则，请使用 Shift 和 Ctrl 键。
- 要删除某条规则，请点击该规则旁的删除图标 ( )。

提示 右键点击规则会显示情景菜单，通过该菜单可剪切、复制、粘贴、编辑、删除网络分析规则和添加新的网络分析规则。

步骤 4 点击 **OK**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 57 章

网络分析策略使用入门

以下主题介绍如何开始使用网络分析策略：

网络分析策略基础知识

网络分析策略管理许多流量预处理选项，并供访问控制策略中的高级设置调用。网络分析相关预处理发生在安全情报黑名单和 SSL 解密之后进行，但在入侵或文件检查开始之前进行。

默认情况下，系统使用平衡的安全性和连接性网络分析策略预处理由访问控制策略处理的所有流量。但是，您可以选择不同的默认网络分析策略执行此预处理。为方便您使用，系统提供多种无法修改的网络分析策略供选择，这些策略由Cisco Talos 安全情报和研究小组 (Talos) 针对安全性和连接的特定平衡专门进行过调整。您也可以用自定义预处理设置创建自定义网络分析策略。

提示

系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，平衡安全性和连接网络分析策略和平衡安全性和连接入侵策略配合工作并可以在入侵规则更新中同时更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。网络分析和入侵策略相互配合，检查您的流量。

您也可以通过以下方式根据特定安全区域、网络和 VLAN 定制流量预处理选项：创建多个自定义网络分析策略，然后分配它们预处理不同流量。（请注意，ASA FirePOWER无法通过 VLAN 限制预处理。）

管理网络分析策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 管理网络分析策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略，第 261 页。
- 创建 - 如果要创建新的网络分析策略，请点击**创建策略 (Create Policy)**，然后如自定义网络分析策略的创建，第 998 页中所述继续操作。
- 删除 - 如果要删除网络分析策略，请点击删除图标 ( )，然后确认是否要删除策略。如果网络分析策略被访问控制策略引用，则无法删除该网络分析策略。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 部署 - 点击**部署 (Deploy)**；请参阅部署配置更改，第 254 页。
- 编辑 - 如果要编辑现有网络分析策略，请点击编辑图标 ( )，然后如网络分析策略设置和缓存的更改，第 1000 页中所述继续操作。

  如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。
- 报告 - 点击报告图标 ( )；请参阅生成当前策略报告，第 262 页。

自定义网络分析策略的创建

当创建新的网络分析策略时，必须为其提供唯一的名称，指定基本策略并选择内联模式。

基本策略定义网络分析策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。

网络分析策略的内联模式允许预处理器修改（标准化）和丢弃流量，从而使攻击者避开检测的可能性最小化。请注意，在被动部署中，无论内联模式如何设置，系统都无法影响流量传输。

创建自定义网络分析策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击 **Create Policy**。如果在另一策略中有未保存的更改，当系统提示您返回 Network Analysis Policy 页面时，请点击 **Cancel**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。
在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 选择初始**基本策略 (Base Policy)**。您可以使用系统提供的策略或自定义策略作为您的基本策略。

步骤 6 如果要允许预处理器影响内联部署中的流量，请启用**内联模式 (Inline Mode)**。

步骤 7 创建策略：

- 点击 **Create Policy** 创建新策略并返回到 Network Analysis Policy 页面。新策略的设置与其基本策略相同。
- 点击**创建并编辑策略 (Create and Edit Policy)**，创建策略并在高级网络分析策略编辑器中将其打开进行编辑。

网络分析策略管理

在“网络分析策略”(Network Analysis Policy) 页面（或**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**）上，您可以查看当前的自定义网络分析策略以及以下信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及执行此修改的用户。

- 是否已启用 **Inline Mode** 设置，该设置允许预处理器影响流量
- 哪些访问控制策略和设备使用网络分析策略来预处理流量
- 策略是否有未保存的更改，以及有关何人（如果有任何人）当前正在编辑该策略的信息

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个网络分析策略使用 Balanced Security and Connectivity 网络分析策略作为其基本策略。两者之间的唯一区别在于其内联模式，在内联策略中允许预处理器影响流量，但在被动策略中禁用了该功能。您可以编辑并使用系统提供的这些自定义策略。

请注意，如果您的 Firepower 系统用户帐户的角色被限制为“入侵策略”(Intrusion Policy) 或“修改入侵策略”(Modify Intrusion Policy)，则您可以创建和编辑网络分析策略及入侵策略。

网络分析策略设置和缓存的更改

当您创建新的网络分析策略时，它具有与其基本策略相同的设置。

当您定制网络分析策略时，特别是在禁用预处理器时，请记住某些预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

注释 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。

编辑网络分析策略

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击想要配置的网络分析策略旁的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑网络分析策略：

- 更改基本策略 - 如果要更改基本策略，请从“策略信息”(Policy Information) 页面上的**基本策略 (Base Policy)** 下拉列表中选择基本策略。
- 管理策略层 - 如果要管理策略层，请点击导航面板中的**策略层 (Policy Layers)**。
- 修改预处理器 - 如果要启用、禁用或编辑预处理器的设置，请点击导航面板中的**设置 (Settings)**。
- 修改流量 - 如果要允许预处理器修改或丢弃流量，请选中“策略信息”(Policy Information) 页面上的**内联模式 (Inline Mode)** 复选框。
- 查看设置 - 如果要查看基本策略中的设置，请点击“策略信息”(Policy Information) 页面上的**管理基本策略 (Manage Base Policy)**。

步骤 4 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 如果希望预处理器生成入侵事件，请启用该预处理器的规则。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

网络分析策略中的预处理器配置

预处理器通过规范化流量和标识协议异常，准备要进行进一步检查的流量。预处理器可以在数据包触发配置的预处理器选项时生成预处理器事件。网络分析策略的基本策略决定了默认情况下启用哪些预处理器及各自的默认配置。

注释 在大多数情况下，配置预处理器要求特定专业知识，并且通常很少需要修改或不需要任何修改。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。

修改预处理器配置要求了解配置及其对网络的潜在影响。

请注意，某些高级传输和网络预处理器设置全局应用于您部署访问控制策略所在的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

另请注意，您在入侵策略中配置敏感数据预处理器，用于检测 ASCII 文本形式的信用卡号和社会安全保障号等敏感数据。

内联部署中预处理器流量的修改

在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），某些预处理器可以修改并阻止流量。例如：

- 内联规范化预处理器将数据包标准化为准备这些数据包，以便由其他预处理器和入侵规则引擎进行分析。您还可以使用预处理器的**允许这些 TCP 选项 (Allow These TCP Options)** 和**阻止无法解析的 TCP 报头异常 (Block Unresolvable TCP Header Anomalies)** 选项阻止某些数据包。
- 系统可以丢弃具有无效校验和的数据包。
- 系统可以丢弃匹配基于速率的攻击防护设置的数据包。

要使网络分析策略中配置的预处理器影响流量，还必须启用并正确配置预处理器，并正确部署内联的受管设备。最后，您必须启用网络分析策略的 **Inline Mode** 设置。

网络分析策略中的预处理器配置说明

当您在网络分析策略的导航面板中选择**Settings**时，策略将按类型列出其预处理器。在Settings页面中，您可以启用或禁用网络分析策略中的预处理器，以及访问预处理器配置页面。

必须启用预处理器，这样您才能对其进行配置。当启用预处理器时，该预处理器配置页面的子链接显示在导航面板中 **Settings** 链接下，并且到配置页的 **Edit** 链接显示在 Settings 页面上的预处理器旁边。

提示 要将预处理器的配置恢复为基本策略中的设置，请点击预处理器配置页面上的**Revert to Defaults**。出现提示时，请确认您要恢复。

当禁用预处理器时，子链接和 **Edit** 链接将不显示，但会保留您的配置。请注意，为了执行其特定分析，许多预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。

如果要评估配置如何在内联部署中起作用，而不会实际修改流量，您可以禁用内联模式。在被动部署或分路模式的内联部署中，系统无法影响流量，无论内联模式设置如何。

注释 禁用内联模式可能会影响入侵事件性能统计数据图表。在内联部署中启用内联模式时，“入侵事件性能”(Intrusion Event Performance) 页面 (**概述 (Overview)** > **摘要 (Summary)** > **入侵事件性能 (Intrusion Event Performance)**) 显示表示已规范化和阻止的数据包的图表。如果禁用内联模式，或者在被动部署中，许多图表显示有关系统应当已规范化或丢弃的流量的数据。

注释 在内联部署中，思科建议您启用内联模式并配置已启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。在被动部署中，思科建议您使用自适应配置文件。

第 58 章

应用层预处理器

以下主题介绍应用层预处理器及其配置方法：

应用层预处理器简介

应用层协议可以通过多种方式表示相同的数据。Firepower 系统提供应用层协议解码器，这些解码器可将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。规范化应用层协议编码使得规则引擎可以有效地将相同的内容相关规则应用于其数据以不同方式呈现的数据包，并获得有意义的结果。

当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

请注意，大多数情况下，除非在入侵策略中启用随附预处理器规则，否则预处理器不会生成事件。

DCE/RPC 预处理器

DCE/RPC 协议使不同网络主机上的进程可以像在同一主机上一样进行通信。这些进程间通信一般通过 TCP 和 UDP 在主机之间传输。在 TCP 传输中，DCE/RPC 也可以进一步封装在 Windows 服务器消息块 (SMB) 协议或 Samba 中；Samba 是一种在由 Windows 和类似 UNIX 或类似 Linux 操作系统组成的混合环境中用于进程间通信的开源 SMB 实现。此外，网络上的 Windows IIS网络服务器可能使用 IIS RPC over HTTP，后者通过防火墙向代理 TCP 传输 DCE/RPC 流量提供分布式通信。

请注意，对 DCE/RPC 预处理器选项和功能的说明包括 DCE/RPC 的 Microsoft 实现（又称为 MSRPC）；对 SMB 选项和功能的说明涉及 SMB 和 Samba。

虽然大多数 DCE/RPC 漏洞出现在针对 DCE/RPC 服务器（实际上可能是网络上任何主机）的 DCE/RPC 客户端请求中，但在服务器响应中也可能出现漏洞。DCE/RPC 预处理器检测封装在 TCP、UDP 和 SMB 传输（包括使用版本 1 RPC over HTTP 的 TCP 传输 DCE/RPC）中的 DCE/RPC 请求和响应。此预处理器分析 DCE/RPC 数据流并检测 DCE/RPC 流量中的异常行为和逃避技术。它还分析 SMB 数据流并检测异常 SMB 行为和逃避技术。

除 IP 分片重组预处理器提供的 IP 分片重组和 TCP 数据流预处理器无缝提供的 TCP 数据流以外，DCE/RPC 预处理器还会将 SMB 分段重组并将 DCE/RPC 分片重组。

最后，DCE/RPC 预处理器会规范化 DCE/RPC 流量，以便规则引擎进行处理。

无连接和面向连接的 DCE/RPC 流量

DCE/RPC 消息符合两种不同的 DCE/RPC 协议数据单元（PDU）之一：

面向连接的 DCE/RPC PDU 协议

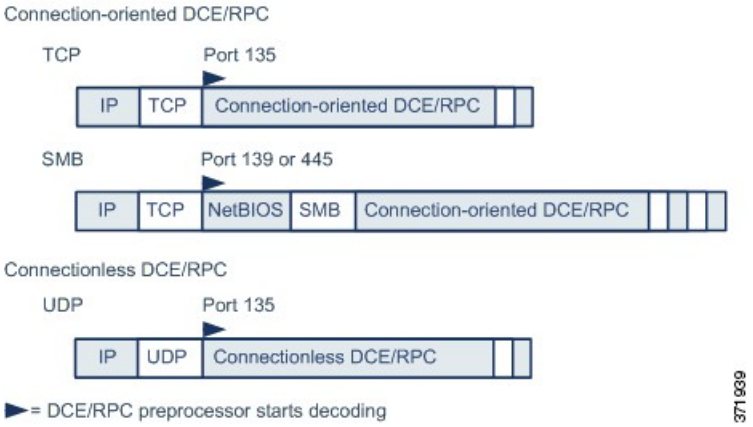
DCE/RPC 预处理器在 TCP、SMB 和 RPC over HTTP 传输中检测面向连接 DCE/RPC。

无连接 DCE/RPC PDU 协议

DCE/RPC 预处理器在 UDP 传输中检测无连接 DCE/RPC。

这两种 DCE/RPC PDU 协议都有独特的报头和数据特性。例如，面向连接的 DCE/RPC 的报头长度通常为 24 字节，而无连接 DCE/RPC 的报头长度固定为 80 字节。此外，分片无连接 DCE/RPC 的正确分片顺序不能通过无连接传输处理，而必须通过无连接 DCE/RPC 报头值提供保证；相比之下，传输协议可确保面向连接 DCE/RPC 的分片顺序正确。DCE/RPC 预处理器使用这些特性及其他特定协议特性监控这两种协议是否存在异常和其他躲避技术，对流量进行解码和分片重组，然后再将流量传送到规则引擎。

下图说明了 DCE/RPC 预处理器开始为不同传输处理 DCE/RPC 流量的点。



对于上图，请注意以下几点：

- 已知 TCP 或 UDP 端口 135 识别 TCP 和 UDP 传输中的 DCE/RPC 流量。
- 图中未包含 RPC over HTTP。

  对于 RPC over HTTP，面向连接 DCE/RPC 在完成 HTTP 初始设置序列后直接通过 TCP 传输（如图所示）。
- DCE/RPC 预处理器通常接收适用于 NetBIOS 会话服务的已知 TCP 端口 139 或以类似方式实现的已知 Windows 端口 445 上的 SMB 流量。

  由于 SMB 具有除传输 DCE/RPC 以外的许多功能，因此，预处理器会首先测试 SMB 流量是否携带 DCE/RPC 流量，如果不是则停止处理，如果是则继续处理。
- IP 封装所有 DCE/RPC 传输。
- TCP 传输所有面向连接 DCE/RPC。
- UDP 传输无连接 DCE/RPC。

DCE/RPC 基于目标的策略

Windows 和 Samba DCE/RPC 的实现有很大不同。例如，在对 DCE/RPC 流量进行分片重组时，所有 Windows 版本都在第一个分片中使用 DCE/RPC 上下文 ID，而所有 Samba 版本都在最后一个分片中使用上下文 ID。再如，Windows Vista 在第一个分片中使用操作编号报头字段来识别特定函数调用，而 Samba 及其他所有 Windows 版本都在最后一个分片中使用操作编号字段。

Windows 和 Samba SMB 的实现也有很大不同。例如，Windows 在与命名管道配合使用时可识别 SMB OPEN 和 READ 命令，而 Samba 不能识别这些命令。

启用 DCE/RPC 预处理器会自动启用默认基于目标的策略。或者，您可以添加将运行不同 Windows 或 Samba 版本的其他主机设为目标的基于目标的策略。默认基于目标的策略适用于未包含在其他基于目标的策略的任何主机。

在每个基于目标的策略中，可以：

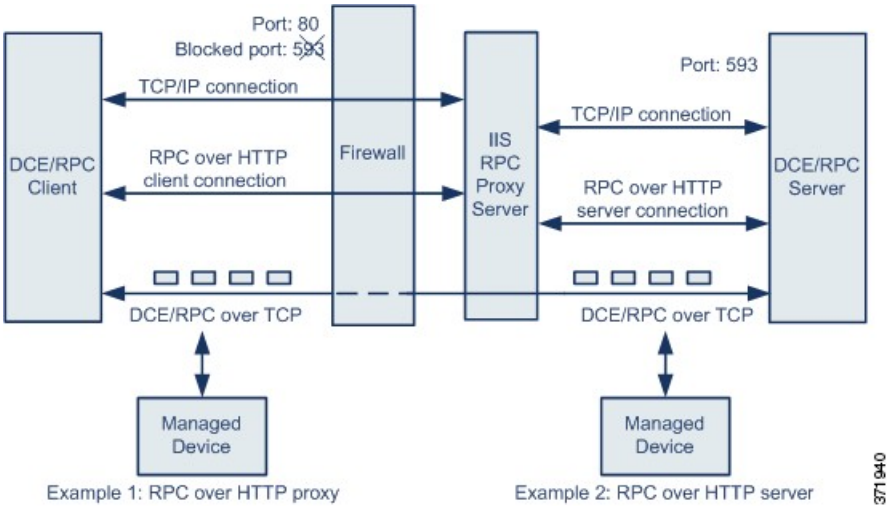
- 启用一个或多个传输并为每个传输指定检测端口
- 启用并指定自动检测端口

- 设置预处理器，以检测尝试连接到一个或多个所识别的共享 SMB 资源的情况
- 将预处理器配置为检测 SMB 流量中的文件，以及检查检测到的文件中的指定字节数
- 修改应仅由具备 SMB 协议专业知识的用户修改的高级选项；通过该选项，可以将预处理器设置为检测链式 SMB AndX 命令数量超过指定最小数量的情况

除在 DCE/RPC 预处理器中启用 SMB 流量文件检测以外，还可以配置文件策略以选择性地捕获和阻止这些文件，或者将这些文件提交到思科 AMP 云以进行动态分析。在策略中，必须创建具有**操作**为 **Detect Files** 或 **Block Files** 且选定**应用协议**为 **Any** 或 **NetBIOS-ssn (SMB)** 的文件规则。

RPC over HTTP 传输

借助 Microsoft RPC over HTTP，可以引导 DCE/RPC 流量穿过防火墙，如下图所示。DCE/RPC 预处理器检测版本 1 Microsoft RPC over HTTP。



Microsoft IIS 代理服务器和 DCE/RPC 服务器可以位于同一主机上，也可以位于不同的主机上。对于这两种情况，都提供独立的代理和服务器选项。对于上图，请注意以下几点：

- DCE/RPC 服务器监控端口 593 的 DCE/RPC 客户端流量，但防火墙阻止该端口。

  默认情况下，防火墙通常会阻止端口 593。

- RPC over HTTP 使用已知 HTTP 端口 80（防火墙通常允许此端口）通过 HTTP 传输 DCE/RPC。
- 在示例 1 中，将会选择 **RPC over HTTP 代理 (RPC over HTTP proxy)** 选项来监控 DCE/RPC 客户端和 Microsoft IIS RPC 代理服务器之间流量。
- 在示例 2 中，如果 Microsoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机，且设备监控这两个服务器之间的流量，将会选择 **RPC OVER HTTP 服务器 (RPC OVER HTTP SERVER)** 选项。
- RPC over HTTP 完成 DCE/RPC 客户端和服务器代理设置后，流量仅包含通过 TCP 传输的面向连接 DCE/RPC。

DCE/RPC 全局选项

DCE/RPC 预处理器全局选项控制预处理器的工作方式。请注意，除 **Memory Cap Reached** 和 **Auto-Detect Policy on SMB Session** 这两个选项外，修改这些选项可能会对性能或检测能力造成负面影响。除非您已充分理解此预处理器及其与已启用的DCE/RPC规则之间的交互，否则请勿修改这些选项。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

最大分片大小 (Maximum Fragment Size)

当选择**启用分片重组 (Enable Defragmentation)** 时，可指定允许的最大 DCE/RPC 分片长度。预处理器会在分片重组前将较大分片截断成为指定的尺寸以便进行处理，但不会改变实际数据包。空白字段将禁用此选项。

确保**最大分片大小 (Maximum Fragment Size)** 选项大于或等于规则需要检测到的深度。

重组阈值 (Reassembly Threshold)

当选择**启用分片重组 (Enable Defragmentation)** 时，0 表示禁用此选项，或者指定分片 DCE/RPC 最小字节数，并且如果适用，则指定在向规则引擎发送已重组的数据包之前要加入队列的分段SMB字节数。值越小，实现早期检测的可能性越高，但可能会对性能造成负面影响。如果启用此选项，应当测试性能所受影响。

确保**重组阈值 (Reassembly Threshold)** 选项大于或等于规则需要检测到的深度。

Enable Defragmentation

指定是否对DCE/RPC流量进行分片整理。当此选项处于禁用状态时，预处理器仍会检测异常并向规则引擎发送 DCE/RPC 数据，但可能会检测不出分片 DCE/RPC 数据中的漏洞。

尽管通过此选项可灵活选择是否对 DCE/RPC 流量进行分片重组，但大多数 DCE/RPC 漏洞都会尝试利用分片隐藏自己。禁用此选项将会忽略大多数已知漏洞，从而造成大量漏报。

Memory Cap Reached

检测达到或超过分配给预处理器的最大内存限制的时间。当达到或超过最大内存上限时，预处理器会释放与造成内存上限事件的会话相关的所有待处理数据并忽略该会话的剩余部分。

可以启用规则 133:1 为此选项生成事件。

SMB 会话上自动检测策略 (Auto-Detect Policy on SMB Session)

检测在 SMB `Session Setup And` 请求和响应中识别出的 Windows 或 Samba 版本。如果检测到的版本不同于为 **Policy** 配置选项配置的 Windows 或 Samba 版本，检测到的版本将会仅覆盖为该会话配置的版本。

例如，如果将 **Policy** 设置为 Windows XP，而预处理器检测到 Windows Vista，预处理器将对该会话使用 Windows Vista 策略。其他设置仍然有效。

如果 DCE/RPC 传输不是 SMB（即，传输协议为 TCP 或 UDP），将无法检测到版本，且策略不能实现自动配置。

要启用此选项，请从下拉列表中选择以下其中一项：

- 选择**客户端 (Client)**，检查该策略类型的服务器到客户端流量。
- 选择**服务器 (Server)**，检查该策略类型的客户端到服务器流量。
- 选择**两者 (Both)**，检查该策略类型的服务器到客户端流量和客户端到服务器流量。

传统 SMB 检测模式 (Legacy SMB Inspection Mode)

指定要检测的 SMB 版本。当启用**传统 SMB 检测模式 (Legacy SMB Inspection Mode)** 时，DCE/RPC 预处理器仅检查 SMB 版本 1 流量。当禁用此选项时，DCE/RPC 预处理器会检查使用 SMB 版本 1、2 和 3 的流量。

DCE/RPC 基于目标的策略选项

在每个基于目标的策略中，都可以启用一个或多个 TCP、UDP、SMB 和 RPC over HTTP 传输。启用传输时，还必须指定一个或多个检测端口（即，已知用于传输 DCE/RPC 流量的端口）。

思科建议使用默认检测端口，这些端口可以是已知端口，也可以是各协议的常用端口。在非默认端口检测到 DCE/RPC 流量的情况下才可以添加端口。

可以在 Windows 基于目标的策略中为一个或多个传输指定任意组合的端口，以便与网络流量匹配，但是，在 Samba 基于目标的策略中只能为 SMB 传输指定端口。

注释 在基于目标的默认策略中必须至少启用一个 DCE/RPC 传输，除非已添加至少启用了一个传输的 DCE/RPC 基于目标的策略。例如，可能要为所有 DCE/RPC 实施指定主机且不将基于目标的默认策略部署到未指定的主机，在此情况下，不会为基于目标的默认策略启用传输。

或者，也可以启用和指定自动检测端口；预处理器会首先对这些端口进行测试，以确定它们是否传输 DCE/RPC 流量，仅在检测到 DCE/RPC 流量的情况下，预处理器才会继续进行处理。

启用自动检测端口时，请确保将端口范围设置为 1025 到 65535，以便覆盖整个临时端口范围。

请注意，仅对于传输检测端口尚未识别的端口才会出现自动检测。

对于“RPC over HTTP 代理自动检测端口”(RPC over HTTP Proxy Auto-Detect Ports) 选项或“SMB 自动检测端口”(SMB Auto-Detect Ports) 选项，不太可能会启用或指定自动检测端口，因为除非是在指定的默认检测端口上，否则任一端口出现流量的可能性极低甚至不可能出现。

每个基于目标的策略都允许指定以下各个选项。如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络

要部署 DCE/RPC 基于目标的服务器策略的主机 IP 地址。此外，当添加基于目标的策略时，命名“添加目标”(Add Target) 弹出窗口中的**服务器地址 (Server Address)** 字段。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可以配置总共 255 个配置文件，包括默认策略。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

策略

目标主机或受监控网段上主机使用的 Windows 或 Samba DCE/RPC 实现。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖每个会话的此选项的设置。

SMB Invalid Shares

用于在尝试连接到指定的共享资源时，识别预处理器将检测的一个或多个 SMB 共享资源。您可以在逗号分隔列表中指定多个共享，或者可以将共享用引号引起来（旧版软件要求这样做，但现在不再有此要求），例如：

```
"C$", D$, "admin", private
```

启用 **SMB 端口 (SMB Ports)** 后，预处理器会检测 SMB 流量中的无效共享。

请注意，大多数情况下，对于被识别为无效共享的 Windows 命名的驱动器，应该在其后面附上一个美元符号。例如，将驱动器 C 标识为 C$ 或 "C$"。

另请注意，要检测 SMB 无效共享，还必须启用 **SMB 端口 (SMB Ports)** 或 **SMB 自动检测端口 (SMB Auto-Detect Ports)**。

可以启用规则 133:26 为此选项生成事件。

SMB Maximum AndX Chain

允许的链式 SMB AndX 命令的最大数量。通常，超过若干链式 AndX 命令即表示存在异常行为，可能代表有躲避行为。指定 1 表示不允许链式命令，指定 0 将会禁止检测链式命令数量。

请注意，预处理器会首先计算链式命令数量，如果随附的 SMB 预处理器规则已启用，并且链式命令数量等于或超过配置的值，预处理器将会生成事件。然后会继续进行处理。

注意 只有 SMB 协议专业人员可以修改 **SMB Maximum AndX Chains** 选项的设置。

可以启用规则 133:20 为此选项生成事件。

RPC proxy traffic only

启用 **RPC over HTTP 代理端口 (RPC over HTTP Proxy Ports)** 指示检测到的客户端 RPC over HTTP 流量只是代理流量还是可能包含其他 Web 服务器流量。例如，端口 80 可能传输代理流量和其他网络服务器流量。

此选项处于禁用状态时，将会同时传输代理流量和其他网络服务器流量。例如，如果服务器是专用代理服务器，请启用此选项。启用此选项后，预处理器会测试流量以确定其是否传输DCE/RPC，如果不是，预处理器将会忽略该流量，如果是，则继续进行处理。请注意，仅在已选择**RPC over HTTP Proxy Ports** 复选框的情况下，此选项才有用。

RPC over HTTP Proxy Ports

如果受管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过每个指定端口传输的 DCE/RPC 流量启用检测。

启用此选项后，可以添加任意发现DCE/RPC流量的端口，但是这项操作一般并不必要，因为网络服务器通常使用默认端口传输 DCE/RPC 和其他流量。启用此选项后，不可以启用 **RPC over HTTP Proxy Auto-Detect Ports**，但如果检测到的客户端 RPC over HTTP 流量仅包含代理流量而不包含其他网络服务器流量，可以启用 **RPC Proxy Traffic Only**。

注释 如有可能，很少会选择此选项。

RPC over HTTP Server Ports

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对每个指定端口上通过 RPC over HTTP 传输的 DCE/RPC 流量启用检测。

启用此选项后，通常还应启用 **RPC over HTTP Server Auto-Detect Ports**（端口范围介于 1025 到 65535 之间），即使不知道网络上是否存在任何代理网络服务器。请注意，RPC over HTTP 服务器端口有时会重新配置，在这种情况下，应该为此选项将重新配置的服务器端口添加到端口列表。

TCP 端口

对每个指定端口上 TCP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **TCP Auto-Detect Ports**（端口范围介于 1025 到 65535 之间）。

UDP 端口

对每个指定端口上 UDP 中的 DCE/RPC 流量启用检测。

合法 DCE/RPC 流量和漏洞可能使用多种端口，高于端口 1024 的其他端口很常用。启用此选项后，通常还应启用 **UDP Auto-Detect Ports**（端口范围介于 1025 到 65535 之间）。

SMB Ports

对每个指定端口上 SMB 中的 DCE/RPC 流量启用检测。

可能会出现使用默认检测端口的 SMB 流量。其他端口很少见。通常使用默认设置。

请注意，可以启用 **Auto-Detect Policy on SMB Session** 全局选项，以便在 DCE/RPC 传输是 SMB 时自动覆盖为每个会话的目标策略配置的策略类型。

RPC over HTTP Proxy Auto-Detect Ports

如果受管设备位于 DCE/RPC 客户端与 MicroSoft IIS RPC 代理服务器之间，可以使用此选项对 RPC over HTTP 通过指定端口传输的 DCE/RPC 流量启用自动检测。

启用此选项后，通常需要指定介于 1025 到 65535 之间的端口范围，以覆盖整个临时端口范围。

RPC over HTTP Server Auto-Detect Ports

当 MicroSoft IIS RPC 代理服务器和 DCE/RPC 服务器位于不同的主机且设备监控这两个服务器之间流量时，对指定端口上通过 RPC over HTTP 传输的 DCE/RPC 启用自动检测。

TCP Auto-Detect Ports

对指定端口上 TCP 中的 DCE/RPC 流量启用自动检测。

UDP Auto-Detect Ports

对指定端口上 UDP 中的 DCE/RPC 流量启用自动检测。

SMB Auto-Detect Ports

对 SMB 中的 DCE/RPC 流量启用自动检测。

注释 如有可能，很少会选择此选项。

SMB File Inspection

启用 SMB 流量检查以检测文件。您有以下选择：

- 选择 **Off** 禁用文件检查。
- 选择 **Only**，检查文件数据但不检查 SMB 中的 DCE/RPC 流量。选择此选项可以提高文件和 DCE/RPC 流量检查性能。
- 选择 **On**，检查 SMB 中的文件和 DCE/RPC 流量。选择此选项可能会影响性能。

以下各项不支持 SMB 流量检查：

- 在启用此选项和应用政策之前在建立的 TCP 或 SMB 会话中传输的文件
- 单一 TCP 或 SMB 会话同时传输的文件
- 在多个 TCP 或 SMB 会话之间传输的文件
- 与非连续数据一起传输的文件（例如，协商了消息签名时）
- 与具有相同偏移量的不同数据一起传输的文件（与数据重叠）
- 在远程客户端打开用于编辑并由客户端保存到文件服务器的文件

SMB File Inspection Depth

如果 **SMB File Inspection** 设置为 **Only** 或 **On**，此选项表示在 SMB 流量中检测到文件时检查的字节数。指定以下各项之一：

- 正值
- `0` 以检查整个文件
- `-1` 以禁用文件检查

在此字段中输入小于或等于访问控制策略中“高级”(Advanced)选项卡的“文件和恶意软件设置”(File and Malware Settings) 部分中定义的值。如果为此选项设置的值大于为**限制执行文件类型检测时检查到的字节数 (Limit the number of bytes inspected when doing file type detection)** 定义的值，则系统使用访问控制策略设置作为有效的最大值。

如果 **SMB File Inspection** 设置为 **Off**，此字段将被禁用。

与流量关联的 DCE/RPC 规则

大多数 DCE/RPC 预处理器规则都会针对 SMB、面向连接的 DCE/RPC 或无连接 DCE/RPC 流量中检测到的异常和规避技术生成事件。下表列出了可为各类流量启用的规则。

表 *168*: 与流量关联的 *DCE/RPC* 规则

交通	预处理器规则 GID:SID
SMB	133:2 到 133:26，以及 133:48 到 133:57
面向连接 DCE/RPC	133:27 到 133:39
检测无连接 DCE/RPC	133:40 到 133:43

配置 DCE/RPC 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

要配置DCE/RPC预处理器，可以修改控制预处理器工作方式的全局选项，并指定一个或多个基于目标的服务器策略，从而通过 IP 地址和运行的 Windows 或 Samba 版本识别网络上的 DCE/RPC 服务器。基于目标的策略配置还包括启用传输协议、指定将DCE/RPC流量传输到这些主机的端口以及设置其他服务器特定选项。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 993 页。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击左侧导航面板中的 **Settings**。

步骤 4 如果**应用层预处理器(Application Layer Preprocessors)** 下的 **DCE/RPC 配置 (DCE/RPC Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **DCE/RPC 配置 (DCE/RPC Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改**全局设置 (Global Settings)** 部分中的选项；请参阅DCE/RPC 全局选项，第 1007 页。

步骤 7 有以下选项可供选择：

- 添加服务器配置文件 - 点击**服务器 (Servers)** 旁边的添加图标 ( )。在**服务器地址 (Server Address)** 字段中指定一个或多个 IP 地址，然后点击**确定 (OK)**。
- 删除服务器配置文件 - 点击策略旁边的删除图标 ( )。
- 编辑服务器配置文件 - 在**服务器 (Servers)** 下点击配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的任何设置；请参阅DCE/RPC 基于目标的策略选项，第 1008 页。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 DCE/RPC 预处理器规则（GID 132 或 133）。有关详细信息，请参阅设置入侵规则状态，第 833 页、DCE/RPC 全局选项，第 1007 页、DCE/RPC 基于目标的策略选项，第 1008 页和与流量关联的 DCE/RPC 规则，第 1012 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

DNS 预处理器

DNS 预处理器会检查 DNS 域称服务器响应中是否存在以下具体漏洞：

- RData 文本字段中的溢出尝试
- 过时的 DNS 资源记录类型
- 试验性 DNS 资源记录类型

最常见的 DNS 域称服务器响应类型提供与促成响应的查询中域名对应的一个或多个 IP 地址。其他服务器响应类型提供邮件消息目的地或者可提供从最初查询的服务器无法获得的信息的域名服务器位置等等。

DNS 响应包括：

- 消息报头
- 包含一个或多个请求的问题部分
- 与问题部分中的请求对应的三个部分

  应答

  权限

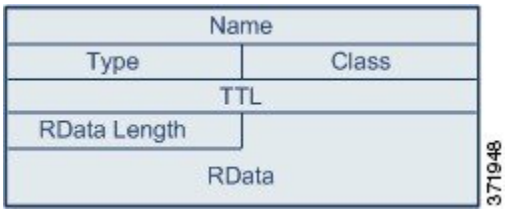
  其他信息 (Additional Information)。

这三个部分中的响应反映域名服务器内保留的资源记录 (RR)。下表将介绍这三个部分。

表 *169*: *DNS* 域名服务器 *RR* 响应

部分	包含的内容	示例
应答	（可选）为查询提供明确答复的一个或多个资源记录	对应于域名的 IP 地址
权限	（可选）指向授权域名服务器的一个或多个资源记录	用于响应的授权域名服务器的名称
更多信息	（可选）提供与 Answer 部分相关的其他信息的一个或多个资源记录	要查询的另一个服务器的 IP 地址

有许多类型的资源记录，全部遵循以下结构：



理论上，任何类型的资源记录均可用于域名服务器响应消息的 Answer、Authority 或 Additional Information 部分。DNS 预处理器会检查这三个响应部分中的资源记录是否存在其会检测的漏洞。

Type 和 RData 资源记录字段对于 DNS 预处理器特别重要。Type 字段识别资源记录类型。RData（资源数据）字段提供响应内容。RData 字段的大小和内容因资源记录类型而异。

DNS 消息通常使用 UDP 传输协议，但如果消息类型需要可靠传输或者消息大小超过 UDP 能力，DNS 消息也会使用 TCP。DNS 预处理器会检查 UDP 和 TCP 流量中的 DNS 服务器响应。

DNS 预处理器不会检查在中途恢复的 TCP 会话，如果会话因丢包而丧失状态，DNS 预处理器将会停止检查。

DNS 预处理器选项

端口

此字段指定 DNS 预处理器应为 DNS 服务器响应监控的源端口。使用逗号分隔多个端口。

为 DNS 预处理器配置的典型端口为已知端口 53，DNS 域名服务器对在 UDP 和 TCP 中传输的 DNS 消息使用该端口。

检测 RData 文本字段中的溢出尝试 (Detect Overflow attempts on RData Text fields)

当资源记录类型为 TXT（文本）时，RData 字段为长度可变的 ASCII 文本字段。

如果选择此选项，系统将会检测条目 CVE-2006-3441 在 MITRE 的当前漏洞和风险数据库中识别出的特定漏洞。这是 Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1、Windows XP Service Pack 2 和 Windows Server 2003 Service Pack 1 中的已知漏洞。攻击者可以利用该漏洞发送或者导致主机接收恶意域名服务器响应，导致 RData 文本字段长度计算错误，造成缓冲区溢出，最终全面控制主机。

如果网络上可能有主机运行尚未升级纠正该漏洞的操作系统，应该启用此选项。

可以启用规则 131:3 为此选项生成事件。

检测过时的 DNS RR 类型 (Detect Obsolete DNS RR Types)

RFC 1035 将多种资源记录类型识别为过时类型。由于这些是过时记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测过时的资源记录类型。下表列出并说明这些记录类型。

表 *170*：过时的 *DNS* 资源记录类型

RR 类型	代码	说明
3	MD	邮件目的地
4	MF	邮件转发器

可以启用规则 131:1 为此选项生成事件。

检测试验性 DNS RR 类型 (Detecting Experimental DNS RR Types)

RFC 1035 将多种资源记录类型识别为试验性类型。由于这些是试验性记录类型，因此，某些系统未对其进行说明，可能容易产生漏洞。在正常 DNS 响应中不会遇到这些记录类型，除非故意将网络配置为包含这些记录类型。

可以将系统配置为会检测试验性资源记录类型。下表列出并说明这些记录类型。

表 *171*：试验性 *DNS* 资源记录类型

RR 类型	代码	说明
7	MB	邮箱域名
8	MG	邮件组成员
9	MR	邮件重命名域名
10	NUL	空资源记录

可以启用规则 131:2 为此选项生成事件。

配置 DNS 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **DNS 配置 (DNS Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **DNS 配置 (DNS Configuration)** 旁边的编辑图标 ()。

步骤 6 修改DNS 预处理器选项，第 1015 页中所述的设置。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 DNS 预处理器规则 (GID 131)。有关详细信息，请参阅设置入侵规则状态，第 833 页和DNS 预处理器选项，第 1015 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

FTP/Telnet 解码器

FTP/Telnet 解码器会分析 FTP 和 Telnet 数据流，对 FTP 和 Telnet 命令进行规范化，再由规则引擎处理这些命令。

全局 FTP 和 Telnet 选项

可以设置全局选项以确定 FTP/Telnet 解码器是否对数据包执行状态检查或无状态检查，是否检测加密 FTP 或 Telnet 会话，以及是否在遇到加密数据后继续检查数据流。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

状态性检查

如果选择此选项，FTP/Telnet 解码器将会保存状态，提供各个数据包的会话情景，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

要检查 FTP 数据传输，必须选择此选项。

Detect Encrypted Traffic

检测加密 Telnet 和 FTP 会话。

可以启用规则 125:7 和 126:2 为此选项生成事件。

Continue to Inspect Encrypted Data

指示预处理器在数据流加密后持续检查数据流，以寻找可处理的最终解密数据。

Telnet 选项

可以通过 FTP/Telnet 解码器启用或禁用 Telnet 命令规范化，启用或禁用特定异常情况，以及设置允许的 Are You There (AYT) 攻击阈值。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指明要实现 Telnet 流量规范化的端口。Telnet 通常连接到 TCP 端口 23。可在此界面列出多个端口，端口之间用逗号分隔。

注意 由于加密流量 (SSL) 无法解码，因此，添加端口 22 (SSH) 可能会产生意外结果。

Normalize

对流向指定端口的 Telnet 流量进行规范化。

Detect Anomalies

检测没有对应 SE（下级协商终点）的 Telnet SB（下级协商起点）。

Telnet 支持以 SB（下级协商起点）开始并且必须以 SE 结束（下级协商终点）的下级协商。但是，Telnet 服务器的某些实现将忽略无对应 SE 的 SB。这是异常行为，可能意味着存在躲避行为。由于 FTP 在控制接口使用 Telnet 协议，因此也容易受此行为影响。

如果在 Telnet 流量中检测到这种异常，可以启用规则 126:3 生成事件；如果在 FTP 命令通道中检测到这种异常，可以启用规则 125:9 生成事件。

Are You There Attack Threshold Number

检测超过指定阈值的连续 AYT 命令数量。思科建议将 AYT 阈值设置为不超过默认值的数值。

可以启用规则 126:1 为此选项生成事件。

服务器级别 FTP 选项

可以在多个FTP服务器上设置解码选项。创建的每个服务器配置文件都包含服务器IP地址以及应监控其流量的服务器端口。可以为特定服务器指定需要验证和可忽略的 FTP 命令，以及设置最大命令参数长度。还可以设置解码器应针对特定命令验证的具体命令语法，以及设置替代最大命令参数长度。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络

使用此选项可指定 FTP 服务器的一个或多个 IP 地址。

可以指定单个IP地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可配置 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定IP地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

端口

使用此选项可指定受管设备应监控其流量的 FTP 服务器上的端口。可在此界面列出多个端口，端口之间用逗号分隔。端口 21 是已知的 FTP 流量端口。

File Get Commands

使用此选项可定义用于从服务器向客户端传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员要求这样做。

注意 请勿修改**文件获取命令 (File Get Commands)** 字段，除非支持人员指示执行此操作。

File Put Commands

使用此选项可定义用于从客户端向服务器传输文件的 FTP 命令。请勿改变此选项的值，除非支持人员要求这样做。

注意 请勿修改**文件放置命令 (File Put Commands)** 字段，除非支持人员指示执行此操作。

Additional FTP Commands

使用此行可指定解码器应检测的其他命令。使用空格隔开其他命令。

可能需要添加的其他命令包括 XPWD、XCWD、XCUP、XMKD 和 XRMD。有关这些命令的详细信息，请参阅网络工作组发布的 RFC775《面向目录的 FTP 命令规范》。

Default Max Parameter Length

在未设置替代最大参数长度的情况下，使用此选项可检测命令的最大参数长度。可以根据需要添加尽可能多的替代最大参数长度。

可以启用规则 125:3 为此选项生成事件。

Alternate Max Parameter Length

使用此选项可指定要为其检测其他最大参数长度的命令，并指定这些命令的最大参数长度。点击**Add** 可添加行，在添加的行中可指定其他最大参数长度，以便检测特定命令。

Check Commands for String Format Attacks

使用此选项可检查指定命令的字符串格式攻击。

可以启用规则 125:5 为此选项生成事件。

Command Validity

使用此选项可为特定命令输入有效格式。点击 **Add** 可添加命令验证行。

可以启用规则 125:2 和 125:4 为此选项生成事件。

Ignore FTP Transfers

使用此选项可禁用除数据传输通道状态检查之外的所有检查，从而提高 FTP 数据传输的性能。

注释　要检查数据传输，必须选择 FTP/Telnet **状态检查 (Stateful Inspection)** 全局选项。

Detect Telnet Escape Codes within FTP Commands

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 为此选项生成事件。

Ignore Erase Commands during Normalization

如果选择了 **Detect Telnet Escape Codes within FTP Commands**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 服务器处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 服务器通常会忽略 Telnet 擦除命令，而旧服务器通常会进行处理。

故障排除选项：记录 FTP 命令验证配置 (Troubleshooting Option: Log FTP Command Validation Configuration)

支持人员可能要求您在故障排除呼叫期间配置系统，以打印为服务器列出的每个 FTP 命令的配置信息。

注意　请勿启用**记录 FTP 命令验证配置 (Log FTP Command Validation Configuration)**，除非支持人员指示执行此操作。

FTP 命令验证语句

为 FTP 命令创建验证语句时，可以通过使用空格隔开参数来指定一组替代参数。还可以在两个参数之间建立二进制 OR 关系，方法是使用竖线 (|) 隔开这两个参数。用方括号 ([]) 引起来的参数是可选参数。用花括号 ({}) 引起来的参数是必要参数。

可以创建 FTP 命令参数验证语句，以验证作为 FTP 通信一部分接收的参数的语法。

下表中列出的任何参数均可用于 FTP 命令参数验证语句中。

表 *172*：*FTP* 命令参数

使用的参数	出现的验证
int	所代表的参数必须是整数。
数字	所代表的参数必须是 1 到 255 之间的整数。
char_chars	所代表的参数必须是单个字符，并且是 _chars 参数中指定的字符成员。 例如，使用验证语句 char SBC 验证 MODE 的命令有效性会检查 MODE 命令的参数是否包含字符 S（表示流模式）、字符 B（表示阻止模式）或字符 C（表示压缩模式）。
date_datefmt	如果 _datefmt 包含 #，所代表的参数必须是数字。 如果 _datefmt 包含 C，所代表的参数必须是字符。 如果 _datefmt 包含文字字符串，所代表的参数必须与文字字符串相匹配。
字符串	所代表的参数必须是字符串。
host_port	所代表的参数必须是有效的主机端口说明符（如网络工作组发布的 RFC959《文件传输协议规范》中所规定）。

可以根据需要结合使用上表中的语法来创建参数验证语句，以便在需要验证流量时能够正确验证每个 FTP 命令。

注释 如果要在TYPE命令中包含复杂的表达式，应将表达式放在空格之间。此外，应将每个操作数放在空格之间。例如，键入 `char A | B`，而非 `char A|B`。

客户端级别 FTP 选项

可以为 FTP 客户端创建配置文件。在每个配置文件中，可以指定来自客户端的 FTP 响应的最大响应长度。还可以配置解码器是否检测反弹攻击，以及为特定客户端在 FTP 命令通道上使用 Telnet 命令。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络

使用此选项可指定 FTP 客户端的一个或多个 IP 地址。

可以指定单个IP地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。最多可指定 1024 个字符，最多可指定 255 个配置文件（包括默认配置文件）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定IP地址或地址块，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

Max Response Length

使用此选项可指定来自 FTP 客户端的响应字符串的最大长度。

可以启用规则 125:6 为此选项生成事件。

Detect FTP Bounce Attempts

使用此选项可检测 FTP 反弹攻击。

可以启用规则 125:8 为此选项生成事件。

Allow FTP Bounce to

使用此选项可配置包含附加主机以及这些主机上端口的列表，在这些主机上，FTP PORT 命令不应被视为 FTP 反弹攻击。

Detect Telnet Escape Codes within FTP Commands

使用此选项可检测何时在 FTP 命令通道上使用 Telnet 命令。

可以启用规则 125:1 为此选项生成事件。

Ignore Erase Commands During Normalization

如果选择了 **Detect Telnet Escape Codes within FTP Commands**，使用此选项可在 FTP 流量规范化过程中忽略 Telnet 字符和行擦除命令。此选项的设置应与 FTP 客户端处理 Telnet 擦除命令的方式相匹配。请注意，新 FTP 客户端通常会忽略 Telnet 擦除命令，而旧客户端通常会进行处理。

配置 FTP/Telnet 解码器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以为 FTP 客户端配置客户端配置文件，以监控来自客户端的 FTP 流量。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 993 页。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)** 已禁用，请点击**已启用 (Enabled)**.。

步骤 5 点击 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)** 旁边的编辑图标 ( )。

步骤 6 设置**全局设置 (Global Settings)** 部分中的选项，如全局 FTP 和 Telnet 选项，第 1017 页中所述。

步骤 7 设置 **Telnet 设置 (Telnet Settings)** 部分中的选项，如Telnet 选项，第 1018 页中所述。

步骤 8 管理 FTP 服务器配置文件：

- 添加服务器配置文件 - 点击 **FTP 服务器 (FTP Server)** 旁边的添加图标 ( )。在**服务器地址 (Server Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。

- 编辑服务器配置文件 - 在 **FTP 服务器 (FTP Servers)** 下点击自定义配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的设置；请参阅服务器级别 FTP 选项，第 1019 页。
- 删除服务器配置文件 - 点击配置文件旁边的删除图标 ( )。

步骤 9 管理 FTP 客户端配置文件：

- 添加客户端配置文件 - 点击 **FTP 客户端 (FTP Client)** 旁边的添加图标 ( )。在**客户端地址 (Client Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可指定 1024 个字符，最多可配置 255 个策略（包括默认策略）。
- 编辑客户端配置文件 - 在 **FTP 客户端 (FTP Client)** 下点击已添加配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改“配置”(Configuration) 页面区域中的设置；请参阅客户端级别 FTP 选项，第 1022 页。
- 删除客户端配置文件 - 点击自定义配置文件旁边的删除图标 ( )。

步骤 10 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 FTP 和 Telnet 预处理器规则（GID 125 和 126）。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

HTTP 检查预处理器

HTTP 检查预处理器负责以下工作：

- 解码和规范化发送到网络上网络服务器的 HTTP 请求以及来自该服务器的 HTTP 响应
- 将发送到网络服务器的消息分成 URI、非 cookie 报头、cookie 报头、方法和消息正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 将从网络服务器接收到的消息分成状态代码、状态消息、非 set-cookie 报头、cookie 报头和响应正文等组成部分，以提高与 HTTP 相关的入侵规则的性能
- 检测可能的 URI 编码攻击
- 使规范化数据可用于附加规则处理

HTTP 流量可以各种格式进行编码，因此规则很难适当地进行检查。HTTP 检查可解码 14 种编码，从而确保 HTTP 流量获得可能的最佳检查。

可以在一个服务器上或者对服务器列表全局配置 HTTP 检查选项。

请注意，预处理器引擎无状态地执行 HTTP 规范化。也就是说，它会逐个数据包进行 HTTP 字符串规范化，并且只能处理已由 TCP 数据流预处理器重组的 HTTP 字符串。

全局 HTTP 规范化选项

为 HTTP 检查预处理器的全局 HTTP 选项用于控制预处理器的工作方式。如果由未指定为网络服务器的端口接收 HTTP 流量，可使用这些选项启用或禁用 HTTP 规范化。

请注意以下几点：

- 如果启用 **Unlimited Decompression**，提交修改时，**Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 选项将会自动设置为 65535。
- 当**最大压缩数据深度 (Maximum Compressed Data Depth)** 或**最大解压缩数据深度 (Maximum Decompressed Data Depth)** 的值在以下位置不同时，将会使用最高值：

  默认网络分析策略

  由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

Detect Anomalous HTTP Servers

检测发送到未指定为网络服务器的端口或由其接收的 HTTP 流量。

注释 如果启用此选项，请确保在“HTTP 配置”(HTTP Configuration) 页面上的服务器配置文件中列出会接收 HTTP 流量的所有端口。如果不这样做，并且启用此选项以及随附的预处理器规则，则与该服务器之间的正常流量会生成事件。默认的服务器配置文件包含所有通常用于 HTTP 流量的端口，但如果修改了该配置文件，可能需要将这些端口添加到另一个配置文件中，以防止生成事件。

可以启用规则 120:1 为此选项生成事件。

Detect HTTP Proxy Servers

检测使用未由 **Allow HTTP Proxy Use** 选项定义的代理服务器的 HTTP 流量。

可以启用规则 119:17 为此选项生成事件。

Maximum Compressed Data Depth

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置要解压缩的压缩数据的最大大小。

Maximum Decompressed Data Depth

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，设置规范化解压缩数据的最大大小。

服务器级别 HTTP 规范化选项

可以为监控的每个服务器、全局地为所有服务器或者为服务器列表设置服务器级别选项。此外，可以根据环境需求，使用预定义的服务器配置文件来设置这些选项，或者单独设置这些选项。可以使用这些选项或设置这些选项的其中一个默认配置文件来指定要规范化其流量的 HTTP 服务器端口、要规范化的服务器响应负载以及要规范化的编码的类型。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

网络

使用此选项可指定一个或多个服务器的 IP 地址。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

除总共最多 255 个配置文件（包括默认配置文件）的限制以外，还可以在 HTTP 服务器列表中包含最多 496 个字符（或大约 26 个条目），并为所有服务器配置文件指定总共最多 256 个地址条目。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

端口

预处理器引擎会对其 HTTP 流量进行规范化的端口。使用逗号分隔多个端口号。

Oversize Dir Length

检测长度超过指定值的 URL 目录。

可以启用规则 119:15 为此选项生成事件。

Client Flow Depth

为要在 **Ports** 中定义的客户端 HTTP 流量中的原始 HTTP 数据包（包括报头和负载数据）中检查的规则指定字节数。如果规则中的 HTTP 内容规则选项检查请求消息的特定部分，客户端流量深度不适用。

可指定以下任意值：

- 正值，检查第一个数据包中的指定字节数。如果第一个数据包包含的字节数小于指定值，将会检查整个数据包。请注意，指定值适用于分段和重组的数据包。

  另请注意，值 300 通常表示许多客户端请求报头末尾出现的大尺寸 HTTP Cookie 无需检查。

- 0 将会检查所有客户端流量，包括会话中的多个数据包，在必要时可超出字节上限。请注意，此值可能会影响性能。
- -1 将会忽略所有客户端流量。

Server Flow Depth

为要在 **Ports** 中指定的服务器端 HTTP 流量中的原始 HTTP 数据包中检查的规则指定字节数。**检查 HTTP 响应 (Inspect HTTP Responses)** 处于禁用状态时，会检查原始报头和负载；**检查 HTTP 响应 (Inspect HTTP Responses)** 处于启用状态时，仅检查原始响应正文。

Server Flow Depth 为要在 **Ports** 中定义的服务器端 HTTP 流量中检查的规则指定会话中原始服务器响应数据的字节数。可以使用此选项来平衡 HTTP 服务器响应数据的性能和检查水平。如果规则中的 HTTP 内容规则选项检查响应消息的特定部分，服务器流量深度不适用。

不同于客户端流量深度，服务器流量深度为要检查的规则指定每个 HTTP 响应而非每个 HTTP 请求数据包的字节数。

可以指定以下任何内容：

- 正值：

  当 **Inspect HTTP Responses** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查非原始 HTTP 报头；当 **Inspect Compressed Data** 处于启用状态时，还会同时检查解压缩数据。

  当 **Inspect HTTP Responses** 处于**禁用**状态时，会检查原始数据包报头和负载。

  如果会话包含的响应字节小于指定值，规则将会根据需要在多个数据包中彻底检查给定会话中的所有响应数据包。如果会话包含的响应字节大于指定值，规则将会根据需要在多个数据包中仅检查该会话中的指定字节数。

  请注意，流量深度值小可能会导致针对 **Ports** 中定义的服务器端流量的规则出现漏报。大多数这些规则针对的是，可能处于非报头数据的大约前 100 字节中的 HTTP 报头或内容。报头长度通常少于 300 字节，但报头大小可以不同。

  另请注意，指定值适用于分段和重组的数据包。

- 0 将会为 **Ports** 中定义的所有 HTTP 服务器端流量检查整个数据包（包括超过 65535 字节的会话中的响应数据）。

  请注意，此值可能会影响性能。

- -1：

  当 **Inspect HTTP Responses** 处于**启用**状态时，仅检查原始 HTTP 响应正文，不会检查原始 HTTP 响应正文。

  当 **Inspect HTTP Responses** 处于**禁用**状态时，会忽略在 **Ports** 中定义的所有服务器端流量。

Maximum Header Length

检测 HTTP 请求中长度超过指定最大字节数的报头字段；如果启用了 **Inspect HTTP Responses**，还会对 HTTP 响应执行此项检查。值 0 将会禁用此选项。指定正值可启用此选项。

可以启用规则 119:19 为此选项生成事件。

Maximum Number of Headers

检测 HTTP 请求中的报头数量超过此设置的情况。值 0 将会禁用此选项。指定正值可启用此选项。

可以启用规则 119:20 为此选项生成事件。

Maximum Number of Spaces

当 HTTP 请求中折线中的空格数量等于或超过此设置时，进行检测。值 0 将会禁用此选项。指定正值可启用此选项。

可以启用规则 119:26 为此选项生成事件。

HTTP Client Body Extraction Depth

指定从 HTTP 客户端请求的消息正文提取的字节数。通过选择 `content` 或 `protected_content` 关键字 **HTTP Client Body** 选项，可以使用入侵规则检查提取的数据。

指定 -1 将会忽略客户端正文。指定 0 将会提取整个客户端正文。请注意，指定特定字节数进行提取可提高系统性能。另请注意，要使 **HTTP 客户端正文 (HTTP Client Body)** 选项在入侵规则中起作用，必须为此选项指定一个大于或等于 0 的值。

Small Chunk Size

指定被认为是小数据块的数据块可包含的最大字节数。指定一个正值。值 0 将会禁用对异常连续小片段的检测。有关详细信息，请参阅 **Consecutive Small Chunks** 选项。

Consecutive Small Chunks

指定在使用分块传输编码的客户端流量或服务器流量中，代表异常大数量的连续小数据块的数量。**Small Chunk Size** 选项指定小数据块的最大大小。

例如，将 **Small Chunk Size** 设置为 10 并将 **Consecutive Small Chunks** 设置为 5，可检测包含 10 个或更少字节的 5 个连续数据块。

对于客户端流量和服务器流量，可分别启用预处理器规则 119:27 和 120:7 针对过多小数据块这种情况触发事件。如果 **Small Chunk Size** 已启用且此选项设置为 0 或 1，启用这些规则将会对每个指定大小或更小的数据块触发事件。

HTTP Methods

指定除系统预期会在流量中遇到的 GET 和 POST 以外的 HTTP 请求方法。使用逗号隔开多个值。

入侵规则将 `content` 或 `protected_content` 关键字与 **HTTP Method** 参数配合使用来搜索 HTTP 方法中的内容。如果在流量中遇到GET、POST或为此选项配置的方法以外的方法，可以启用规则119:31生成事件。

No Alerts

当随附的预处理器规则处于启用状态时禁用入侵事件。

注释 此选项**不会**禁用 HTTP 标准文本规则和共享对象规则。

Normalize HTTP Headers

当 **Inspect HTTP Responses** 处于启用状态时，启用请求和响应报头中非 cookie 数据的规范化。如果**未**启用 **Inspect HTTP Responses**，启用请求和响应报头中 HTTP 报头（包括 cookie）的规范化。

Inspect HTTP Cookies

允许从 HTTP 请求提取 cookie。如果 **Inspect HTTP Responses** 已启用，还允许从响应报头提取 set-cookie 数据。当不需要提取 cookie 时，禁用此选项可提高性能。

请注意，`Cookie:` 和 `Set-Cookie:` 报头名称、标题行中的前导空格以及终止标题行的 `CRLF` 将作为报头的一部分而非 cookie 的一部分进行检查。

Normalize Cookies in HTTP headers

启用 HTTP 请求报头中 cookie 的规范化。当 **Inspect HTTP Responses** 处于启用状态时，还会启用响应报头中 set-cookie 数据的规范化。选择了 **Inspect HTTP Cookies** 之后才能选择此选项。

Allow HTTP Proxy Use

允许将受监控的网络服务器用作 HTTP 代理。此选项仅用于检查 HTTP 请求。

Inspect URI Only

仅检查规范化 HTTP 请求数据包的 URI 部分。

Inspect HTTP Responses

启用对 HTTP 响应的延展检查，从而使预处理器不仅会对 HTTP 请求消息进行解码和规范化，还会提取响应字段以供规则引擎进行检查。启用此选项后，系统会提取响应报头、正文、状态代码等；如果还启用了 **Inspect HTTP Cookies**，系统还会提取 set-cookie 数据。

可以启用规则 120:2 和 120:3 为此选项生成事件。

Normalize UTF Encodings to UTF-8

如果启用了 **Inspect HTTP Responses**，此选项检测 HTTP 响应中的 UTF-16LE、UTF-16BE、UTF-32LE 和 UTF32-BE 编码，并将其规范化为 UTF-8。

可以启用规则 120:4 为此选项生成事件。

Inspect Compressed Data

当 **Inspect HTTP Responses** 已启用时，此选项启用 HTTP 响应正文中的 gzip 和兼容 deflate 的压缩数据的解压，以及对规范化解压缩数据的检查。系统将检查分块和非分块 HTTP 响应数据。系统会根据需要逐一检查多个数据包中的解压缩数据；也就是说，系统不会将来自不同数据包的解压缩数据合并来进行检查。当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值

时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。您可以使用 `file_data` 规则关键字来检查解压缩数据。

可以启用规则 120:6 为此选项生成事件。

Unlimited Decompression

启用 **Inspect Compressed Data**（或者 **Decompress SWF File (LZMA)**、**Decompress SWF File (Deflate)** 或 **Decompress PDF File (Deflate)**）后，跨多个数据包覆盖 **Maximum Decompressed Data Depth**；也就是说，此选项支持跨多个数据包无限解压缩。请注意，启用此选项不会影响单个数据包中的 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth**。另请注意，如果启用此选项，提交修改时 **Maximum Compressed Data Depth** 和 **Maximum Decompressed Data Depth** 将会设置为 65535。

Normalize Javascript

当 **Inspect HTTP Responses** 已启用时，此选项启用对 HTTP 响应正文中 Javascript 的检测和规范化。预处理器会对模糊 JavaScript 数据（例如，unescape 函数、decodeURI 函数和 String.fromCharCode 方法）进行规范化。预处理器会对 unescape、decodeURI 和 decodeURIComponent 函数中的以下编码进行规范化：

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

预处理器检测连续空格，并将其规范化为一个空格。此选项处于启用状态时，配置字段允许您指定模糊 Javascript 数据中允许的最大连续空格数量。可输入 1 到 65535 之间的值。值 0 将会禁止生成事件，不管与该字段相关的预处理器规则 (120:10) 是否启用。

预处理器还会对 Javascript 加号 (+) 运算符进行规范化，并使用该运算符连接字符串。

您可以使用 `file_data` 入侵规则关键字使入侵规则指向规范化的 Javascript 数据。

可以启用规则 120:9、120:10 和 120:11 为此选项生成事件，如下所示：

表 *173*：规范化 *Javascript* 选项规则

规则	会触发事件的情况
120:9	预处理器内的模糊级别大于或等于 2。
120:10	Javascript 模糊数据中的连续空格数量大于或等于为允许的最大连续空格数量配置的值。
120:11	经转义或编码的数据包含多于一种类型的编码。

“解压缩 SWF 文件 (LZMA)”(Decompress SWF File [LZMA]) 和“解压缩 SWF 文件 (Deflate)”(Decompress SWF File [Deflate])

启用 **HTTP Inspect Responses** 后，这些选项解压缩位于 HTTP 请求的 HTTP 响应主体中文件的压缩部分。.

注释 您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

- **Decompress SWF File (LZMA)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 LZMA 兼容压缩部分。
- **Decompress SWF File (Deflate)** 解压缩 Adobe ShockWave Flash (`.swf`) 文件的 deflate 兼容压缩部分。

当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。您可以使用 `file_data` 入侵规则关键字来检查解压缩数据。

可以启用规则 120:12 和 120:13 来为此选项生成事件，如下所示：

表 *174*: 解压缩 *SWF* 文件选项规则

规则	会触发事件的情况
120:12	deflate 文件解压缩失败。
120:13	LZMA 文件解压缩失败。

Decompress PDF File (Deflate)

检查 HTTP 响应 (Inspect HTTP Responses) 处于启用状态时，**解压缩 SWF 文件 (Deflate) (Decompress PDF File [Deflate])** 会解压缩位于 HTTP 请求的 HTTP 响应主体中可移植文档格式 (`.pdf`) 文件的 deflate 兼容压缩部分。系统只能使用 `/FlateDecode` 数据流过滤器解压缩 PDF 文件。不支持其他数据流过滤器（包括 `/FlateDecode /FlateDecode`）。

注释 您只能解压缩在 HTTP GET 响应中找到的文件的压缩部分。

当达到 **Maximum Compressed Data Depth** 或 **Maximum Decompressed Data Depth** 中指定的值，或者达到压缩数据末尾时，解压缩将会结束。当达到 **Server Flow Depth** 中指定的值时，对解压缩数据的检查将会结束，除非还选择了 **Unlimited Decompression**。您可以使用 `file_data` 入侵规则关键字来检查解压缩数据。

您可以启用规则 120:14、120:15、120:16 和 120:17 来为此选项生成事件，如下所示：

表 *175*: 解压缩 *PDF* 文件 *(Deflate)* 选项规则

规则	会触发事件的情况
120:14	文件解压缩失败。
120:15	由于压缩类型不受支持，文件解压缩失败。
120:16	由于 PDF 数据流过滤器不受支持，文件解压缩失败。
120:17	文件解析失败。

Extract Original Client IP Address

允许从 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头提取原始客户端 IP 地址。可以在入侵事件表视图中显示提取的原始客户端 IP 地址。

您可以启用规则 119:23、119:29 和 119:30 为此选项生成入侵事件。

XFF Header Priority

启用 **Extract Original Client IP Address** 后，指定系统处理原始客户端 IP HTTP 报头的顺序。如果在受监控网络上预计会遇到除 X-Forwarded-For (XFF) 或 True-Client-IP 以外的客户端 IP 地址，请点击 **添加 (Add)** 向优先级列表中添加其他报头名称。然后使用每种报头类型旁边的向上和向下箭头图标调整其优先级。请注意，如果在 HTTP 请求中显示多个 XFF 报头，则系统仅处理优先级最高的报头。

Log URI

允许从 HTTP 请求数据包提取原始 URI（如果有），并将该 URI 与为会话生成的所有入侵事件相关联。

启用此选项后，可以在入侵事件表视图的 HTTP URI 列中显示提取的 URI 的前 50 个字符。可以在数据包视图中显示完整的 URI（最多 2048 字节）。

Log Hostname

允许从 HTTP 请求主机报头中提取主机名（如果有），并将该主机名与为会话生成的所有入侵事件相关联。如果存在多个主机报头，将会从第一个报头提取主机名。

启用此选项后，可以在入侵事件表视图的 HTTP Hostname 列中显示提取的主机名的前 50 个字符。可以在数据包视图中显示完整的主机名（最多 256 字节）。

可以启用规则 119:25 为此选项生成事件。

请注意，在启用了预处理器和规则 119:24 的情况下，如果在 HTTP 请求中检测到多个主机报头，预处理器将会生成入侵事件，不管此选项的设置如何。

配置文件

指定为 HTTP 流量规范化的编码的类型。系统提供了一个适用于大多数服务器的默认配置文件、适用于 Apache 服务器和 IIS 服务器的若干默认配置文件以及自定义默认设置，您可以对这些设置进行自定义，以满足受监控流量的需求：

- 选择 **All** 将会使用适用于所有服务器的标准默认配置文件。
- 选择 **IIS** 将会使用系统提供的 IIS 配置文件。
- 选择 **Apache** 将会使用系统提供的 Apache 配置文件。
- 选择**自定义 (Custom)** 将会创建您自己的服务器配置文件。

服务器级别 HTTP 规范化编码选项

将 HTTP 服务器级别**配置文件 (Profile)** 选项设置为 `Custom` 时，可以指定为 HTTP 流量规范化的编码类型，并启用 HTTP 预处理器规则以根据包含不同编码类型的流量生成事件。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

ASCII 编码 (ASCII Encoding)

对编码的 ASCII 字符进行解码，并指定规则引擎是否生成关于 ASCII 编码 URI 的事件。

可以启用规则 119:1 为此选项生成事件。

UTF-8 Encoding

对 URI 中的标准 UTF-8 Unicode 序列进行解码。

可以启用规则 119:6 为此选项生成事件。

Microsoft %U Encoding

对 IIS %u 编码方案进行解码，该编码方案使用 %u，后跟四个字符；其中这四个字符是与 IIS Unicode 代码点相关的十六进制编码值。

提示 合法的客户端很少使用 %u 编码，因此思科建议对使用 %u 编码的 HTTP 流量进行解码。

可以启用规则 119:3 为此选项生成事件。

裸字节 UTF-8 编码 (Bare Byte UTF-8 Encoding)

对裸字节编码进行解码（这种解码方法使用非 ASCII 字符作为解码 UTF-8 值时的有效值）。

提示 裸字节编码允许用户模拟 IIS 服务器和正确解释非编码标准。思科建议启用此选项，因为合法的客户端不以这种方式编码 UTF-8。

可以启用规则 119:4 为此选项生成事件。

Microsoft IIS Encoding

使用 Unicode 代码点映射进行解码。

提示 思科建议启用此选项，因为它主要出现在攻击和躲避尝试中。

可以启用规则 119:7 为此选项生成事件。

双重编码 (Double Encoding)

通过在每个进行解码的请求 URI 中形成两条通道，解码 IIS 双编码流量。思科建议启用此选项，因为它通常只存在于攻击情况中。

可以启用规则 119:2 为此选项生成事件。

多斜杠混淆 (Multi-Slash Obfuscation)

将连续的多个斜杠规范化为一个斜杠。

可以启用规则 119:8 为此选项生成事件。

IIS Backslash Obfuscation

将反斜杠规范化为正斜杠。

可以启用规则 119:9 为此选项生成事件。

目录遍历

对目录遍历和自引用目录进行规范化。如果启用随附的预处理器规则来生成关于此类型流量的事件，可能会产生误报，因为有些网站使用目录遍历来引用文件。

可以启用规则 119:10 和 119:11 为此选项生成事件。

制表符混淆 (Tab Obfuscation)

规范化有关对空格分隔符使用制表符的非 RFC 标准。Apache 及其他非 IIS网络服务器在 URL 中使用制表符 (0x09) 作为分隔符。

注释 无论此选项的配置如何，如果制表符前有空格字符 (0x20)，HTTP 检查预处理器都将制表符看作空格。

可以启用规则 119:12 为此选项生成事件。

RFC 分隔符无效 (Invalid RFC Delimiter)

规范化 URI 数据中的换行符 (\n)。

可以启用规则 119:13 为此选项生成事件。

Webroot 目录遍历 (Webroot Directory Traversal)

检测穿过 URL 中初始目录的目录遍历。

可以启用规则 119:18 为此选项生成事件。

制表符 URI 分隔符 (Tab URI Delimiter)

将制表符 (0x09) 用作 URI 的分隔符。Apache、新版本的 IIS 以及其他一些网络服务器使用制表符作为 URL 的分隔符。

注释 无论此选项的配置如何，如果制表符前有空格字符 (0x20)，HTTP 检查预处理器都将制表符看作空格。

非 RFC 字符 (Non-RFC characters)

检测在相应字段中添加的并出现在传入或传出 URI 数据中的非 RFC 字符列表。修改该字段时，请使用表示字节字符的十六进制格式。如果要配置此选项，请谨慎设置它的值。使用极常见的字符可能会生成大量事件。

可以启用规则 119:14 为此选项生成事件。

最大块编码大小 (Max Chunk Encoding Size)

检测 URI 数据中异常大的数据块的大小。

可以启用规则 119:16 和 119:22 为此选项生成事件。

禁用管道解码 (Disable Pipeline Decoding)

禁止对管道化请求进行 HTTP 解码。禁用此选项可提高性能，因为不会对管道中等待的 HTTP 请求进行解码和分析，且只会使用通用模式匹配对这些请求进行检查。

非严格 URI 解析 (Non-Strict URI Parsing)

允许非严格的 URI 解析。应仅在接受 "GET /index.html abc xo qr \n" 格式的非标准 URI 的服务器上使用此选项。此选项处于启用状态时，解码器会假设 URI 在第一和第二空格之间，即使第二个空格后没有有效的 HTTP 标识符。

扩展的 ASCII 编码 (Extended ASCII Encoding)

允许对 HTTP 请求 URI 中的扩展 ASCII 字符进行解析。请注意，此选项仅适用于自定义的服务器配置文件，不适用于为 Apache、IIS 或所有服务器提供的默认配置文件。

配置 HTTP 检查预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 993 页。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **HTTP 配置 (HTTP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **HTTP 配置 (HTTP Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改“全局设置”(Global Settings) 页面区域中的选项；请参阅全局 HTTP 规范化选项，第 1025 页。

步骤 7 此时，您有三种选择：

- 添加服务器配置文件 - 点击**服务器 (Servers)** 部分中的添加图标 ( )。在**服务器地址 (Server Address)** 字段中为客户端指定一个或多个 IP 地址，然后点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。最多可在列表中包含 496 个字符，为所有服务器配置文件总共最多可指定 256 个地址条目，总共最多可创建 255 个配置文件（包括默认配置文件）。
- 编辑服务器配置文件 - 在**服务器 (Servers)** 下点击已添加配置文件的已配置地址，或者点击**默认值 (default)**。您可以修改**配置 (Configuration)** 部分中的任何设置；请参阅服务器级别 HTTP 规范化选项，第 1026 页。如果为**配置文件 (Profile)** 值选择**自定义 (Custom)**，还可以修改服务器级别 HTTP 规范化编码选项，第 1033 页中所述的编码选项。
- 删除服务器配置文件 - 点击自定义配置文件旁边的删除图标 ( )。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 HTTP 预处理器规则 (GID 119)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

其他 HTTP 检查预处理器规则

可以启用下表的 **Preprocessor Rule GID:SID** 列中的规则，为与特定配置选项无关的 HTTP 检查预处理器规则生成事件。

表 *176*：其他 *HTTP* 检查预处理器规则

预处理器规则 GID:SID	说明
120:5	如果在 HTTP 响应流量中遇到 UTF-7 编码，将会生成事件；UTF-7 应仅在需要 7 位奇偶校验的情况下出现，例如，SMTP 流量。
119:21	如果 HTTP 请求报头包含多于一个 `content-length` 字段，将会生成事件。
119:24	如果 HTTP 请求包含多于一个主机报头，将会生成事件。
119:28 120:8	如果启用，这些规则不生成事件。
119:32	如果在流量中遇到 HTTP 0.9，将会生成事件。请注意，还必须启用 TCP Stream Configuration。
119:33	如果 HTTP URI 包含非转义空格，将会生成事件。
119:34	如果 TCP 连接包含 24 个或更多管道化 HTTP 请求，将会生成事件。

Sun RPC 预处理器

远程过程调用 (RPC) 规范化采用分片 RPC 记录，并将这些记录规范化为单个记录，以便规则引擎可以检查完整的记录。例如，攻击者可能会试图发现 RPC `admind` 运行所在的端口。某些 UNIX 主机使用 RPC `admind` 执行远程分布式系统任务。如果主机执行弱身份验证，恶意用户可能会控制远程管理。Snort ID (SID) 为 575 的标准文本规则 (GID: 1) 会搜索特定位置中的内容，并识别不适当的 `portmap GETPORT` 请求，以此来检测这种攻击。

Sun RPC 预处理器选项

端口

指定要规范化其流量的端口。可在此界面列出多个端口，端口之间用逗号分隔。典型的RPC端口为111 和 32771。如果网络将 RPC 流量发送到其他端口，可考虑添加这些端口。

Detect fragmented RPC records

检测 RPC 分片记录。

可以启用规则 106:1 和 106:5 为此选项生成事件。

Detect multiple records in one packet

在每个数据包（或重组数据包）中检测多于一个 RPC 请求。

可以启用规则 106:2 为此选项生成事件。

Detect fragmented record sums which exceed one fragment

检测超过当前数据包长度的重组分片记录长度。

可以启用规则 106:3 为此选项生成事件。

Detect single fragment records which exceed the size of one packet

检测部分记录

可以启用规则 106:4 为此选项生成事件。

配置 Sun RPC 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **Sun RPC 配置 (Sun RPC Configuration)** 被禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **Sun RPC 配置 (Sun RPC Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改Sun RPC 预处理器选项，第 1038 页中所述的设置。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 Sun RPC 预处理器规则 (GID 106)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

SIP 预处理器

会话初始协议 (SIP) 为客户端应用（例如网络电话、多媒体会议、即时消息、网络游戏和文件传输）的一个或多个用户提供一个或多个会话的呼叫建立、修改和取消。每个 SIP 请求中的“方法”(*method*) 字段识别请求的目的，请求 URI 则指定发送请求的目的地。每个 SIP 响应中的状态代码指明请求操作的结果。

使用 SIP 建立呼叫后，实时传输协议 (RTP) 负责随后的音频和视频通信；会话的此部分有时又称为呼叫通道、数据通道或音频/视频数据通道。对于数据通道参数协商、会话公告和会话邀请，RTP 在 SIP 消息正文中使用会话描述协议 (SDP)。

SIP 预处理器负责：

- 解码和分析 SIP 2.0 流量
- 提取包括 SDP 数据（如果有）在内的 SIP 报头和消息正文，并将提取的数据传递给规则引擎，以进行进一步检查
- 在检测到以下条件并且相应的预处理器规则已启用的情况下，将会生成事件：

  SIP 数据包中存在异常和已知漏洞

  调用序列乱序和无效

- 或者，忽略呼叫通道

预处理器会根据在 SDP 消息中识别出的端口来识别 RTP 通道（该消息嵌入在 SIP 消息正文中），但预处理器不提供 RTP 协议检查。

使用 SIP 预处理器时，请注意以下几点：

- UDP 通常传输 SIP 支持的媒体会话。UDP 数据流预处理为 SIP 预处理器提供 SIP 会话跟踪。
- SIP 规则关键字允许您指向 SIP 数据包报头或消息正文，并限制为对特定 SIP 方法或状态代码进行数据包检测。

SIP 预处理器选项

对于以下选项，您可以指定从 1 到 65535 字节的正值或 0，以禁用选项的事件生成（无论是否启用关联规则）。

- **Maximum Request URI Length**
- **Maximum Call ID Length**
- **Maximum Request Name Length**
- **Maximum From Length**
- **Maximum To Length**
- **Maximum Via Length**
- **Maximum Contact Length**
- **Maximum Content Length**

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 SIP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Methods to Check

指定 SIP 检测方法。可以指定以下当前定义的任何 SIP 方法：

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

方法不区分大小写。方法名称可以包含字母字符、数字和下划线字符。不允许任何其他特殊字符。使用逗号隔开多种方法。

由于将来可能会定义新的 SIP 方法，因此，配置可以包含当前未定义的字母字符串。 系统最多支持 32 种方法，包括 21 种当前定义的方法和 11 种其他方法。系统将忽略您可能配置的任何未定义的方法。

请注意，除为此选项指定的任何方法外，总共 32 种方法包括入侵规则中使用 `sip_method` 关键字指定的方法。

Maximum Dialogs within a Session

指定数据流会话中允许的最大对话数量。如果创建了多于此数量的对话，将会丢弃最早的对话，直至对话数量不超过指定的最大数量；如果启用了规则 140:27，还将触发事件。

可指定 1 到 4194303 之间的整数。

Maximum Request URI Length

指定 Request-URI 报头字段中允许的最大字节数。如果启用了规则 140:3，长度大于此设置的 URI 将会触发事件。请求 URI 字段指明请求的目标路径或目标页面。

Maximum Call ID Length

指定请求或响应 Call-ID 报头字段中允许的最大字节数。如果启用了规则 140:5，长度大于此设置的 Call-ID 字段将会触发事件。Call-ID 字段唯一地识别请求和响应中的 SIP 会话。

Maximum Request Name Length

指定请求名称中允许的最大字节数（该名称是 CSeq 事务标识符中指定的方法的名称）。如果启用了规则 140:7，长度大于此设置的请求名称将会触发事件。

Maximum From Length

指定请求或响应 From 报头字段中允许的最大字节数。如果启用了规则 140:9，长度大于此设置的 From 字段将会触发事件。From 字段识别消息发起方。

Maximum To Length

指定请求或响应 To 报头字段中允许的最大字节数。如果启用了规则 140:11，长度大于此设置的 To 字段将会触发事件。To 字段识别消息收件人。

Maximum Via Length

指定请求或响应 Via 报头字段中允许的最大字节数。如果启用了规则 140:13，长度大于此设置的 Via 字段将会触发事件。Via 字段提供请求的路径，并在响应中提供回执信息。

Maximum Contact Length

指定请求或响应 Contact 报头字段中允许的最大字节数。如果启用了规则 140:15，长度大于此设置的 Contact 字段将会触发事件。Contact 字段提供用以指定与后续消息进行联系的位置的 URI。

Maximum Content Length

指定在请求或响应消息正文的内容中允许的最大字节数。如果启用了规则 140:16，长度大于此设置的内容将会触发事件。

Ignore Audio/Video Data Channel

启用和禁用数据通道流量检查。请注意，如果启用了此选项，预处理器会继续检查其他非数据通道 SIP 流量。

配置 SIP 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SIP 配置 (SIP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **SIP 配置 (SIP Configuration)** 旁边的编辑图标 ()。

步骤 6 修改SIP 预处理器选项，第 1040 页中所述的选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 SIP 预处理器规则 (GID 140)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

其他 SIP 预处理器规则

下表中的 SIP 预处理器规则与特定配置选项无关。与其他 SIP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。

表 *177*: 其他 *SIP* 预处理器规则

预处理器规则 GID:SID	说明
140:1	如果预处理器正在监控系统允许的最大 SIP 会话数量，将会生成事件。
140:2	如果必填的 Request_URI 字段在 SIP 请求中为空，将会生成事件。
140:4	如果 Call-ID 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:6	如果 SIP 请求或响应 CSeq 字段中的序列号值不是小于 231 的 32 位无符号整数，将会生成事件。

预处理器规则 GID:SID	说明
140:8	如果 From 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:10	如果 To 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:12	如果 Via 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:14	如果必填的 Contact 报头字段在 SIP 请求或响应中为空，将会生成事件。
140:17	如果 UDP 流量中的单个 SIP 请求或响应数据包包含多条消息，将会生成事件。请注意，旧版本 SIP 支持多条消息，但 SIP 2.0 仅在每个数据包中支持一条消息。
140:18	如果 UDP 流量中的 SIP 请求或响应中消息正文的实际长度与 SIP 请求或响应中的 Content-Length 报头字段中指定的值不匹配时，将会生成事件。
140:19	如果预处理器无法识别 SIP 响应的 CSeq 字段中的方法名称，将会生成事件。
140:20	如果 SIP 服务器不质询经过身份验证的邀请消息，将会生成事件。请注意，当有 InviteReplay 计费攻击时，会出现这种情况。
140:21	如果会话信息在建立呼叫前发生变化，将会生成事件。请注意，当有 FakeBusy 计费攻击时，会出现这种情况。
140:22	如果响应状态代码不是一个三位数字，将会生成事件。
140:23	如果 Content-Type 报头字段未指定内容类型且消息正文包含数据，将会生成事件。
140:24	如果 SIP 版本不是 1、1.1 或 2.0，将会生成事件。
140:25	如果 CSeq 报头字段中指定的方法与 SIP 请求中的 method 字段不匹配，将会生成事件。
140:26	如果预处理器无法识别在 SIP 请求方法字段中命名的方法，将会生成事件。

GTP 预处理器

通用分组无线业务 (GPRS) 隧道协议 (GTP) 实现通过 GTP 核心网络进行通信。GTP 预处理器检测 GTP 流量中的异常，并将命令通道信令消息转发到规则引擎以进行检查。可以使用 `gtp_version`、`gtp_type` 和 `gtp_info` 规则关键字检查 GTP 命令通道流量中是否存在漏洞。

单一配置选项允许为预处理器进行 GTP 命令通道消息检查的端口修改默认设置。

GTP 预处理器规则

如果要下表中所列的 GTP 预处理器规则生成事件，必须启用它们。

表 *178*: *GTP* 预处理器规则

预处理器规则 GID:SID	说明
143:1	如果预处理器检测到无效的消息长度，将会生成事件。
143:2	如果预处理器检测到无效的信息元素长度，将会生成事件。
143:3	如果预处理器检测到无序的信息元素，将会生成事件。

配置 GTP 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以使用以下程序修改 GTP 预处理器监控以获取 GTP 命令消息的端口。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击左侧导航面板中的 **Settings**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **GTP 命令通道配置 (GTP Command Channel Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **GTP 命令通道配置 (GTP Command Channel Configuration)** 旁边的编辑图标 ( )。

步骤 6 输入**端口 (Ports)** 值。

使用逗号分隔多个端口。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要启用入侵事件，请启用 GTP 预处理器规则 (GID 143)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

IMAP 预处理器

互联网邮件应用协议 (IMAP) 用于从远程 IMAP 服务器检索邮件。IMAP 预处理器检查服务器到客户端的IMAP4流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器IMAP4流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

IMAP 预处理器选项

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

注意 更改 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)**在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。 的值

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 IMAP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 Decoding Depth

指定要从每个Base64编码的MIME邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

如果启用此选项，可以启用规则 141:4，以在解码失败时生成事件；导致解码失败的原因包括编码不正确或数据损坏等。

7-Bit/8-Bit/Binary Decoding Depth

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

当启用此选项时，您可以启用规则 141:6，在提取失败时生成事件；提取可能会由于损坏的数据而失败。

Quoted-Printable Decoding Depth

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

当启用此选项时，您可以启用规则 141:5，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

Unix-to-Unix Decoding Depth

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

当启用此选项时，您可以启用规则 141:7，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

配置 IMAP 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **IMAP 配置 (IMAP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **IMAP 配置 (IMAP Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改IMAP 预处理器选项，第 1045 页中所述的设置。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要启用入侵事件，请启用 IMAP 预处理器规则 (GID 141)；请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

其他 IMAP 预处理器规则

下表中的 IMAP 预处理器规则与特定配置选项无关。与其他 IMAP 预处理器规则一样，如果要使这些规则生成事件，必须启用它们。

表 *179*：其他 *IMAP* 预处理器规则

预处理器规则 GID:SID	说明
141:1	如果预处理器检测到未在 RFC 3501 中定义的客户端命令，将会生成事件。
141:2	如果预处理器检测到未在 RFC 3501 中定义的服务器响应，将会生成事件。
141:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

POP 预处理器

邮局协议 (POP) 用于从远程 POP 邮件服务器检索邮件。POP 预处理器检查服务器到客户端的 POP3 流量，如果相关的预处理器规则已启用，还会生成关于异常流量的事件。此预处理器还可以提取和解码客户端到服务器 POP3 流量中的邮件附件，并将附件数据发送到规则引擎。可以在入侵规则中使用 `file_data` 关键字以指向附件数据。

提取和解码涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

POP 预处理器选项

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

注意 更改 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)**在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。 的值

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定用于检查 POP 流量的端口。可指定 0 到 65535 之间的整数。使用逗号分隔多个端口号。

Base64 Decoding Depth

指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

当启用此选项时，您可以启用规则 142:4，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

7-Bit/8-Bit/Binary Decoding Depth

指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。

当启用此选项时，您可以启用规则 142:6，在提取失败时生成事件；提取可能会由于损坏的数据而失败。

Quoted-Printable Decoding Depth

指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。

当启用此选项时，您可以启用规则 142:5，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

Unix-to-Unix Decoding Depth

指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。

当启用此选项时，您可以启用规则 142:7，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

配置 POP 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **POP 配置 (POP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **POP 配置 (POP Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改POP 预处理器选项，第 1048 页中所述的设置。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要启用入侵事件，请启用 POP 预处理器规则 (GID 142)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

其他 POP 预处理器规则

下表中的POP预处理器规则与特定配置选项无关。与其他POP预处理器规则一样，如果要使这些规则生成事件，必须启用它们。

表 *180*: 其他 *POP* 预处理器规则

预处理器规则 GID:SID	说明
142:1	如果预处理器检测到未在 RFC 1939 中定义的客户端命令，将会生成事件。
142:2	如果预处理器检测到未在 RFC 1939 中定义的服务器响应，将会生成事件。
142:3	如果预处理器正在使用系统允许的最大内存量，将会生成事件。在这种情况下，预处理将会停止解码，直至内存可用。

SMTP 预处理器

SMTP 预处理器指示规则引擎对 SMTP 命令进行规范化。预处理器还可以提取和解码客户端到服务器流量中的邮件附件，并根据不同的软件版本，提取邮件的文件名、地址和报头数据，以在显示 SMTP 流量触发的入侵事件时提供上下文。

SMTP 预处理器选项

可以启用或禁用规范化，还可以对选项进行配置以控制 SMTP 解码器检测的异常流量类型。

请注意，解码（或提取，如果 MIME 邮件附件不要求解码）涵盖多个附件（如果有）以及同时存在于多个数据包中的大型附件。

另请注意，当 **Base64 Decoding Depth**、**7-Bit/8-Bit/Binary Decoding Depth**、**Quoted-Printable Decoding Depth** 或 **Unix-to-Unix Decoding Depth** 选项的值在以下设置中不同时，将会使用最高值：

- 默认网络分析策略
- 由同一访问控制策略中的网络分析规则调用的任何其他自定义网络分析策略

注意 更改 **Base64 解码深度 (Base64 Decoding Depth)**、**7 位/8 位/二进制解码深度 (7-Bit/8-Bit/Binary Decoding Depth)**、**Quoted-Printable 解码深度 (Quoted-Printable Decoding Depth)** 或 **Unix-to-Unix 解码深度 (Unix-to-Unix Decoding Depth)**在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。 的值

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

端口

指定要实现 SMTP 流量规范化的端口。可以指定大于或等于 0 的值。使用逗号分隔多个端口。

Stateful Inspection

如果选择此选项，SMTP 解码器将会保存状态，提供各个数据包的会话上下文，并且仅检查重组的会话。如果清除此选项，将会在没有会话上下文的情况下分析每个数据包。

Normalize

如果设置为 `All`，将会规范化所有命令。会检查命令后是否有多个空格字符。

如果设置为 `None`，则不会对命令进行规范化。

如果设置为 `Cmds`，将会规范化**自定义命令 (Custom Commands)** 中列出的命令。

Custom Commands

如果**规范化 (Normalize)** 设置为 `Cmds`，则会规范化列出的命令。

可在文本框中指定应进行规范化的命令。会检查命令后是否有多个空格字符。

空格 (ASCII 0x20) 和制表符 (ASCII 0x09) 字符被视为是用于规范化目的的空格字符。

Ignore Data

不处理邮件数据；仅处理 MIME 邮件报头数据。

Ignore TLS Data

不处理根据传输层安全协议加密的数据。

No Alerts

当随附的预处理器规则处于启用状态时禁用入侵事件。

Detect Unknown Commands

检测 SMTP 流量中的未知命令。

您可以启用规则 124:5 为此选项生成事件。

Max Command Line Len

检测 SMTP 命令行的长度何时大于此值。指定 `0` 将不会检测命令行长度。

RFC2821（网络工作组制定的关于简单邮件传输协议的规范）建议将最大命令行长度设置为 512。

可以启用规则 124:1 为此选项生成事件。

Max Header Line Len

检测 SMTP 数据报头行的长度何时大于此值。指定 `0` 将不会检测数据报头行长度。

可以启用规则 124:2 和 124:7 为此选项生成事件。

Max Response Line Len

检测 SMTP 响应行的长度何时大于此值。指定 0 将不会检测响应行长度。

RFC 2821 建议将最大响应行长度设置为 512。

您可以启用规则 124:3 为此选项和**替代最大命令行长度 (Alt Max Command Line Len)** 选项（如已启用）生成事件。

Alt Max Command Line Len

检测任何指定命令的SMTP命令行的长度何时大于此值。指定0将不会检测指定命令的命令行长度。为众多命令设置了不同的默认行长度。

此设置将覆盖指定命令的 Max Command Line Len 设置。

您可以启用规则 124:3 为此选项和**最大响应行长度 (Max Response Line Len)** 选项（如已启用）生成事件。

Invalid Commands

检测命令是否是从客户端发出的。

您可以启用规则 124:6 为此选项和**无效命令 (Invalid Commands)** 选项生成事件。

Valid Commands

允许此列表中的命令。

即使此列表为空，预处理器仍允许下列有效命令：ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

注释 RCPT TO 和 MAIL FROM 是 SMTP 命令。对这两个命令，预处理器配置分别使用命令名 RCPT 和 MAIL。在代码中，预处理器会将 RCPT 和 MAIL 映射到正确的命令名。

您可以启用规则 124:4 为此选项和**无效命令 (Invalid Commands)** 选项（如已配置）生成事件。

Data Commands

列出以与 SMTP DATA 命令按照 RFC5321 的要求发送数据相同的方法发起数据发送的命令。使用空格分隔多个命令。

Binary Data Commands

列出以与 BDAT 命令按照 RFC 3030 的要求发送数据类似的方法发起数据发送的命令。使用空格分隔多个命令。

Authentication Commands

列出发起客户端和服务器之间的身份认证交换的命令。使用空格分隔多个命令。

Detect xlink2state

检测作为 X-Link2State Microsoft Exchange 缓冲区数据溢出攻击的一部分的数据包。在内联部署中，系统还可以丢弃这些数据包。

可以启用规则 124:8 为此选项生成事件。

Base64 Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Base64 编码的 MIME 邮件附件中提取和解码的最大字节数。可指定一个正值，或者指定 0 以解码所有 Base64 数据。指定 -1 将会忽略 Base64 数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

请注意，不能被 4 整除的正值将向上舍入为最接近的 4 的倍数，但值 65533、65534、65535 除外，因为它们将向下舍入为 65532。

当启用此选项时，您可以启用规则 124:10，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

请注意，此选项取代已被弃用的 **Enable MIME Decoding** 和 **Maximum MIME Decoding Depth** 选项，后两个选项由于具有向后兼容性，因此在现有入侵策略中仍受到支持。

7-Bit/8-Bit/Binary Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个不要求解码的 MIME 邮件附件中提取的数据的最大字节数。这些附件类型包括 7 位、8 位、二进制以及各种多部分内容类型（例如，纯文本、jpeg 图像、mp3 文件等）。可指定一个正值，或者指定 0 以提取数据包中的所有数据。指定 -1 将会忽略非解码数据。如果选择了 **Ignore Data**，预处理器将不会提取数据。

Quoted-Printable Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Quoted-Printable (QP) 编码的 MIME 邮件附件中提取和解码的最大字节数。

可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 QP 编码数据。指定 -1 将会忽略 QP 编码数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

当启用此选项时，您可以启用规则 124:11，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

Unix-to-Unix Decoding Depth

在 **Ignore Data** 已禁用的情况下，指定要从每个 Unix-to-Unix 编码（UuEncode 编码）的 MIME 邮件附件中提取和解码的最大字节数。可指定 1 到 65535 字节，或者指定 0 以解码数据包中的所有 UuEncode 编码数据。指定 -1 将会忽略 UuEncode 编码数据。如果选择了 **Ignore Data**，预处理器将不会对数据进行解码。

当启用此选项时，您可以启用规则 124:13，在解码失败时生成事件；解码可能会由于不正确的编码或损坏的数据而失败。

Log MIME Attachment Names

允许从 MIME Content-Disposition 报头提取 MIME 附件文件名，并将提取的文件名与为会话生成的所有入侵事件相关联。支持多个文件名。

启用此选项后，可以在入侵事件表视图的 Email Attachment 列中查看与事件相关的文件名。

Log To Addresses

允许从 SMTP RCPT TO 命令提取收件人邮件地址，并将提取的收件人地址与为会话生成的所有入侵事件相关联。支持多个收件人。

启用此选项后，可以在入侵事件表视图的 Email Recipient 列中查看与事件相关的收件人。

Log From Addresses

允许从 SMTP MAIL FROM 命令提取发件人邮件地址，并将提取的发件人地址与为会话生成的所有入侵事件相关联。支持多个发件人地址。

启用此选项后，可以在入侵事件表视图的 Email Sender 列中查看与事件相关的收件人。

Log Headers

允许提取邮件报头。要提取的字节数取决于 **Header Log Depth** 中指定的值。

可以使用 `content` 或 `protected_content` 关键字来编写将邮件报头数据用作模式的入侵规则。还可以在入侵事件数据包视图中查看提取的邮件报头。

Header Log Depth

指定在 **Log Headers** 已启用的情况下要提取的邮件报头的字节数。可指定 0 到 20480 字节。值 0 将会禁用 **Log Headers**。

配置 SMTP 解码

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航窗格中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SMTP 配置 (SMTP Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **SMTP 配置 (SMTP Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改SMTP 预处理器选项，第 1050 页中所述的选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要启用入侵事件，请启用 SMTP 预处理器规则 (GID 124)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

SSH 预处理器

SSH 预处理器检测：

- 质询-响应缓冲区溢出攻击
- CRC-32 攻击
- SecureCRT SSH 客户端缓冲区溢出攻击
- 协议不匹配
- SSH 消息方向不正确
- 任何版本字符串（版本 1 和 2 除外）

密钥交换后，会发生质询-响应缓冲区溢出攻击和 CRC-32 攻击，并会因此进行加密。这两种攻击在身份验证质询之后立即向服务器发送超过 20 KB 的反常态大量负载。CRC-32 攻击仅适用于 SSH 版本 1；质询-响应缓冲区溢出攻击仅适用于 SSH 版本 2。会话开始时可读取版本字符串。除了版本字符串中存在差异外，这两种攻击都可以同样的方式加以处理。

在密钥交换之前尝试进行连接时，会发生 SecureCRT SSH 攻击和协议不匹配攻击。SecureCRT 漏洞会向客户端发送超长协议标识符字符串，从而导致缓冲区溢出。如果非 SSH 客户端应用试图连接到安全 SSH 服务器或者服务器和客户端的版本号不匹配，会出现协议不匹配攻击。

可以将 SSH 预处理器配置为检查指定端口或端口列表的流量，或者自动检测 SSH 流量。预处理器将会继续检查 SSH 流量，直至传递了未超过指定字节数的指定数量的加密数据包，或者直至超过指定数量的数据包中指定的最大字节数。如果超过最大字节数，系统将会假设出现了 CRC-32（SSH 版本 1）攻击或质询-响应缓冲区溢出（SSH 版本 2）攻击。请注意，预处理器检测时无需配置任何版本字符串值（版本 1 和 2 除外）。

另请注意，SSH 预处理器不处理蛮力攻击。

SSH 预处理器选项

如果发生以下任何一种情况，预处理器将停止检查会话流量：

- 对于某个数量的加密数据包，服务器与客户端之间发生有效交换；连接继续保持。
- 在达到要检查的加密数据包数量之前，先达到**服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)** 中设置的值；假设发生了攻击。

在**要检查的加密数据包数量 (Number of Encrypted Packets to Inspect)** 中设置的数量内的每个有效服务器响应会重置**服务器无响应时可发送的字节数 (Number of Bytes Sent Without Server Response)**，且数据包计数继续进行。

可考虑以下 SSH 预处理器配置示例：

- **Server Ports**：22
- **Autodetect Ports**：off
- **Maximum Length of Protocol Version String**：80
- **Number of Encrypted Packets to Inspect**：25
- **Number of Bytes Sent Without Server Response**：19,600
- 所有检测选项均启用。

在本示例中，预处理器仅检查端口 22 的流量。也就是说，自动检测被禁用，因此只检查指定的端口。

此外，如果发生以下任何一种情况，本示例中的预处理器会停止检查流量：

- 客户端发送 25 个加密数据包，这些数据包总共不超过 19,600 字节。假设没有发生攻击。
- 客户端发送 25 个加密数据包，这些数据包总共不超过 19,600 字节。在这种情况下，预处理器可将发生的攻击视为质询-响应缓冲区溢出攻击，因为本示例中的会话为 SSH 版本 2 会话。

本示例中的预处理器还将检测处理流量过程中发生的以下任何情况：

- 服务器溢出，由大于 80 字节的版本字符串触发，表明为 SecureCRT 攻击
- 协议不匹配
- 数据包的传输方向错误

最后，预处理器将自动检测任何版本字符串（版本 1 和 2 除外）。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

服务器端口

指定 SSH 预处理器应检查其流量的端口。

可以配置单个端口或端口的逗号分隔列表。

Autodetect Ports

将预处理器设置为会自动检测 SSH 流量。

如果选择此选项，预处理器会检查某个 SSH 版本号的所有流量。如果客户端和服务器数据包均没有包含版本号，预处理器将会停止处理。如果禁用此选项，预处理器只检查在 **Server Ports** 选项中确定的流量。

Number of Encrypted Packets to Inspect

指定每个会话待检查的加密数据包的数量。

将此选项设置为 0 将允许所有流量通过。

减少待检查的加密数据包的数量可能会导致一些攻击避开检测。增加待检查的加密数据包的数量可能会对性能造成负面影响。

Number of Bytes Sent Without Server Response

指定在假设存在质询-响应缓冲区溢出或 CRC-32 攻击之前，SSH 客户端在未获得响应的情况下可以向服务器发送的最大字节数。

如果预处理器对于质询-响应缓冲区溢出或 CRC-32 攻击生成误报，请增加此选项的值。

Maximum Length of Protocol Version String

指定在假设存在 SecureCRT 攻击之前，服务器版本字符串中允许的最大字节数。

Detect Challenge-Response Buffer Overflow Attack

启用或禁用质询-响应缓冲区溢出攻击检测。

可以启用规则 128:1 为此选项生成事件。

Detect SSH1 CRC-32 Attack

启用或禁用 CRC-32 攻击检测。

可以启用规则 128:2 为此选项生成事件。

Detect Server Overflow

启用或禁用 SecureCRT SSH 客户端缓冲区溢出攻击检测。

可以启用规则 128:3 为此选项生成事件。

Detect Protocol Mismatch

启用或禁用协议不匹配检测。

可以启用规则 128:4 为此选项生成事件。

Detect Bad Message Direction

允许或禁止检测流量传输方向错误这种情况（即，如果假定的服务器生成客户端流量，或者客户端生成服务器流量）。

可以启用规则 128:5 为此选项生成事件。

Detect Payload Size Incorrect for the Given Payload

允许或禁止检测负载大小不正确的数据包，例如，SSH 数据包中指定的长度与 IP 报头中指定的总长度不一致，或者消息被截断（即，无足够的数据用于整个 SSH 报头）。

可以启用规则 128:6 为此选项生成事件。

Detect Bad Version String

请注意，启用预处理器后，它在检测时无需配置任何版本字符串（版本 1 和 2 除外）。

可以启用规则 128:7 为此选项生成事件。

配置 SSH 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SSH 配置 (SSH Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **SSH 配置 (SSH Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改SSH 预处理器选项，第 1056 页中所述的选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要启用入侵事件，请启用 SSH 预处理器规则 (GID 128)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

SSL 预处理器

SSL 预处理器可供您配置 SSL 检查，从而可以阻止、解密或使用访问控制检查已加密的流量。无论是否配置 SSL 检查，SSL 预处理器也会分析在流量中检测到的 SSL 握手消息，并确定会话何时被加密。系统通过识别已加密流量可以停止对已加密负载执行入侵和文件检查，这有助于减少误报并提高性能。

SSL 预处理器还可以检查已加密流量以检测 Heartbleed 漏洞攻击尝试，并在检测到此类漏洞攻击时生成事件。

会话加密之后，可以暂停检查流量是否存在入侵和恶意软件。如果配置 SSL 检查，则 SSL 预处理器还将确定您可以阻止、解密或使用访问控制进行检查的已加密流量。

使用 SSL 预处理器解密已加密流量无需许可证。所有其他 SSL 预处理器功能（包括暂停检查已加密负载是否存在恶意软件和入侵，并检测 Heartbleed 漏洞攻击）均需要保护许可证。

SSL 预处理的工作原理

如果配置了 SSL 检查，则 SSL 预处理器停止对已加密数据进行入侵和文件检查，然后使用 SSL 策略对已加密流量进行检查。这有助于清除误报。SSL 预处理器在检查 SSL 握手时会维护状态信息，跟踪该会话的状态和 SSL 版本。如果预处理器检测到会话状态已被加密，系统会将该会话的流量标记为“加密”。可将系统配置为在确定会话已加密时停止处理已加密会话中的所有数据包，并在检测到 Heartbleed 漏洞攻击尝试时生成事件。

对于每个数据包，SSL 预处理器都会验证流量是否包含 IP 报头、TCP 报头和 TCP 负载，以及流量发生在指定适用于 SSL 预处理的端口上。对于符合条件的流量，可根据以下情况确定流量是否已加密：

- 系统观察会话中的所有数据包，未启用**服务器端数据受信任 (Server side data is trusted)**，并且会话包含来自服务器和客户端的“已完成”消息以及至少一个来自各端的数据包（包含应用记录但不包含警报记录）。
- 系统遗漏某些流量，未启用**服务器端数据受信任 (Server side data is trusted)**，并且会话至少包含一个来自服务器端和客户端的数据包（包含未使用警报记录应答的应用记录）。
- 系统观察会话中的所有数据包，已启用**服务器端数据受信任 (Server side data is trusted)**，并且会话包含来自客户端的“已完成”消息和至少一个来自客户端的数据包（包含应用记录但不包含警报记录）。
- 系统遗漏某些流量，已启用**服务器端数据受信任 (Server side data is trusted)**，并且会话至少包含一个来自客户端的数据包（包含未使用警报记录应答的应用记录）。

如果选择停止处理加密流量，系统会在将该会话标记为“加密”后忽略其中的后续数据包。

此外，在 SSL 握手期间，预处理器监控检测信号请求和响应。检测到以下对象时，预处理器生成事件。

- 包含大于负载本身的负载长度值的检测信号请求
- 大于 Max Heartbeat Length 字段中存储的值的检测信号响应

注释 可向某规则添加 `ssl_state` 和 `ssl_version` 关键字，以便在该规则中使用 SSL 状态或版本信息。

SSL 预处理器选项

注释 默认情况下，系统提供的网络分析策略启用 SSL 预处理器。如果预期有已加密流量通过您的网络，思科建议不要在自定义部署中禁用 SSL 预处理器。

如果未配置 SSL 检查，则系统尝试检查已加密流量是否存在恶意软件和入侵，而不对其进行解密。如果启用了 SSL 预处理器，它会检测会话加密的时间。启用 SSL 预处理器后，规则引擎可以调用预处理器来获得 SSL 状态和版本信息。如果在某个入侵策略中启用使用 `ssl_state` 和 `ssl_version` 关键字的规则，则还应在该策略中启用 SSL 预处理器。

端口

指定 SSL 预处理器应监控加密会话流量的端口（用逗号隔开）。只会检查此字段中指定端口的加密流量。

注释 如果 SSL 预处理器检测到指定用于 SSL 监控的端口上有非 SSL 流量，它会尝试将该流量作为 SSL 流量进行解码，然后将其标记为“损坏”。

停止检查加密流量 (Stop inspecting encrypted traffic)

启用或禁止在会话被标记为“加密”后检查会话中的流量。

启用此选项以禁止检查和重组加密的会话。SSL 预处理器会维护会话状态，因此，它可以禁止对会话中所有流量的检查。如果满足以下两个条件，则系统只会停止检查加密会话中的流量：

- 已启用 SSL 预处理
- 已选择此选项

如果清除此选项，则无法修改**服务器端数据受信任 (Server side data is trusted)** 选项。

服务器端数据受信任 (Server side data is trusted)

当“停止检查加密流量”(Stop inspecting encrypted traffic) 启用时，将支持仅根据客户端流量识别加密流量。

最大检测信号长度 (Max Heartbeat Length)

通过指定数个字节，支持检查 SSL 握手内的检测信号请求和响应以了解是否存在 Heartbleed 漏洞攻击尝试。您可以指定介于 1 和 65535 之间的整数，或指定 0 禁用该选项。

如果预处理器检测的检测信号请求的负载长度大于实际负载长度且规则 137:3 已启用，或者检测信号响应的大小大于当规则 137:4 已启用时为此选项配置的值，则预处理器会生成事件。

配置 SSL 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**应用层预处理器 (Application Layer Preprocessors)** 下的 **SSL 配置 (SSL Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **SSL 配置 (SSL Configuration)** 旁边的编辑图标 ( )。

步骤 6 修改SSL 预处理器选项，第 1060 页中所述的任意设置。

- 在**端口 (Ports)** 字段中输入值。多个值之间用逗号隔开。
- 选中或清除**停止检查加密流量 (Stop inspecting encrypted traffic)** 复选框。
- 如果选中**停止检查加密流量 (Stop inspecting encrypted traffic)**，请选中或清除**服务器端数据受信任 (Server side data is trusted)**。
- 在**最大检测信号长度 (Max Heartbeat Length)** 字段中输入值。

  提示 值为 0 将会禁用此选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要启用入侵事件，请启用 SSL 预处理器规则 (GID 137)。有关详细信息，请参阅设置入侵规则状态，第 833 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

SSL 预处理器规则

如果要启用入侵事件，请启用 SSL 预处理器规则 (GID 137)。

下表说明了可启用的 SSL 预处理器规则。

表 *181*：*SSL* 预处理器规则

预处理器规则 GID:SID	说明
137:1	在 ServerHello 消息之后检测 ClientHello 消息，此操作无效并被视为异常行为。
137:2	在禁用 SSL 预处理器选项**服务器端数据受信任 (Server side data is trusted)** 时检测没有 ClientHello 消息的 ServerHello 消息，此操作无效并被视为异常行为。
137:3	在 SSL 预处理器选项**最大检测信号长度 (Max Heartbeat Length)** 包含非零值时检测负载长度大于负载本身的检测信号请求，此操作指示尝试利用 Heartbleed 漏洞。
137:4	检测大于 SSL 预处理器选项**最大检测信号长度 (Max Heartbeat Length)** 中指定的非零值的检测信号响应，此操作指示尝试利用 Heartbleed 漏洞。

第 59 章

SCADA 预处理器

以下主题介绍监控和数据采集 (SCADA) 协议的预处理器及其配置方法：

SCADA 预处理器简介

监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。Firepower 系统为可在网络分析策略中配置的 Modbus 和 DNP3 SCADA 协议提供预处理器。

如果在相应的入侵策略中启用了包含 Modbus 或 DNP3 关键字的规则，系统将自动分别使用带有当前设置的 Modbus 或 DNP3 预处理器，尽管该预处理器在网络分析策略网络界面中保持禁用状态。

Modbus 预处理器

Modbus 协议由 Modicon 于 1979 年首次发布，是一种广泛使用的 SCADA 协议。Modbus 预处理器可检测 Modbus 流量中的异常，解码 Modbus 协议以供规则引擎进行处理（规则引擎使用 Modbus 关键字来访问某些协议字段）。

单一配置选项允许为预处理器进行 Modbus 流量检查的端口修改默认设置。

Modbus 预处理器端口选项

端口

指定预处理器检查 Modbus 流量的端口。使用逗号分隔多个端口。

配置 Modbus 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

如果您的网络不包含任何支持 Modbus 的设备，则不应该在应用于流量的网络分析策略中启用此预处理器。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **Modbus 配置 (Modbus Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **Modbus 配置 (Modbus Configuration)** 旁边的编辑图标 ()。

步骤 6 在**端口 (Ports)** 字段中输入值。

多个值之间用逗号隔开。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 Modbus 预处理器规则 (GID 144)。有关详细信息，请参阅设置入侵规则状态，第 833 页和Modbus 预处理器规则，第 1064 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

Modbus 预处理器规则

如果要下表中所列的 Modbus 预处理器规则生成事件，必须启用这些规则。

表 *182*: *Modbus* 预处理器规则

预处理器规则 GID:SID	说明
144:1	如果 Modbus 报头中的长度与 Modbus 函数代码所要求的长度不匹配，将会生成事件。 每个 Modbus 函数都有预期的请求和响应格式。如果消息长度与预期格式不匹配，将会生成此事件。
144:2	如果 Modbus 协议 ID 未非零值，将会生成事件。协议 ID 字段用于将其他协议与 Modbus 协议复用。由于预处理器并不处理此类其他协议，因此会生成此事件。
144:3	如果预处理器检测到保留的 Modbus 函数代码，将会生成事件。

DNP3 预处理器

分布式网络协议 (DNP3) 是一种 SCADA 协议，最初开发用于为电站之间提供一致的通信。DNP3 还广泛应用于供水、废物处置、运输及其他行业。

DNP3 预处理器可检测 DNP3 流量中的异常，解码 DNP3 协议以供规则引擎进行处理（规则引擎使用 DNP3 关键字来访问某些协议字段）。

DNP3 预处理器选项

端口

启用对每个指定端口的 DNP3 流量检查。可以指定单个端口或端口的逗号分隔列表。

Log bad CRCs

验证包含在 DNP3 链路层帧中的校验和。具有无效校验和的帧将被忽略。

可以启用规则 145:1，以便在检测到无效校验和时生成事件。

配置 DNP3 预处理器

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

如果您的网络不包含任何支持 DNP3 的设备，则不应该在应用于流量的网络分析策略中启用此预处理器。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果 **SCADA 预处理器 (SCADA Preprocessors)** 下的 **DNP3 配置 (DNP3 Configuration)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **DNP3 配置 (DNP3 Configuration)** 旁边的编辑图标 ()。

步骤 6 为**端口数 (Ports)** 输入一个值。

多个值之间用逗号隔开。

步骤 7 选中或清除**记录不良 CRC (Log bad CRCs)** 复选框。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 DNP3 预处理器规则 (GID 145)。有关详细信息，请参阅设置入侵规则状态，第 833 页、DNP3 预处理器选项，第 1065 页和DNP3 预处理器规则，第 1066 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

DNP3 预处理器规则

如果要下表中所列的 DNP3 预处理器规则生成事件，必须启用这些规则。

表 *183*: *DNP3* 预处理器规则

预处理器规则 GID:SID	说明
145:1	在 **Log bad CRC** 已启用的情况下，如果预处理器检测到具有无效校验和的链路层帧，将会生成事件。
145:2	如果预处理器检测到具有无效长度的 DNP3 链路层帧，将会生成事件并阻止该数据包。
145:3	如果预处理器检测到具有无效序列号的传输层分段，将会生成事件并在重组期间阻止数据包。

预处理器规则 **GID:SID**	说明
145:4	如果需要清除 DNP3 重组缓冲区后才能重组完整的分片，将会生成事件。如果在其他分片已加入队列后出现带有 FIR 标志的分片，将会发生这种情况。
145:5	如果预处理器检测到使用保留地址的 DNP3 链路层帧，将会生成事件。
145:6	如果预处理器检测到使用保留函数代码的 DNP3 请求或响应，将会生成事件。

第 60 章

传输层和网络层预处理器

以下主题介绍传输层和网络层预处理器及其配置方式：

传输层和网络层预处理器简介

网络层和传输层预处理器检测对 IP 分片、校验和验证及 TCP 和 UDP 会话预处理加以利用的攻击。在将数据包发送到预处理器之前，数据包解码器将数据包报头和负载转换为便于预处理器和入侵规则引擎使用的格式，并检测数据包报头的各种异常行为。在数据包解码后到将数据包发送到其他预处理器之前这段期间，内联规范化预处理器会对流量进行规范化以便进行内联部署。

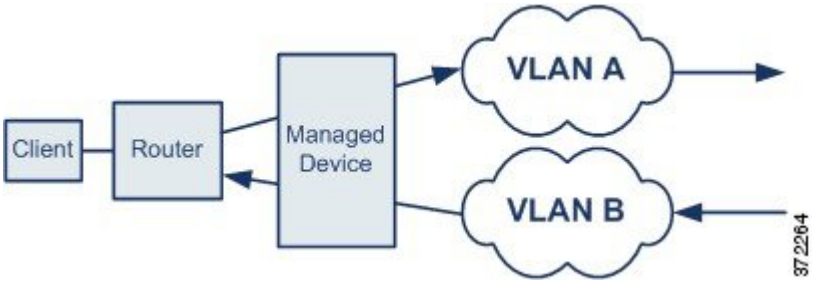
当入侵规则或规则参数要求禁用的预处理器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

高级传输/网络预处理器设置

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

忽略的 VLAN 报头

同一连接但行进方向不同的流量中的不同 VLAN 标记会影响流量重组和规则处理。例如，在下图中，同一连接的流量可以通过 VLAN A 进行传输，并通过 VLAN B 进行接收。



您可以将系统配置为忽略 VLAN 报头，从而可以针对您的部署正确处理数据包。

注释 在 ASA FirePOWER 上不支持此选项。

入侵丢弃规则的活动响应

丢弃规则是指规则状态设置为 Drop and Generate Events 的入侵规则或预处理器规则。在内联部署中，系统通过丢弃触发数据包并阻止数据包起始的会话来对 TCP 或 UDP 丢弃规则作出响应。在被动部署中，系统无法丢弃数据包，并且除使用活动响应的情况以外，不会阻止会话。

提示 由于在会话方面通常未考虑 UDP 数据流，因此数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别 UDP 会话。

您可以配置系统来启动一个或多个活动响应，从而在有问题的数据包触发 TCP 或 UDP 丢弃规则时，更精确具体地关闭 TCP 连接或 UDP 会话。

在内联部署中启用活动响应后，系统通过丢弃触发数据包并在客户端和服务器流量中均插入 TCP 重置 (RST) 数据包来对 TCP 丢弃规则作出响应。系统在被动部署中无法丢弃数据包；在被动部署中启用活动响应时，系统通过向 TCP 连接的客户端和服务器端均发送 TCP 重置来对 TCP 丢弃规则作出响应。在内联部署或被动部署中启用活动响应后，系统通过向会话的两端发送 ICMP 不可达数据包来关闭 UDP 会话。活动响应在内联部署中最有效，因为重置更有可能及时到达以影响连接或会话。

根据您的配置，如果系统看到连接或会话的任一端有其他流量，也可以启动其他活动响应。自从先前响应以来经过指定的秒数后，系统最多会启动数量为指定最大值的每个其他活动响应。

高级传输/网络预处理器选项

在跟踪连接时忽略 VLAN 报头 (Ignore the VLAN header when tracking connections)

指定在识别流量时是忽略还是包含 VLAN 报头，如下所示：

- 选择此选项时，系统会忽略VLAN报头。此设置用于在按不同方向传播的流量中可能检测到同一连接的不同 VLAN 标签的已部署设备
- 当禁用此选项时，系统会包含VLAN报头。此设置用于在按不同方向传播的流量中不会检测到同一连接的不同 VLAN 标签的已部署设备。

注释 在 ASA FirePOWER 上不支持此选项。

Maximum Active Responses

指定每个 TCP 连接的最大活动响应数。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 会禁用丢弃规则触发的活动响应，并禁用 **resp** 或 **react** 规则触发的其他活动响应。

请注意，无论此选项的配置如何，已触发的 **resp** 或 **react** 规则也会启动活动响应；但是，此选项控制系统是否通过与其控制丢弃规则的最大活动响应数相同的方式来启动 **resp** 和 **react** 规则的其他活动响应。

您还可以使用 `config response` 命令配置要使用的活动响应接口以及要在被动部署中尝试的 TCP 重置次数。

最小响应秒数 (Minimum Response Seconds)

指定在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应之前等待的秒数，直至出现**最大活动响应数 (Maximum Active Responses)**。

故障排除选项：会话终止日志记录阈值 (Troubleshooting Options: Session Termination Logging Threshold)

注意 请勿修改“会话终止日志记录阈值”(Session Termination Logging Threshold)，除非支持人员指示执行此操作。

支持人员可能会在故障排除呼叫期间要求您配置系统，以在单个连接超过指定阈值时记录消息。更改此选项的设置会影响性能，应仅在支持人员的指导下进行操作。

此选项指定一个字节数，当会话终止并超过该指定数字时，将会记录消息。

注释 1GB 的上限还受数据流处理分配的受管设备上的内存容量限制。

配置高级传输/网络预处理器设置

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡。

步骤 2 点击“传输/网络层设置”(Transport/Network Layer Settings) 部分旁边的编辑图标 ( )。

步骤 3 修改高级传输/网络预处理器选项，第 1070 页中描述的选项，故障排除选项**会话终止日志记录阈值 (Session Termination Logging Threshold)** 除外。

注释 **跟踪连接时忽略 VLAN 报头 (Ignore the VLAN header when tracking connectons)** 选项在 ASA FirePOWER 模块上不可用。

注意 请勿修改**会话终止日志记录阈值 (Session Termination Logging Threshold)**，除非支持人员指示执行此操作。

步骤 4 点击 **OK**。

接下来的操作

- 或者，进一步配置策略，如编辑访问控制策略，第 614 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

校验和验证

系统可验证所有协议级校验和，以确保接收完整的 IP、TCP、UDP 和 ICMP 传输，且基本级别的数据包在传输过程中未被篡改或意外修改。校验和使用算法来验证数据包中协议的完整性。如果系统计算所得的值与终端主机在数据包中写入的值相同，则数据包将被视为未更改。

禁用校验和验证可能使网络容易受到插入攻击。请注意，系统不生成校验和验证事件。在内联部署中，您可以将系统配置为会丢弃校验和无效的数据包。

校验和验证选项

在被动或内联部署中，可以将以下任何选项设置为**已启用 (Enabled)** 或**已禁用 (Disabled)**；或在内联部署中设置为**丢弃 (Drop)**：

- **ICMP 校验和**
- **IP 校验和**
- **TCP 校验和**
- **UDP 校验和**

要丢弃恶意数据包，除将选项设置为**丢弃 (Drop)** 以外，还必须在关联网络分析策略中启用**内联模式 (Inline Mode)** 并确保设备为内联部署。

在被动部署中或在分流模式下的内联部署中，将这些选项设置为**丢弃 (Drop)** 与将其设置为**已启用 (Enabled)** 的作用相同。

所有校验和验证选项默认为**已启用 (Enabled)**。

验证校验和

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**校验和验证 (Checksum Verification)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**校验和验证 (Checksum Verification)** 旁边的编辑图标 ( )。

步骤 6 修改校验和验证，第 1072 页中所述的选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

内联规范化预处理器

内联规范化预处理器会将流量规范化，从而尽可能降低攻击者在内联部署中得以避开检测的可能性。

注释 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向受管设备部署相关配置。

您可以指定 IPv4、IPv6、ICMPv4、ICMPv6 和 TCP 流量的任意组合的规范化。大多数规范化由内联规范化预处理器逐个数据包执行。但是，TCP 数据流预处理器处理大多数状态相关的数据包和数据流规范化，包括 TCP 负载规范化。

在数据包解码器进行解码后会立即执行内联规范化，直至其他预处理器进行处理。规范化从内数据包层继续执行到外数据包层。

内联规范化预处理器不会生成事件；它准备数据包以供内联部署中的其他预处理器和规则引擎使用。预处理器还有助于确保系统处理的数据包与网络中主机接收的数据包相同。

注释 在内联部署中，思科建议您启用内联模式并配置已启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。在被动部署中，思科建议您使用自适应配置文件。

内联规范化选项

Minimum TTL

当**重置 TTL (Reset TTL)** 大于或等于为此选项设置的值时，请指定以下设置：

- 启用 **Normalize IPv4** 后系统允许 IPv4 Time to Live (TTL) 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对 **Reset TTL** 设置的值
- 启用 **Normalize IPv6** 后系统允许 IPv6 Hop Limit 字段使用的最小值；较小的值会导致将 TTL 的数据包值规范化为针对 **Reset TTL** 设置的值

此字段为空时，系统假设值为 1。

当数据包解码**检测协议报头异常 (Detect Protocol Header Anomalies)** 选项已启用时，可以启用解码器规则类别中的以下规则来生成此选项的事件：

- 您可以启用规则 116:428，以在系统检测到 TTL 小于指定最小值的 IPv4 数据包时生成事件。
- 您可以启用规则 116:270，以在系统检测到跳数限制小于指定最小值的 IPv6 数据包时生成事件。

Reset TTL

如果设置为大于或等于**最小 TTL (Minimum TTL)** 的值，请规范化以下字段：

- IPv4 TTL 字段（如果启用了 **Normalize IPv4**）
- IPv6 Hop Limit 字段（如果启用了 **Normalize IPv6**）

当数据包值小于 **Minimum TTL** 时，系统会通过将其 TTL 或 Hop Limit 值更改为针对此选项设置的值来规范化数据包。将此字段留空或设置为 0，或设置为小于**最小 TTL (Minimum TTL)** 的任意值会禁用该选项。

规范化 IPv4

启用 IPv4 流量规范化。在以下时候，系统还会根据需要规范化 TTL 字段：

- 此选项启用，且
- 为**重置 TTL (Reset TTL)** 设置的值启用 TTL 规范化。

此选项启用时，还可以启用额外的 IPv4 选项。

启用此选项时，系统执行以下基本 IPv4 规范化：

- 将具有多余负载的数据包截断至 IP 报头中指定的数据报长度
- 清除 Differentiated Services (DS) 字段（以前称为 Type of Service (TOS) 字段）
- 将所有选项八位元设置为 1 (No Operation)

规范化 Don't Fragment 位

清除 IPv4 Flags 报头字段的 1 位 Don’t Fragment 子字段。通过启用此选项，下游路由器可在必要时对数据包进行分片而不是将其丢弃；启用此选项还可以根据要丢弃的构造数据包来防止躲避检测。必须启用 **Normalize IPv4** 后才可以选择此选项。

规范化 Reserved 位

清除 IPv4 Flags 报头字段的 1 位 Reserved 子字段。通常会启用此选项。必须启用 **Normalize IPv4** 后才可以选择此选项。

规范化 TOS 位

清除一个字节的 Differentiated Services 字段（以前称为 Type of Service）。必须启用 **Normalize IPv4** 后才可以选择此选项。

规范化多余负载

将具有多余负载的数据包截断至 IP 报头中指定的数据报长度加上第 2 层（例如以太网）报头，但是不截断为小于最小帧长度。必须启用 **Normalize IPv4** 后才可以选择此选项。

规范化 IPv6

将 Hop-by-Hop Options 和 Destination Options 扩展报头中的所有 Option Type 字段设置为 00（跳过并继续处理）。此选项处于启用状态并且为 **Reset TTL** 设置的值会启用跳数限制规范化时，系统还会根据需要规范化 Hop Limit 字段。

规范化 ICMPv4

清除 ICMPv4 流量中 Echo (Request) 和 Echo Reply 消息内的 8 位 Code 字段。

规范化 ICMPv6

清除 ICMPv6 流量中 Echo (Request) 和 Echo Reply 消息内的 8 位 Code 字段。

Normalize/Clear Reserved Bits

清除 TCP 报头中的保留位。

Normalize/Clear Option Padding Bytes

清除任何 TCP 选项填充字节。

Clear Urgent Pointer if URG=0

如果未设置紧急 (URG) 控制位，则清除 16 位 TCP 报头 Urgent Pointer 字段。

Clear Urgent Pointer/URG on Empty Payload

如果没有负载，则清除 TCP 报头 Urgent Pointer 字段和 URG 控制位。

Clear URG if Urgent Pointer is Not Set

如果未设置紧急指针，则清除 TCP 报头 URG 控制位。

Normalize Urgent Pointer

如果指针大于负载长度，则将两字节的 TCP 报头 Urgent Pointer 字段设置为负载长度。

规范化 TCP 负载

启用 TCP Data 字段的规范化以确保重传数据的一致性。无法正确重组的所有数据段都会被丢弃。

Remove Data on SYN

如果 TCP 操作系统策略**不是** Mac OS，则移除同步 (SYN) 数据包中的数据。

此选项还会禁用规则 129:2 的事件生成，该规则原本会在 TCP 数据流预处理器**策略 (Policy)** 选项未设置为 **Mac OS** 时生成事件。

Remove Data on RST

从 TCP 重置 (RST) 数据包中移除所有数据。

Trim Data to Window

将 TCP Data 字段修剪为在 Window 字段中指定的大小。

Trim Data to MSS

如果负载长度大于 MSS，则将 TCP Data 字段修剪为 Maximum Segment Size (MSS)

阻止不可解析的 TCP 报头异常 (Block Unresolvable TCP Header Anomalies)

启用此选项时，系统阻止异常 TCP 数据包，这些数据包在规范化的情况下会无效，并可能受到接收主机的阻止。例如，系统阻止后续传输到已建立的会话上的任何 SYN 数据包。

无论是否启用规则，系统都会丢弃与以下任何 TCP 数据流预处理器规则匹配的任何数据包：

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 至 129:19

Total Blocked Packets 性能图跟踪内联部署中阻止的数据包的数量，并且，在被动部署和轻触模式下的内联部署中，跟踪在内联部署中已阻止的数量。

显式堵塞通知

对显式堵塞通知 (ECN) 标志启用逐个数据包或逐条数据流规范化，如下所示：

- 选择 **Packet** 以逐个数据包清除 ECN 标志（无论协商与否）
- 选择 **Stream** 以逐条数据流清除 ECN 标志（如果未协商 ECN 的使用）

如果选择**数据流 (Stream)**，您还必须确保启用 TCP 数据流预处理器的**需要 TCP 三次握手 (Require TCP 3-Way Handshake)** 选项以进行此规范化。

清除现有 TCP 选项 (Clear Existing TCP Options)

启用**允许这些 TCP 选项 (Allow These TCP Options)**。

.

允许这些 TCP 选项

禁用您在流量中允许的特定 TCP 选项的规范化。

系统不对您明确允许的选项进行规范化。系统会通过将您未明确允许的选项设置为 No Operation（TCP 选项 1）来规范化这些选项。

由于这些选项常用于实现最佳 TCP 性能，因此系统始终会允许以下选项，而不管**允许这些 TCP 选项 (Allow These TCP Options)** 的配置如何：

- 最大分片大小 (MSS)
- 窗口比例
- 时间戳 TCP

系统不会自动允许其他不太常用的选项。

您可以通过配置选项关键字和/或选项编号的逗号分隔列表来允许特定选项，如下例所示：

```
sack, echo, 19
```

指定选项关键字等同于指定与该关键字相关的一个或多个 TCP 选项的编号。例如，指定 `sack` 等同于指定 TCP 选项 4（允许选择性确认 [Selective Acknowledgment Permitted]）和选项 5（选择性确认 [Selective Acknowledgment]）。选项关键字不区分大小写。

您还可以指定 `any`，这样将会允许所有 TCP 选项并有效地禁用所有 TCP 选项的规范化。

下表总结了如何指定要允许的 TCP 选项。如果将字段留空，则系统仅允许 MSS、Window Scale 和 Time Stamp 选项。

指定.....	以允许.....
sack	TCP 选项 4 (Selective Acknowledgment Permitted) 和选项 5 (Selective Acknowledgment)
echo	TCP 选项 6 (Echo Request) 和选项 7 (Echo Reply)
partial_order	TCP 选项 9 (Partial Order Connection Permitted) 和选项 10 (Partial Order Service Profile)
conn_count	TCP 连接计数选项 11 (CC)、选项 12 (CC.New) 和选项 13 (CC.Echo)
alt_checksum	TCP 选项 14 (Alternate Checksum Request) 和选项 15 (Alternate Checksum)
md5	TCP 选项 19 (MD5 Signature)
选项编号（2 至 255）	特定选项，包括没有关键字的选项
any	所有 TCP 选项；此设置会有效地禁用 TCP 选项规范化

如果没有为此选项指定 `any`，则规范化会包含以下内容：

- 除 MSS、Window Scale、Time Stamp 及任何明确允许的选项以外，所有选项字节都设置为 No Operation（TCP 选项 1）
- 如果时间戳存在但无效，或者有效但未协商，则将时间戳八位元设置为 No Operation
- 如果 Time Stamp 已协商但不存在，则阻止数据包
- 如果未设置 Acknowledgment (ACK) 控制位，则清除 Time Stamp Echo Reply (TSecr) 选项字段
- 如果未设置 SYN 控制位，则将 MSS 和 Window Scale 选项设置为 No Operation (TCP Option 1)

配置内联规范化

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

开始之前

- 如果要规范化或丢弃恶意数据包，请启用**内联模式 (Inline Mode)**，如内联部署中预处理器流量的修改，第 1002 页中所述。受管设备也必须内联部署。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**内联规范化 (Inline Normalization)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**内联规范化 (Inline Normalization)** 旁边的编辑图标 ( )。

步骤 6 设置选项，如内联规范化预处理器，第 1073 页中所述。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要让内联规范化的“最小 TTL”(Minimum TTL) 选项生成入侵事件，请启用任一或两个数据包解码器规则：116:429 (IPv4) 和 116:270 (IPv6)。有关详细信息，请参阅设置入侵规则状态，第 833 页和内联规范化选项，第 1074 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

IP 分片重组预处理器

由于 IP 数据报大于最大传输单位 (MTU) 而将其分为两个或多个更小的 IP 数据报，这个过程即为数据报分片。单个 IP 数据报片段可能未包含足够的信息来识别隐藏攻击。攻击者可能尝试通过将攻击数据传输到分片数据包中来躲避检测。在规则引擎对分片的 IP 数据报执行规则之前，IP 分片重组预处理器会重组这些数据报，以便规则可以更适当地识别这些数据包中的攻击。如果分片的数据报无法重组，则不对其执行规则。

IP 分片重组漏洞

启用 IP 分片重组可以帮助您检测针对网络上主机的攻击（例如泪滴 [teardrop] 攻击）和针对系统本身的资源消耗攻击（例如 Jolt2 攻击）。

泪滴攻击利用某些操作系统中在尝试重组重叠 IP 片段时会导致这些操作系统崩溃的漏洞。IP 分片重组预处理器在被启用并配置为识别重叠片段之后，会执行此操作。IP 分片重组预处理器会检测重叠片段攻击（例如泪滴攻击）中的第一批数据包，但对于同一攻击不会检测后续数据包。

Jolt2 攻击会发送同一分片的 IP 数据包的大量副本，以尝试过度使用 IP 分片重组器并导致拒绝服务攻击。内存使用上限会中断此攻击以及 IP 分片重组预处理器中的类似攻击，并在全面检查基础上注重系统自我保护。这样，系统不会因攻击而崩溃，可保持运行，并继续检查网络流量。

不同的操作系统以不同方式重组分片数据包。可以确定主机运行的操作系统的攻击者还可以对恶意数据包进行分片，以便目标主机以特定方式对这些数据包进行重组。由于系统不知道受监控网络上的主机运行的操作系统，因此预处理器可能会不正确地重组和检查数据包，致使漏洞成功躲过检测。要缓解这种攻击，您可以配置分片重组预处理器，使其会针对网络中的每个主机使用适当方法对数据包进行分片重组。

请注意，您也可以在被动部署中使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 IP 分片重组预处理器动态选择基于目标的策略。

基于目标的分片重组策略

主机的操作系统使用三个条件来确定当重组数据包时支持的数据包分片。

- 操作系统收到分片的顺序
- 其偏移量（分片与数据包开始位置之间的距离，按字节计算）
- 它与重叠分片相比的开始和结束位置。

虽然每个操作系统都使用这些条件，但是不同的操作系统在重组分片数据包时支持不同的片段。因此，网络中具有不同操作系统的两个主机可能会以完全不同的方式重组同一组重叠片段。

攻击者（了解其中一个主机的操作系统）可能会尝试通过发送隐藏在重叠数据包片段中的恶意内容来逃避检测并利用该主机。该数据包经过重组和检查后看似无害，但是由目标主机进行重组后则会包含恶意的漏洞。但是，如果将 IP 分片重组预处理器配置为可感知受监控网络段上运行的操作系统，则它会以与目标主机相同的方式重组分片，从而识别攻击。

IP 分片重组选项

您可以选择只是启用或禁用 IP 分片重组；但是，思科建议以更精细的级别指定已启用的 IP 分片重组预处理器的行为。

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

可以配置以下全局选项：

预分配片段

预处理器一次可以处理的最大单个片段数量。指定要预分配的片段节点的数量会启用静态内存分配。

注意 处理单个片段会使用大约 1550 字节的内存。如果预处理器需要比受管设备的预定允许内存限制更多的内存来处理单个片段，则设备的内存限制优先。

您可以为每个 IP 分片重组策略配置以下选项：

网络

要对其应用分片重组策略的一个或多个主机的 IP 地址。

可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以指定总共最多 255 个配置文件（包括默认策略）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的 `default` 设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 `any`（例如，0.0.0.0/0 或 ::/0）。

策略

要为受监控网段上的主机组使用的分片重组策略。

根据目标主机的操作系统，可以选择七个分片重组策略之一。下表列出了这七个策略以及使用每个策略的操作系统。First 和 Last 这两个策略名称反映这些策略是否支持原始或后续重叠数据包。

表 *184*：基于目标的分片重组策略

策略	Operating Systems
BSD	AIX FreeBSD IRIX VAX/VMS

策略	Operating Systems
BSD-right	HP JetDirect
姓氏	Mac OS HP-UX
Linux	Linux OpenBSD
名字	思科 IOS
Solaris	SunOS
Windows 的 ISE 安全评估代理	Windows 的 ISE 安全评估代理

Timeout

指定预处理器引擎在重组分片数据包时可用的最长时间（以秒为单位）。如果在指定的时间段内无法重组数据包，则预处理器引擎会停止尝试重组数据包并丢弃接收到的片段。

最小 TTL

指定数据包可具有的可接受最小 TTL 值。此选项检测基于 TTL 的插入攻击。

可以启用规则 123:11 为此选项生成事件。

检测异常

确定分片问题，例如重叠片段。

您可以启用以下规则来生成此选项的事件：

- 123:1 至 123:4
- 123:5（BSD 策略）
- 123:6 至 123:8

重叠限制

指定在检测到会话中存在所配置数量的重叠片段时，将会停止该会话的分片重组。

必须启用 **Detect Anomalies** 后才可以配置此选项。不指定值将会禁用此选项。值为 0 指定重叠片段的数量不受限制。

您可以启用规则 123:12 来生成此选项的事件。

Minimum Fragment Size

指定在检测到小于所配置数量的非最后一个分片时，数据包将被视为恶意。

必须启用 **Detect Anomalies** 后才可以配置此选项。不指定值将会禁用此选项。值 0 表示无限字节数。

您可以启用规则 123:13 来生成此选项的事件。

配置 IP 分片重组

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的任何网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 993 页。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的 **IP 分片重组 (IP Defragmentation)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击 **IP 分片重组 (IP Defragmentation)** 旁边的编辑图标 ( )。

步骤 6 或者，在**预分配片段 (Preallocated Fragments)** 字段中输入值。

步骤 7 有以下选项可供选择：

- 添加服务器配置文件 - 点击页面左侧**服务器 (Servers)** 旁边的添加图标 ( )，然后在**主机地址 (Host Address)** 字段中输入值并点击**确定 (OK)**。可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。您可以创建总共255个基于目标的策略（包括默认策略）。
- 编辑服务器配置文件 - 点击页面左侧**服务器 (Servers)** 下的已配置地址，或点击**默认 (default)**。

- 删除配置文件 - 点击策略旁边的删除图标 ( )。

步骤 8 修改IP 分片重组选项，第 1081 页中所述的选项。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 IP 分片重组 (IP Defragmentation) 规则 (GID 123)。有关详细信息，请参阅设置入侵规则状态，第 833 页和IP 分片重组选项，第 1081 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

数据包解码器

在将捕获的数据包发送到预处理器之前，系统首先会将数据包发送到数据包解码器。数据包解码器将数据包报头和负载转换为便于预处理器和规则引擎使用的格式。每个堆栈层依次进行解码，从数据链路层开始并继续直至网络层和传输层。

数据包解码器选项

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

解码 GTP 数据信道

解码封装的 GTP（通用分组无线业务 [GPRS] 隧道协议）数据通道。默认情况下，解码器会解码端口 3386 上的版本 0 数据和端口 2152 上的版本 1 数据。您可以使用 `GTP_PORTS` 默认变量修改用于识别封装的 GTP 流量的端口。

您可以启用规则 116:297 和 116:298 来生成此选项的事件。

检测非标准端口上的 Teredo (Detect Teredo on Non-Standard Ports)

检查除端口 3544 以外的其他 UDP 端口上识别的 IPv6 流量的 Teredo 隧道。

系统始终检查存在的 IPv6 流量。默认情况下，IPv6 检查包括 4in6、6in4、6to4 和 6in6 隧道方案，如果 UDP 报头指定端口 3544，还包括 Teredo 隧道。

在 IPv4 网络中，IPv4 主机可以使用 Teredo 协议通过 IPv4 网络地址转换 (NAT) 设备传输 IPv6 流量。Teredo 将 IPv6 数据包封装在 IPv4 UDP 数据报中，以允许在 IPv4 NAT 设备后面进行 IPv6 连接。系统通常使用 UDP 端口 3544 识别 Teredo 流量。但是，攻击者可能会使用非标准端口来尝试避开检测。您可以启用 **Detect Teredo on Non-Standard Ports** 来促使系统检查 Teredo 隧道的所有 UDP 负载。

Teredo 解码仅发生在第一个 UDP 报头上，并且仅当 IPv4 用于外部网络层时才会发生。如果由于 IPv6 数据中封装的 UDP 数据而在 Teredo IPv6 层之后出现第二个 UDP 层，则规则引擎会使用 UDP 入侵规则对内部和外部 UDP 层均进行分析。

请注意，**policy-other** 规则类别中的入侵规则 12065、12066、12067 和 12068 会检测 Teredo 流量，但不对这些流量进行解码。您可以根据需要在内联部署中使用这些规则丢弃 Teredo 流量；但是，启用 **Detect Teredo on Non-Standard Ports** 时，应确保这些规则处于禁用状态或者设置为生成事件而不丢弃流量。

检测多余长度值 (Detect Excessive Length Value)

在数据包报头指定的数据包长度大于实际数据包长度时进行检测。

您可以启用规则 116:6、116:47、116:97 和 116:275 来生成此选项的事件。

检测无效 IP 选项 (Detect Invalid IP Options)

检测无效 IP 报头选项以识别使用无效 IP 选项的漏洞。例如，存在针对防火墙的拒绝服务攻击，该攻击导致系统冻结。防火墙尝试解析无效的 Timestamp 和 Security IP 选项且未能检查到零长度，导致无法恢复的无限循环。规则引擎会识别零长度选项并提供可用于缓解对防火墙的攻击的信息。

您可以启用规则 116:4 和 116:5 来生成此选项的事件。

检测试验性 TCP 选项 (Detect Experimental TCP Options)

检测具有试验性 TCP 选项的 TCP 报头。下表介绍了这些选项。

TCP 选项	说明
9	允许的偏序连接
10	偏序服务配置文件
14	替代校验和请求
15	替代校验和数据
18	尾部校验和
20	空间通信协议标准 (SCPS)
21	选择性否定确认 (SCPS)
22	记录边界 (SCPS)
23	损坏 (SPCS)
24	SNAP
26	TCP 压缩过滤器

由于这些是试验性选项，因此，某些系统未对其进行说明，可能容易产生漏洞。

注释 除上表中列出的试验性选项外，系统还将选项编号大于 26 的任何 TCP 选项视为试验性选项。

您可以启用规则 116:58 来生成此选项的事件。

检测过时 TCP 选项 (Detect Obsolete TCP Options)

检测具有过时 TCP 选项的 TCP 报头。由于这些是过时选项，因此，某些系统未对其进行说明，可能容易产生漏洞。下表介绍了这些选项。

TCP 选项	说明
6	回应
7	应答
16	Skeeter
17	Bubba
19	MD5 签名
25	未分配

您可以启用规则 116:57 来生成此选项的事件。

检测 T/TCP (Detect T/TCP)

检测带有 CC.ECHO 选项的 TCP 报头。CC.ECHO 选项确认使用的是事务 TCP (T/TCP)。由于 T/TCP 报头选项未广泛使用，因此，某些系统未对其进行说明，可能容易产生漏洞。

您可以启用规则 116:56 来生成此选项的事件。

检测其他 TCP 选项 (Detect Other TCP Options)

检测具有其他 TCP 解码事件选项未检测到的无效 TCP 选项的 TCP 报头。例如，此选项检测长度不正确或者选项数据长度超过 TCP 报头范围的 TCP 选项。

您可以启用规则 116:54、116:55 和 116:59 来生成此选项的事件。

检测协议报头异常 (Detect Protocol Header Anomalies)

检测更具体的 IP 和 TCP 解码器选项未检测到的其他解码错误。例如，解码器可能会检测到格式错误的数据链路协议报头。

要生成此选项的事件，可以启用以下任一规则：

GID:SID	在以下情况下生成事件：
116:467	数据包小于用　思科 FabricPath 报头封装的数据包的最小尺寸。
116:468	报头中的思科元数据 (CMD) 字段包含长度小于有效 CMD 报头最小尺寸的报头。CMD 字段与思科 Trustsec 协议相关联。
116:469	报头中的 CMD 字段包含无效字段长度。
116:470	报头中的 CMD 字段包含无效安全组标记 (SGT) 选项类型。
116:471	报头中的 CMD 字段包含具有保留值的 SGT。

您也可以启用与其他数据包解码器选项不关联的任何数据包解码器规则。

配置数据包解码

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的**数据包解码 (Packet Decoding)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**数据包解码 (Packet Decoding)** 旁边的编辑图标 ( )。

步骤 6 启用或禁用数据包解码器选项，第 1084 页中所述的选项。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用数据包解码器规则(GID 116)。有关详细信息，请参阅设置入侵规则状态，第 833 页和数据包解码器选项，第 1084 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

TCP 数据流预处理

TCP 协议定义连接可以处于的各种状态。每个 TCP 连接通过源 IP 地址和目标 IP 地址以及源端口和目标端口进行识别。TCP 一次仅允许存在一个具有相同连接参数值的连接。

状态相关的 TCP 漏洞

如果向入侵规则添加带有 `established` 参数的 `flow` 关键字，则入侵规则引擎会在有状态模式下检查与规则和流指令匹配的数据包。状态模式仅评估通过客户端与服务器之间的合法三次握手建立的TCP会话所包含的流量。

您可以配置系统，以便预处理器对无法识别为已建立的 TCP 会话的一部分的任何 TCP 流量进行检测；但是，对于典型使用不建议此操作，因为事件会使系统迅速过载且不会提供有意义的数据。

stick 和 snot 之类的攻击使用系统的广泛的规则集和数据包检测自身。这些工具根据基于 Snort 的入侵规则生成数据包，并通过网络发送这些数据包。如果您的规则不包括用于为状态检查配置规则的 `flow` 或 `flowbits` 关键字，则每个数据包将触发规则，进而导致系统过载。您可以通过状态检查来忽略这些数据包，因为它们不是已建立的 TCP 会话的一部分，而且不提供有意义的信息。执行状态检查时，规则引擎仅检测属于已建立的 TCP 会话的一部分的那些攻击，从而使分析人员关注这些攻击而不是由 stick 或 snot 攻击导致的事件量。

基于目标的 TCP 策略

不同操作系统以不同方法实施 TCP。例如，Windows 和其他一些操作系统需要 TCP 重置段以具有精确的 TCP 序列号来重置会话，而 Linux 和其他操作系统则允许使用一系列序列号。在本示例中，数据流预处理器必须明确了解目标主机会如何根据序列号对重置作出响应。仅当目标主机认为重置有效时，数据流预处理器才会停止跟踪会话，因此，攻击在预处理器停止检查数据流后无法通过发送数据包来躲避检测。在 TCP 实施中的其他变化包括操作系统是否采用 TCP 时间戳选项，并且在采用时如何处理时时间戳，以及操作系统接受还是忽略 SYN 数据包中的数据等等方面。

不同操作系统也以不同方式重组重叠的 TCP 数据段。重叠的 TCP 数据段可能会反映未确认的 TCP 流量的正常重传。它们也可能表示攻击者（了解其中一个主机的操作系统）尝试通过发送隐藏在重叠数据段中的恶意内容来躲避检测并利用该主机。但是，您可以将数据流预处理器配置为可感知受监控网段上运行的操作系统，使其以与目标主机相同的方式重组数据段，从而识别攻击。

您可以创建一个或多个 TCP 策略，以根据受监控网段上的不同操作系统定制 TCP 数据流检查和重组。对于每个策略，可识别 13 个操作系统策略之一。您根据需要使用尽可能多的 TCP 策略将每个

TCP 策略绑定到特定 IP 地址或地址块，以识别使用其他操作系统的任意或所有主机。默认 TCP 策略适用于在任何其他 TCP 策略中未识别的受监控网络上的任何主机，因此无需为默认 TCP 策略指定 IP 地址或地址块。

请注意，您也可以在被动部署中使用自适应配置文件，通过数据包中目标主机的主机操作系统信息来为 TCP 流预处理器动态选择基于目标的策略。

TCP 数据流重组

数据流预处理器收集和重组属于 TCP 会话的服务器到客户端通信数据流和/或客户端到服务器通信数据流的一部分的所有数据包。这允许规则引擎将数据流作为单个已重组实体进行检查，而不是仅检查属于指定数据流的一部分的个别数据包。

数据流重组允许规则引擎识别基于数据流的攻击，在检查个别数据包时它可能无法检测此类攻击。您可以根据网络需要指定规则引擎重组哪些通信数据流。例如，在监控网络服务器上的流量时，您可能只希望检查客户端流量，因为您不太可能从自己的网络服务器接收到恶意流量。

在每个 TCP 策略中，您可以指定用于识别要重组的数据流预处理器流量的端口的逗号分隔列表。启用自适应配置文件后，您还可以列出用于识别要重组的流量的服务（以替代端口或端口组合的形式）。

您可以指定端口和/或服务。您可以为客户端端口和/或服务器端口的任意组合指定单独的端口列表。您还可以为客户端服务和/或服务器服务指定单独的服务列表。例如，假设您要重组以下内容：

- 来自客户端的 SMTP（端口 25）流量
- FTP 服务器响应（端口 21）
- 两个方向的 telnet（端口 23）流量

您可以配置以下内容：

- 对于客户端端口，指定 `23 和 25`
- 对于服务器端口，指定 `21 和 23`

或者，您可以配置以下内容：

- 对于客户端端口，指定 `25`
- 对于服务器端口，指定 `21`
- 对于客户端端口和服务器端口，指定 `23`

此外，请参考以下示例，该示例将端口和服务进行组合，并在启用自适应配置文件后有效：

- 对于客户端端口，指定 `23`
- 对于客户端服务，指定 `smtp`
- 对于服务器端口，指定 `21`
- 对于服务器服务，指定 `telnet`

取消一个端口（例如，!80）可通过阻止 TCP 数据流预处理器处理该端口的流量来提升性能。

虽然您也可以指定all作为参数来为所有端口提供重组，但是思科不建议将端口设置为all，因为这样做可能会不必要地增加此预处理器检查的流量并降低性能。

TCP 重组自动透明地包括添加到其他预处理器的端口。但是，如果明确向已添加到其他预处理器配置的 TCP 重组列表中添加端口，则会正常处理这些附加端口。这包括下列预处理器的端口列表：

- FTP/Telnet（服务器级 FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- 会话发起协议
- POP
- IMAP
- SSL

请注意，重组其他流量类型（客户端和/或服务器）会增加资源需求。

TCP 数据流预处理选项

如果在以下描述中未提及任何预处理器规则，则此选项未与预处理器规则关联。

可以配置以下全局 TCP 选项：

Packet Type Performance Boost

支持忽略已启用规则中未指定的所有端口和应用协议的 TCP 流量，但在源端口和目标端口均设置为any的 TCP 规则具有flow或flowbits选项时除外。这种性能改进可能会导致未能检测出某些攻击。

可为每个 TCP 策略配置以下选项：

网络

指定要对其应用 TCP 数据流重组策略的主机 IP 地址。

可以指定单个 IP 地址或地址块。总共最多可以指定 255 个配置文件（包括默认策略）。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

请注意，默认策略中的default设置指定受监控网段上其他基于目标的策略未涵盖的所有 IP 地址。因此，不能且不需要为默认策略指定 IP 地址或 CIDR 块/前缀长度，并且不能在其他策略中将此设置留空或使用地址记法来表示 any（例如，0.0.0.0/0 或 ::/0）。

策略

识别一个或多个目标主机的 TCP 策略操作系统。如果选择除 **Mac OS** 以外的其他策略，则系统会从同步 (SYN) 数据包中删除数据并禁用规则 129:2 的事件生成。请注意，启用内联规范化预处理器的 **SYN 时删除数据 (Remove Data on SYN)** 选项也会禁用规则 129:2。

下表列出了操作系统策略以及使用每个策略的主机操作系统。

表 *185*: *TCP* 操作系统策略

策略	Operating Systems
姓氏	未知 OS
名字	思科 IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 内核 Linux 2.6 内核
旧 Linux	Linux 2.2 及更低版本的内核
Windows 的 ISE 安全评估代理	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 及更高版本
HPUX 10	HP-UX 10.2 及更低版本
Mac OS	Mac OS 10 (Mac OS X)

提示 当您不知道主机操作系统时，First操作系统策略可以提供一些保护。但是，它可能会导致未能检测出某些攻击。如果您知道操作系统，则应该编辑策略以指定正确的操作系统。

Timeout

规则引擎在状态表中保持数据流处于非活动状态的秒数（介于 1 和 86400 之间）。如果数据流在指定时间内未重组，则入侵规则引擎会将其从状态表中删除。

注释 如果受管设备部署在网络流量可能达到设备的带宽限制的网段上，则应该考虑将该值设置为较高的值（例如 600 秒），以降低处理开销。

最大 TCP 窗口

指定由接收主机指定的所允许的最大 TCP 窗口大小（1 至 1073725440 字节）。值设置为 0 会禁用检查 TCP 窗口大小。

注意 上限是 RFC 允许的最大窗口大小，旨在防止攻击者躲避检测；但是，设置明显过大的最大窗口大小可能导致自愿接受的拒绝服务。

状态检查异常 (Stateful Inspection Anomalies) 处于启用状态时，可以启用规则 129:6 为此选项生成事件。

重叠限制

指定在检测到某会话中存在所配置数量（介于 0 [无限制] 和 255 之间）的重叠分段时，针对该会话的分段重组将会停止，并且，如果 **Stateful Inspection Anomalies** 以及随附的预处理器规则均处于启用状态，将会生成事件。

您可以启用规则 129:7 来生成此选项的事件。

刷新因数 (Flush Factor)

在内联部署中，指定在经过所配置数量（介于 1 和 2048 之间）的大小未减小的分段后检测到大小减小的分段时，系统会刷新为进行检测而累积的分段数据。值设置为 0 会禁用此分段模式的检测（这可能意味着请求或响应结束）。请注意，必须启用内联规范化的**规范化 TCP 负载 (Normalize TCP Payload)** 选项，才会使此选项生效。

状态检测异常

检测 TCP 堆栈中的异常行为。启用随附的预处理器规则后，如果 TCP/IP 堆栈编写得不好，可能会生成许多事件。

您可以启用以下规则来生成此选项的事件：

- 129:1 至 129:5

- 129:6（仅适用于 Mac OS）
- 129:8 至 129:11
- 129:13 至 129:19

请注意以下提示：

- 为了让规则 129:6 生成事件，还必须为**最大 TCP 窗口 (Maximum TCP Window)** 配置一个大于 0 的值。
- 为了让规则 129:9 和 129:10 生成事件，还必须启用 **TCP 会话劫持 (TCP Session Hijacking)**。

TCP 会话劫持

通过针对会话上接收到的后续数据包验证三次握手期间从 TCP 连接两端检测到的硬件 (MAC) 地址来检测 TCP 会话劫持。当一端或另一端的 MAC 地址不匹配时，如果启用了 **Stateful Inspection Anomalies** 以及两个对应的预处理器规则之一，系统会生成事件。

您可以启用规则 129:9 和 129:10 来生成此选项的事件。请注意，为了让这些规则中任一个生成事件，还必须启用**状态检查异常 (Stateful Inspection Anomalies)**。

连续小分片 (Consecutive Small Segments)

启用 **Stateful Inspection Anomalies** 后，可指定允许的连续 TCP 小分段的最大数量（1 至 2048）。值设置为 0 会禁止连续小分段。

此选项必须与 **Small Segment Size** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，在无干预确认的情况下接收多达 2000 个连续分段，即使每个分段长度为 1 字节，分段数量也会远远超出您通常的预期。

您可以启用规则 129:12 来生成此选项的事件。

小分片大小 (Small Segment Size)

启用 **Stateful Inspection Anomalies** 后，可指定被视为小分段的 TCP 分段大小（1 至 2048 字节）。值设置为 0 会禁止指定小分段的大小。

此选项必须与 **Consecutive Small Segments** 选项一起进行设置；您可以同时禁用这两个选项或者将它们都设置为非零值。请注意，一个 2048 字节的 TCP 分段大于普通的 1500 字节的以太网帧。

忽略小分片的端口 (Ports Ignoring Small Segments)

状态检查异常 (Stateful Inspection Anomalies)、**连续小分片 (Consecutive Small Segments)** 和**小分片大小 (Small Segment Size)** 处于启用状态时，可指定一个或多个会忽略小 TCP 分片检测的端口的逗号分隔列表。将此选项留空表示未忽略任何端口。

您可以向列表中添加任何端口，但是列表仅影响 TCP 策略中的某个 **Perform Stream Reassembly on port** 列表中指定的端口。

需要 TCP 三次握手

指定仅在 TCP 三次握手完成后，会话才被视为已建立的会话。禁用此选项可提高性能，防御 SYN 泛洪攻击，并允许在部分异步环境中操作。启用此选项可避免尝试通过发送不属于已建立的 TCP 会话的信息来生成误报的攻击。

您可以启用规则 129:20 来生成此选项的事件。

三次握手超时

指定启用 **Require TCP 3-Way Handshake** 后必须允许用于完成握手的时间（0 [无限制] 至 86400 秒 [24 小时]）。必须启用 **Require TCP 3-Way Handshake** 后才能修改此选项的值。

数据包大小性能提升

将预处理器设置为在重组缓冲区中不对大数据包进行排队。这种性能改进可能会导致未能检测出某些攻击。禁用此选项可防止使用 1 到 20 字节的小数据包尝试躲避检测。当您肯定所有流量都由超大数据包组成并因此无此类攻击时，可启用此选项。

旧版重组

重组数据包时，将数据流预处理器设置为模拟废弃的数据流 4 预处理器，借此可以将该数据流预处理器重组的事件与基于数据流 4 预处理器重组的相同数据流的事件相比较。

异步网络 (Asynchronous Network)

指定受监控网络是否为异步网络，即，系统只能看到一半流量的网络。启用此选项后，系统不重组 TCP 数据流来提高性能。

对客户端端口执行数据流重组

根据连接的客户端的端口启用数据流重组。换句话说，它对目标为网络服务器、邮件服务器或通常由 $HOME_NET 中指定的 IP 地址定义的其他 IP 地址的数据流进行重组。如果您预计客户端会发出恶意流量，请使用此选项。

对客户端服务执行数据流重组

根据连接的客户端的服务启用数据流重组。如果您预计客户端会发出恶意流量，请使用此选项。

必须为选择的每个客户端服务至少启用一个客户端检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用启用检测器，则系统会自动为应用启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对服务器端口执行数据流重组

根据连接的服务器端的端口启用数据流重组。换句话说，它对从网络服务器、邮件服务器或通常由 $EXTERNAL_NET 中指定的 IP 地址定义的其他 IP 地址发出的数据流进行重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定端口来禁用此选项。

对服务器服务执行数据流重组

根据连接的服务器端的服务启用数据流重组。当您要监控服务器端攻击时，请使用此选项。您可以通过不指定服务来禁用此选项。

必须至少启用一个检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为服务启用检测器，则系统会自动为相关应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为该应用协议启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

对客户端端口和服务器端口执行数据流重组 (Perform Stream Reassembly on Both Ports)

根据连接的客户端和服务器端的端口启用数据流重组。如果您预计相同端口的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。您可以通过不指定端口来禁用此选项。

对客户端服务和服务器服务执行数据流重组 (Perform Stream Reassembly on Both Services)

根据连接的客户端和服务器端的服务启用数据流重组。如果您预计相同服务的恶意流量在客户端和服务器之间可能以任一方向传播，请使用此选项。可以通过不指定服务来禁用此选项。

必须至少启用一个检测器。默认情况下，思科提供的所有检测器均已激活。如果没有为相关客户端应用或应用协议启用检测器，则系统会自动为应用或应用协议启用思科提供的所有检测器；如果不存在任何检测器，则系统会为应用或应用协议启用最近修改的用户定义的检测器。

此功能需要保护和控制许可证。

Troubleshooting Options: Maximum Queued Bytes

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据量。值 0 表示无限字节数。

注意 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

Troubleshooting Options: Maximum Queued Segments

支持人员可能会在故障排除呼叫期间要求您指定可以在 TCP 连接的一端排队的数据段的最大字节数。值 0 表示无限的数据段字节数。

注意 更改此故障排除选项的设置会影响性能，应仅在支持人员的指导下进行操作。

配置 TCP 数据流预处理

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

开始之前

- 确认您要在基于目标的自定义策略中识别的网络匹配，或者是其父网络分析策略所处理的网络、区域和 VLAN 的子集。有关详细信息，请参阅网络分析策略的高级设置，第 993 页。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要修改的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击左侧导航面板中的 **Settings**。

步骤 4 如果“传输/网络层预处理器”(Transport/Network Layer Preprocessors) 下的 **TCP 数据流配置 (TCP Stream Configuration)** 设置已禁用，请通过点击**已启用 (Enabled)** 进行启用。

步骤 5 点击 **TCP 数据流配置 (TCP Stream Configuration)** 旁边的编辑图标 ( )。

步骤 6 选中或清除**全局设置 (Global Settings)** 部分中的**数据包类型性能提升 (Packet Type Performance Boost)** 复选框。

步骤 7 您可以执行以下操作：

- 添加基于目标的策略 - 点击“目标”(Targets) 部分中的**主机 (Hosts)** 旁边的添加图标 ( )。在**主机地址 (Host Address)** 字段中指定一个或多个 IP 地址。可以指定单个 IP 地址或地址块。您可以创建总共 255 个基于目标的策略（包括默认策略）。完成后，点击**确定 (OK)**。
- 编辑基于目标的现有策略 - 在**主机 (Hosts)** 下，点击要编辑的策略的地址，或点击默认值以在**默认值 (default)** 中编辑默认配置值。
- 修改 TCP 数据流预处理选项 - 请参阅 TCP 数据流预处理选项，第 1090 页。

  注意 请勿修改**最大排队字节数 (Maximum Queued Bytes)** 或**最大排队分片数 (Maximum Queued Segments)**，除非支持人员指示执行此操作。

  提示 要根据客户端服务和/或服务器服务修改数据流重组设置，请在要修改的字段内点击，或者点击要修改的字段旁边的**编辑 (Edit)**。使用箭头按钮在弹出窗口中的**可用 (Available)** 和**已启用 (Enabled)** 列表之间移动服务，然后点击**确定 (OK)**。

- 删除基于目标的现有策略 - 点击要删除的策略旁边的删除图标 ( )。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用 TCP 数据流预处理器规则 (GID 129)。有关详细信息，请参阅设置入侵规则状态，第 833 页和TCP 数据流预处理选项，第 1090 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

UDP 数据流预处理

当规则引擎使用以下任何参数根据包含 `flow` 关键字的 UDP 规则处理数据包时，会发生 UDP 数据流预处理：

- 建立
- `To Client`
- `From Client`
- 到服务器
- `From Server`

在会话方面通常未考虑 UDP 数据流。UDP 是一个无连接协议，并不提供在两个终端之间建立通信信道、交换数据和关闭该信道的方法。但是，数据流预处理器使用封装 IP 数据报报头中的源和目标 IP 地址字段及 UDP 报头中的端口字段来确定流动方向并识别会话。当超过可配置的计时器时，或者当任一终端收到表明另一个终端不可达或所请求的服务不可用的 ICMP 消息时，会话将会结束。

请注意，系统不生成与 UDP 数据流预处理相关的事件；但是，您可以启用相关数据包解码器规则来检测 UDP 协议报头异常。

UDP 数据流预处理选项

Timeout

指定预处理器在状态表中保持非活动数据流的秒数。如果在指定时间内看不到其他数据报，预处理器会从状态表中删除数据流。

Packet Type Performance Boost

将预处理器设为忽略已启用规则中未指定的所有端口和应用协议的 UDP 流量，但在源端口和目标端口均设置为 `any` 的 UDP 规则具有 `flow` 或 `flowbits` 选项时除外。这种性能改进可能会导致未能检测出某些攻击。

配置 UDP 数据流预处理

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**传输/网络层预处理器 (Transport/Network Layer Preprocessors)** 下的 **UDP 数据流配置 (UDP Stream Configuration)** 已禁用，请点击**启用 (Enabled)**。

步骤 5 点击 **UDP 数据流配置 (UDP Stream Configuration)** 旁边的编辑图标 ( )。

步骤 6 设置选项，如UDP 数据流预处理选项，第 1097 页中所述。

步骤 7 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的缓存更改。

接下来的操作

- 如果要生成入侵事件，请启用相关数据包解码器规则 (GID 116)。有关详细信息，请参阅设置入侵规则状态，第 833 页和数据包解码器，第 1084 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

第 61 章

检测特定威胁

以下主题介绍如何在网络分析策略中使用预处理器检测特定威胁：

特定威胁检测简介

您可以在网络分析策略中使用若干预处理器检测对受监控网络的具体威胁（例如，后洞攻击、若干端口扫描类型和尝试通过大量流量淹没网络的基于速率的攻击）。请注意，当入侵规则或规则参数要求禁用的预处理器时，尽管预处理器在网络分析策略网络界面中保持禁用状态，系统还会自动使用其当前设置。

您还可以使用在入侵规则中配置的敏感数据检测来检测以非安全方式传输的敏感数字数据。

Back Orifice 检测

Firepower 系统提供用于检测是否存在 Back Orifice 程序的预处理器。此程序可用于获取对 Windows 主机的管理员访问权限。

Back Orifice 检测预处理器

Back Orifice 预处理器为 Back Orifice 神奇 cookie "*!*QWTY?"（位于数据包的前八个字节且使用 XOR 加密）分析 UDP 流量。

Back Orifice 预处理器具有配置页面，但没有配置选项。如果启用此预处理器，还必须为其启用预处理器规则，以生成相应的事件。

表 *186*: *Back Orifice GID:SID*

预处理器规则 **GID:SID**	说明
105:1	检测到 Back Orifice 流量
105:2	检测到 Back Orifice 客户端流量
105:3	检测到 Back Orifice 服务器流量
105:4	检测到 Back Orifice Snort 缓冲区攻击

检测 Back Orifice

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**设置 (Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的 **Back Orifice 检测 (Back Orifice Detection)** 已禁用，请点击**已启用 (Enabled)**。

注释 Back Orifice 无用户可配置选项。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 如果要生成入侵事件，请启用 Back Orifice 检测规则 105:1、105:2、105:3 或 105:4。有关详细信息，请参阅入侵规则状态，第 832 页和Back Orifice 检测预处理器，第 1099 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

端口扫描检测

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者将特制的数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

端口扫描本身不算是攻击。事实上，攻击者使用的一些端口扫描技术也可能会被网络上的合法用户使用。思科的端口扫描检测器旨在通过检测活动模式来帮助确定哪些端口扫描可能是恶意的。

端口扫描类型、协议和过滤的灵敏度级别

攻击者可能会使用多种方法来探测网络。他们通常使用不同的协议从目标主机获取不同的响应，以期即使某一种协议被阻止，也可以使用另一种。

表 *187*：协议类型

协议	说明
TCP	检测 TCP 探针，例如 SYN 扫描、ACK 扫描、TCP connect() 扫描和带异常标志组合（如 Xmas tree、FIN 和 NULL）的扫描
UDP	检测 UDP 探针，如零字节 UDP 数据包
ICMP	检测 ICMP 回应请求 (ping)
IP	检测 IP 协议扫描。这些扫描与 TCP 和 UDP 扫描不同，因为攻击者不是查找开放端口，而是尝试去发现目标主机支持哪些 IP 协议。

根据目标主机的数量、扫描主机的数量和扫描的端口数量，端口扫描通常分为四种类型。

表 *188*：端口扫描类型

类型	说明
端口扫描检测	一对一端口扫描，在这种扫描中，攻击者使用一个或几个主机扫描单个目标主机上的多个端口。 一对一端口扫描具有如下特征： • 扫描主机的数量少 • 扫描单个主机 • 扫描的端口数量多 此选项检测 TCP、UDP 和 IP 端口扫描。
端口清扫	一对多端口清扫，在这种扫描中，攻击者使用一个或几个主机扫描多个目标主机上的单个端口。 端口清扫具有如下特征： • 扫描主机的数量少 • 扫描的主机数量多 • 扫描的唯一端口数量少 此选项检测 TCP、UDP、ICMP 和 IP 端口清扫。
诱骗端口扫描	一对一端口扫描，在这种攻击中，攻击者将伪造的源 IP 地址与真实的扫描 IP 地址混合在一起。 诱骗端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量少 • 扫描的主机为一个（或数量少） 诱骗端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。
分布式端口扫描	多对一端口扫描，在这种攻击中，多个主机查询单个主机是否有开放端口。 分布式端口扫描具有如下特征： • 扫描主机的数量多 • 一次扫描的端口数量多 • 扫描的主机为一个（或数量少） 分布式端口扫描选项检测 TCP、UDP 和 IP 协议端口扫描。

端口扫描检测器所了解的关于探针的信息主要是基于查看探测主机的否定响应。例如，当网络客户端尝试连接到网络服务器时，客户端会使用端口 80/tcp 且可以依靠服务器将该端口打开。但是，当攻击者探测服务器时，攻击者事先并不知道该服务器是否提供 Web 服务。当端口扫描检测器看到否定响应（即，无法到达 ICMP 或 TCP RST 数据包）时，它会将响应记录为潜在的端口扫描。当目标主机位于设备（例如，过滤否定响应的防火墙或路由器）的另一端，这个过程更难以执行。在这种情况下，端口扫描检测器可以根据选择的灵敏度级别生成已过滤端口扫描事件。

表 *189*: 灵敏度级别

Level	说明
低	只检测目标主机的否定响应。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描（慢速扫描、过滤扫描）。 此级别使用最短的时间周期进行端口扫描检测。
中等	根据主机的连接数量检测端口扫描，这意味着，可以检测过滤的端口扫描。但是，非常活跃的主机（例如网络地址转换器和代理）可能会生成误报。 请注意，可以将这些活跃主机的 IP 地址添加到 **Ignore Scanned** 字段以减少此类误报。 此级别使用较长的时间周期进行端口扫描检测。
高	根据时间周期侦测端口扫描，这意味着，可以检测基于时间的端口扫描。但是，如果使用此选项，应通过**忽略已扫描项 (Ignore Scanned)** 和**忽略扫描工具 (Ignore Scanner)** 字段中指定 IP 地址，随时间推移小心地调整检测器。 此级别使用更长的时间周期进行端口扫描检测。

端口扫描事件生成

当启用端口扫描检测时，必须启用生成器 ID (GID) 为 122 且 Snort ID (SID) 为 1 至 27 的规则，从而为每种启用的端口扫描类型生成事件。

注释 对于端口扫描连接检测器生成的事件，协议号设置为 255。由于默认情况下端口扫描没有特定协议与之关联，因此，互联网编号分配机构 (IANA) 未将协议号分配给它。IANA 指定 255 作为保留号码，因此，该号码用于端口扫描事件中以指明事件没有关联的协议。

表 *190*：端口扫描检测 *SID (GID 122)*

端口扫描类型	协议:	灵敏度级别	预处理器规则 **SID**
端口扫描检测	TCP UDP ICMP IP	低 中或高 低 中或高 低 中或高 低 中或高	1 5 17 21 不生成事件。 不生成事件。 9 13
端口清扫	TCP UDP ICMP IP	低 中或高 低 中或高 低 中或高 低 中或高	3, 27 7 19 23 25 26 11 15
诱骗端口扫描	TCP UDP ICMP IP	低 中或高 低 中或高 低 中或高 低 中或高	2 6 18 22 不生成事件。 不生成事件。 10 14

端口扫描类型	协议:	灵敏度级别	预处理器规则 SID
分布式端口扫描	TCP UDP ICMP IP	低 中或高 低 中或高 低 中或高 低 中或高	4 8 20 24 不生成事件。 不生成事件。 12 16

端口扫描事件数据包视图

启用随附的预处理器规则后，端口扫描检测器会生成入侵事件，可以像任何其他事件一样进行查看。但是，数据包视图上显示的信息不同于其他类型的入侵事件。

首先使用入侵事件视图钻取到端口扫描事件的数据包视图。请注意，不能下载端口扫描数据包，因为单个端口扫描事件是基于多个数据包；但是，端口扫描数据包视图提供了所有可用的数据包信息。

对于所有IP地址，可点击地址查看上下文菜单并选择**whois**以在IP地址上执行查找，或者选择**View Host Profile**以查看该主机的主机配置文件。

表 *191*：端口扫描数据包视图

信息	说明
设备	检测事件的设备。
Time	事件发生的时间。
消息	预处理器生成的事件消息。
源 IP	扫描主机的 IP 地址。
目标 IP	被扫描主机的 IP 地址。
Priority Count	被扫描主机发出的否定响应（例如，TCP RST 和 ICMP unreachable）的数量。否定响应的数量越多，优先级计数就越高。
Connection Count	主机上的活动连接数量。此值对于基于连接的扫描（例如 TCP 和 IP）而言更准确。

信息	说明
IP Count	与被扫描主机联系的 IP 地址变化的次数。例如，如果第一个 IP 地址是 10.1.1.1，第二个 IP 是 10.1.1.2，第三 IP 是 10.1.1.1，那么 IP 计数为 3。 此数字对于活跃的主机（例如代理和 DNS 服务器）而言不太准确。
Scanner/Scanned IP Range	被扫描主机或扫描主机的 IP 地址范围，具体取决于扫描类型。对于端口清扫，此字段显示被扫描主机的 IP 范围。对于端口扫描，此字段显示扫描主机的 IP 范围。
Port/Proto Count	对于 TCP 和 UDP 端口扫描，是指正被扫描的端口变化的次数。例如，如果扫描的第一个端口是 80，扫描的第二个端口是 8080，扫描的第三个端口又是 80，那么端口计数为 3。 对于 IP 协议端口扫描，是指正用于连接至被扫描主机的协议变化的次数。
Port/Proto Range	对于 TCP 和 UDP 端口扫描，是指被扫描端口的范围。 对于 IP 协议端口扫描，是指已用于尝试连接至扫描的主机的 IP 协议号的范围。
Open Ports	在被扫描主机上打开的 TCP 端口。此字段仅在端口扫描检测到一个或多个开放端口时显示。

配置端口扫描检测

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

端口扫描检测配置选项可用于精细调整端口扫描检测器如何报告扫描活动。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 单击“设置”。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**端口扫描检测 (Portscan Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**端口扫描检测 (Portscan Detection)** 旁边的编辑图标 ( )。

步骤 6 在**协议 (Protocol)** 字段中，指定要启用的协议。

注释 必须确保已启用 TCP 数据流处理以在 TCP 上检测扫描，并且确保已启用 UDP 流处理以在 UDP 上检测扫描。

步骤 7 在**扫描类型 (Scan Type)** 字段中，指定要检测的的端口扫描类型。

步骤 8 从**灵敏度级别 (Sensitivity Level)** 列表中选择级别；请参阅端口扫描类型、协议和过滤的灵敏度级别，第 1101 页。

步骤 9 如果要监控特定主机的端口扫描活动迹象，请在**监视 IP (Watch IP)** 字段中输入主机 IP 地址。
可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。将此字段留空则监视所有网络流量。

步骤 10 如果要忽略作为扫描工具的主机，请在**忽略扫描工具 (Ignore Scanners)** 字段中输入主机 IP 地址。
可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

步骤 11 如果要忽略作为扫描对象的主机，请在**忽略已扫描项 (Ignore Scanned)** 字段中输入主机 IP 地址。
可以指定单个 IP 地址或地址块，或者单个 IP 地址和/或地址块的逗号分隔列表。

提示 可使用**忽略扫描工具 (Ignore Scanners)** 和**忽略已扫描项 (Ignore Scanned)** 字段指示在网络上特别活跃的主机。可能需要随时间修改此主机列表。

步骤 12 如果要对中途恢复的会话中断监控，请清除**检测 Ack 扫描 (Detect Ack Scans)** 复选框。

注释 检测中途会话有助于识别 ACK 扫描，但可能会导致错误事件，特别是在含大流量和丢弃数据包的网络中。

步骤 13 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 如果要生成端口扫描入侵事件，请启用端口扫描检测规则 122:1 到 122:27。有关详细信息，请参阅入侵规则状态，第 832 页和端口扫描事件生成，第 1103 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

基于速率的攻击防御

基于速率的攻击是取决于连接频率或攻击实施重复次数的攻击。可以使用基于速率的检测标准检测发生的基于速率的攻击，采取应对措施，在攻击停止后返回到常规检测设置。

可以将网络分析策略配置为包括基于速率的过滤器，这种过滤器可检测针对网络中主机的过多活动。可以在内联模式下部署的受管设备上使用此功能，以在指定时间内阻止基于速率的攻击，然后恢复为仅生成事件而不丢弃流量。

SYN 攻击防御选项有助于保护网络主机免受 SYN 泛洪攻击。可以根据在一段时间内看到的数据包数量保护单个主机或整个网络。如果设备采用被动部署，可以生成事件。如果设备采用内联部署，还可以丢弃恶意数据包。超时周期结束后，如果速率条件已停止，将会停止事件生成和数据包丢弃。

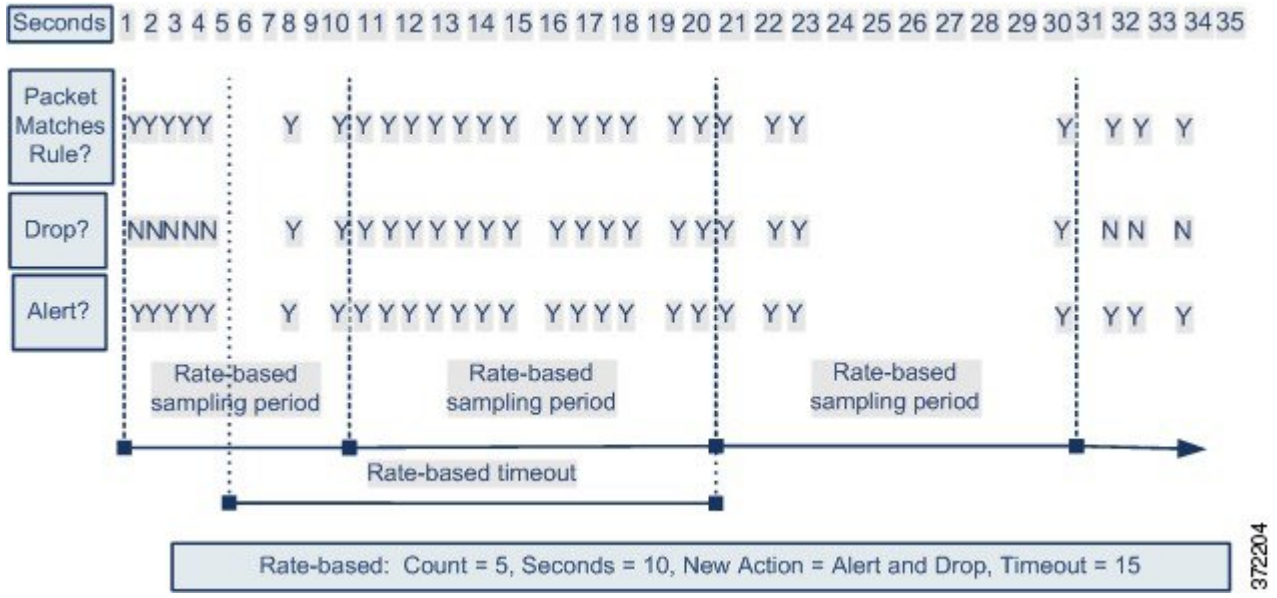
例如，可以配置一项设置以允许任一 IP 地址发出最多 10 个 SYN 数据包，并连续 60 秒阻止来自该 IP 地址的进一步连接。

可以限制与网路上主机之间的 TCP/IP 连接，以防止拒绝服务 (DoS) 攻击或用户进行过多活动。当系统检测到与指定 IP 地址成功连接的配置数量或地址范围时，它会对额外连接生成事件。基于速率的事件生成继续进行，直到超时周期结束且未发生速率条件。在内联部署中，可以选择丢弃数据包，直到速率条件超时。

例如，可以配置一项设置以允许任一 IP 地址发出最多 10 个成功的同步连接，并连续 60 秒阻止来自该 IP 地址的进一步连接。

下图显示的例子中，攻击者正在尝试访问主机。反复尝试查找密码触发了配置有基于速率的攻击防御的规则。当在 10 秒的时间跨度内发生五次规则匹配之后，基于速率的设置会将规则属性更改为 Drop and Generate Events。新的规则属性在 15 秒之后超时。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样速率高于当前或前一个采样周期的阈值，新操作将继续。只有在采样周期完毕而采样速率低于阈值速率之后，新操作才会恢复为生成事件。



基于速率的攻击防御示例

关键字 detection_filter、阈值和抑制功能提供了其他方式来过滤流量或系统生成的事件。可以单独使用基于速率的攻击防御，也可以将其与阈值、抑制功能或 detection_filter 关键字随意组合使用。

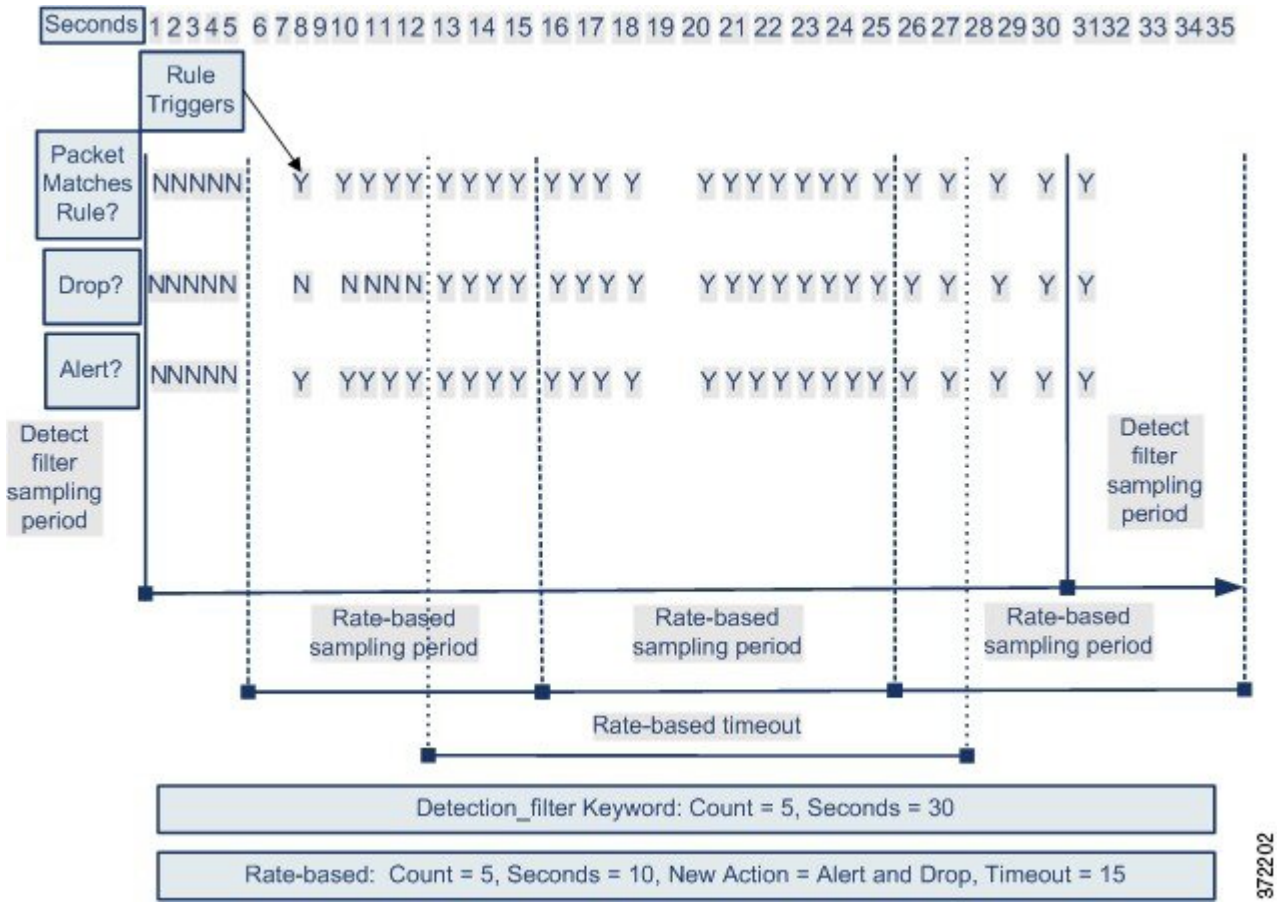
detection_filter 关键字、阈值或抑制以及基于速率的条件可能全都适用于同一流量。为规则启用抑制功能后，系统会为指定 IP 地址抑制事件，即使发生基于速率的变化。

detection_filter 关键字示例

以下示例显示了尝试强行登录的攻击者。重复尝试查找密码会触发还包含 detection_filter 关键字且计数设置为 5 的规则。此规则已配置基于速率的攻击防御。如果在 10 秒内出现五次规则匹配，基于速率的设置会将规则属性更改为 Drop and Generate Events 并保持 20 秒。

如图所示，与规则匹配的前五个数据包不会生成事件，因为在速率超过 detection_filter 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作 Drop and Generate Events。

如果符合基于速率的标准，将会生成事件并会丢弃数据包，直到基于速率的超时周期结束且速率低于阈值。20 秒之后，基于速率的操作超时。请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。由于采样的速率高于之前采样周期的阈值速率，因此发生超时时，基于速率的操作会继续。



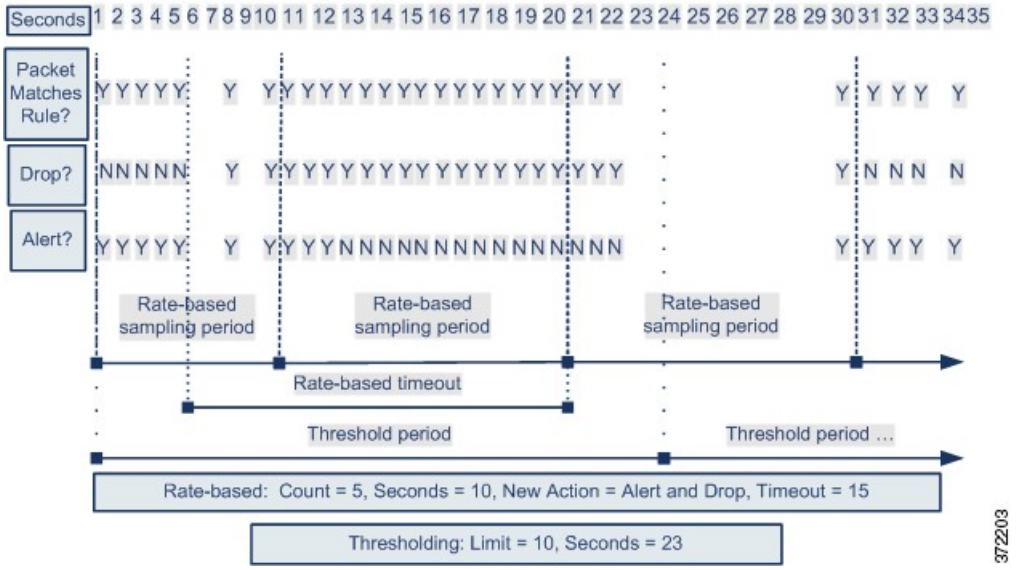
请注意，虽然示例未进行描述，但可以将 Drop and Generate Events 规则状态与 `detection_filter` 关键字结合使用，以在规则的匹配速率达到指定速率时开始丢弃流量。确定是否为规则配置基于速率的设置时，请考虑将规则设置为 Drop and Generate Events 和包含 `detection_filter` 关键字是否会获得相同的结果，或者是否要在入侵策略中管理速率和超时设置。

动态规则状态阈值或抑制示例

以下示例显示了尝试强行登录的攻击者。重复尝试查找密码会触发已配置基于速率的攻击防御的规则。如果在 10 秒内出现五次规则攻击，基于速率的设置会将规则属性更改为 Drop and Generate Events 并保持 15 秒。此外，极限阈值会在 23 秒内将规则可生成的事件数量限制为 10。

如图所示，规则为前五个匹配数据包生成事件。五个数据包之后，基于速率的标准会触发新操作 Drop and Generate Events，对于接下来的五个数据包，规则会生成事件且系统会丢弃数据包。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，新操作将会继续。新操作只会在采样周期结束后恢复生成事件，在此情况下采样的速率低于阈值速率。



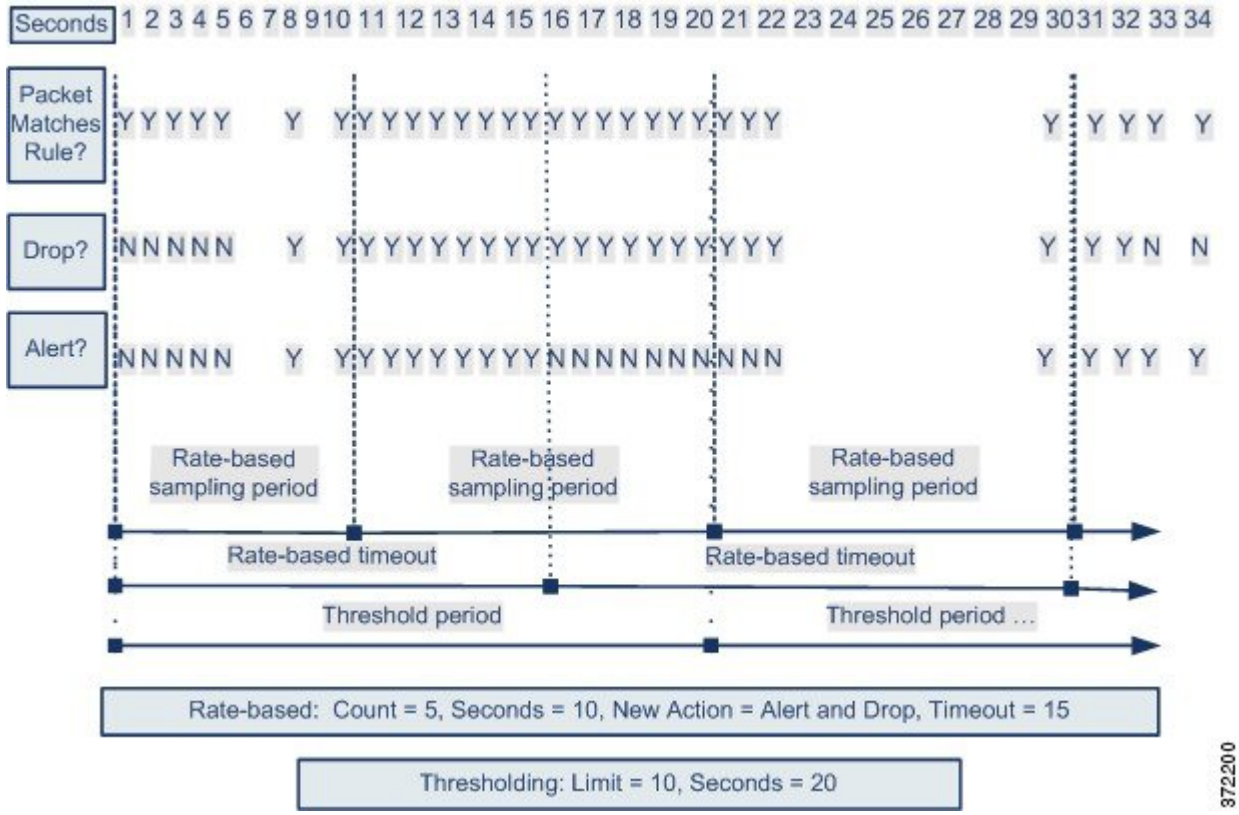
请注意，虽然本例中未显示，但如果在达到阈值后因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作从 Generate Events 更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

整个策略基于速率的检测和阈值或抑制示例

以下示例显示了尝试对网络中的主机进行拒绝服务 (DoS) 攻击的攻击者。许多来自相同源的同步主机连接会触发策略范围的 Control Simultaneous Connections 设置。如果在 10 秒内一个源有五个连接，设置会生成事件并丢弃恶意流量。此外，全局极限阈值会在 20 秒内将所有规则或设置可生成的事件数量限制为 10。

如图所示，策略范围的设置会为前十个匹配数据包生成事件并丢弃流量。第十个数据包之后，已达到极限阈值，因此，对于剩余的数据包，不会生成事件，但会丢弃数据包。

请注意，到达超时时间后，在接下来的基于速率的采样周期内，系统仍然丢弃数据包。如果采样的速率高于当前或之前采样周期的阈值速率，生成事件和丢弃流量这两种基于速率的操作将会继续。基于速率的操作只在采样周期结束后停止，在此情况下采样的速率低于阈值速率。



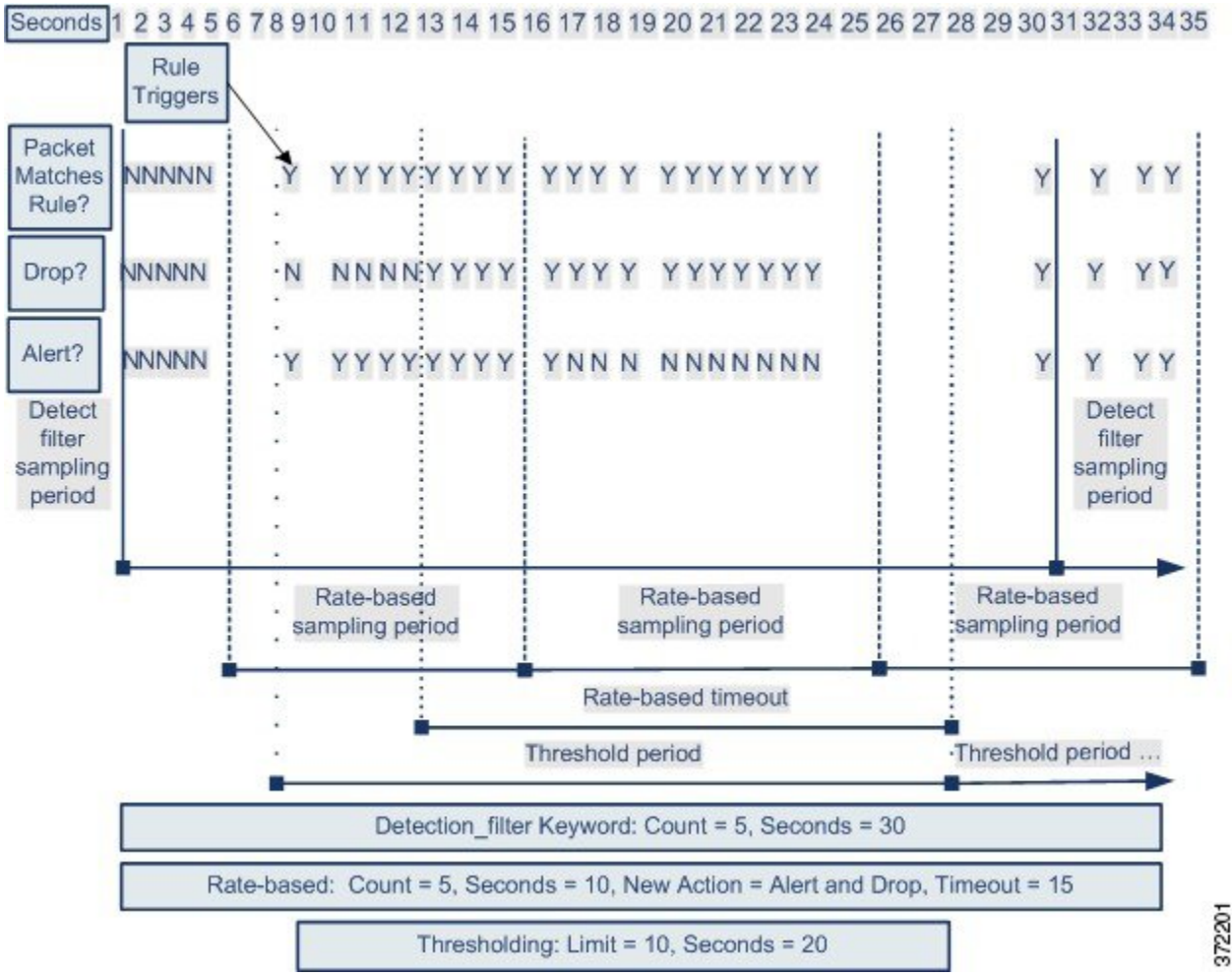
请注意，虽然本例中未显示，但如果在达到阈值后因基于速率的标准而触发新操作，系统会生成一个事件以指示操作变化。因此，例如，对于第 14 个数据包，如果达到极限阈值 10，系统停止生成事件且操作更改为 Drop and Generate Events，系统会生成第十一个事件以指示操作变化。

使用多种过滤方法进行基于速率的检测示例

以下示例显示了尝试强行登录的攻击者，并描述了 `detection_filter` 关键字、基于速率的过滤和阈值功能交互的情况。重复尝试查找密码会触发包括 `detection_filter` 关键字且计数设置为 5 的规则。此规则还具有基于速率的攻击防御设置，如果在 15 秒内出现五次规则匹配，该设置会将规则属性更改为 Drop and Generate Events 并保持 30 秒。此外，极限阈值会在 30 秒内将规则限为 10 个事件。

如图所示，与规则匹配的前五个数据包不会产生事件通知，因为在速率超过 `detection_filter` 关键字所指示的速率之前规则不会触发。规则触发后，事件通知开始，但基于速率的标准在再通过五个数据包之前不会触发新操作 Drop and Generate Events。如果符合基于速率的标准，系统会为数据包 11 至 15 生成事件并丢弃数据包。第十五个数据包之后，已达到极限阈值，因此，对于剩余的数据包，系统不会生成事件，但会丢弃数据包。

请注意，基于速率的超时后，数据包仍会在随后的基于速率的采样周期内丢弃。因为采样的速率高于之前采样周期的阈值速率，新操作将会继续。



基于速率的攻击防御选项和配置

基于速率的攻击防御可确定异常流量模式，并可将这些流量对合法请求的影响降至最低。基于速率的攻击通常具有以下其中一种特征：

- 任何包含与网络主机之间过多不完整连接的流量，表示 SYN 泛洪攻击
- 任何包含与网络主机之间过多完整连接的流量，表示 TCP/IP 泛洪攻击
- 在流向特定目标 IP 地址或来自特定源 IP 地址的流量中规则匹配过多。
- 所有流量中某个特定规则的匹配过多。

在网络分析策略中，您可以为整个策略配置 SYN 泛洪或 TCP/IP 连接泛洪检测；在入侵策略中，您可以为单独的入侵或预处理器规则设置基于速率的过滤器。请注意，不能手动将基于速率的过滤器添加到 GID 135 规则或修改其规则状态。GID 为 135 的规则使用客户端作为源值，使用服务器作为目标值。

启用 **SYN 攻击防御 (SYN Attack Prevention)** 选项还会激活规则 135:1。手动激活此规则是无效的。规则状态始终显示为 Disabled，不会改变。如果此选项已启用且超过定义的速率条件，规则会生成事件。

启用**控制同步连接 (Control Simultaneous Connections)** 选项还会激活规则 135:2 和 135:3。手动激活这些规则没有效果。规则状态始终显示为 Disabled，不会改变。当超过已定义的速率条件时，规则 135:2 规则生成事件。当会话关闭或超时时，规则 135:2 生成事件。

每个基于速率的过滤器都包含下列几个组成部分：

- 网络地址名称（适用于整个策略或基于规则的源或目标设置）
- 规则的匹配速率，配置为特定秒数内的规则匹配项数量
- 超过该速率时要执行的新操作

  为整个策略设置基于速率的设置时，系统会在其检测到基于速率的攻击时生成事件，并且可以在内联部署中丢弃流量。为具体规则设置基于速率的操作时，有三个可用的操作：Generate Events、Drop and Generate Event 和 Disable。
- 操作的持续时间，配置为超时值

请注意，新操作自开始之后，在到达超时时间之前会一直执行，即使速率在这段时间内降到配置的速率以下亦不会停止。当超时周期结束后，如果速率低于阈值，则规则的操作会恢复到最初为该规则配置的操作。对于策略范围的设置，操作会恢复到流量匹配的每个规则的操作；如果不匹配任何规则，操作会停止。

在内联部署中，可以将基于速率的攻击防御临时或永久配置为拦截攻击。在没有基于速率的配置的情况下，设置为 Generate Events 的规则会创建事件，但系统不会丢弃这些规则的数据包。但是，如果攻击流量所匹配的规则配置了基于速率的条件，则基于速率的操作可能会导致系统在该操作处于活动状态的时间内丢弃数据包，即便这些规则最初并未设置为 Drop and Generate Events。

注释 基于速率的操作无法启用禁用的规则，也无法丢弃与禁用的规则匹配的流量。但是，如果在策略级别设置基于速率的过滤器，则可以在指定时段内生成事件或生成事件并丢弃包含过多 SYN 数据包或 SYN/ACK 交互的流量。

可以对同一规则定义多个基于速率的过滤器。入侵策略中列出的第一个过滤器优先级最高。请注意，当两个基于速率的过滤器操作相冲突时，系统会实施第一个基于速率的过滤器的操作。同样，如果对整个策略设置的基于速率的过滤器与对具体规则设置的基于速率的过滤器相冲突，前者优先。

基于速率的攻击防御、检测过滤和阈值或抑制

关键字 `detection_filter` 可防止触发规则，直至在指定时间内出现规则匹配项的阈值数量为止。当规则包含 `detection_filter` 关键字时，系统会在每个超时周期跟踪传入数据包与规则中的模式相匹配的次数。系统可以从特定的源或目标 IP 地址计算该规则的匹配次数。速率超过规则中的速率后，会开始针对该规则的事件通知。

可以使用阈值和抑制来减少过多的事件，方法是限制规则、源或目标的事件通知数量或者抑制该规则的所有通知。您还可以配置适用于没有首要特定阈值的每个规则的全局规则阈值。

如果对规则应用抑制，则系统会为所有适用的IP地址抑制该规则的事件通知，即使由于策略范围或规则特定的基于速率的设置而发生基于速率的操作更改也如此。

配置基于速率的攻击防御

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以在策略级别配置基于速率的攻击防御以阻止SYN泛洪攻击，也可以阻止来自特定源或到达特定目标的过多连接。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**，然后点击**网络分析策略 (Network Analysis Policy)**。

注释　如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 单击“**设置**”。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**基于速率的攻击防御 (Rate-Based Attack Prevention)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**基于速率的攻击防御 (Rate-Based Attack Prevention)** 旁边的编辑图标 ( )。

步骤 6 您有两种选择：

- 要防止旨在对主机发起泛洪攻击的不完整连接，请点击 **SYN Attack Prevention** 下的 **Add**。
- 要防止过多连接，请点击 **Control Simultaneous Connections** 下的 **Add**。

步骤 7 指定要跟踪流量的方式：

- 要跟踪来自特定源或一系列源的所有流量，请从**跟踪方式(Track By)**下拉列表中选择**源 (Source)**，然后在**网络 (Network)** 字段中输入单个 IP 地址或地址块。
- 要跟踪到达特定目标或一系列目标的所有流量，请从**跟踪方式 (Track By)** 下拉列表中选择**目标 (Destination)**，然后在**网络 (Network)** 字段中输入单个 IP 地址或地址块。

注释 系统会单独跟踪**网络 (Network)** 字段中包含的每个 IP 地址的流量。来自超过所配置速率的 IP 地址的流量会带来仅为该 IP 地址生成的事件。例如，进行网络设置时，可将源 CIDR 块设置为 `10.1.0.0/16` 并将系统配置为在有十个同步连接打开时生成事件。如果 10.1.4.21 有八个连接打开，10.1.5.10 有六个连接打开，则系统不会生成事件，因为这两个源地址的打开连接均未达到触发数量。但是，如果 10.1.4.21 有十一个同步连接打开，系统只会为来自 10.1.4.21 的连接生成事件。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 8 指定速率跟踪设置的触发速率：

- 对于 SYN 攻击配置，在**速率 (Rate)** 字段中输入每个秒数的 SYN 数据包数量。
- 对于同步连接配置，在**计数 (Count)** 字段中输入连接数量。

步骤 9 要丢弃与基于速率的攻击防御设置匹配的数据包，请选中**丢弃 (Drop)** 复选框。

步骤 10 在**超时 (Timeout)** 字段中输入时间段，在该时间段结束后将会停止生成针对具有 SYN 的匹配模式或同步连接的流量的事件（如适用，丢弃）。

注意 设置较高的超时值可能会完全阻止连接到内联部署中的某个主机。

步骤 11 点击 **OK**。

步骤 12 要保存自上次策略确认以来在此策略中进行的更改，请点击**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 62 章

自适应配置文件

以下主题介绍如何配置自适应配置文件：

自适应配置文件基础知识

通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

自适应配置文件（就像可在网络分析策略中手动配置的基于目标的配置文件）有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

手动配置的基于目标的配置文件要么应用选择的默认操作系统配置文件，要么应用绑定到特定主机的配置文件。自适应配置文件但是，自适应配置文件会根据目标主机的主机配置文件中的操作系统切换到相应的操作系统配置文件。

假设您为 10.6.0.0/16 子网配置自适应配置文件，并将默认 IP 分片重组基于目标的策略设置为 Linux。配置设置的Firepower 管理中心中有一个包括 10.6.0.0/16 子网的网络映射。

- 当系统检测到来自主机 A（不在 10.6.0.0/16 子网中）的流量时，它使用基于 Linux 目标的策略重组 IP 分片。
- 当系统检测到来自主机 B（在 10.6.0.0/16 子网中）的流量时，它从网络映射检索主机 B 的操作系统数据。系统使用基于该操作系统的配置文件对传送到主机 B 的流量进行分片重组。

自适应配置文件和 Firepower 建议的规则

自适应配置文件功能是访问控制策略中的高级设置，全局应用于由该访问控制策略调用的所有入侵策略。Firepower 建议的规则功能适用于您在其中配置该功能的各个入侵策略。

与 Firepower 建议的规则一样，自适应配置文件将规则中的元数据与主机信息进行比较，确定是否应为某个特定主机应用规则。然而，虽然 Firepower 建议的规则为使用该信息的启用或禁用规则提供建议，但是自适应配置文件仍使用这些信息将特定规则应用于特定流量。

Firepower 建议的规则需要您的互动才能对规则状态执行建议的更改。另一方面，自适应配置文件不能修改入侵策略。规则自适应处理在逐包基础上进行。

此外，Firepower 建议的规则可能会启用已禁用的规则。相比之下，自适应配置文件仅影响在入侵策略中已启用的规则的应用。自适应配置文件永不改变规则状态。

您可以组合使用自适应配置文件和 Firepower 建议的规则。当部署入侵策略来确定是否纳入某条规则作为应用备选项时，自适应配置文件使用该规则的规则状态，您是选择接受还是拒绝建议均反映在该规则状态中。您可以同时使用这两个功能以确保您已启用或禁用每个监测网络中最合适的规则，然后应用对特定流量最为有效的已启用规则。

自适应配置文件选项

自适应配置文件 - 已启用

启用或禁用自适应配置文件

自适应配置文件 - 属性更新间隔

可以控制网络映射数据从 Firepower 管理中心同步到其受管设备的频率（以分钟为单位）。系统使用该数据确定处理流量时应使用哪些配置文件。增大此选项的值可提升大型网络的性能。

自适应配置文件 - 网络

或者，您可以通过将自适应配置文件限制在逗号分隔的 IP 地址、地址块和网络变量列表中来提高性能。如果使用网络变量，则系统会为您的访问控制策略使用与默认入侵策略相关联的变量集中的变量值。例如，可以输入：192.168.1.101, 192.168.4.0/24, $HOME_NET。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。如果启用并执行祖先策略中的自适应配置文件，则思科建议您保留默认网络限制 0.0.0.0/0，或使用网络变量值 `any`。此设置将自适应配置文件应用于所有子域中的所有受监控主机。

配置自适应配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

在被动部署中，思科建议您配置自适应配置文件。在内联部署中，请配置启用**规范化 TCP 负载 (Normalize TCP Payload)** 选项的内联规范化预处理器。

注意 启用或禁用自适应配置文件在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，然后点击“检测增强设置”(Detection Enhancement Settings) 部分旁的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明设置从祖先策略继承，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 如自适应配置文件选项，第 1118 页中所述，设置自适应配置文件。

步骤 3 点击 **OK**。

步骤 4 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 XVI 部分

发现和身份

第 63 章

网络发现和身份简介

以下主题介绍网络发现和身份策略与数据：

主机、应用和用户检测

Firepower 系统使用网络发现和身份策略收集网络上流量的主机、应用和用户数据。您可以使用特定类型的发现和身份数据构建全面的网络资产映射，执行调查分析、行为剖析和访问控制并缓解和应对组织最易遭受的漏洞和攻击。

主机和应用数据

主机和应用数据由主机身份源和应用检测器根据网络发现策略中的设置进行收集。受管设备会观察指定网段上的流量。系统确定：

- 网络中主机的数量和类型（包括网络设备）

  您可以使用所导出的 NetFlow 记录、Nmap 主动扫描和主机输入功能中的数据补充网络发现主机数据。

- 这些主机上的操作系统、活动应用和开放端口

有关详细信息，请参阅主机和应用检测基础知识，第 1125 页。

用户数据

用户数据由用户身份源根据网络发现和身份策略中的设置进行收集。

- 非授权基于流量的检测收集用户感知的用户数据。如果要配置受管设备以检测 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录，请参阅基于流量的检测身份源，第 1204 页。
- 授权用户代理报告收集用户感知和用户控制的用户数据。如果要配置用户代理对用户登录和注销主机或使用 Active Directory 凭证进行身份验证的情况进行监控，请参阅用户代理身份源，第 1199 页。
- 授权身份服务引擎 *(ISE)* 报告收集用户感知和用户控制的用户数据。如果您具有 ISE 部署并要配置 ISE 对用户使用 Active Directory 域控制器 (DC） 凭证进行身份验证的情况进行监控，请参阅身份服务引擎 (ISE) 身份源，第 1201 页。
- 授权强制网络门户身份验证主动验证网络上的用户并收集用户感知和用户控制的用户数据。如果要将虚拟路由器配置为执行强制网络门户主动身份验证，请参阅强制网络门户主动身份验证身份源，第 1203 页。

有关详细信息，请参阅用户检测基础知识，第 1130 页。

主机、应用和用户发现域身份数据的使用

通过记录发现和身份数据，您可以利用 Firepower 系统中的许多功能，包括：

- 查看网络映射（网络映射是对网络资产和拓扑的详细表示，可通过对主机和网络设备、主机属性、应用协议或漏洞进行分组来查看）
- 查看主机配置文件（配置文件可完整展示检测到的主机的所有可用信息）
- 查看控制面板（控制面板提供有关网络资产和用户活动的概览及其他功能）
- 查看关于系统记录的发现事件和用户活动的详细信息
- 根据发现数据创建报告
- 执行应用和用户控制，即，使用应用、领域、用户、用户组和 ISE 属性条件编写访问控制规则
- 将主机及其运行的任何服务器或客户端与它们容易受到的攻击关联，这样可识别和减少漏洞，评估入侵事件对网络的影响，以及调整入侵规则状态以使它们能够为网络资产提供最大程度的保护
- 在系统生成具有特定影响标志的入侵事件或特定类型的发现事件时，通过邮件、SNMP 陷阱或系统日志向您发出警报
- 监控组织是否遵守允许的操作系统、客户端、应用协议和协议的白名单
- 在系统生成发现事件或检测用户活动时，创建具有会触发和生成关联事件的规则的关联策略
- 如果记录 NetFlow 连接，使用这些连接数据

主机和应用检测基础知识

您可以配置网络发现策略，以执行主机和应用检测。

有关详细信息，请参阅概述：主机数据收集，第 1137 页和概述：应用检测，第 1177 页。

操作系统和主机数据被动检测

被动检测通过分析系统被动收集的流量对主机操作系统、客户端和应用信息进行检测。系统使用 VDB 中的信息来帮助识别网络资产。

如果系统无法识别主机上的操作系统，则可对其进行手动确定，然后创建自定义服务器或客户端指纹来帮助系统识别其他主机上有着类似操作系统特征的操作系统。

系统可使用为主机操作系统收集的所有被动指纹来创建派生指纹。系统通过应用公式来创建派生指纹，该公式使用每个收集的指纹的置信值和身份之间的证实指纹数据的数量来计算最有可能的身份。常见元素在标识之间进行识别

如果在网络上使用自定义应用，则可通过创建自定义应用检测器来扩充系统的应用检测功能，自定义应用检测器可向系统提供其识别这些应用所需的信息。来自 NetFlow 导出器的数据还可将被动检测到的应用信息添加到网络映射。

注释 系统不会使用分类为未知的应用协议和操作系统数据，因为其无法解释数据。受管设备会将该标识向Firepower 管理中心报告为未知，标识数据将不用于派生指纹。

操作系统和主机数据主动检测

主动检测会将主动源收集的主机信息添加到网络映射。例如，可使用 Nmap 扫描器仪主动扫描网络上的目标主机。Nmap 可发现主机上的操作系统和应用。

此外，主机输入功能可用于将主机输入数据主动添加到网络映射。有两种不同类别的主机输入数据：

- 用户输入数据 - 通过 FirePOWER 系统用户界面添加数据。您可以通过此界面修改主机操作系统或应用身份。
- 托管导入输入数据 - 使用命令行实用程序导入的数据。

系统将为每个主动源保留一个标识。如果运行 Nmap 扫描实例，例如，先前的扫描结果将替代为新的扫描结果。然而，如果运行 Nmap 扫描，然后用结果通过命令行导入的客户端的数据替代这些结果，系统将同时保留来自 Nmap 结果的标识以及来自导入客户端的标识。然后，系统会使用网络发现策略中设置的优先级来确定用作当前身份的主动身份。

请注意，用户输入视为一个源，即使其来自不同的源。例如，如果用户 A 通过主机配置文件设置操作系统，然后用户 B 通过主机配置文件更改该定义，用户 B 设置的定义将保留，而用户 A 设置的定义将丢弃。此外，请注意，用户输入会覆盖所有其他的主动源，并会用作当前标识（如果其存在）。

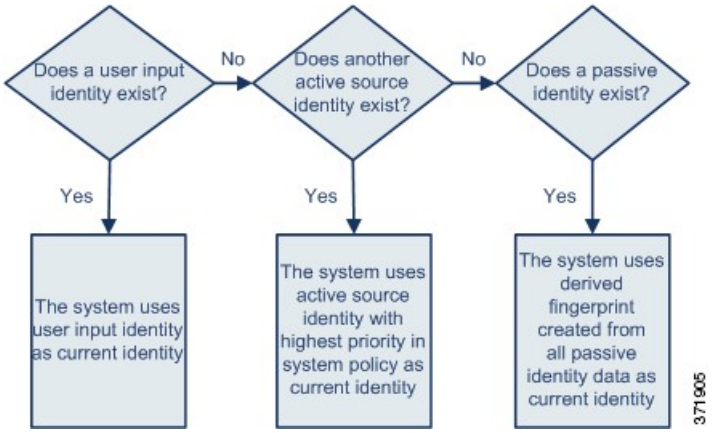
应用和操作系统的当前身份

主机上的应用或操作系统的当前身份是系统发现最有可能正确的身份。

系统会将操作系统或应用的当前标识用于以下用途：

- 分配漏洞至主机
- 影响评估
- 评估针对操作系统标识、主机配置文件合格性以及合规性白名单写入的相关性规则
- 在工作流程的“主机和服务器”表格视图中进行显示
- 在主机配置文件中进行显示
- 在 Discovery Statistics 页面上计算操作系统和应用统计

系统会使用源优先级来确定哪个主动标识应该用作应用或操作系统的当前标识。



例如，如果用户在主机上将操作系统设置为 Windows 2003 Server，则 Windows 2003 Server 为当前标识。针对该主机上的 Windows 2003 Server 漏洞的攻击将被赋予更高的影响，而主机配置文件中为该主机列出的漏洞包括 Windows 2003 Server 漏洞。

对于主机上的操作系统或特定应用，数据库可能保留来自多个源的信息。

如果数据的源拥有最高的源优先级，系统会将操作系统或应用标识视作当前标识。可能的源拥有以下的优先级顺序：

1. 用户

2. 扫描程序和应用（在网络发现策略中设置）

3. 受管设备

4.NetFlow 记录

如果优先级更高的新应用身份拥有的详细信息比当前身份少，则不会覆盖当前应用身份。

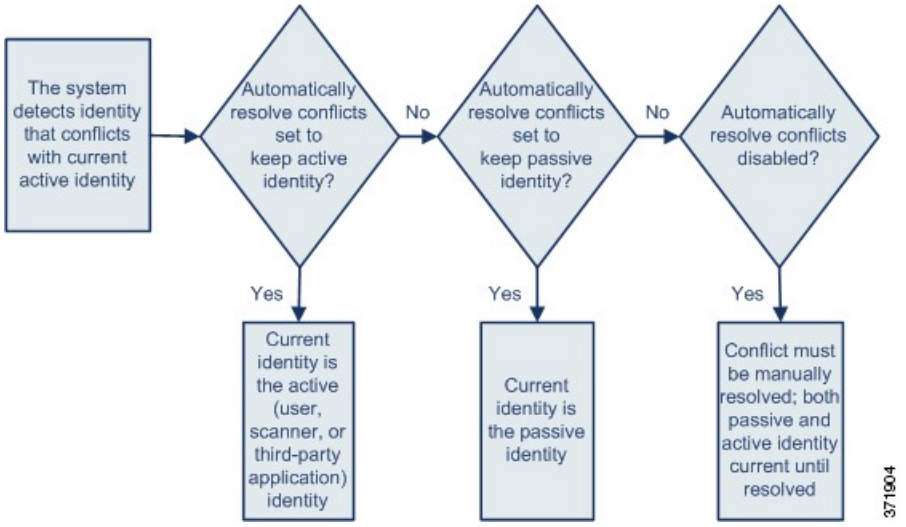
此外，如果出现身份冲突，冲突的解决取决于网络发现策略中的设置或者手动解决。

应用和操作系统的身份冲突

如果系统报告新的被动标识与当前主动标识和先前报告的被动标识冲突，就会发生标识冲突。例如，如将操作系统先前的被动标识报告为 Windows 2000，则主动标识 Windows XP 成为当前标识。接下来，系统检测到新的被动标识 Ubuntu Linux 8.04.1。标识 Windows XP 和 Ubuntu Linux 发生冲突。

如果主机的操作系统或主机上的某个应用存在标识冲突，系统会将两个冲突的标识均列为当前标识，并将二者用于影响评估，直到冲突解决。

有管理员权限的用户可自动解决标识冲突，只需选择始终使用被动标识或始终使用主动标识。除非禁用标识冲突的自动解决，否则标识冲突始终会自动解决。



有管理员权限的用户还可配置系统，从而在标识冲突发生时生成事件。然后，该用户可设置带有相关性规则的关联策略，规则将Nmap扫描用作相关性响应。如果事件发生，Nmap会扫描主机以获取经过更新的主机操作系统和应用数据。

Firepower 系统中的 Netflow 数据

NetFlow 是一款思科 IOS 应用，可以提供有关流经路由器的数据包的统计信息。它在思科网络设备上可用，还可以嵌入到 Juniper、FreeBSD 和 OpenBSD 设备中。

在网络设备上启用 NetFlow 时，设备（NetFlow 缓存）上的数据库会存储通过路由器的数据流的记录。数据流（在Firepower系统中称为连接）是使用特定端口、协议和应用协议表示源主机和目标主机之间的会话的数据包序列。可以将网络设备配置为导出此 NetFlow 数据。在本文档中，通过此方式配置的网络设备称为 *NetFlow* 导出器。

Firepower 系统受管设备可以配置为从 NetFlow 导出器收集记录，根据这些记录中的数据生成单向连接结束事件，最后将这些事件发送到Firepower管理中心以记录在连接事件数据库中。您还可以配置网络发现策略，以根据 NetFlow 连接中的信息将主机和应用协议信息添加到数据库。

可以使用这些发现和连接数据补充受管设备直接收集到的数据。这在让 NetFlow 导出器监控受管设备无法监控的网络时尤为有用。

使用 NetFlow 数据的要求

在配置 Firepower 系统以分析 NetFlow 数据之前，必须在计划使用的路由器或其他支持 NetFlow 的设备上启用 NetFlow 功能，并且配置设备以将 NetFlow 数据广播到连接了受管设备传感接口的目标网络。

Firepower 系统可以分析 NetFlow 版本 5 和 NetFlow 版本 9 记录。如果要将数据导出到 Firepower 系统，则 NetFlow 导出器**必须**使用这些版本之一。此外，系统还要求在已导出的 NetFlow 模板和记录中存在特定字段。如果 NetFlow 导出器使用的是可以自定义的版本 9，则**必须**确保已导出的模板和记录按任意顺序包含以下字段：

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

由于 Firepower 系统使用受管设备分析 NetFlow 数据，因此，部署必须至少包括一个可监控 NetFlow 导出器的受管设备。该受管设备上的至少一个传感接口必须连接到可以收集已导出的 NetFlow 数据的网络。由于受管设备上的感应接口通常不具有 IP 地址，因此系统不支持直接收集 NetFlow 记录。

请注意，在某些网络设备上可用的采样 NetFlow 功能只会收集有关经过设备的数据包子集的 NetFlow 统计信息。尽管启用此功能可以提高网络设备上的 CPU 利用率，但可能会影响收集以供 Firepower 系统分析的 NetFlow 数据。

NetFlow 和受管设备数据之间的差异

FirePOWER 系统不直接分析 NetFlow 数据代表的流量。相反，系统会将导出的 NetFlow 记录转换为连接日志以及主机和应用协议数据。

因此，转换后的 NetFlow 数据与受管设备直接收集到的发现数据和连接数据之间存在一些差异。在执行具有以下要求的分析时，应记住这些差异：

- 需要检测到的连接次数的统计信息
- 需要与操作系统及其他主机相关的信息（包括漏洞）
- 需要应用数据，包括客户端信息、网络应用信息以及供应商和版本服务器信息

- 需要知道连接中的主机哪个是发起方，哪个是响应方

网络发现策略与访问控制策略

可以使用网络发现策略中的规则来配置 NetFlow 数据收集（包括连接日志记录）。可以将这种数据收集与 Firepower 系统受管设备（根据访问控制规则进行配置）检测到的连接的连接日志记录进行比较。

连接事件的类型

由于 NetFlow 数据收集与网络而不是访问控制规则相关联，因此您不能非常精细地控制系统记录的 NetFlow 连接。

NetFlow 数据无法生成安全情报事件。

基于 NetFlow 的连接事件只能存储在连接事件数据库中；无法将这些事件发送到系统日志或 SNMP 陷阱服务器。

每个受监控会话生成的连接事件的数量

对于受管设备直接检测到的连接，可将访问控制规则配置为在连接开始和/或结束时记录双向连接事件。

相反，由于导出的 NetFlow 记录包含单向连接数据，因此系统会为其处理的每个 NetFlow 记录生成至少两个连接事件。这也意味着，对于基于 NetFlow 数据的每次连接，摘要的连接数会每次递增 2，从而提供网络上实际发生的快速增长的连接数量。

由于 NetFlow 导出器会以固定间隔输出记录（即使连接仍在继续），因此长期运行的会话可能会导致多个导出的记录，每个记录生成一个连接事件。例如，如果 NetFlow 导出器每 5 分钟导出一次，且特定连接持续 12 分钟，那么系统将会为该会话生成 6 个连接事件：

- 前 5 分钟生成一对事件
- 第二个 5 分钟生成一对事件
- 连接终止时生成最后一对事件

主机和操作系统数据

从 NetFlow 数据添加到网络映射的主机不具有操作系统、NetBIOS 或主机类型（主机与网络设备）信息。但是，可以使用主机输入功能手动设置主机的操作系统身份。

应用程序数据

对于受管设备直接检测到的连接，系统可以通过检查连接中的数据包来识别应用协议、客户端和网络应用。

系统处理 NetFlow 记录时，会使用 `/etc/sf/services` 中的端口关联来推断应用协议身份。但是，这些应用协议不包含供应商或供应商信息，而且连接日志不包含关于会话中使用的客户端或网络应用的信息。但是，可以使用主机输入功能手动提供这些信息。

请注意，简单端口关联意味着在非标准端口上运行的应用协议可能不会被识别或被错误识别。此外，如果不存在关联，系统会在连接日志中将应用协议标记为 unknown。

漏洞映射

系统无法将漏洞映射到 NetFlow 导出器监控的主机，除非使用主机输入功能手动设置主机操作系统的身份或应用协议身份。请注意，由于 NetFlow 连接中没有客户端信息，因此您无法将客户端漏洞与根据 NetFlow 数据创建的主机相关联。

连接中发起方和响应方信息

对于受管设备直接检测到的连接，系统可确定哪个主机是发起方（即，源），哪个主机是响应方（即，目标）。但是，NetFlow 数据不包含发起方或响应方信息。

当 Firepower 系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息：

- 如果使用的两个端口都不是公认端口，系统会将端口号较小的那个主机视为响应方。
- 如果只有一个主机在使用公认端口，系统会将该主机视为响应方。

为此，公认端口是编号为 1 到 1023 的任意端口，或包含受管设备上 /etc/sf/services 中应用协议信息的端口。

此外，对于由受管设备直接检测到的连接，系统会在对应的连接事件中记录两个字节计数：

- **发起方字节数 (Initiator Bytes)** 字段记录发送的字节数。
- **响应方字节数 (Responder Bytes)** 字段记录接收的字节数。

基于单向 NetFlow 记录的连接事件只包含一个字节计数（系统分配到**发起方字节数 [Initiator Bytes]** 或**响应方字节数 [Responder Bytes]**），具体取决于基于端口的算法。系统将另一个字段设置为 0。请注意，如果查看 NetFlow 记录的连接摘要（汇聚的连接数据），则这两个字段都可能会填充。

纯 NetFlow 连接事件字段

从 NetFlow 记录生成的连接事件中只存在少量字段；请参阅连接事件字段中的可用信息，第 1529 页。

用户检测基础知识

可以使用网络发现和身份策略监控网络上的用户活动，以便将威胁、终端和网络智能与用户身份信息关联起来。通过将网络行为、流量和事件直接与单个用户相关联，系统可帮助您识别策略违规、攻击或网络漏洞的来源。例如，您可以确定：

- 谁拥有作为影响程度为 Vulnerable（级别 1：红色）的入侵事件的目标的主机
- 谁发起了内部攻击或端口扫描
- 谁正在尝试对重要主机进行未经授权的访问
- 谁正在耗用异常大量的带宽

- 谁尚未应用关键操作系统更新
- 谁正在使用即时消息软件或 P2P 文件共享应用，而这样做是违反公司的 IT 策略的

借助这些信息，可以使用 Firepower 系统的其他功能降低风险，执行访问控制以及采取措施防止中断他人的活动。这些功能还可以大大改善审核控制并提高合规性。

在配置用户身份源以收集用户数据后，您可以执行用户感知和用户控制。

用户感知

能够查看和分析用户数据。有关详细信息，请参阅使用发现和身份工作流程，第 1648 页。

用户控制

能够配置用户控制规则条件，以根据从用户感知得出的结论监控、信任、阻止或允许网络流量中的用户或用户活动。有关详细信息，请参阅用户、领域和 ISE 属性条件（用户控制），第 286 页。

支持的用户身份源

可以获取授权身份源（在身份策略中配置）和非授权身份源（在网络发现策略中配置）的用户数据。

授权身份源

受信任的服务器已验证用户登录。您可以使用从授权登录获取的数据执行用户感知和用户控制。授权用户登录是从被动和主动身份验证中获取：

- 被动身份验证发生在用户通过外部服务器进行身份验证时。用户代理和 ISE 是 Firepower 系统支持的被动身份验证方法。
- 主动身份验证发生在用户通过 7000 或 8000 系列设备进行身份验证时。强制网络门户是 Firepower 系统唯一支持的主动身份验证方法。

非授权身份源

未知或不受信任的服务器已验证用户登录。基于流量的检测是 Firepower 系统唯一支持的未授权身份源。您可以使用从非授权登录获取的数据执行用户感知。

下表提供 Firepower 系统支持的用户身份源的简要概述。

用户身份源	策略	服务器要求	Source Type	身份验证类型	用户感知？	用户控制？	有关详细信息，请参阅.....
用户代理	身份识别	Microsoft Active Directory	授权登录	passive	是	是	用户代理身份源，第 1199 页

用户身份源	策略	服务器要求	Source Type	身份验证类型	用户感知?	用户控制?	有关详细信息，请参阅.....
ISE	身份识别	Microsoft Active Directory	授权登录	passive	是	是	身份服务引擎 (ISE) 身份源，第 1201 页
强制网络门户	身份识别	LDAP 或 Microsoft Active Directory	授权登录	active	是	是	强制网络门户主动身份验证身份源，第 1203 页
基于流量的检测	网络发现	n/a	非授权登录	n/a	是	否	基于流量的检测身份源，第 1204 页

当选择要部署的身份源时，请考虑以下事项：

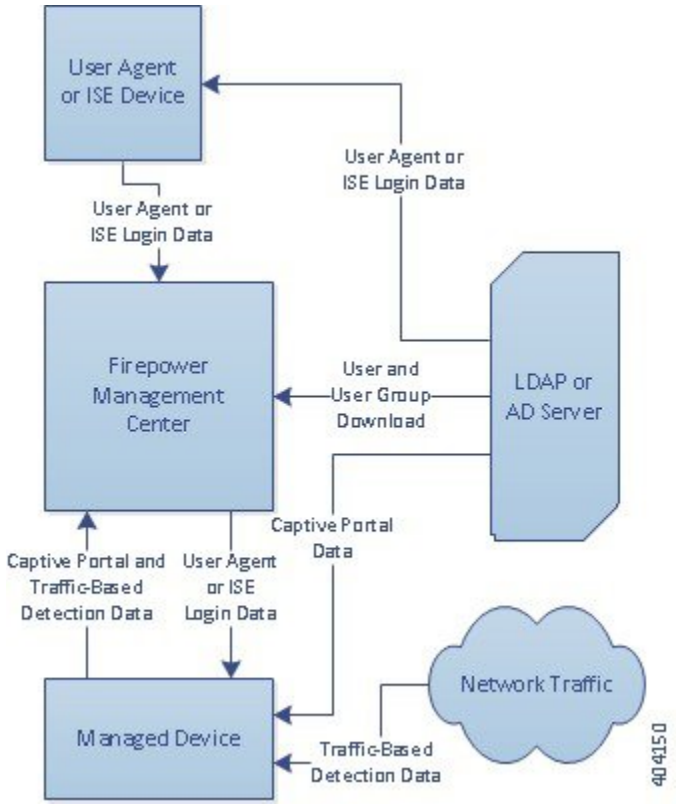
- 必须使用基于流量的检测来检测非 LDAP 用户登录。例如，如果仅使用安装在 Microsoft Active Directory 服务器上的用户代理检测用户活动，限制非 LDAP 登录将不起作用。
- 必须使用基于流量的检测或强制网络门户来记录失败的登录或身份验证活动。如果登录或身份验证尝试失败，则不会将新用户添加到数据库的用户列表中。
- 必须为传感接口（例如，虚拟路由器）部署具有 IP 地址的设备才能使用强制网络门户。

有关详细信息，请参阅概述：用户身份源，第 1197 页。

用户发现/用户身份部署

系统从任何身份源检测到用户登录的用户数据时，会将登录用户与 Firepower 管理中心用户数据库中的用户列表进行比对。如果登录用户与现有用户匹配，则登录数据将会分配给该用户。如果登录与现有用户不匹配，会导致创建新用户，除非登录是在 SMTP 流量中。SMTP 流量中不匹配的登录将被丢弃。

下图展示 Firepower 系统如何收集和存储用户数据。



用户活动数据库

Firepower管理中心上的用户活动数据库包含已配置的所有身份源检测或报告的网络上的用户活动记录。系统会在以下情况下记录事件：

- 系统检测到单独的登录或注销
- 系统检测到新用户
- 您手动删除用户
- 系统检测到不在数据库中的用户，但因已达到用户限制而无法添加该用户

可以使用Firepower 管理中心网络界面查看系统检测到的用户活动。

用户数据库

Firepower管理中心中的用户数据库包含所有已配置身份源检测或报告的每个用户的记录。通过授权来源获取的数据可用于用户控制。

以下是支持的身份源：

- 受管设备进行基于流量的非授权检测
- 用户代理进行授权报告

- ISE 进行授权报告
- 使用强制网络门户进行授权身份验证

Firepower 管理中心可存储的用户总数取决于 Firepower 管理中心模型。达到限制后，当系统检测到之前未检测到的新用户时，会根据其身份源确定用户数据的优先级：

- 如果新用户来自非授权身份源，则系统不会将该用户添加到数据库。要允许添加新用户，您必须手动或使用数据库清除删除用户。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新用户添加到数据库。

如果身份源配置为排除特定用户名，则这些用户名的用户活动数据将不会报告给 Firepower 管理中心。这些已排除的用户名仍保留在数据库中，但不与 IP 地址关联。有关系统存储的数据类型的详细信息，请参阅用户数据，第 1683 页。

如果您已配置 Firepower 管理中心高可用性且主要管理中心发生故障，则在故障切换期间，用户代理、ISE 或强制网络门户设备报告的所有登录均无法在 10 分钟的停机时间内进行识别，即使之前已发现用户并将其下载到 Firepower 管理中心也不例外。无法识别的用户在 Firepower 管理中心上记录为“未知”(Unknown) 用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

系统检测到新用户会话时，用户会话数据会保留在用户数据库中，直至出现以下其中一种情形：

- 某个 Firepower 管理中心用户从“用户”(Users) 表中手动删除用户会话。
- 某个身份源报告该用户会话的注销操作。
- 某个领域根据其**用户会话超时：通过身份验证的用户 (User Session Timeout: Authenticated Users)**、**用户会话超时：身份验证失败的用户 (User Session Timeout: Failed Authentication Users)** 或**用户会话超时：访客用户 (User Session Timeout: Guest Users)** 设置结束用户会话。

可以使用Firepower 管理中心网络界面查看用户数据库的内容。

当前用户身份

当系统检测到不同用户多次登录到同一主机时，系统会假设一次只有一个用户登录任何给定主机，且主机的当前用户是最后一次授权用户登录。如果只有非授权用户登录用户登录主机，则最后的非授权用户登录用户将被视为当前用户。如果有多个用户通过远程会话登录，则服务器报告的最后用户是报告给 Firepower 管理中心的用户。

当系统检测到同一用户多次登录到同一主机时，系统会记录用户在特定主机的首次登录并忽略后续的登录。如果单个用户是唯一登录到特定主机的人员，则系统唯一记录的登录为原始登录。

然而，如果另一用户登录到该主机，则系统会记录新的登录。如果原始用户再次登录，将会记录其新的登录。

Firepower 系统主机和用户限制

您的Firepower管理中心型号确定您可以通过部署监控的单独主机数量，以及可以您可以监控和用于执行用户控制的用户数。

Firepower 系统主机限制

当在监控网络中检测到与IP地址相关联的活动时，系统会将主机添加到网络映射，如网络发现策略中所定义。Firepower 管理中心可以监控因而存储在网络映射中的主机数取决于其型号。

表 *192*：按 *Firepower* 管理中心型号列出的主机限制

管理中心 型号	主机数
MC750	2000
MC1500	50,000
FS2000	150,000
MC3500	300,000
MC4000	600,000
虚拟打印机	50,000

您无法查看不在网络映射中的主机的情景数据。但是，您可以执行访问控制。例如，您可以对不在网络映射中的主机接收和发出的流量进行应用控制，即使您无法使用合规白名单监控主机的网络合规性。

注释 系统分别从IP地址和MAC地址识别的主机对仅MAC主机进行计数。与一台主机关联的所有IP地址均视为一台主机共同计数。

达到主机限制与删除主机

网络发现策略控制在您达到主机限制后检测到新主机时发生的情况；您可以丢弃新主机或替代非活动时间最长的主机。您也可以设置系统在主机处于非活动状态多长时间后将其从网络映射中删除的时间段。虽然您可以从网络映射中手动删除主机、整个子网或所有主机，但如果系统检测到与已删除主机相关的活动，它会重新添加该主机。

在多域部署中，每个枝叶域都有自己的网络发现策略。因此，当系统发现新主机时，每个枝叶域会管理自己的行为。

Firepower 系统用户限制

Firepower管理中心型号确定可监控的个人用户数量。当系统检测到新用户的活动时，会将该用户将添加到 Firepower 管理中心上的“用户”(Users) 数据库。可以使用用户代理、ISE、TS 代理、强制网络门户以及基于流量的检测来检测用户。

可考虑两种类型的用户限制：

- 授权用户限制，即可以存储在数据库中并用于访问控制的访问受控用户数。授权用户数据由用户代理、ISE、TS 代理和强制网络门户收集。
- 总用户限制，即可以存储在数据库中的授权和非授权用户数。此限制包括用户代理、ISE、TS 代理和强制网络门户，以及使用基于流量的检测收集的非授权用户数据。

表 *193*：按 *Firepower* 管理中心型号列出的用户限制

管理中心 型号	授权用户	用户总数
MC750	2000	2000
MC1500	50,000	50,000
FS2000	64,000	150,000
MC3500	64,000	300,000
MC4000	64,000	600,000
虚拟打印机	50,000	50,000

达到限制后，当系统检测到之前未检测到的新用户时，会根据其身份源确定用户数据的优先级：

- 如果新用户来自非授权身份源，则系统不会将该用户添加到数据库。要允许添加新用户，您必须手动或使用数据库清除删除用户。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新用户添加到数据库。

注释 如果部署包含通过 ASDM 管理的 ASA FirePOWER 模块，则无论 Firepower 管理中心型号如何，最多可以存储 2,000 个授权用户。

提示 请注意，如果使用的是基于流量的检测，则您可按协议限制客户日志记录，以最大程度低减少用户名干扰并保留数据库空间。例如，您可以防止系统添加在 AIM、POP3 和 IMAP 流量中发现的用户，因为您了解此流量来自您不想监控的特定承包商或访客。

第 64 章

主机身份源

以下主题提供有关主机身份源的信息：

概述：主机数据收集

由于 Firepower 系统被动监控流经网络的流量，因此，它会根据既定的定义（称为指纹）比较特定数据包报头值以及来自网络流量的其他唯一数据，以确定关于网络上主机的信息，包括：

- 主机的数量和类型（包括网络设备，例如网桥、路由器、负载均衡器和 NAT 设备）
- 基本网络拓扑数据（包括从网络上的发现点到主机之间的跳数）。
- 主机上运行的操作系统
- 主机上的应用以及与这些应用关联的用户

如果系统无法识别主机的操作系统，则您可以创建自定义客户端或服务器指纹。系统将会使用这些指纹来识别新主机。可以将指纹映射到漏洞数据库 (VDB) 中的系统，以便在使用自定义指纹识别主机时显示适当的漏洞信息。

注释 除从受监控网络流量中收集主机数据以外，系统还可以从导出的 NetFlow 记录收集主机数据，并且您可以使用 Nmap 扫描和主机输入功能主动添加主机数据。

Custom Fingerprinting

Firepower 系统包含系统用于识别其检测的每个主机上的操作系统的操作系统指纹。然而，有时系统会因为不存在与操作系统匹配的指纹而无法识别主机操作系统，或者错误地识别主机操作系统。要纠正此问题，可创建自定义指纹，指纹提供未知或识别错误的操作系统所独有的操作系统特征模式，以便提供用于标识的操作系统名称。

如果系统无法匹配主机操作系统，则无法识别主机漏洞，因为系统通过其操作系统指纹为每个主机派生漏洞列表。例如，如果系统检测到运行 Microsoft Windows 的主机，则表明系统存储了 Microsoft Windows 漏洞列表，其根据检测到的 Windows 操作系统将该列表添加至该主机的主机配置文件。

例如，如果网络上有多个运行新试用版 Microsoft Windows 的设备，则系统无法确定操作系统，或无法将漏洞映射到主机。然而，知道系统拥有 Microsoft Windows 的漏洞列表，您可能想要为某个主机创建自定义指纹，以帮助识别运行相同操作系统的其他主机。可将 Microsoft Windows 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

创建自定义指纹时，Firepower 管理中心将为运行相同操作系统的任何主机列出与该指纹关联的漏洞集。如果创建的自定义指纹没有任何漏洞映射，则系统将使用该指纹来分配在其中提供的自定义操作系统信息。当系统看到之前检测的主机发出的新流量时，系统用新指纹信息更新主机。首次检测到使用该操作系统的任何新主机时，系统还会使用新的指纹来识别这些主机。

在创建自定义指纹前，应确定主机未被正确识别的原因，从而确定自定义指纹是否为可行的解决方案。

可使用系统创建两种类型的指纹：

- 客户端指纹，这种指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。
- 服务器指纹，这种指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。

注释 如果客户端和服务器指纹均与相同的主机匹配，将会使用客户端指纹。

创建指纹后，必须先将其激活，然后系统才可以将其与主机关联。

管理指纹

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

指纹创建和激活后，可编辑指纹以便做出更改或添加漏洞映射。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。如果系统正在等待数据以便创建指纹，将会每 10 秒自动刷新页面，直到指纹已创建。

步骤 3 管理自定义指纹：

- 激活/停用 - 激活或停用指纹，如激活和停用指纹，第 1139 页中所述。
- 创建 - 创建指纹，如指纹识别客户端，第 1141 页和指纹识别服务器，第 1143 页中所述。
- 编辑 - 编辑指纹，如编辑活动指纹，第 1140 页和编辑非活动指纹，第 1140 页中所述。
- 删除 - 点击要删除的指纹旁边的删除图标 ( )，并点击**确定 (OK)** 以进行确认。只能删除已停用的指纹。

激活和停用指纹

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

必须先激活自定义指纹，然后系统才能将其用于识别主机。新指纹激活后，系统会将其用于重新识别先前发现的主机并发现新的主机。

如果想要停止使用指纹，可将其停用。停用指纹后，其就不再可用，但仍保留其在系统上。停用指纹后，对于使用该指纹的主机，操作系统被标记为未知。如果再次检测到这些主机，并且这些主机与不同的活动指纹匹配，则该活动指纹将对其进行识别。

删除指纹会将其从系统中完全删除。停用指纹后，即可将其删除。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击要激活或停用的指纹旁边的滑块。

注释 激活选项仅当创建的指纹有效时才可用。如果滑块不可用，请尝试再次创建指纹。

编辑活动指纹

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

如果指纹处于活动状态，可修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

可以修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**

步骤 3 点击想要编辑的指纹旁的编辑图标 ( )。

步骤 4 必要时修改指纹名称、描述和自定义操作系统显示。

步骤 5 如果要删除漏洞映射，请点击页面的**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 部分中映射旁边的**删除 (Delete)**。

步骤 6 如果要为漏洞映射添加额外的操作系统，请选择**产品 (Product)**，且在适用的情况下，选择**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)**，然后点击**添加操作系统定义 (Add OS Definition)**。
漏洞映射会添加到**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 列表。

步骤 7 点击**保存 (Save)**。

编辑非活动指纹

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

如果指纹处于非活动状态，可修改指纹的所有元素，并将其重新提交至Firepower管理中心。这包括创建指纹时指定的所有属性，如指纹类型、目标IP地址与端口、漏洞映射等。编辑非活动指纹并将其提交时，会将它重新提交至系统，如果指纹是客户端指纹，必须先将流量重新发送至设备，然后才可以将其激活。请注意，对于非活动指纹，仅可选择单一漏洞映射。激活指纹后，可将额外的操作系统和版本映射至其漏洞列表。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击想要编辑的指纹旁的编辑图标 ( )。

步骤 4 请在必要时更改指纹：

- 如果要修改客户端指纹，请参阅指纹识别客户端，第 1141 页。
- 如果要修改服务器指纹，请参阅指纹识别服务器，第 1143 页。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 如已修改客户端指纹，切记将流量从主机发送至收集指纹的设备。

指纹识别客户端

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

客户端指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。

如果Firepower管理中心不与受监控的主机直接联系，指定客户端指纹属性时，可以指定管理中心管理的离想要为其设置指纹的主机最近的设备。

开始指纹设置流程之前，获取想要为其设置指纹的主机的以下相关信息：

- 主机与Firepower管理中心或用于获取指纹的设备之间的网络跳数。（思科强烈建议将Firepower管理中心或设备直接连接到与主机所连接到的同一子网）。
- 连接至主机所在网络的（Firepower 管理中心或设备上的）网络接口。
- 主机的实际的操作系统供应商、产品和版本。
- 访问主机以便生成客户端流量。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。

在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 从**设备 (Device)** 下拉列表中，选择要用于收集指纹的 Firepower 管理中心或设备。

步骤 4 输入**指纹名称 (Fingerprint Name)**。

步骤 5 输入**指纹说明 (Fingerprint Description)**。

步骤 6 从**指纹类型 (Fingerprint Type)** 列表中，选择**客户端 (Client)**。

步骤 7 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。
请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

步骤 8 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意 此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 9 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意 由于多个原因，思科建议**不要**将受管设备上的传感接口用于设置指纹。首选，如果传感接口位于镜像端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。然而，可使用管理接口或任何其他可用接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 10 如果要在设置指纹的主机的主机配置文件中显示自定义信息（或者如果要设置指纹的主机不在**操作系统漏洞映射 [OS Vulnerability Mappings]** 部分中），请选择**使用自定义操作系统显示 (Use Custom OS Display)**，并对于以下各项提供要显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 11 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。
如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定**供应商 (Vendor)** 和**产品 (Product)** 值。

要为所有版本的操作系统映射漏洞，请仅指定**供应商 (Vendor)** 和**产品 (Product)** 值。

注释 并非 **Major Version**、**Minor Version**、**Revision Version**、**Build**、**Patch** 和 **Extension** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为主要版本。

示例：
要添加所有版本的 Palm 操作系统，请从 **供应商 (Vendor)** 列表中选择 **PalmSource, Inc.**，从**产品 (Product)** 列表中选择 **Palm 操作系统 (Palm OS)**，并让所有其他列表保持其默认设置。

步骤 12 点击**创建**。
状态会短暂显示 `New`，然后切换至 `Pending`，此状态会保持不变，直到发现匹配指纹的流量。发现流量后，状态会切换至`就绪 (Ready)`。

“自定义指纹”(Custom Fingerprint) 状态页面每隔 10 秒进行刷新，直到其收到来自所述主机的数据。

步骤 13 将指定的 IP 地址用作目标 IP 地址，访问您尝试为其设置指纹的主机，并发起至设备的 TCP 连接。要创建准确的指纹，收集指纹的设备**必须**发现流量。如果通过交换机进行连接，系统可能不会发现流向系统而不是设备的流量。

示例：
从要为其设置指纹的主机访问 Firepower 管理中心的 Web 界面，或者从主机使用 SSH 登录管理中心。如果使用的是 SSH，请使用以下命令，其中，localIPv6address 是在步骤 7 中指定的当前已分配到主机的 IPv6 地址，DCmanagementIPv6address 是管理中心的管理 IPv6 地址。然后，Custom Fingerprint 页面重新加载，其状态为“就绪”。

```
ssh -b localIPv6address DCmanagementIPv6address
```

接下来的操作

- 激活指纹，如激活和停用指纹，第 1139 页中所述。

指纹识别服务器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

服务器指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。在开始之前，应获取关于想要为其设置指纹的主机的以下信息：

- 主机与用于获取指纹的设备之间的网络跳数。思科强烈建议将设备上不使用的接口直接连接到主机所连接到的相同子网。
- 连接至主机所在网络的（设备上的）网络接口。
- 主机的实际的操作系统供应商、产品和版本。
- 未在使用的 IP 地址，并在主机所在网络上得到授权。

提示 如果Firepower 管理中心不与受监控的主机直接联系，指定服务器指纹属性时，可以指定离想要为其设置指纹的主机最近的受管设备。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 从**设备 (Device)** 列表中，选择要用于收集指纹的 Firepower 管理中心或受管设备。

步骤 4 输入**指纹名称 (Fingerprint Name)**。

步骤 5 输入**指纹说明 (Fingerprint Description)**。

步骤 6 从**指纹类型 (Fingerprint Type)** 列表中，选择**服务器 (Server)** 以显示服务器指纹选项。

步骤 7 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。
请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

注意 只可以使用运行 5.2 及更高版本的 Firepower 系统的设备捕获 IPv6 指纹。

步骤 8 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意 此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 9 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意 由于多个原因，思科建议**不要**将受管设备上的传感接口用于设置指纹。首选，如果传感接口位于镜像端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。然而，可使用管理接口或任何其他可用接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 10 点击 **Get Active Ports**。

步骤 11 在**服务器端口 (Server Port)** 字段中，输入想要设备选择用于收集指纹以便向其发起联系的端口，或者从**获取活动端口 (Get Active Ports)** 下拉列表选择端口。
可使用主机上已知开放的任何服务器端口（例如，80，如果主机正在运行网络服务器）。

步骤 12 在**源 IP 地址 (Source IP Address)** 字段中，输入应用于尝试与主机通信的 IP 地址。
应使用经授权可在网络上使用，但目前未在使用的源 IP 地址，例如，当前未在使用的 DHCP 池地址。创建指纹时，这可防止临时访问另一离线主机。

创建指纹时，应从网络发现策略的监控中排除该IP地址。否则，网络映射和发现事件视图中将会出现大量关于该 IP 地址代表的主机的不准确信息。

步骤 13 在**源子网掩码 (Source Subnet Mask)** 字段中，输入正在使用的 IP 地址的子网掩码。

步骤 14 如果 **Source Gateway** 字段显示，输入应用于建立至主机的路由的默认网关 IP 地址。

步骤 15 如果要在设置指纹的主机的主机配置文件中显示自定义信息，或者如果要使用的指纹名称在“操作系统定义”(OS Definition) 部分中不存在，则可以在“自定义操作系统显示”(Custom OS Display) 部分中选择**使用自定义操作系统显示 (Use Custom OS Display)**。
对于以下项提供想要在主机配置文件中显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 16 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。
如果想要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，必须在此部分指定供应商和产品名称。

要为所有版本的操作系统映射漏洞，请仅指定供应商和产品名称。

注释 并非 **Major Version**、**Minor Version**、**Revision Version**、**Build**、**Patch** 和 **Extension** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：
如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

示例：
要添加所有版本的 Palm 操作系统，请从 **供应商 (Vendor)** 列表中选择 **PalmSource, Inc.**，从**产品 (Product)** 列表中选择 **Palm 操作系统 (Palm OS)**，并让所有其他列表保持其默认设置。

步骤 17 点击**创建**。
“自定义指纹”(Custom Fingerprint) 状态页面每 10 秒刷新一次并应以“就绪”状态重新加载。

注释 如果目标系统在设置指纹的过程中停止响应，状态将会显示 `ERROR: No Response` 消息。如果看到此消息，请再次提交指纹。等待 3 至 5 分钟（时长可能因目标系统而异），点击编辑图标 () 访问 Custom Fingerprint 页面，然后点击 **Create**。

接下来的操作

- 激活指纹，如激活和停用指纹，第 1139 页中所述。

主机输入数据

您可以通过从第三方导入网络映射数据来扩充网络映射。还可使用主机输入功能，只需使用网络界面修改操作系统或应用标识，或删除应用协议、协议、主机属性或客户端。

系统可协调来自多个源的数据，以确定操作系统或应用的当前标识。

从网络映射中删除受影响的主机后，将会丢弃除第三方漏洞之外的所有数据。有关设置脚本或导入文件的详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

要将已导入数据纳入影响关联中，必须将数据映射至数据库中的操作系统和应用定义。

第三方数据使用要求

可以从网络上的第三方系统导入发现数据。但是，要启用将入侵和发现数据结合使用的功能（例如Firepower建议、自适应配置文件或影响评估），应将其中尽可能多的元素映射到对应的定义。考虑对使用第三方数据的以下要求：

- 如果拥有在您的网络资产上有特定数据的第三方系统，则可使用主机输入功能导入该数据。但是，由于第三方可能会以不同的方式命名产品，因此必须将第三方供应商、产品和版本映射到对应的思科产品定义。映射产品后，必须在 Firepower 管理中心配置中为影响评估启用漏洞映射，以允许影响关联。对于无版本或无供应商的应用协议，需要在 Firepower 管理中心配置中映射应用协议的漏洞。
- 如果导入来自第三方的修补程序信息，并想要将修补程序修补的所有漏洞标记为无效，则必须将第三方修补程序的名称映射至数据库中的定义。修补程序针对的所有漏洞随后会从添加该修补程序所在的主机中移除。
- 如果导入来自第三方的操作系统和应用协议漏洞，并想将其用于影响关联，则必须将第三方漏洞标识字符串映射至数据库中的漏洞。请注意，尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。映射漏洞后，必须在 Firepower 管理中心配置中为影响评估启用第三方漏洞映射。要使没有供应商或版本信息的应用协议映射到漏洞，管理用户还必须在 Firepower 管理中心配置中映射应用的漏洞。
- 如果导入应用数据并要将该数据用于影响关联，则必须将每个应用协议的供应商字符串映射到对应的应用协议定义。

第三方产品映射

如果通过用户输入功能将第三方数据添加至网络映射，则必须将第三方使用的供应商、产品和版本名称映射到思科产品定义。将产品映射到思科定义后，将根据这些定义分配漏洞。

类似地，如果正在导入第三方修补程序信息，如修补程序管理产品，则必须将修补程序的名称映射至适当供应商和产品以及数据库中的相应修补程序。

映射第三方产品

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果从第三方导入数据，则必须将思科产品映射到第三方名称，以分配漏洞并使用该数据执行影响关联。映射产品可以将思科漏洞信息与第三方产品名称关联，这样，系统就可使用该数据执行影响关联。

如果使用主机输入导入功能导入数据，还可以在导入过程中，使用 AddScanResult 函数将第三方产品映射至操作系统和应用漏洞。

例如，如果从将 Apache Tomcat 列为应用的第三方导入数据，并且知道它是该产品的第 6 版，则可以添加第三方映射，其中：

- **供应商名称 (Vendor Name)** 设置为 `Apache`。
- **产品名称 (Product Name)** 设置为 `Tomcat`。
- **Apache** 是从**供应商 (Vendor)** 下拉列表中选择。
- **Tomcat** 是从**产品 (Product)** 下拉列表中选择。
- **6** 是从**版本 (Version)** 下拉列表中选择。

该映射会使 Apache Tomcat 6 的任何漏洞分配到其应用列出了 Apache Tomcat 的主机。

请注意，对于无版本或无供应商的应用，必须在Firepower管理中心配置中为应用类型映射漏洞。尽管许多客户端具有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。

提示 如已在另一Firepower管理中心上创建了第三方映射，则将其导出后可导入至此管理中心。然后，可根据自己的需求编辑已导入的映射

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。

- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的编辑图标 ()。如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加产品映射 (Add Product Map)**。
- 编辑 - 要编辑现有第三方产品映射集，请点击要修改的映射集旁边的编辑图标 ()。如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 输入第三方产品使用的**供应商字符串 (Vendor String)**。

步骤 8 输入第三方产品使用的**产品字符串 (Product String)**。

步骤 9 输入第三方产品使用的**版本字符串 (Version String)**。

步骤 10 在“产品映射”(Product Mappings) 部分中，从以下字段为漏洞映射选择要使用的操作系统、产品和版本：**供应商 (Vendor)**、**产品 (Product)**、**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)**。

示例：
如果要运行其名称包含第三方字符串的产品的主机使用 Red Hat Linux 9 的漏洞，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 11 点击**保存 (Save)**。

映射第三方产品修补程序

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果将修补程序名称映射至数据库中的特定修补程序集，则可从第三方修补程序管理应用中导入数据，并将修补程序应用至主机集。修补程序名称导入至主机后，对于该主机，系统会将修补程序针对的所有漏洞标记为无效。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的编辑图标 ( )。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加修补程序映射 (Add Fix Map)**。
- 编辑 - 要编辑现有第三方产品映射，请点击映射旁边的编辑图标 ( )。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 在**第三方修补程序名称 (Third-Party Fix Name)** 字段中，输入要映射的修补程序的名称。

步骤 8 在**产品映射 (Product Mappings)** 部分中，从以下字段为修补程序映射选择要使用的操作系统、产品和版本：

- **Vendor**
- **Product**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **构建**
- **修补**
- **分机**

示例：
如果想要映射将 Red Hat Linux 9 的修补程序分配到应用补丁的主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 9 点击 **Save**，以保存修补程序映射。

映射第三方漏洞

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

要将第三方的漏洞信息添加至VDB，必须将每个导入的漏洞的第三方标识字符串映射至任何现有的SVID、Bugtraq或SID。为漏洞创建映射之后，该映射适用于已导入网络映射中主机的所有漏洞，且可为这些漏洞执行影响关联。

必须为第三方漏洞启用影响关联，才能允许关联发生。对于无版本或无供应商的应用，还必须在Firepower 管理中心配置中为应用类型映射漏洞。

尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能将第三方客户端漏洞用于影响评估。

提示 如已在另一Firepower管理中心上创建了第三方映射，则将其导出后可导入至此管理中心。然后，可根据自己的需求编辑已导入的映射

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新漏洞集，请点击**创建漏洞映射集 (Create Vulnerability Map Set)**。
- 编辑 - 要编辑现有漏洞集，请点击漏洞集旁边的编辑图标 ( )。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击 **Add Vulnerability Map**。

步骤 5 在**漏洞 ID (Vulnerability ID)** 字段中输入第三方漏洞标识。

步骤 6 输入**漏洞说明 (Vulnerability Description)**。

步骤 7 或者：

- 在 **Snort 漏洞 ID 映射 (Snort Vulnerability ID Mappings)** 字段中输入 Snort ID。
- 在 **SVID 映射 (SVID Mappings)** 字段中输入旧版漏洞 ID。
- 在 **Bugtraq 漏洞 ID 映射 (Bugtraq Vulnerability ID Mappings)** 字段中输入 Bugtraq 标识号。

步骤 8 点击 **Add**。

Custom Product Mappings

可以使用产品映射来确保由第三方输入的服务器与适当的思科定义相关联。定义并激活产品映射后，具有映射供应商字符串的受监控主机上的所有服务器或客户端都使用自定义产品映射。为此，您可能想要为网络中带有特定供应商字符串的服务器映射漏洞，而不是显式地为服务器设置供应商、产品和版本。

创建自定义产品映射

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果系统无法将服务器映射到VDB中的供应商和产品，您可以手动创建映射。激活自定义产品映射后，系统会将指定供应商和产品的漏洞映射到出现该供应商字符串的网络映射中的所有服务器。

注释 自定义产品映射将应用于所有出现应用协议的位置，无论应用数据的源为何（如 Nmap、主机输入功能或 Firepower 系统自身）。然而，如果使用主机输入功能导入的数据的第三方漏洞映射与通过自定义产品映射设置的映射发行冲突，则输入出现时，第三方漏洞映射将覆盖自定义产品映射并使用第三方漏洞映射设置。

可创建产品映射列表，然后通过激活或停用每份列表而一次性启用或禁用多个映射。指定将要映射到的供应商后，系统将更新产品列表，以仅包含该供应商提供的产品。

创建自定义产品映射后，必须激活自定义产品映射列表。激活自定义产品映射列表后，系统将更新出现指定供应商字符串的所有服务器。对于通过主机输入功能导入的数据，漏洞将更新，除非已为此服务器显式设置产品映射。

例如，如果贵公司将您的 Apache Tomcat Web 服务器的横幅修改为 `Internal Web Server`，则可将供应商字符串 `Internal Web Server` 映射到供应商 **Apache** 和产品 **Tomcat**，然后激活包含该映射的列表，出现标有 `Internal Web Server` 的服务器的所有主机均拥有数据库中的 Apache Tomcat 漏洞。

提示 可使用此功能将漏洞映至至本地入侵规则，只需将规则的 SID 映射至另一漏洞。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**

步骤 3 点击 **Create Custom Product Mapping List**。

步骤 4 输入**自定义产品映射列表名称 (Custom Product Mapping List Name)**。

步骤 5 点击**添加供应商字符串 (Add Vendor String)**。

步骤 6 在**供应商字符串 (Vendor String)** 字段中，输入供应商字符串，该字符串标识应映射到所选供应商和产品值的应用。

步骤 7 从**供应商 (Vendor)** 下拉列表，选择要映射的供应商。

步骤 8 从**产品 (Product)** 下拉列表，选择要映射的产品。

步骤 9 点击**添加 (Add)**，以将已映射的供应商字符串添加到列表。

步骤 10 或者，在必要时，重复第 4 至 8 步，将额外的供应商字符串映射添加至列表。

步骤 11 点击**保存 (Save)**。

接下来的操作

- 激活自定义产品映射列表。有关详细信息，请参阅激活和停用自定义产品映射，第 1153 页。

编辑自定义产品映射列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可修改现有自定义产品映射列表，只需添加或移除供应商字符串或更改列表名称。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**。

步骤 3 点击要编辑的产品映射列表旁边的编辑图标 ()。

如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 对列表进行更改，如创建自定义产品映射，第 1151 页中所述。

步骤 5 完成后，点击 **Save**。

激活和停用自定义产品映射

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可一次性启用或禁用整个自定义产品映射列表。激活自定义产品映射列表后，该列表上的每个映射均应用所有带有指定供应商字符串的应用，无论是通过受管设备检测到的，还是通过主机输入功能导入的。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**。

步骤 3 点击要激活或停用的自定义产品映射列表旁边的滑块。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

eStreamer 服务器流传输

通过 Event Streamer (eStreamer)，您可以将多种事件数据从 Firepower 管理中心或 7000 或 8000 系列设备流传输至自定义开发的客户端应用。有关详细信息，请参阅《*Firepower eStreamer* 集成指南》。

您必须将 eStreamer 服务器配置为向客户端发送 eStreamer 事件，提供关于客户端的信息并生成建立通信时要使用的身份验证凭据集，然后，要用作 eStreamer 服务器的设备才能开始向外部客户端流传输 eStreamer 事件。可从设备的用户界面执行所有这些任务。一旦保存设置，收到请求时，您选择的事件将转发至 eStreamer 客户端。

您可以控制 eStreamer 服务器能够向发出请求的客户端传输的事件类型。

表 *194*：*eStreamer* 服务器可传输的事件类型

事件类型	说明	在 管理中心上提供	在 7000 和 8000 系列设备上提供
入侵事件	受管设备生成的入侵事件	是	是
入侵事件数据包数据	与入侵事件关联的数据包	是	是
入侵事件额外数据	与入侵事件关联的额外数据，如通过 HTTP 代理或负载均衡器连接至 Web 服务器的客户端的源 IP 地址	是	是

事件类型	说明	在 管理中心上提供	在 7000 和 8000 系列设备上提供
Discovery Events	发现事件	是	否
关联和白名单事件	关联和白名单事件	是	否
Impact Flag Alerts	管理中心生成的影响警报	是	否
User Events	用户事件	是	否
Malware Events	恶意软件事件	是	否
File Events	文件事件	是	否
连接事件	有关被监控主机与所有其他主机之间的会话流量的信息。	是	是

选择 eStreamer 事件类型

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	管理中心 7000 和 8000 系列	任意	管理

eStreamer 事件配置 (eStreamer Event Configuration) 复选框控制 eStreamer 服务器可传输的事件。您的客户端仍必须在发送到 eStreamer 服务器的请求消息中，特别请求您要其接收的事件类型。有关详细信息，请参阅《*Firepower eStreamer* 集成指南》。

在多域部署中，您可以在任何域级别配置 eStreamer 事件配置。但是，如果祖先域已启用特定事件类型，则无法禁用后代域中的事件类型。

过程

步骤 1 选择**配置 (Configuration)** > **ASA FirePOWER 配置 (ASA FirePOWER Configuration)** > **集成 (Integration)** > **eStreamer**。

步骤 2 点击 **eStreamer** 选项卡。

步骤 3 在 **eStreamer 事件配置 (eStreamer Event Configuration)** 下，选中或清除想要 eStreamer 转发到请求客户端的事件类型旁边的复选框（在eStreamer 服务器流传输，第 1153 页中进行了介绍）。

步骤 4 点击**保存 (Save)**。

配置 eStreamer 客户端通信

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	管理中心 7000 和 8000 系列	任意	管理员/发现管理员

必须先从 eStreamer 页面将客户端添加到 eStreamer 服务器的对等体数据库，然后 eStreamer 才能向该客户端发送 eStreamer 事件。您还必须将 eStreamer 服务器生成的身份验证证书复制到该客户端。完成这些步骤后，无需重新启动 eStreamer 服务即可使客户端能够连接到 eStreamer 服务器。

在多域部署中，可以在任何域中创建 eStreamer 客户端。通过身份验证证书，可以仅从客户端证书的域和任何后代域请求事件。eStreamer 配置页面仅显示与当前域相关联的客户端，因此，如果要下载或吊销证书，请切换到创建了客户端的域。

过程

步骤 1 选择**配置 (Configuration)** > **ASA FirePOWER 配置 (ASA FirePOWER Configuration)** > **集成 (Integration)** > **eStreamer**。

步骤 2 点击 **eStreamer** 选项卡。

步骤 3 点击 **Create Client**。

步骤 4 在**主机名 (Hostname)** 字段中，输入运行 eStreamer 客户端的主机的主机名或 IP 地址。

注释 如果尚未配置 DNS 解析，请使用 IP 地址。

步骤 5 如果想要对证书文件进行加密，请在 **Password** 字段中输入密码。

步骤 6 点击**保存 (Save)**。
eStreamer 服务器现在允许主机访问 eStreamer 服务器上的端口 8302，并创建要在客户端-服务器身份验证期间使用的身份验证证书。

步骤 7 点击客户端主机名旁边的下载图标 ( ) 以下载证书文件。

步骤 8 将证书文件保存至客户端用于 SSL 身份验证的适当目录。

步骤 9 要撤消客户端的访问权限，请点击想要移除的主机旁的删除图标 ( )。
请注意，无需重新启动 eStreamer 服务；系统将立即撤销访问权限。

配置主机输入客户端

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	管理中心	任意	管理员/发现管理员

主机输入功能允许您从另一台设备上运行的客户端程序更新Firepower管理中心的网络映射。例如，您可以从网络映射添加或删除主机，或者更新主机操作系统和服务信息。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

只有先从 Host Input Client 页面将客户端添加至Firepower 管理中心的对等数据库，然后才能运行远程客户端。还必须将管理中心生成的身份验证证书复制至客户端。完成这些步骤之后，客户端可连接到 管理中心。

在多域部署中，可以在任何域中创建客户端。身份验证证书允许客户端为与客户端证书的域关联的任何枝叶域提交网络映射更新。如果您为祖先域创建证书（或如果您的证书域在添加后代域之后成为祖先域），则使用该证书的任何客户端都必须指定每个事务的目标枝叶域，如《*Firepower* 系统主机输入 *API* 指南》中所述。

“主机输入客户端”(Host Input Client) 选项卡仅显示与当前域关联的客户端，因此，如果您要下载或撤销证书，请切换至创建客户端时所在的域。

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**主机输入客户端 (Host Input Client)** 选项卡。

步骤 3 点击 **Create Client**。

步骤 4 在 **Hostname** 字段中，输入运行主机输入客户端的主机的主机名称或 IP 地址。

注释 如果尚未配置 DNS 解析，请使用 IP 地址。

步骤 5 如果想要对证书文件进行加密，请在 **Password** 字段中输入密码。

步骤 6 点击**保存 (Save)**。
主机输入服务将允许主机访问Firepower 管理中心上的 8307 端口，并创建在客户端-服务器身份验证过程中使用的身份验证证书。

步骤 7 点击证书文件旁边的下载文件图标 ( )。

步骤 8 将证书文件保存至客户端用于 SSL 身份验证的目录。

步骤 9 要撤消客户端的访问权限，请点击想要移除的主机旁的删除图标 ( )。

Nmap Scanning

Firepower 系统通过对网络上的流量进行被动分析构建网络映射。根据系统的情况，通过这种被动分析获取的信息有时可能并不完整。不过，您可以主动扫描主机，获取完整信息。例如，如果主机有一台服务器在开放端口上运行但在系统监控网络期间未收发流量，则系统不向网络映射添加有关该服务器的信息。但是，如使用主动扫描仪直接扫描主机，则可检测到服务器的存在。

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。

使用 Nmap 扫描主机时，系统会：

- 将之前未检测到的开放端口上的服务器添加至该主机配置文件中的服务器列表。主机配置文件在“扫描结果”部分列出在已过滤或关闭 TCP 端口或 UDP 端口上检测到的任何服务器。默认情况下，Nmap 扫描超过 1660 个 TCP 端口。

  如果系统识别在 Nmap 扫描中已确定的服务器且有对应的服务器定义，系统会将 Nmap 用于该服务器的名称映射至对应的思科服务器定义。

- 然后，将扫描结果与超过 1500 个已知操作系统指纹进行对比，确定操作系统，并为每个操作系统评分。分配给主机的操作系统是得分最高的操作系统指纹。

  系统会将 Nmap 操作系统名称映射至思科操作系统定义。

- 为添加的服务器和操作系统将漏洞分配至主机。

注意：

- 只有网络映射中存在主机，Nmap 才能将其结果附加至主机配置文件。
- 如果从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

提示 有些扫描选项（例如，端口扫描）会显著增加低带宽网络的负载。请将此类扫描安排在网络使用量较低的时段运行。

有关用于扫描的基础 Nmap 技术的详细信息，请参阅 http://insecure.org/ 上的 Nmap 文档。

Nmap 补救选项

可以创建 Nmap 补救以定义 Nmap 扫描设置。Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。

请注意，Nmap 提供的服务器和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能希望设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。

下表介绍 Firepower 系统可配置的 Nmap 补救选项。

表 *195*: *Nmap* 补救选项

选项	说明	对应的 Nmap 选项
Scan Which Address(es) From Event?	将 Nmap 扫描用作对关联规则的响应时，选择以下其中一个选项以控制扫描事件中的哪个地址，源主机的地址和/或目标主机的地址： • **扫描源地址和目标地址 (Scan Source and Destination Addresses)**，扫描事件中源 IP 地址和目标 IP 地址代表的主机。 • **仅扫描源地址 (Scan Source Address Only)**，扫描事件的源 IP 地址代表的主机。 • **仅扫描目标地址 (Scan Destination Address Only)**，扫描事件的目标 IP 地址代表的主机。	不适用

选项	说明	对应的 Nmap 选项
Scan Types	选择 Nmap 如何扫描端口： • **TCP 同步 (TCP Syn)** 扫描可以快速连接到数千个端口，无需使用完整的 TCP 握手。此选项可用于在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机。如果主机确认在 TCP Syn 扫描中发送的 Syn 数据包，Nmap 会重置连接。 • **TCP Connect** 扫描使用 `connect()` 系统调用，打开穿过主机操作系统的连接。如果 Firepower 管理中心或受管设备上的 `admin` 用户在主机上没有原始数据包权限，或正在扫描 IPv6 网络，则可使用“TCP 连接”(TCP Connect) 扫描。换句话说，在无法使用 TCP Syn 扫描的情况下使用此选项。 • **TCP ACK** 扫描发送 ACK 数据包，检查端口是否已被过滤。 • **TCP Window** 扫描的工作方式与 TCP ACK 扫描相同，但也可确定端口已打开还是关闭。 • **TCP Maimon** 扫描使用 FIN/ACK 探针识别 BSD 派生系统。	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
Scan for UDP ports	启用此选项，可扫描 UDP 端口以及 TCP 端口。请注意，扫描 UDP 端口可能比较耗时，因此，如果想快速扫描，请避免使用此选项。	`-sU`
Use Port From Event	如果计划将补救用作关联政策中的响应，请启用此选项，使补救仅扫描在触发关联响应的事件中指定的端口。 • 选择**打开 (On)** 以扫描关联事件中的端口，而不是在 Nmap 补救配置过程中指定的端口。如果扫描关联事件中的端口，请注意，补救将扫描在 Nmap 补救配置过程中指定的 IP 地址上的端口。这些端口也会添加至补救的动态扫描目标。 • 选择**关闭 (Off)**，仅扫描在 Nmap 补救配置过程中指定的端口。 也可控制 Nmap 是否收集操作系统信息和服务器信息。启用 **Use Port From Event** 选项，可扫描与新服务器关联的端口。	不适用
Scan from reporting detection engine	启用此选项，可从报告主机的检测引擎所驻留的设备扫描主机。 • 要从运行报告检测引擎的设备扫描，请选择 **On**。 • 要从已在补救中配置的设备扫描，请选择 **Off**。	不适用

选项	说明	对应的 Nmap 选项
Fast Port Scan	启用此选项，仅扫描 `nmap-services` 文件中所列的 TCP 端口，而忽略其他端口设置，该文件位于执行扫描设备上的 `/var/sf/nmap/share/nmap/nmap-servicesservices` 目录中。请注意，不能同时使用此选项与 **Port Ranges and Scan Order** 选项。 • 要仅扫描 `nmap-services` 文件中列出的端口，而忽略其他端口设置，请选择 **On**，该文件可在扫描设置上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中找到。 • 要扫描所有 TCP 端口，请选择 **Off**。	`-F`
Port Ranges and Scan Order	使用Nmap端口规范语法设置要扫描的特定端口及其扫描顺序。请注意，不能同时使用此选项与 **Fast Port Scan** 选项。	`-p`
Probe open ports for vendor and version information	启用此选项，可检测服务器厂商和版本信息。如探测开放端口以获取服务器厂商和版本信息，Nmap将获取其用来识别服务器的服务器数据。然后，它会为该服务器替换思科服务器数据。 • 选择 **On**，扫描主机上的开放端口以获取服务器信息，识别服务器厂商和版本。 • 选择**关闭 (Off)**，继续使用主机的思科服务器信息。	`-sV`
Service Version Intensity	选择适用于服务器版本的 Nmap 探针强度。 • 要使用更多探针进行更精确、更长久的扫描，请选择一个较大的数字。 • 要使用更少探针进行不太精确、更加快速的扫描，请选择一个较小的数字。	`--version-intensity <强度>`
Detect Operating System	启用此选项，可检测主机的操作系统信息。 如果配置主机的操作系统检测，Nmap将扫描主机，使用扫描结果创建每个操作系统的评级，反映操作系统在主机上运行的可能性。 • 选择 **On**，扫描主机获取信息，识别操作系统。 • 选择**关闭 (Off)**，继续使用主机的思科操作系统信息。	`-o`

选项	说明	对应的 Nmap 选项
Treat All Hosts As Online	启用此选项，可跳过主机发现过程，在目标范围的每台主机上运行端口扫描。请注意，启用此选项时，Nmap 会忽略 **Host Discovery Method** 和 **Host Discovery Port List** 的设置。 • 要跳过主机发现过程，在目标范围中的每台主机上运行端口扫描，请选择 **On**。 • 要使用 **Host Discovery Method** 和 **Host Discovery Port List** 设置执行主机发现，并跳过任何不可用的主机上的端口扫描，请选择 **Off**。	`-PN`
Host Discovery Method	选择此选项，在 **Host Discovery Port List** 中列出的端口上，为目标范围中的所有主机执行主机发现，或者，如未列出端口，则在适用于主机发现方法的默认端口上执行。 然而，请注意，如也启用 **Treat All Hosts As Online**，**Host Discovery Method** 选项不起作用，不执行主机发现。 选择 Nmap 进行测试以查看主机是否存在且可用时使用的方法： • 如果收到响应，**TCP SYN** 选项将发送设置了 SYN 标记的空 TCP 数据包，并认为主机可用。默认情况下，TCP SYN 扫描端口 80。请注意，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。 • 如果收到响应，**TCP ACK** 选项将发送设置了 ACK 标志的空 TCP 数据包，并认为主机可用。默认情况下，TCP ACK 扫描端口 80。请注意，TCP ACK 扫描不太可能被设有无状态防火墙规则的防火墙拦截。 • 如果端口不可达响应来自已关闭端口，**UDP** 选项将发送 UDP 数据包，并假设主机可用性。默认情况下，UDP 扫描端口 40125。	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
Host Discovery Port List	指定在执行主机发现时要扫描的自定义端口列表，用逗号隔开。	主机发现方法端口列表
Default NSE Scripts	启用此选项，运行默认 Nmap 脚本集，执行主机发现以及服务器、操作系统和漏洞检测。请登录 https://nmap.org/nsedoc/categories/default.html，查看默认脚本列表。 • 要运行默认 Nmap 脚本集，请选择 **On**。 • 要跳过默认 Nmap 脚本集，请选择 **Off**。	`-sC`

选项	说明	对应的 Nmap 选项
计时模板	选择扫描过程的时间；选择的数字越大，扫描越快、越不全面。	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 扫描准则

尽管主动扫描可以获取宝贵信息，但过度使用 Nmap 等工具可能会使您的网络资源超载，甚至使重要的主机瘫痪。使用任何主动式扫描工具时，应遵循这些准则创建扫描策略，确保仅扫描需要扫描的主机和端口。

选择适当的扫描目标

配置 Nmap 时，可创建扫描目标以识别要扫描的主机。扫描目标包括一个 IP 地址、CIDR 块或八位字节 IP 地址范围、IP 地址范围或要扫描的 IP 地址或范围列表，以及一台或多台主机上的端口。

可通过以下方式指定目标：

- 对于 IPv6 主机：

  精确的 IP 地址（例如 `192.168.1.101`）

- 对于 IPv4 主机：

  精确的 IP 地址（例如，`192.168.1.101`）或 IP 地址列表（用逗号或空格隔开）

  使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机）

  使用八位字节范围寻址的 IP 地址范围（例如，`192.168.0-255.1-254` 扫描 192.168.x.x 范围内的所有地址，但以 .0 和 .255 结尾的地址除外）

  使用连字符的 IP 地址范围（例如，`192.168.1.1 - 192.168.1.5` 扫描在 192.168.1.1 和 192.168.1.5（含）之间的六台主机）

  地址或范围列表，用逗号或空格隔开（例如，`192.168.1.0/24，194.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机，以及 194.168.1.1 和 194.168.1.254（含）之间的 254 台主机）

Nmap扫描的理想扫描目标包括有系统无法识别的操作系统的主机、有无法识别的服务器的主机，或者最近在网络上检测到的主机。请记住，Nmap 结果不能添加到不存在于网络映射中主机的网络映射。

注意

- Nmap 提供的服务器和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。
- 如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。
- 请确保您有权限扫描您的目标。使用 Nmap 扫描不属于您或贵公司的主机可能违法。

选择适当端口进行扫描

可为已配置的每个扫描目标选择要扫描的端口。您可以指定各个端口号、端口范围或一系列端口号和端口范围，识别应当在每个目标上扫描的精确端口集。

默认情况下，Nmap 扫描 TCP 端口 1 至端口 1024。如果计划将补救用作关联政策中的响应，则可使补救仅扫描在触发关联响应的事件中指定的端口。如果按需运行补救或将补救作为预定任务加以运行，或者，如不使用来自事件的端口，则可使用其他端口选项确定哪些端口已扫描。可选择仅扫描在 `nmap-services` 文件中列出的 TCP 端口，忽略其他端口设置。除 TCP 端口外，还可扫描 UDP 端口。请注意，扫描UDP端口可能比较耗时，因此，如要快速扫描，请避免使用此选项。为选择要扫描的特定端口或端口范围，请使用 Nmap 端口规范语法识别端口。

设置主机发现选项

在开始主机的端口扫描之前，可决定是否执行主机发现，或者，可假设计划要扫描的所有主机均在线。如果选择不将所有主机视为在线，则可选择要使用的主机发现方法，如果需要，自定义在主机发现过程中扫描的端口列表。主机发现不能从已列出端口探测操作系统或服务器信息；它仅使用特殊端口上的响应确定主机是否活动且可用。如果执行主机发现且主机不可用，Nmap则不扫描该主机上的端口。

示例：使用 Nmap 解析未知操作系统

本示例介绍用于解析未知操作系统的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅管理 Nmap 扫描，第 1164 页。

如果系统无法确定网络上主机的操作系统，则可使用Nmap主动扫描主机。Nmap使用其通过扫描获取的信息对可能的操作系统进行评级。然后，它使用评级最高的操作系统作为主机操作系统标识。

如使用 Nmap 向新主机质询操作系统和服务器信息，则将停用系统为已扫描主机对该数据进行的监控。如果使用Nmap发现主机的主机操作系统和服务器操作系统，系统会标记为拥有未知操作系统，您可以识别相似的主机组。然后，可根据其中一个主机组创建自定义指纹，使系统能够根据 Nmap 扫描，将指纹与已知在主机上运行的操作系统相关联。尽可能创建自定义指纹，而不是通过第三方来源（例如，Nmap）输入静态数据，因为自定义指纹允许系统继续监控主机操作系统并按需更新。

在本例中，您将：

1. 配置扫描实例，如添加 Nmap 扫描实例，第 1165 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。

- 启用**检测操作系统 (Detect Operating System)** 以检测主机的操作系统信息。
- 启用 **Probe open ports for vendor and version information**，可检测服务器厂商和版本信息。
- 启用 **Treat All Hosts as Online**，因为已知存在主机。

3 创建在系统检测到具有未知操作系统的主机时触发的关联规则。该规则应在**发生发现事件**并且**主机的操作系统信息已更改**且符合以下条件时触发：**操作系统名称未知**。

4 创建包含关联规则的关联策略。

5 在关联策略中，将第 2 步中创建的 Nmap 补救作为响应添加至第 3 步中创建的规则。

6 激活关联策略。

7 清除网络映射上的主机，强制网络发现重新启动，重建网络映射。

8 一两天后，搜索关联策略生成的事件。分析在主机上检测到的操作系统的 Nmap 结果，弄清网络上是否有系统无法识别的特殊主机配置。

9 如果发现未知操作系统的 Nmap 结果相同的主机，请为其中一台主机创建自定义指纹，并用它识别未来的类似主机。

示例：使用 Nmap 响应新主机

此示例介绍旨在对新主机作出响应的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅管理 Nmap 扫描，第 1164 页。

当系统在子网中检测到可能被入侵的新主机时，您可能想扫描该主机，确保获取该主机漏洞的准确信息。

要完成此操作，可创建和激活关联策略，当子网中出现新主机时进行检测，启动补救以对主机上执行 Nmap 扫描。

为此，将会执行以下操作：

1 配置扫描实例，如添加 Nmap 扫描实例，第 1165 页中所述。

2 使用以下设置创建 Nmap 补救：

- 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
- 启用**检测操作系统 (Detect Operating System)** 以检测主机的操作系统信息。
- 启用 **Probe open ports for vendor and version information**，可检测服务器厂商和版本信息。
- 启用 **Treat All Hosts as Online**，因为已知存在主机。

3 创建当系统在特定子网上检测到新主机时触发的关联规则。此规则应在**发生发现事件**并**检测到新主机时**触发。

4 创建包含关联规则的关联策略。

5 在关联策略中，将在以前步骤中创建的 Nmap 补救作为响应添加至在第 3 步中创建的规则。

6 激活关联策略。

7 收到出现新主机的通知时，检查主机配置文件，查看 Nmap 扫描结果，解决任何适用于主机的漏洞。

激活策略后，可以定期检查补救状态视图（**分析 (Analysis)** > **关联 (Correlation)** > **状态 (Status)**）以查看补救启动时间。补救的动态扫描目标应当包括其因服务器检测而扫描的主机的 IP 地址。根据 Nmap 检测的操作系统和服务器，查看这些主机的主机配置文件，弄清主机上是否存在需要解决的漏洞。

注意 如有大型或动态网络，新主机检测可能太频繁，而无法使用扫描进行响应。为防止资源超载，请避免使用 Nmap 扫描响应频繁发生的事件。另请注意，如果使用 Nmap 向新主机质询操作系统和服务器信息，则会停用思科对已扫描主机的该数据进行的监控。

管理 Nmap 扫描

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

要使用 Nmap 扫描，至少必须配置一个 Nmap 扫描实例和一个 Nmap 补救。是否配置 Nmap 扫描目标可以选择。

过程

步骤 1 配置 Nmap 扫描：

- 如添加 Nmap 扫描实例，第 1165 页中所述，添加 Nmap 扫描实例。
- 如创建 Nmap 补救，第 1169 页中所述，创建 Nmap 补救。
- 或者，也可以如添加 Nmap 扫描目标，第 1167 页中所述，添加 Nmap 扫描目标。

步骤 2 运行 Nmap 扫描：

- 如运行按需 Nmap 扫描，第 1171 页中所述，运行按需 Nmap 扫描。
- 如Nmap 扫描自动化，第 160 页中所述，配置自动 Nmap 扫描。
- 如安排 Nmap 扫描，第 160 页中所述，安排自动 Nmap 扫描。

接下来的操作

- 通过查看相关任务，监控正在进行的 Nmap 扫描；请参阅查看任务消息，第 239 页。
- 或者，也可以优化扫描：

如编辑 Nmap 扫描实例，第 1166 页中所述，编辑 Nmap 扫描实例。

如编辑 Nmap 扫描目标，第 1168 页中所述，编辑 Nmap 扫描目标。

如编辑 Nmap 补救，第 1171 页中所述，编辑 Nmap 补救。

添加 Nmap 扫描实例

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

可为要用于扫描网络漏洞的每个 Nmap 模块设置独立的扫描实例。可为 Firepower 管理中心上的本地 Nmap 模块以及要用于远程运行扫描的任何设备设置扫描实例。每次扫描的结果始终存储在Firepower 管理中心上，可在这里配置扫描，即使是从远程设备运行扫描。为防止意外或恶意扫描关键任务主机，可创建实例黑名单，指示绝不使用该实例扫描的主机。

不能添加名称与任何现有扫描实例相同的扫描实例。

在多域部署中，系统会显示在当前域中创建的扫描实例，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描实例，您不可以对其进行编辑。要查看和编辑较低域中的扫描实例，请切换至该域。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。
- 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 添加补救：

- 如果通过上述第一种方法访问列表，请找到“添加新实例”(Add a New Instance) 部分，从下拉列表中选择“Nmap 补救”(Nmap Remediation) 模块，然后点击**添加 (Add)**。
- 如果通过上述第二种方法访问该列表，请点击**添加 Nmap 实例 (Add Nmap Instance)**。

步骤 3 输入**实例名称 (Instance Name)**。

步骤 4 输入**说明 (Description)**。

步骤 5 或者，在**列入黑名单的扫描主机 (Black Listed Scan hosts)** 字段中，使用以下语法指定任何绝不应当使用此扫描实例扫描的主机或网络：

- 对于 IPv6 主机，精确的 IP 地址（例如，`2001:DB8::fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址（例如，`192.168.1.101`）或使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 `192.168.1.1` 和 `192.168.1.254`（含）之间的 254 台主机）

- 请注意，不能使用感叹号 (!) 否定地址值。

注释 如果明确将黑名单网络中的主机作为扫描目标，该扫描将不运行。

步骤 6 或者，要从远程设备而非Firepower 管理中心运行扫描，请在 **Remote Device Name** 字段中指定设备的 IP 地址或名称，因为它会显示在 管理中心网络界面中的设备 Information 页面中。

步骤 7 点击**创建**。
系统创建完实例后，以编辑模式显示实例。

步骤 8 或者，将 Nmap 补救添加到实例。为此，请找到实例的“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**，然后创建补救，如创建 Nmap 补救，第 1169 页中所述。

步骤 9 点击**取消 (Cancel)**，返回实例列表。

注释 如果您通过**扫描程序 (Scanners)** 访问 Nmap 扫描实例列表，系统不会显示您添加的实例，除非您也将补救添加到该实例。要查看尚未添加补救的实例，请使用**实例 (Instances)** 菜单选项访问列表。

编辑 Nmap 扫描实例

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

当编辑扫描实例时，可以查看、添加和删除与实例关联的补救。不再想使用 Nmap 扫描实例中描述的 Nmap 模块时，请删除该 Nmap 扫描实例。请注意，如果删除扫描实例，也将删除使用该实例的任何补救。

在多域部署中，系统会显示在当前域中创建的扫描实例，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描实例，您不可以对其进行编辑。要查看和编辑较低域中的扫描实例，请切换至该域。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。
- 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 点击要编辑的实例旁边的查看图标 ( )。

步骤 3 对扫描实例设置进行更改，如添加 Nmap 扫描实例，第 1165 页中所述。

步骤 4 点击**保存 (Save)**。

步骤 5 点击 **Done**。

接下来的操作

- 或者，将新补救添加到扫描实例；请参阅 创建 Nmap 补救 ， 第 1169 页
- 或者，编辑与实例关联的补救；请参阅编辑 Nmap 补救 ， 第 1171 页。
- 或者，删除与实例关联的补救；请参阅运行按需 Nmap 扫描 ， 第 1171 页。
- 或者，通过点击扫描实例旁边的删除图标 ( ) 删除该扫描实例。

添加 Nmap 扫描目标

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

配置 Nmap 模块时，可创建和保存扫描目标，识别想在执行按需或预定扫描时作为扫描目标的主机和端口，从而避免每次构建新扫描目标。扫描目标包括一个或一组要扫描的 IP 地址，以及一台或多台主机上的端口。对于 Nmap 目标，也可使用 Nmap 八位字节范围寻址或 IP 地址范围。有关 Nmap 八位组范围寻址的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

注意：

- 扫描包含大量主机的扫描目标可能需要延长的时间。作为一种解决方法，每次仅扫描几台主机。
- Nmap 提供的服务器和操作系统数据将保持不变，直到您运行另一个 Nmap 扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。
- 在多域部署中，系统会显示在当前域中创建的扫描目标，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描目标，您不可以对其进行编辑。要查看和编辑较低域中的扫描目标，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击 **Create Scan Target**。

步骤 4 在**名称 (Name)** 字段中，输入要用于此扫描目标的名称。

步骤 5 在 **IP 范围 (IP Range)** 文本框中，使用Nmap 扫描准则， 第 1161 页中所述的语法指定要扫描的一个或多个主机。

注释 如果在扫描目标中的 IP 地址或范围列表中使用逗号，则保存目标时，逗号将转换为空格。

步骤 6 在 **Ports** 字段中，指定要扫描的端口。
可使用从 1 到 65535 的值输入以下任意项：

- 端口号
- 用逗号分隔的端口列表
- 用连接号分隔的端口号范围
- 用连接号连接的端口号范围，用逗号分隔

步骤 7 点击**保存 (Save)**。

编辑 Nmap 扫描目标

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

提示 如果不想使用补救扫描特定 IP 地址，但是该 IP 地址已添加至目标，则可能想编辑补救的动态扫描目标，因为主机参与了启动补救的关联策略违反事件。

如果不再想扫描已在扫描目标中列出的主机，请删除扫描目标。

在多域部署中，系统会显示在当前域中创建的扫描目标，您可以对其进行编辑。系统还会显示在祖先域中创建的扫描目标，您不可以对其进行编辑。要查看和编辑较低域中的扫描目标，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击要编辑的扫描目标旁边的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 按需进行修改。有关详细信息，请参阅添加 Nmap 扫描目标，第 1167 页。

步骤 5 点击**保存 (Save)**。

步骤 6 或者，通过点击扫描目标旁边的删除图标 ( ) 来删除扫描目标。

创建 Nmap 补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

Nmap补救只可以通过将它添加到现有Nmap扫描实例来创建。补救定义了扫描的设置。它可用作关联策略中的响应、按需运行或在指定时间作为预定任务运行。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

有关 Nmap 功能的一般信息，请参阅 http://insecure.org 上的 Nmap 文档。

在多域部署中，系统会显示在当前域中创建的 Nmap 补救，您可以对其进行编辑。系统还会显示在祖先域中创建的 Nmap 补救，您不可以对其进行编辑。要查看和编辑较低域中的 Nmap 补救，请切换至该域。

开始之前

- 如添加 Nmap 扫描实例，第 1165 页中所述，添加 Nmap 扫描实例。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 点击要添加补救的实例旁边的查看图标 ( )。

步骤 3 在“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**。

步骤 4 输入**补救名称 (Remediation Name)**。

步骤 5 输入**说明 (Description)**。

步骤 6 如果计划使用此补救响应在发生入侵事件、连接事件或用户事件时触发的关联规则，请配置**扫描事件中的哪个地址？(Scan Which Address(es) From Event?)** 选项。

提示 如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

注释 请**不要**分配 Nmap 补救作为在流量配置文件变化时触发的关联规则的响应。

步骤 7 配置**扫描类型 (Scan Type)** 选项。

步骤 8 或者，除了 TCP 端口，还要扫描 UDP 端口，请为**扫描 UDP 端口 (Scan for UDP ports)** 选项选择**开启 (On)**。

提示 UDP 端口扫描比 TCP 端口扫描需要更多的时间。要加速扫描，请禁用此选项。

步骤 9 如果计划使用此补救响应关联策略违反事件，请配置**使用事件中的端口 (Use Port From Event)** 选项。

步骤 10 如果计划使用此补救响应关联策略违反事件，并希望使用运行检测引擎来检测事件的设备运行扫描，请配置**从报告检测引擎扫描 (Scan from reporting detection engine)** 选项。

步骤 11 配置**快速端口扫描 (Fast Port Scan)** 选项。

步骤 12 在**端口范围和扫描顺序 (Port Ranges and Scan Order)** 字段中，输入要在默认情况下使用 Nmap 端口规范语法按自己想要的顺序扫描的端口。
使用以下格式：

- 指定从 1 到 65535 的值。
- 使用逗号或空格分隔端口。
- 使用连字符指明端口范围。
- 扫描 TCP 和 UDP 端口时，以 T 作为要扫描的 TCP 端口列表的开端，以 U 作为 UDP 端口列表的开端。

注释 启动补救以响应关联策略违反事件时，**使用事件中的端口 (Use Port From Event)** 选项将覆盖此设置，如第 8 步中所述。

示例：
要扫描 UDP 流量的端口 53 和 111，然后扫描 TCP 流量的端口 21-25，请输入 `U:53,111,T:21-25`。

步骤 13 要探测开放端口以了解服务器厂商和版本信息，请配置**探测开放端口以获取供应商和版本信息 (Probe open ports for vendor and version information)**。

步骤 14 如果选择探测开放端口，请从**服务版本强度 (Service Version Intensity)** 下拉列表中选择一个数字，设置使用的探针数量。

步骤 15 要扫描操作系统信息，请配置**检测操作系统 (Detect Operating System)** 设置。

步骤 16 要确定主机发现是否发生，是否仅针对可用端口运行端口扫描，请配置**将所有主机视为在线 (Treat All Hosts As Online)**。

步骤 17 要设置希望 Nmap 在测试主机可用性时使用的方法，请从**主机发现方法 (Host Discovery Method)** 下拉列表中选择一种方法。

步骤 18 如果要在主机发现过程中扫描自定义端口列表，请在**主机发现端口列表 (Host Discovery Port List)** 字段中输入适合所选主机发现方法的端口列表，用逗号隔开。

步骤 19 配置**默认 NSE 脚本 (Default NSE Scripts)** 选项，控制是否使用默认 Nmap 脚本集进行主机发现以及服务器、操作系统和漏洞发现。

提示 请参阅 http://nmap.org/nsedoc/categories/default.html，获取默认脚本列表。

步骤 20 要设置扫描过程的时间选择，请从**计时模板 (Timing Template)** 下拉列表中选择计时模板编号。
选择的编号越大，速度越快，扫描越不全面；而选择的编号越小，速度越慢，扫描越全面。

步骤 21 点击**创建**。

系统创建完补救后，在编辑模式中显示它。

步骤 22 点击**完成 (Done)** 以返回相关实例。

步骤 23 点击**确定 (OK)** 以返回实例列表。

编辑 Nmap 补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

对 Nmap 补救所做的更改不会影响正在进行的扫描。新设置将在下一次扫描开始时生效。删除不再需要的 Nmap 补救。

在多域部署中，系统会显示在当前域中创建的 Nmap 补救，您可以对其进行编辑。系统还会显示在祖先域中创建的 Nmap 补救，您不可以对其进行编辑。要查看和编辑较低域中的 Nmap 补救，请切换至该域。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。
- 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 访问要编辑的补救：

- 如果通过上述第一种方法访问列表，请点击相关实例旁的查看图标()，然后在要在“已配置补救”部分中编辑的补救旁边再次点击该补救。
- 如果通过上述第二种方法访问列表，请点击要编辑的补救边的查看图标 ()。

步骤 3 根据需要进行修改，如创建 Nmap 补救，第 1169 页中所述。

步骤 4 如果要保存更改，请点击**保存 (Save)**，或者如果要不保存而直接退出，请点击**完成 (Done)**。

步骤 5 或者，通过点击补救旁边的删除图标 () 删除补救。

运行按需 Nmap 扫描

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

可在需要时启动按需 Namp 扫描。可以通过输入要扫描的 IP 地址和端口或者通过选择现有扫描目标，指定按需扫描目标。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

开始之前

- 或者，添加 Nmap 扫描目标；请参阅添加 Nmap 扫描目标，第 1167 页。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 在要用于执行扫描的 Nmap 补救旁边，点击扫描图标 ( )。

步骤 3 或者，要使用已保存的扫描目标进行扫描，请从**已保存的目标 (Saved Targets)** 下拉列表中选择目标，然后点击**加载 (Load)**。

注释 要添加扫描目标，可以点击对话框顶部的编辑图标 ( )。

步骤 4 在 **IP 范围 (IP Range[s])** 字段中，指定要扫描或修改已加载列表的主机的 IP 地址。
注意：

- 对于带 IPv4 地址的主机，可指定多个 IP 地址，用逗号隔开，或者使用 CIDR 表示法。也可在 IP 地址前面添加感叹号 (!)，否定 IP 地址。
- 对于带 IPv6 地址的主机，请使用精确的 IP 地址。不支持地址范围。

步骤 5 在 **Ports** 字段中，指定要扫描的端口或修改已加载的列表。
可输入一个端口号、用逗号隔开的端口列表或者用连接号隔开的端口号范围。

步骤 6 在多域部署中，使用**域 (Domain)** 字段指定要执行扫描的枝叶域。

步骤 7 点击 **Scan Now**。

接下来的操作

- 或者，监控任务状态；请参阅查看任务消息，第 239 页。

Nmap 扫描结果

您可以监控正在进行的Nmap扫描，导入先前通过Firepower系统执行的扫描中的结果或在Firepower系统外执行的结果，以及查看和分析扫描结果。

可查看作为弹出窗口中渲染页面的扫描结果（使用本地Nmap模块创建）。也可下载原始XML格式的 Nmap 结果文件。

还可在主机配置文件和网络映射中查看由 Nmap 检测到的操作系统和服务器信息。如果主机扫描为已过滤或已关闭端口上的服务器生成服务器信息，或者如果扫描收集无法包含在操作系统信息或服务器部分中的信息，主机配置文件会将这些结果纳入 Nmap Scan Results 部分。

查看 Nmap 扫描结果

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

当 Nmap 扫描完成后，可以查看扫描结果表。

可以根据所查找的信息操作结果视图。访问扫描结果时看到的页面因使用的工作流程而异。可使用预定义的工作流程，其中包括扫描结果表视图。您也可以创建自定义工作流程，仅显示符合您具体要求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

可在 http://insecure.org 上下载 Nmap 结果，并使用 Nmap 1.01 DTD 查看。

还可清除扫描结果。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 在工具栏上，点击**扫描结果 (Scan Results)**。

步骤 3 有以下选项可供选择：

- 调整时间范围，如事件时间限制，第 1458 页中所述。
- 要使用不同的工作流程（包括自定义工作流程），请按工作流程标题点击（**切换工作流程 ([switch workflow])**。
- 要查看作为弹出窗口中渲染页面的扫描结果，请在扫描作业旁点击 **View**。
- 要保存扫描结果文件的副本，以便在任何文本编辑器中查看原始 XML 代码，请在扫描作业旁点击 **Download**。
- 要对扫描结果排序，请点击列标题。再次点击列标题以反转排列顺序。
- 要限制显示的列，请在要隐藏的列标题中点击关闭图标 ( )。在显示的弹出窗口中，点击 **Apply**。

  提示 要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击**已禁用列 (Disabled Columns)** 下的列名称。

- 要向下展开到工作流程中的下一个页面，请参阅使用向下钻取页面，第 1450 页。
- 要配置扫描实例和补救，请点击工具栏中的**扫描工具 (Scanners)** 并参阅管理 Nmap 扫描，第 1164 页。

- 要在工作流程页面之内及在各工作流程页面之间导航，请参阅工作流程页面导航工具，第 1447 页。
- 要导航至其他事件视图以查看关联的事件，请从**跳至 (Jump to)** 下拉列表中选择要查看的事件视图的名称。
- 要搜索扫描结果，请在相应字段中输入搜索条件。

Nmap 扫描结果字段

运行 Nmap 扫描时，Firepower 管理中心 在数据库中收集扫描结果。下表介绍了扫描结果表中可以查看和搜索的字段。

表 *196*：扫描结果字段

字段	说明
开始时间	生成结果的扫描的开始日期和时间。
结束时间	生成结果的扫描的结束日期和时间。
Target	生成结果的扫描的扫描目标的 IP 地址（或主机名，如果 DNS 解析已启用）。
Scan Type	要么是 `Nmap`，要么是第三方扫描仪的名称，指明生成结果的扫描的类型。
Scan Mode	生成结果的扫描的模式： • `按需 (On Demand)` - 来自按需扫描的结果。 • `Imported` - 来自不同系统上扫描的结果，已导入 Firepower 管理中心。 • `Scheduled` - 来自作为预定任务运行的扫描的结果。
结果	扫描的结果。
域	扫描目标的域。此字段只存在于多域部署中。

导入 Nmap 扫描结果

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

您可以导入在 Firepower 系统外执行的 Nmap 扫描所创建的 XML 结果文件。您还可以导入先前从 Firepower 系统下载的 XML 结果文件。要导入 Nmap 扫描结果，结果文件必须采用 XML 格式，且兼容于 Nmap 1.01 DTD。有关创建 Nmap 结果的详细信息以及 Nmap DTD 的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

主机必须已存在于网络映射中，然后 Nmap 才能将其结果附加到主机配置文件。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **扫描工具 (Scanners)**。

步骤 2 在工具栏上，点击 **Import Results**。

步骤 3 在多域部署中，从**域 (Domain)** 下拉列表中选择枝叶域以指定要存储导入结果的位置。

步骤 4 点击 **Browse**，导航至结果文件。

步骤 5 返回 Import Results 页面后，点击 **Import**，导入结果。

第 65 章

应用检测

以下主题介绍 Firepower 系统应用检测：

概述：应用检测

当 Firepower 系统分析 IP 流量时，它会尝试识别网络上的常用应用。应用感知对于应用控制至关重要。

系统检测的应用有三种类型：

- 应用协议（例如 HTTP 和 SSH），代表主机之间的通信
- 客户端（例如 网络浏览器和邮件客户端），代表在主机上运行的软件
- 网络应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL

系统根据在检测器中指定的特征识别网络流量中的应用。例如，系统可以通过数据包报头中的 ASCII 模式识别应用。此外，安全套接字层 (SSL) 协议检测程序使用安全会话的信息来识别会话中的应用。

在 Firepower 系统中有两个应用检测器来源：

- 系统提供的检测器检测 Web 应用、客户端和应用协议。

  系统提供的应用检测器（和操作系统）的可用性取决于 Firepower 系统的版本和已安装的 VDB 版本。版本说明和公告包含关于新的和更新的检测程序的信息。也可以导入专业服务开发的单个检测程序。有关所检测到的应用的完整列表，请参阅支持站点。

- 自定义应用协议检测器由用户创建并检测 Web 应用、客户端和应用协议。

您还可以通过隐含应用协议检测来检测应用协议，此检测根据对客户端的检测暗示应用协议的存在。

如在网络发现策略中所定义，系统仅识别受监控网络中的主机上运行的应用协议。例如，如果内部主机访问未受监控的远程站点的 FTP 服务器，系统不会将应用协议识别为 FTP。另一方面，如果远程或内部主机访问正受监控主机上的 FTP 服务器，系统能够正确识别应用协议。

如果系统可以识别受监控主机用于连接到未受监控服务器的客户端，则系统会识别客户端的对应应用协议，但是不将该协议添加到网络映射中。请注意，客户端会话必须包括来自要发生应用检测的服务器的响应。

系统会确定其检测到的每个应用的特征；请参阅应用特征，第 278 页。系统使用这些特征创建应用组，称为应用过滤器。应用过滤器用于执行访问控制以及限制报告和控制面板构件中使用的搜索结果和数据。

您还可以使用导出的 NetFlow 记录、Nmap 主动扫描和主机输入功能补充应用检测器数据。

应用检测器基础知识

Firepower 系统分析 IP 流量时，将使用检测器来识别网络上常用的应用。您可以使用“检测器”(Detectors) 页面（**策略 (Policies)** > **应用检测器 (Application Detectors)**）自定义 Firepower 系统的检测功能并查看每个检测器的相关信息，包括：

- 检测器的名称
- 检测器检查的流量的协议
- 检测器的类型是应用协议、客户端、网络应用还是内部检测器
- 检测到的应用的相关详细信息，包括与检测器检测到的应用关联的名称、描述、任务、业务相关性、标记和类别
- 检测器的状态（活动或非活动）

注释 切记，检测器列表可能会发生变化，具体取决于已安装的 Firepower 系统和 VDB 的版本以及可能已导入或创建的任何个别检测器。应仔细阅读每个 Firepower 系统更新的版本说明以及每次 VDB 更新的公告以便获得有关已更新检测器的信息。

系统仅使用活动检测器来分析应用流量。

您可能会注意到，列出的检测器拥有不同的属性。例如，可查看部分检测器的设置，但是不能查看其他检测器的设置。类似地，可删除部分检测器，但是不能删除其他检测器。这是因为，存在多种不同类型的检测器，如下所述。

思科提供的内部检测器

内部检测器是仅随Firepower系统更新提供的应用检测器。取决于检测器，内部检测器可以检测客户端、网络应用或应用协议流量，但它们被分类为内部检测器，而不是其他类型中的一种，因为它们是内置检测器，而且无法停用。

内部检测器始终处于开启状态；无法对其进行停用、删除或配置。内部检测器的示例包括：内置Amazon 检测器和内置 AppleTalk 检测器。

思科提供的客户端检测器

思科提供的客户端检测器可检测客户端流量，通过 VDB 更新提供，也可能随 Firepower 系统更新提供。思科专业服务也能以可导入检测器的形式提供这些检测器。

可根据贵组织的需求激活和停用客户端检测器。VDB更新也可激活或停用客户端检测器。仅当导入客户端检测器后，才可以将其导出。

客户端检测器的示例包括：Google Earth 和 Immunet 检测器。

思科提供的 Web 应用检测器

思科提供的 *Web* 应用检测器可检测 HTTP 流量负载中的 Web 应用，通过 VDB 更新提供，也可能随 Firepower 系统更新提供。

可根据贵组织的需求激活和停用网络应用检测器。VDB更新可以激活或停用网络应用检测器。网络应用检测器的示例包括：Blackboard 和 LiveJournal 检测器。

思科提供的应用协议（端口）检测器

思科提供的基于端口的应用协议检测器基于对已知端口的网络流量检测。这些检测器通过VDB更新提供，也可能随 Firepower 系统更新提供，或由思科专业服务以可导入检测器的形式提供。

可根据贵组织的需求激活和停用应用协议检测器。还可查看检测器定义，以便将其用作自定义检测器的基础。VDB 更新可激活或停用应用协议检测器。

端口检测器的示例包括：chargen 和 finger 检测器。

思科提供的应用协议 (Firepower) 检测器

思科提供的基于 *Firepower* 的应用协议检测器基于使用 Firepower 应用指纹的网络流量检测。这些检测器通过 VDB 更新提供，也可能随 Firepower 系统更新提供。

可根据贵组织的需求激活和停用应用协议检测器。VDB更新可以激活或停用思科提供的应用协议检测器。基于 Firepower 的应用协议检测器的示例包括 Jabber 和 Steam 检测器。

自定义应用检测器

自定义应用检测器基于模式，检测客户端、Web 应用或应用协议流量发出的数据包中的模式。您可根据您的组织的需求激活和停用应用检测器。

您可完全控制导入和自定义的检测器，可将其激活、停用、编辑、导入、导出和删除。

在 Web 界面中识别应用协议

下表概述 Firepower 系统如何识别检测到的应用协议：

表 *197*：*Firepower* 系统识别应用协议

标识	说明
应用协议名称	如果应用协议属于以下情况，Firepower 管理中心将会使用应用协议名称来识别应用协议： • 由系统正确识别出 • 使用 NetFlow 数据识别出，并且 `/etc/sf/services` 中有端口应用协议关联 • 使用主机输入功能手动识别出 • 由 Nmap 或其他活动源识别出
`pending`	如果系统既不能正确识别也不能错误识别应用，Firepower 管理中心会将应用协议识别为 `pending`。 大多数情况下，系统需要收集和分析更多的连接数据才能识别待处理应用。 在应用详细信息表、服务器表和主机配置文件中，只会对在其中检测到（而不是由检测到的客户端或 Web 应用流量推断）特定应用协议流量的应用协议显示 `pending` 状态。
`unknown`	在以下情况下，Firepower 管理中心会将应用协议识别为 `unknown`： • 应用不匹配系统的任何检测器 • 应用协议是使用 NetFlow 数据识别出的，但 `/etc/sf/services` 中没有端口应用协议关联
空白	已检查检测到的所有可用数据，但没有识别出应用协议。在应用详细信息表、服务器表中和主机配置文件中，对于在其中没有检测到应用协议的非 HTTP 通用客户端数据流量，应用协议留空。

通过客户端检测进行隐含应用协议检测

如果系统可以识别受监控主机用于访问未受监控主机的客户端，Firepower管理中心会推断该连接使用与该客户端对应的应用协议。（由于系统仅跟踪监控网络上的应用，因此，连接日志通常不包含有关监控主机用于访问未受监控的服务器的连接的应用协议信息。）

此过程，或隐含应用协议检测，具有以下结果：

- 由于系统不会为这些服务器生成新的 TCP 端口或新的 UDP 端口事件，因此，服务器不会显示在服务器表中。此外，不能将对这些应用协议的检测作为条件来触发事件警报或关联规则。

- 由于应用协议未与主机关联，因此，不能查看主机配置文件中的详细信息，不能设置其服务器身份，也不能使用流量量变曲线或关联规则的主机配置文件限定条件中的信息。此外，系统不会根据此类检测将漏洞与主机关联。

但是，您可以触发有关连接中是否存在应用协议信息的关联事件。还可以使用连接日志中的应用协议信息创建连接跟踪程序和流量量变曲线。

主机限制和发现事件日志记录

如果系统检测到客户端、服务器或网络应用，它会生成发现事件，除非关联的主机已达到客户端、服务器或网络应用的最大数量。

主机配置文件最多为每个主机显示 16 个客户端、100 个服务器和 100 个网络应用。

请注意，依赖于客户端、服务器或网络应用检测的操作不受此限制的影响。例如，经配置要在服务器上触发的访问控制规则仍会记录连接事件。

应用检测的特殊注意事项

Squid

在以下情况下，系统会正确识别 Squid 服务器流量：

- 系统检测监控网络上主机与启用了代理身份验证的 Squid 服务器之间的连接；或
- 系统检测从受监控网络上的 Squid 代理服务器到目标系统（即，客户端正在其中请求信息或其他资源的目标服务器）的连接。

但是，在以下情况下，系统无法识别 Squid 业务流量：

- 监控网络上的主机连接到已禁用代理身份验证的 Squid 服务器；或
- Squid 代理服务器被配置为会从其 HTTP 响应中移除 Via: 报头字段

SSL 应用检测

系统提供可以使用安全套接字层 (SSL) 会话中的会话信息识别会话中的应用协议、客户端应用或 Web 应用的应用检测器。

如果系统检测到加密连接，它会将该连接标记为通用 HTTPS 连接或更为具体的安全协议，例如 SMTPS（如果适用）。如果系统检测到 SSL 会话，它会将 `SSL client` 添加到该会话的连接事件中的 **Client** 字段。如果识别到会话的 Web 应用，系统会为该流量生成发现事件。

对于 SSL 应用流量，受管设备还可以检测服务器证书中的公用名并将其与 SSL 主机模式的客户端或 Web 应用比对。当系统识别到特定客户端时，会将 `SSL 客户端` 替换为该客户端的名称。

由于 SSL 应用流量已加密，因此，系统只能使用证书中的信息（而不是加密数据流中的应用数据）进行识别。为此，SSL 主机模式有时只能识别作为应用编写者的公司，因此，同一公司开发的 SSL 应用可能有相同的标别。

在某些情况下，例如HTTPS会话是从HTTP会话内部发起时，受管设备会从客户端数据包中的客户端证书检测服务器名称。

要启用SSL应用标别，必须创建监控响应方流量的访问控制规则。这些规则必须包含适用于SSL应用的应用条件或者使用来自SSL证书的URL的URL条件。对于网络发现，响应方IP地址必须位于要在网络发现策略中监控的网络上；访问控制策略配置决定是否识别流量。要识别SSL应用的检测，您可以在应用检测器列表中或在访问控制规则中添加应用条件时按 `SSL protocol` 标记进行过滤。

推荐的 Web 应用

Web服务器有时会将流量推荐到其他网站，这些网站通常是广告服务器。为帮助您更好地理解网络上出现的推荐流量的情景，系统在推荐会话的事件的 **Web 应用 (Web Application)** 字段中列出推荐流量的Web应用。VDB包含已知被推荐站点的列表。如果系统检测到来自这些站点之一的流量，会将推荐站点连同该流量的事件一起存储。例如，如果通过Facebook访问的广告实际在Advertising.com上托管，检测到的Advertising.com流量与Facebook网络应用相关。系统还可以检测到HTTP流量中的推荐URL，例如当网站提供与另一站点的简单链接时；在这种情况下，推荐URL出现在HTTP Referrer事件字段。

在事件中，如果存在推荐应用，它将被列为流量的网络应用，而URL则是被推荐站点的URL。在上述示例中，用于流量的连接事件的网络应用是Facebook，但URL是Advertising.com。在下列情况下，被推荐的应用可能显示为Web应用：未检测到推荐Web应用，主机推荐其本身，或者存在推荐链。在控制面板中，网络应用的连接和字节数包括网络应用与该应用推荐的流量相关的会话。

请注意，如果创建专门针对被推荐流量的规则，应该为被推荐应用（而不是为推荐应用）添加条件。例如，要阻止从Facebook推荐的Advertising.com流量，可以向Advertising.com应用的访问控制规则添加应用条件。

自定义应用检测器

如果在网络上使用自定义应用，您可以创建自定义的Web应用、客户端或应用协议检测器，它们可向系统提供识别应用所需的信息。应用检测器的类型由您在**协议 (Protocol)**、**类型 (Type)** 和**方向 (Direction)** 字段中进行的选择确定。

只有客户端会话包含来自服务器的响应器数据包，系统才能开始检测和识别服务器流量中的应用协议。请注意，对于UDP流量，系统将响应器数据包的来源指定为服务器。

如果已经在另一Firepower管理中心上创建了检测器，可将其导出后，再导入至此Firepower管理中心。然后，可根据自己的需求编辑已导入的检测器。您可导出和导入自定义检测器以及思科专业服务提供的检测器。但是，您**无法**导出或导入思科提供的任何其他类型检测器。

自定义应用检测器和用户定义的应用字段

可以使用以下字段配置自定义应用检测器和用户定义的应用。

自定义应用检测器字段：常规

使用以下字段配置基本和高级自定义应用检测器。

应用协议

要检测的应用协议。这可以是系统提供的应用或用户定义的应用。

如果要让应用免于执行主动身份验证（在身份规则中配置），则必须选择或创建带用户代理排除项 (User-Agent Exclusion) 标记的应用协议。

说明

应用检测器的说明。

Name

应用检测器的名称。

检测器类型 (Detector Type)

检测器的类型，基本 (Basic) 或高级 (Advanced)。基本应用检测器是在 Web 界面中作为一系列字段而创建的。高级应用检测器是在外部创建并作为自定义 .lua 文件上传的。

自定义应用检测器字段：检测模式

使用以下字段配置基本自定义应用检测器的检测模式。

Direction

检测器应当检查的流量源，包括客户端 (Client) 或服务器 (Server)。

Offset

以字节为单位表示的在数据包中的位置，从数据包负载起始位置（系统应开始搜索模式的位置）开始。

因为数据包负载从0字节开始，请按以下方法计算偏移：将想要从数据包负载起始位置前移的字节数减去 1。例如，要查找数据包的第 5 个位中的模式，在 `Offset` 字段中键入 **4**。

Pattern

与您选择的**类型 (Type)** 相关联的模式字符串。如果未指定模式，则必须配置检测器检查流量，以便匹配一个或多个端口。

端口

检测器应检查流量的端口。

协议

要检测的协议。选择的协议将确定是显示**类型 (Type)** 还是 **URL** 字段。

该协议（以及在某些情况下，您在**类型 [Type]** 和**方向 [Direction]** 字段中的后续选择）将确定您创建的应用检测器类型：Web 应用、客户端或应用协议。

应用检测器类型	协议	类型或方向
Web 应用	HTTP	**类型 (Type)** 为内容类型 (Content Type) 或 URL
	RTMP	任意
	SSL	任意
Client	HTTP	**类型 (Type)** 为用户代理 (User Agent)
	SIP	任意
	TCP 或 UDP	**方向 (Direction)** 为客户端 (Client)
应用协议	TCP 或 UDP	**方向 (Direction)** 为服务器 (Server)

Type

输入的模式字符串类型。您看到的选项由您已选择的**协议 (Protocol)** 确定。如果已选择 RTMP 作为协议，则系统将显示 **URL** 字段而非**类型 (Type)** 字段。

注释 如果选择用户代理 (User Agent) 作为**类型 (Type)**，则系统自动将应用的**标记 (Tag)** 设为用户代理排除项 (User-Agent Exclusion)。

类型选择	字符串特征
Ascii	字符串使用 ASCII 编码。
Common Name	字符串是服务器响应消息中 commonName 字段的值。
内容类型	字符串是服务器响应报头中 content-type 字段的值。
十六进制 (Hex)	字符串使用十六进制表示。
组织单位	字符串是服务器响应消息中 organizationName 字段的值。
SIP 服务器 (SIP Server)	字符串是消息报头中 From 字段的值。
SSL 主机 (SSL Host)	字符串是 ClientHello 消息中 server_name 字段的值。
URL	字符串是一个 URL。 **注释** 检测器假设输入的字符串是完整的URL部分。例如，输入 cisco.com 将匹配 www.cisco.com/support 和 www.cisco.com，但不匹配 www.wearecisco.com。
用户代理	字符串是 GET 请求报头中 user-agent 字段的值。它还可用于 SIP 协议，表示字符串是 SIP 消息报头中 user-agent 字段的值。

URL

来自 RTMP 数据包的 C2 消息内 swfURL 字段的完整 URL 或部分 URL。选择 RTMP 作为**协议 (Protocol)** 时，系统将显示此字段而非**类型 (Type)** 字段。

注释 检测器假设输入的字符串是完整的 URL 部分。例如，输入 cisco.com 将匹配 www.cisco.com/support 和 www.cisco.com，但不匹配 www.wearecisco.com。

用户定义的应用字段

使用以下字段在基本和高级自定义应用检测器内配置用户定义的应用。

业务相关性

应用被用于您的组织的业务运营中（而不是用于娱乐目的）的可能性：非常高 (Very High)、高 (High)、中 (Medium)、低 (Low) 或非常低 (Very Low)。选择最能描述应用的选项。

类别

说明应用的最基本功能的应用通用分类。

说明

应用的说明。

Name

应用的名称。

风险

应用被用于违反您的组织安全策略的目的之可能性：非常高 (Very High)、高 (High)、中 (Medium)、低 (Low) 或非常低 (Very Low)。选择最能描述应用的选项。

标签

提供有关应用的其他信息的一个或多个预定义标记。如果要让应用免于执行主动身份验证（在身份规则中配置），则必须为应用添加用户代理排除项 (User-Agent Exclusion) 标记。

配置自定义应用检测器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

您可以配置基本或高级自定义应用检测器。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击**创建自定义检测器 (Create Custom Detector)**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**。

步骤 4 选择 **Application Protocol**。您有以下选择：

- 如果是为现有应用协议创建检测器（例如，如果要检测非标准端口上的特定应用协议），请从下拉列表中选择应用协议。

- 如果是为用户定义的应用创建检测器，请按照创建用户定义的应用，第1187页中概述的程序执行操作。

步骤 5 选择**检测器类型 (Detector Type)**。

步骤 6 点击 **OK**。

步骤 7 配置**检测模式 (Detection Patterns)** 或**检测条件 (Detection Criteria)**：

- 如果配置的是基本检测器，请指定预设**检测模式 (Detection Patterns)**，如指定基本检测器中的检测模式，第 1188 页中所述。
- 如果配置的是高级检测器，请指定自定义**检测条件 (Detection Criteria)**，如指定高级检测器中的检测条件，第 1189 页中所述。

  注意 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

步骤 8 如果配置的是高级检测器，请使用**数据包捕获 (Packet Captures)** 测试新检测器，如测试自定义应用协议检测器，第 1190 页中所述。如果配置的是基本检测器，则此步骤是可选的。

步骤 9 点击**保存 (Save)**。

注释 如果在访问控制规则中包含该应用，则检测器会自动激活，并且在使用时不能停用。

接下来的操作

- 激活检测器，如激活和停用检测器，第 1194 页中所述。

创建用户定义的应用

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

此处创建的应用、类别和标记在访问控制规则以及在应用过滤对象管理器中均可用。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。

过程

步骤 1 在 Create Detector 页面上，点击 **Add**。

步骤 2 键入**名称 (Name)**。

步骤 3 键入**说明 (Description)**。

步骤 4 选择 **Business Relevance**。

步骤 5 选择 **Risk**。

步骤 6 点击“类别”(Categories) 旁的**添加 (Add)** 以添加类别，并键入新的类别名称，或者从**类别 (Categories)** 下拉列表选择现有类别。

步骤 7 或者，也可以点击"标记"(Tags) 旁的**添加 (Add)** 以添加标记，并键入新的标记名称，或者从**标记 (Tags)** 下拉列表选择现有标记。

步骤 8 点击 **OK**。

接下来的操作

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

指定基本检测器中的检测模式

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

可以配置自定义应用协议检测器以搜索应用协议数据包报头中的特定模式字符串。也可配置检测器，使其搜索多个模式，在这种情况下，应用协议流量必须匹配所有模式，以便检测器主动识别应用协议。

应用协议检测器可使用任何偏移搜索 ASCII 或十六进制模式。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。

过程

步骤 1 在“创建检测器”(Create Detector) 页面上的“检测模式”(Detection Patterns) 部分中，点击**添加 (Add)**。

步骤 2 在**协议 (Protocol)** 中选择检测器应检查的流量的协议。

步骤 3 在**类型 (Type)** 中指定要检测的模式类型。

步骤 4 键入与指定的**类型 (Type)** 相匹配的**模式字符串 (Pattern String)**。

步骤 5 或者，键入**偏移 (Offset)**（以字节为单位）。

步骤 6 或者，要根据其使用的端口识别应用协议流量，请在**端口 (Port[s])** 字段中键入从 1 到 65535 的端口。要使用多个端口，请用逗号分隔它们。

步骤 7 或者，选择**方向 (Direction)**：客户端 (Client) 或服务器 (Server)。

步骤 8 点击 **OK**。

提示 如果要删除模式，请点击要删除的模式旁边的删除图标 ()。

接下来的操作

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

指定高级检测器中的检测条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

注意 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

注意 不要上传来自不可信来源的 .lua 文件。

自定义 .lua 文件包含自定义应用检测器设置。创建自定义 .lua 文件需要具备 lua 编程语言的高级知识和思科的 C-lua API 经验。思科强烈建议使用以下材料来准备 .lua 文件：

- lua 编程语言的第三方说明和参考资料
- 开源检测器开发人员指南： https://www.snort.org/downloads
- OpenAppID Snort 社区资源： http://blog.snort.org/search/label/openappid

注释 系统不支持引用系统调用或文件 I/O 的 .lua 文件。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。
- 通过下载和学习类似检测器的 .lua 文件，为创建有效的 .lua 文件做准备。有关下载检测器文件的详细信息，请参阅查看或下载检测器详细信息，第 1191 页。
- 创建包含自定义应用检测器设置的有效 .lua 文件。

过程

步骤 1 在高级自定义应用检测器的“创建检测器”(Create Detector) 页面的“检测条件”(Detection Criteria) 部分，点击**添加 (Add)**。

步骤 2 点击**浏览...(Browse...)** 以导航至 .lua 文件并将其上传。

步骤 3 点击 **OK**。

接下来的操作

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

测试自定义应用协议检测器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

如您拥有的数据包捕获 (pcap) 文件包含的数据包带有要检测的应用协议的流量，则可针对该 pcap 文件测试自定义的应用协议检测器。思科建议使用简单、干净的 pcap 文件，没有不必要的流量。

Pcap 文件必须为 256 KB 或更小；如果尝试针对较大的 pcap 文件测试检测器，Firepower 管理中心会自动将其截断并测试不完整文件。在使用该文件测试检测器之前，必须修复 pcap 中无法确定的校验和。

开始之前

- 配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。

过程

步骤 1 在“创建检测器”(Create Detector) 页面上的“数据包捕获”(Packet Captures) 部分，点击**添加 (Add)**。

步骤 2 在弹出式窗口中浏览至 pcap 文件，然后点击**确定 (OK)**。

步骤 3 要针对 pcap 文件的内容测试检测器，点击 pcap 文件旁的评估图标。系统显示消息，指示测试是否成功。

步骤 4 或者，重复第 1至 3 步，针对额外的 pcap 文件测试检测器。

提示 要删除 pcap 文件，点击想要删除的文件旁的删除图标 ()。

接下来的操作

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 1186 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

查看或下载检测器详细信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

可以使用检测器列表来查看应用检测器详细信息（所有检测器）和下载检测器详细信息（仅自定义应用检测器）。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 要查看检测器详细信息，请点击信息图标 () 以查看风险、业务关联性、标记和类别，如概述：应用检测，第 1177 页中所述。

步骤 3 要下载自定义应用检测器的检测器详细信息，请点击下载图标 ()。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

检测器列表排序

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

默认情况下，Detectors 页面将按名称以字母顺序列出检测器。列标题旁边的向上或向下箭头表示页面按该列升序或降序排序。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击相应的列标题。

过滤检测器列表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 展开检测器列表的过滤器组，第 1192 页中所述的其中一个过滤器组并选择过滤器旁边的复选框。要选择组中的所有过滤器，右键单击组名称，然后选择 **Check All**。

步骤 3 如果要移除某个过滤器，请点击移除图标 ( )（位于**过滤器 [Filters]** 字段的过滤器名称中）或禁用过滤器列表中的过滤器。要移除组中的所有过滤器，右键单击组名称，然后选择 **Uncheck All**。

步骤 4 如果要移除所有过滤器，请点击已应用至检测器的过滤器列表旁边的**全部清除 (Clear alls)**。

检测器列表的过滤器组

可单独或组合使用多个过滤器组，以过滤检测器列表。

Name

查找名称或描述包含您键入的字符串的检测器。字符串可能包含任何字母数字或特殊字符。

自定义过滤器

查找与对象管理页面上创建的自定义应用过滤器匹配的检测器。

作者

按检测器的创建者查找检测器。可按以下内容过滤检测器：

- 创建或导入自定义检测器的任何个别用户
- 思科代表所有思科提供的检测器，单独导入的附加检测器除外（您是自己导入的任何检测器的作者）
- **任何用户 (Any User)**，代表非思科提供的所有检测器

省/自治区

根据检测器的状态（即 **Active** 或 **nactive**）查找检测器。

Type

根据检测器类型查找检测器，如应用检测器基础知识，第 1178 页中所述。

协议

根据检测器检查的流量协议查找检测器。

类别

根据分配至所检测应用的类别查找检测器。

标签

根据分配至所检测应用的标记查找检测器。

风险

根据分配至所检测应用的风险查找检测器：**Very High**、**High**、**Medium**、**Low** 和 **Very Low**。

业务相关性

根据分配至所检测应用的业务相关性查找检测器：**Very High**、**High**、**Medium**、**Low** 和 **Very Low**。

导航至其他检测器页面

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 如果要查看下一页，请点击右箭头图标 ( )。

步骤 3 如果要查看上一页，请点击左箭头图标 ( )。

步骤 4 如果要查看另一页，请键入页码并按 Enter 键。

步骤 5 如果要跳到最后一个页面，请点击右箭头图标 ( )。

步骤 6 如果要跳到第一个页面，请点击左箭头图标 ( )。

激活和停用检测器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

必须激活检测器，然后才能将其用于分析网络流量。默认情况下，思科提供的所有检测器均已激活。

可为每个端口激活多个应用检测器，以补充系统的检测能力。

在策略的访问控制规则中包含应用并部署策略时，如果该应用没有活动检测器，一个或多个检测器将会自动激活。类似地，在已部署策略中使用应用时，如果停用检测器会使该应用没有活动检测器，则不能停用检测器。

提示 为提高性能，请停用任何您不打算使用的应用协议、客户端或 Web 应用检测器。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击要激活或停用的检测器旁边的滑块。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

注释 其他检测器可能需要某些应用检测器。如果停用其中一个这些检测器，系统将显示警告来指示依赖该检测器的检测器也被禁用。

编辑自定义应用检测器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

使用以下程序修改自定义应用检测器。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击要修改的检测器旁边的编辑图标 ()。如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 对检测器进行更改，如配置自定义应用检测器，第 1186 页中所述。

步骤 4 根据检测器的状态，您具有以下保存选择：

- 要保存非活动检测器，请点击**保存 (Save)**。
- 要将非活动检测器另存为新的非活动检测器，请点击**另存为新项目 (Save as New)**。
- 要保存活动检测器并立即开始使用，请点击**保存并重新激活 (Save and Reactivate)**。
- 要将活动检测器另存为新的非活动检测器，请点击**另存为新项目 (Save as New)**。

删除检测器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

可以删除自定义检测器以及单独导入的由思科专业服务提供的附加检测器。不能删除思科提供的任何其他检测器，不过可以停用其中许多检测器。

注释 当检测器正在已部署的策略中使用时，不能删除该检测器。

过程

步骤 1 选择**策略 (Policies)** > **应用检测器 (Application Detectors)**。

步骤 2 点击要删除的检测器旁边的删除图标 ( )。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **OK**。

第 66 章

用户身份源

以下主题介绍 Firepower 系统用户身份源：

概述：用户身份源

Firepower 系统支持以下身份源：

- 非授权基于流量的检测收集用户感知的用户数据。如果要配置受管设备以检测 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录，请参阅基于流量的检测身份源，第 1204 页。
- 授权用户代理报告被动收集用户感知和用户控制的用户数据。如果要配置用户代理对用户登录和注销主机或使用 Active Directory 凭证进行身份验证的情况进行监控，请参阅用户代理身份源，第 1199 页。
- 授权身份服务引擎 *(ISE)* 报告被动收集用户感知和用户控制的用户数据。如果您具有 ISE 部署并要配置 ISE 对用户使用 Active Directory 域控制器 (DC） 凭证进行身份验证的情况进行监控，请参阅身份服务引擎 (ISE) 身份源，第 1201 页。
- 授权强制网络门户身份验证主动验证网络上的用户并收集用户感知和用户控制的用户数据。如果要将虚拟路由器配置为执行强制网络门户主动身份验证，请参阅强制网络门户主动身份验证身份源，第 1203 页。

这些身份源的数据存储在Firepower管理中心的用户数据库和用户活动数据库中。您可以配置Firepower管理中心服务器用户下载，以将新用户数据定期自动下载到您的数据库中。

有关 Firepower 系统中用户检测的详细信息，请参阅用户检测基础知识，第 1130 页。

对用户身份源问题进行故障排除

请参阅以下部分以了解对身份源问题进行故障排除的信息。有关其他相关故障排除信息，请参阅对领域和用户下载问题进行故障排除，第 1234 页和对用户控制进行故障排除，第 289 页。

用户代理

如果遇到用户代理连接问题，请参阅《《*Firepower* 用户代理配置指南》》。

如果遇到用户代理报告的用户数据的问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的用户代理用户的活动后，会从服务器检索其相关信息。在某些情况下，系统需要最多 60 分钟的时间从 Active Directory 服务器成功检索此信息。在数据检索成功之前，用户代理用户发现的活动**不**由访问控制规则处理，并且**不**显示在 Web 界面中。
- 如果您已配置 Firepower 管理中心高可用性且主要管理中心发生故障，则在故障切换期间，用户代理、ISE 或强制网络门户设备报告的所有登录均无法在 10 分钟的停机时间内进行识别，即使之前已发现用户并将其下载到 Firepower 管理中心也不例外。无法识别的用户在 Firepower 管理中心上记录为“未知”(Unknown) 用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

ISE

如果您遇到 ISE 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与 Firepower 系统成功集成。
- **FMC 服务器证书 (FMC Server Certificate)** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。
- ISE 设备上的时间必须与Firepower管理中心上的时间同步。如果设备不同步，系统可在非预期时间间隔时执行用户超时。
- 如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。
- 如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

如果遇到 ISE 报告的用户数据的问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。在某些情况下，系统需要最多 60 分钟的时间从 Active Directory 服务器成功检索此信息。在数据检索成功之前，ISE 用户发现的活动**不**由访问控制规则处理，并且**不**显示在 Web 界面中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- Firepower 管理中心不接收 ISE 访客服务用户的用户数据。

- 您的 ISE 版本和配置会影响您在 Firepower 系统中使用 ISE 的方式。有关详细信息，请参阅身份服务引擎 (ISE) 身份源，第 1201 页。
- 如果您已配置 Firepower 管理中心高可用性且主要管理中心发生故障，则在故障切换期间，用户代理、ISE 或强制网络门户设备报告的所有登录均无法在 10 分钟的停机时间内进行识别，即使之前已发现用户并将其下载到 Firepower 管理中心也不例外。无法识别的用户在 Firepower 管理中心上记录为“未知”(Unknown) 用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

强制网络门户

如果您遇到强制网络门户证问题，请检查以下事项：

- 强制网络门户上的时间必须与 Firepower 管理中心上的时间同步。
- 如果您已配置 Firepower 管理中心高可用性且主要管理中心发生故障，则在故障切换期间，用户代理、ISE 或强制网络门户设备报告的所有登录均无法在 10 分钟的停机时间内进行识别，即使之前已发现用户并将其下载到 Firepower 管理中心也不例外。无法识别的用户在 Firepower 管理中心上记录为“未知”(Unknown) 用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

用户代理身份源

用户代理是一种被动身份验证方法，并且是 Firepower 系统支持的授权身份源之一。与 Firepower 系统集成时，代理会在用户登录和注销主机或使用 Active Directory 凭证进行身份验证时对其进行监控。用户代理不报告失败的登录尝试。从用户代理获取的数据可用于用户感知和用户控制。您可在身份策略中调用被动身份验证。

安装和使用用户代理可让您执行用户控制；代理会将用户与其 IP 地址进行关联，从而允许触发具有用户条件的访问控制规则。您可以使用一个代理监控最多五个 Active Directory 服务器上的用户活动，并将加密数据发送到最多五个 Firepower 管理中心。

用户代理需要多步骤配置，包括以下内容：

- 已安装代理的计算机或服务器。
- Firepower 管理中心与已安装代理的计算机或 Active Directory 服务器之间的连接。
- 每个 Firepower 管理中心与受监控 Active Directory 服务器（配置为身份领域内的目录）之间的连接。

有关多步骤用户代理配置的详细信息以及服务器要求的全面介绍，请参阅《《*Firepower* 用户代理配置指南》》。

注释 请确保您的计算机或 Active Directory server 上的时间与 Firepower 管理中心上的时间同步。如果设备不同步，系统可在非预期时间间隔时执行用户超时。

Firepower管理中心连接不仅允许检索用户代理检测到的登录和注销用户的元数据，还可用于指定在访问控制规则中使用的用户和组。如果代理配置为排除特定用户名，那么这些用户名的登录数据不会报告给 Firepower 管理中心。用户代理数据存储在 Firepower 管理中心上的用户数据库和用户活动数据库中。

注释 代理无法向Firepower 管理中心发送以 $ 字符结尾的 Active Directory 用户名。如果您要监控这些用户，则必须移除最后的 $ 字符。

如果有多个用户使用远程会话登录主机，代理可能无法正常检测到该主机上的登录。有关如何防止此情况的信息，请参阅《《*Firepower* 用户代理配置指南》》。

配置用户代理连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/访问管理员/网络管理员

有关用户代理的详细信息，请参阅用户代理身份源，第 1199 页。

开始之前

- 如果您计划使用用户代理数据执行用户控制，请为用户代理连接配置并启用 Active Directory 领域，如创建领域，第 1235 页中所述。

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 选择**身份源 (Identity Sources)** 选项卡。

步骤 3 为**服务类型 (Service Type)** 选择**用户代理 (User Agent)** 以启用用户代理连接。

注释 要禁用连接，请选择**无 (None)**。

步骤 4 点击**添加新代理 (Add New Agent)** 按钮以添加新代理。

步骤 5 在**主机名 (Hostname)** 或**地址 (Address)** 中键入计划要安装代理的计算机的主机名或地址。必须使用 IPv4 地址；不能将 Firepower 管理中心配置为使用 IPv6 地址连接到用户代理。

步骤 6 点击 **Add**。

步骤 7 要删除连接，请点击删除图标 ( ) 并确认删除。

接下来的操作

- 继续设置用户代理，如《*Firepower* 用户代理配置指南》中所述。

身份服务引擎 (ISE) 身份源

可以将思科 ISE 部署与 Firepower 系统集成，以使用 ISE 进行被动身份验证。

ISE 是授权身份源。从 ISE 获取的所有用户身份数据都可在 Firepower 管理中心上用于用户感知。从 ISE 获取的有关通过 AD 域控制器进行了身份验证的用户的数据可用于用户控制。不能对通过 LDAP、RADIUS 或 RSA 域控制器进行身份验证的用户执行用户控制。

ISE 不报告 ISE 访客服务用户的失败登录尝试或活动。

Firepower 系统的此版本支持思科 ISE 版本 1.3。您的 ISE 版本和配置会影响您在 Firepower 系统中使用 ISE 的方式。例如：

- ISE 版本 1.3 不包括对启用 IPv6 的终端的支持。您无法在启用 IPv6 的终端上收集用户身份数据或执行补救。
- 如果将 ISE 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，根据领域或用户条件的访问控制规则可能无法按预期进行触发。

注释 请确保 ISE 服务器上的时间与 Firepower 管理中心上的时间同步。如果设备不同步，系统可在非预期时间间隔时执行用户超时。

配置 ISE 连接还会使用 ISE 属性数据填充 Firepower 管理中心数据库。ISE 属性可用于用户感知以及在规则条件中使用。

安全组标记 (SGT)

安全组标记 (SGT) 指定受信任网络中的流量源的权限。当用户在 TrustSec 或 ISE 中添加安全组时，安全组访问（思科 TrustSec 和思科 ISE 都具备的功能）会自动生成 SGT。然后，当数据包进入网络时，SGA 会应用 SGT 属性。您可以通过将 ISE 配置为身份源。

终端位置 (Endpoint Location)

“终端位置”(Endpoint Location) 属性是使用 ISE 对用户进行身份验证的网络设备的 IP 地址，如 ISE 所识别。

Endpoint Profile

“终端配置文件”(Endpoint Profile) 属性是用户的终端设备类型，如 ISE 所识别。

有关思科 ISE 产品的详细信息，请参阅《思科身份服务引擎管理员指南》。

ISE 配置字段

以下字段用于配置与 ISE 的连接。

主要和辅助主机名/IP 地址 (Primary and Secondary Host Name/IP Address)

主要和辅助（可选）ISE 服务器的主机名或 IP 地址。

pxGrid 服务器 CA (pxGrid Server CA)

pxGrid 框架的证书颁发机构。如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。

MNT 服务器 CA (MNT Server CA)

当执行批量下载时 ISE 证书的证书颁发机构。如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

FMC 服务器证书 (FMC Server Certificate)

当连接到 ISE 或执行批量下载时 Firepower 管理中心必须提供给 ISE 的证书和密钥。

注释 **FMC 服务器证书 (FMC Server Certificate)** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

ISE 网络过滤器 (ISE Network Filter)

一个可选过滤器，可以将其设置为限制 ISE 报告给 Firepower 管理中心的数据。如果提供网络过滤器，则 ISE 会报告来自该过滤器中的网络的数据。可通过以下方式指定过滤器：

- 将此字段留空以指定任意 (any) 值。
- 使用 CIDR 符号输入单一 IPv4 地址块。
- 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

注释 无论您的 ISE 是何版本，此版本的 Firepower 系统均不支持使用 IPv6 地址进行过滤。

配置 ISE 连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/访问管理员/网络管理员

有关ISE 的详细信息，请参阅身份服务引擎 (ISE) 身份源，第 1201 页和ISE 配置字段，第 1202 页。

开始之前

- 如果计划使用 ISE 数据实施用户控制，请配置并启用担任 pxGrid 角色的 ISE 服务器的领域，如创建领域，第 1235 页中所述。

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 选择**身份源 (Identity Sources)** 选项卡。

步骤 3 为**服务类型 (Service Type)** 选择**身份服务引擎 (Identity Services Engine)** 以启用 ISE 连接。

注释 要禁用连接，请选择**无 (None)**。

步骤 4 输入**主要主机名/IP 地址 (Primary Host Name/IP Address)** 以及**辅助主机名/IP 地址 (Secondary Host Name/IP Address)**（后者为可选）。

步骤 5 从 **pxGrid 服务器 CA (pxGrid Server CA)** 和 **MNT 服务器 CA (MNT Server CA)** 下拉列表中选择相应的证书颁发机构，然后从 **FMC 服务器证书 (FMC Server Certificate)** 下拉列表中选择相应的证书。

或者，点击添加图标 () 以即时创建受信任证书颁发机构对象或内部证书对象。

注释 **FMC 服务器证书 (FMC Server Certificate)** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

步骤 6 或者，使用 CIDR 块符号输入 **ISE 网络过滤器 (ISE Network Filter)**。

步骤 7 如果要测试连接，请点击**测试 (Test)**。

强制网络门户主动身份验证身份源

强制网络门户是 Firepower 系统支持的授权身份源之一。它是 Firepower 系统唯一支持的主动身份验证方法，其中用户可通过受管设备验证网络登录。您可以将强制网络门户配置为要求用户凭证，或者允许访客接入。在系统对强制网络门户用户进行身份验证后，会根据访问控制配置处理其用户流量。仅对 HTTP 和 HTTPS 流量执行主动身份验证。

强制网络门户还记录失败的身份验证尝试。如果尝试失败，则不会将新用户添加到数据库的用户列表中。强制网络门户报告的身份验证活动失败的用户活动类型是**身份验证失败的用户 (Failed Auth User)**。

从强制网络门户获取的身份验证数据可用于用户感知和用户控制。

在身份策略中配置和部署强制网络门户时，来自指定领域的用户会通过以下设备进行身份验证，以访问您的网络：

- 7000 和 8000 系列设备上的虚拟路由器
- 在透明模式下运行版本 9.5(2) 或更高版本的 ASA FirePOWER设备。

在身份策略中配置强制网络门户并在身份规则中进行调用（主动身份验证）。在访问控制策略中调用身份策略。有关详细信息，请参阅配置强制网络门户主动身份验证，第 1241 页。

只有配置了路由接口的设备能执行强制网络门户主动身份验证。如果您的访问控制策略引用的身份策略包含一个或多个强制网络门户身份规则，且您将策略部署在管理以下设备的 Firepower 管理中心：

- 配置路由接口的一个或多个设备，策略部署成功且路由接口执行主动身份验证。
- 未配置路由接口的专有设备，策略部署成功但匹配这些规则的流量中的用户被识别为“未知”(Unknown)。
- 一个或多个 NGIPSv 设备，策略部署失败。

请注意以下要求和限制：

- 系统每秒最多支持 20 次强制网络门户登录。
- 必须允许流量流向计划用于强制网络门户的设备的IP地址和端口。如果根据访问控制不允许目标通过，则无法使用强制网络门户对流量进行身份验证。
- 要对 HTTPS 流量执行强制网络门户主动身份验证，必须使用 SSL 策略解密来自要对其进行身份验证的用户的流量。您无法解密受管设备上强制网络门户用户的Web浏览器和强制网络门户后台守护程序之间的连接中的流量；此连接用于对强制网络门户用户进行身份验证。

基于流量的检测身份源

基于流量的检测是Firepower系统唯一支持的未授权身份源。进行配置后，受管设备会检测您指定的网络上的 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录。从基于流量的检测获取的数据仅可用于用户感知。与授权身份源不同，您可在网络发现策略中配置基于流量的检测，如配置基于流量的用户检测，第 1218 页中所述。

请注意以下限制：

- 基于流量的检测仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。受管设备无法检测使用协议（例如 SSL 或 TLS）的加密 LDAP 身份验证。
- 基于流量的检测只能检测使用 OSCAR 协议的 AIM 登录。无法检测使用 TOC2 的 AIM 登录。
- 基于流量的检测无法限制 SMTP 日志记录。这是因为未根据 SMTP 登录将用户添加到数据库；虽然系统会检测 SMTP 登录，这些登录不会被记录下来，除非数据库中包含已具有匹配邮件地址的用户。

基于流量的检测还会记录失败的登录尝试。如果登录尝试失败，不会将新用户添加到数据库的用户列表中。基于流量的检测功能检测到的登录失败活动的用户活动类型是**登录失败的用户 (Failed User Login)**。

注释 系统无法区分失败和成功的 HTTP 登录。要查看 HTTP 用户信息，您必须在基于流量的检测配置中启用**捕获登录失败尝试 (Capture Failed Login Attempts)**。

基于流量的检测数据

设备使用基于流量的检测功能检测到登录时，它会将以下信息发送到Firepower管理中心（这些信息将被记录为用户活动）：

- 识别出的登录用户名
- 登录时间
- 登录使用的 IP 地址，可能是用户的主机（用于 LDAP、POP3、IMAP 和 AIM 登录）、服务器（用于 HTTP、MDNS、FTP、SMTP 和 Oracle 登录）或会话发起方（用于 SIP 登录）的 IP 地址
- 用户的邮件地址（用于 POP3、IMAP 和 SMTP 登录）
- 检测到登录的设备名称

如果之前已检测到该用户，Firepower 管理中心会更新该用户的登录历史记录。请注意，Firepower 管理中心可以使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 用户 关联。举例来说，这意味着如果 Firepower 管理中心检测到新的 IMAP 登录，且 IMAP 登录中的邮件地址与某个现有 LDAP 用户的邮件地址匹配，则 IMAP 登录不会创建新用户，而是会更新该 LDAP 用户的历史记录。

如果之前从未检测到该用户，Firepower 管理中心会将该用户添加到用户数据库。唯一的 AIM、SIP 和Oracle登录始终会创建新用户记录，因为这些登录事件中没有Firepower管理中心可与其他登录类型关联的数据。

在以下情况下，Firepower 管理中心不会记录用户活动或用户身份：

- 网络发现策略被配置为忽略该登录类型。
- 受管设备检测到 SMTP 登录，但用户数据库不包含之前使用匹配的邮件地址检测到的 LDAP、POP3 或 IMAP 用户

用户数据将被添加到用户表中。

基于流量的检测策略

可以限制在其中发现用户活动的协议，以减少检测到的用户的总数，以便将重点放在可能提供最完整用户信息的用户。限制协议检测有助于最大程度地减少用户名混乱以及预留Firepower管理中心上的存储空间。

当选择基于流量的检测协议时，请注意以下事项：

- 如果通过协议（例如 AIM、POP3 和 IMAP）获取用户名，可能会由于承包商、访客及其他访客的网络访问而引入与组织无关的用户名。

- AIM、Oracle 和 SIP 登录可能会创建外来用户记录。之所以会发生这种情况，是因为这些登录类型没有与系统从 LDAP 服务器获取的任何用户元数据关联，也没有与受管设备会检测的其他类型登录中包含的任何信息关联。因此，Firepower 管理中心无法将这些用户与其他类型的用户关联。

用户下载

您可以配置领域以在 Firepower 管理中心和 LDAP 或 AD 服务器之间建立连接，从而检索检测到的某些用户的用户和用户组元数据：

- 由强制网络门户进行身份验证或由用户代理或 ISE 报告的 LDAP 和 AD 用户。这些元数据可用于用户感知和用户控制。
- 基于流量的检测功能检测到的 POP3 和 IMAP 用户登录（如果这些用户的邮箱地址与 LDAP 或 AD 用户相同）。这些元数据可用于用户感知。

您可将单个服务器连接配置为领域内的目录。您必须选择**下载用于访问控制的用户和用户组(Download users and user groups for access control)** 复选框以下载领域的用户和用户组数据并将其用于用户感知和用户控制。

Firepower 管理中心获取关于每个用户的以下信息和元数据：

- LDAP 用户名
- 名和姓
- 邮件地址
- department
- 电话号码

第 67 章

网络发现策略

以下主题介绍如何创建、配置和管理网络发现策略：

概述：网络发现策略

Firepower 管理中心上的网络发现策略控制系统如何收集有关组织网络资产以及哪些网段和端口受监控的数据。

在多域部署中，每个枝叶域具有独立的网络发现策略。网络发现策略规则和其他设置不能共享、继承或在域之间复制。只要创建新域，系统就会使用默认设置为新域创建网络发现策略。您必须将任何所需自定义应用于新策略。

策略中的发现规则指定 Firepower 系统监控哪些网络和端口来根据流量中的网络数据生成发现数据，以及指定策略部署到的区域。在规则中，您可以配置是否发现主机、应用和非管理用户。可以创建规则来将网络和区域排除在发现范围外。您可以从 NetFlow 导出器配置数据发现，并且限制在网络上发现了用户数据的流量的协议。

网络发现策略包含一个配置为从观察到的所有流量发现应用的默认规则。该规则不排除任何网络、区域或端口，未配置主机和用户发现，并且规则未配置为监控 NetFlow 导出器。当受管设备注册到 Firepower 管理中心时，此策略默认部署到任何受管设备。要开始收集主机或用户数据，必须添加或修改发现规则并将策略重新部署到设备。

如果要调整网络发现范围，可以创建其他发现规则，并修改或移除默认规则。

请记住，每个受管设备的访问控制策略都定义面向该设备允许的流量，以及因此可使用网络发现监控的流量。如果使用访问控制阻止某些流量，则系统无法检查主机、用户和应用活动的该流量。例如，如果访问控制策略阻止对社交网络应用的访问，则系统无法在这些应用上提供任何发现数据。

如果在发现规则中启用基于流量的用户检测，则可以通过使用一组应用协议的流量中的用户登录活动来检测非管理用户。如有需要，可以禁用用于所有规则的特定协议中的发现。禁用某些协议有助于避免达到与Firepower管理中心型号关联的用户限制，从而为来自其他协议的用户保留可用用户计数。

借助高级网络发现设置，可以管理记录哪些数据、如何存储发现数据、哪些危害表现 (IOC) 规则处于活动状态、哪些漏洞映射用于影响评估，以及如果源提供冲突发现数据将会发生什么情况。您还可以添加要监控的主机输入和 NetFlow 导出器的源。

网络发现自定义

Firepower系统收集的有关网络流量的信息对您最有价值，因为系统可以参考该信息来识别网络上最易受攻击和最重要的主机。

例如，如果网络上有多个运行自定义版本的 SuSE Linux 的设备，系统无法识别操作系统，因此无法将漏洞映射至主机。然而，知道系统拥有 SuSE Linux 的漏洞列表，您可能想要为某个主机创建自定义的指纹，以便随后可将该指纹用来识别运行相同操作系统的其他主机。可将 SuSE Linux 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

系统还允许使用主机输入功能，将来自第三方系统的主机数据直接输入至网络映射。然而，第三方操作系统或应用数据不会自动映射至漏洞信息。如果想要为使用第三方操作系统、服务器和应用协议数据的主机查看漏洞并执行影响关联，必须将来自第三方系统的供应商和版本信息映射至漏洞数据库 (VDB) 中列出的供应商和版本。您也可能想要持续维护主机输入数据。请注意，即使将应用数据映射到 Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

如果系统无法识别网络主机上运行的应用协议，则可创建用户定义的应用协议检测器以便系统根据端口或模式识别应用。您还可以导入、激活和停用某些应用检测器，以便进一步自定义Firepower系统的应用检测功能。

还可使用 Nmap 主动扫描器的扫描结果替换操作系统和应用数据的检测，或者使用第三方漏洞来扩充漏洞列表。系统可以协调来自多个源的数据，从而确定应用的标识。

配置网络发现策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

在多域部署中，每个域具有独立的网络发现策略。如果用户帐户可以管理多个域，请切换至要配置策略的枝叶域。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 配置策略的以下组件：

- 发现规则 - 请参阅配置网络发现规则，第 1209 页。
- 基于流量的用户检测 - 请参阅配置基于流量的用户检测，第 1218 页。
- 高级网络发现选项 - 请参阅配置高级网络发现选项，第 1218 页。
- 自定义操作系统定义（指纹）- 请参阅指纹识别客户端，第 1141 页和指纹识别服务器，第 1143 页。

网络发现规则

通过网络发现规则，您可以将为网络映射发现的信息定制为仅包含所需的特定数据。网络发现策略中的规则按顺序接受评估。您可以使用重叠的监控条件创建规则，但这样做可能会影响系统性能。

将主机或网络排除在监控范围外之后，被排除的主机或网络将不会显示在网络映射中，系统也不会为其报告事件。思科建议将负载均衡器（或负载均衡器上的特定端口）和NAT设备排除在监控范围外。这些设备可能会创建过量并有误导性的事件，从而填充数据库并使Firepower管理中心过载。例如，受监控的NAT设备可能会在短时间内显示其操作系统的多个更新。如果知道负载均衡器和NAT设备的 IP 地址，可以将它们排除在监控范围外。

提示 系统可通过检查网络流量识别许多负载均衡器和 NAT 设备。

此外，如果需要创建自定义服务器指纹，应暂时禁止监控用于与正在创建指纹的主机通信的 IP 地址。否则，网络映射和发现事件视图中将会出现大量关于该IP地址代表的主机的不准确信息。创建指纹后，可以配置策略，以便再次监控该 IP 地址。

思科还建议不监控NetFlow导出器和Firepower系统受管设备的相同网段。尽管在理想情况下应使用不重叠的规则来配置网络发现政策，但系统不会丢弃受管设备生成的重复连接日志。但是，不能丢弃受管设备和 NetFlow 导出器均检测到的连接的重复连接日志。

配置网络发现规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

可以配置发现规则，以根据自身需求定制主机和应用数据的发现。

开始之前

- 确保正在为要在其中发现网络数据的流量记录连接；请参阅连接日志记录策略，第 1502 页。

- 如果要收集导出的NetFlow记录，请按照将 NetFlow 导出器添加到网络发现策略，第 1224 页中所述添加 NetFlow Exporter。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Add Rule**（**添加规则**）。

步骤 3 如操作和发现的资产，第 1210 页中所述，为规则设置**操作 (Action)**。

步骤 4 设置可选的发现参数：

- 将规则操作限定于特定网络；请参阅限制受监控网络，第 1211 页。
- 将规则操作限定于特定区域中的流量；请参阅配置网络发现规则中的区域，第 1216 页。
- 将端口排除在监控范围外；请参阅排除网络发现规则中的端口，第 1214 页。
- 为 NetFlow 数据发现配置规则；请参阅配置用于 NetFlow 数据发现的规则，第 1212 页。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

操作和发现的资产

配置发现规则时，必须为规则选择操作。规则操作的影响取决于规则是用于从受管设备还是NetFlow导出器发现数据。

下表说明了规则使用这两种方案中指定的操作设置发现的资产。

表 *198*：发现规则操作

	受管设备	NetFlow 导出器
排除	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。
发现：主机	根据发现事件将主机添加到网络映射。（可选操作；如果启用了用户发现，则为必要操作。）	根据NetFlow记录将主机添加到网络映射并记录连接。（必要操作）

	受管设备	NetFlow 导出器
发现：应用	根据应用检测程序将应用添加到网络映射。请注意，在没有发现应用的情况下，无法发现规则中的主机或用户。（必要操作）	根据 NetFlow 记录和 `/etc/sf/services` 中的端口应用协议关联将应用协议添加到网络映射。（可选）
发现：用户	将用户添加到用户表，并根据对网络发现策略中配置的用户协议进行的基于流量的检测记录用户活动。（可选）	n/a
记录 NetFlow 连接	n/a	仅记录 NetFlow 连接。不发现主机或应用。

如果要让规则监控受管设备流量，则应用日志记录为必要操作。如果要让规则监控用户，则主机日志记录为必要操作。如果要让规则监控导出的 NetFlow 记录，则您无法将其配置为记录用户，并且记录应用为可选操作。

注释 系统根据网络发现策略中的**操作 (Action)** 设置检测 NetFlow 记录中的连接。系统根据访问控制策略设置检测受管设备中的连接。

受监控网络

发现规则仅用于发现指定网络上主机收到和发出的流量中的受监控资产。对于发现规则，会为符合以下条件的连接执行发现：在指定的网络中至少有一个 IP 地址；且只为要监控的网络中的 IP 地址生成事件。默认发现规则从所有观察到的流量中发现应用（`0.0.0.0/0` 表示所有 IPv4 流量，`::/0` 表示所有 IPv6 流量）。

如果将规则配置为处理 NetFlow 发现并仅记录连接数据，则系统还会记录发向和来自指定网络中 IP 地址的连接。请注意，网络发现规则提供记录 NetFlow 网络连接的唯一方法。

也可以使用网络对象或对象组指定要监控的网络。

限制受监控网络

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

每个发现规则必须至少包含一个网络。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Add Rule**（添加规则）。

步骤 3 如果**网络 (Networks)** 选项卡还未打开，请点击该选项卡。

步骤 4 或者，将网络对象添加到“可用网络”(Available Networks) 列表，如在配置发现规则期间创建网络对象，第 1213 页中所述。

注释 如果修改网络发现策略中使用的网络对象，则更改对于发现不会生效，直至部署配置更改为止。

步骤 5 指定网络：

- 从**可用网络 (Available Networks)** 列表中选择网络。

  提示 如果网络没有立即显示在列表中，请点击重新加载图标 ()。

- 将 IP 地址输入到“可用网络”(Available Networks) 标签下方的文本框中。

步骤 6 点击 **Add**。

步骤 7 或者，重复前两个步骤以添加其他网络。

步骤 8 点击**保存 (Save)** 以保存所做的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置用于 *NetFlow* 数据发现的规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

Firepower 系统可以使用来自 NetFlow 导出器的数据生成连接和发现事件，并将主机和应用数据添加到网络映射。

如果选择某个发现规则中的 NetFlow 导出器，该规则将被限制为为指定网络发现 NetFlow 数据。应先选择要监控的 NetFlow 设备，然后再配置规则行为的其他方面，因为在选择 NetFlow 设备时可用规则操作会变化。不能为监控 NetFlow 导出器配置端口排除。

开始之前

- 将支持 NetFlow 的设备添加到网络发现策略；请参阅将 NetFlow 导出器添加到网络发现策略，第 1224 页。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。

在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Add Rule**（添加规则）。

步骤 3 选择 **NetFlow 设备 (NetFlow Device)** 选项卡。

步骤 4 从 **NetFlow 设备 (NetFlow Device)** 下拉列表中，选择要监控的 NetFlow 导出器的 IP 地址。

步骤 5 指定要让 Firepower 系统受管设备收集的 NetFlow 数据类型：

- 仅连接 - 从操作 (Action) 下拉列表中选择 **Log NetFlow Connections**。
- 主机、应用和连接 - 从操作 (Action) 下拉列表中选择 **Discover**。系统会自动选中**主机 (Hosts)** 复选框并启用连接数据的收集。或者，可以选中**应用 (Application)** 复选框以收集应用数据。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

在配置发现规则期间创建网络对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

将新的网络对象添加到可重用网络对象和组列表中，即可将其添加到发现规则中显示的可用网络列表中。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 在**网络 (Networks)** 选项卡中，点击**添加规则 (Add Rule)**。

步骤 3 点击**可用网络 (Available Networks)** 旁边的添加图标 ()。

步骤 4 按照创建网络对象，第 306 页中所述创建网络对象。

步骤 5 按照配置网络发现规则，第 1209 页中所述完成添加网络发现规则。

端口排除

可以将特定端口排除在监控范围外，就像将主机排除在监控范围外一样。例如：

- 负载均衡器可在短时间内报告同一端口上的多个应用。可以配置网络发现规则，以便将该端口排除在监控范围外，例如排除处理 Web 场的负载均衡器上的端口 80。

- 组织可以使用采用特定端口范围的自定义客户端。如果来自该客户端的流量生成过多有误导性的事件，可以排除对这些端口的监控。同样，可以决定是否要监控DNS流量。在这种情况下，可以配置规则，使发现策略不监控端口 53。

添加要排除的端口时，可以决定是使用Available Ports列表中的可重用端口对象，将端口直接添加到源或目标排除列表，还是创建新的可重用端口然后将其移至排除列表。

注释 不能排除处理 NetFlow 数据发现的规则中的端口。

排除网络发现规则中的端口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

不能排除处理 NetFlow 数据发现的规则中的端口。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Add Rule**（添加规则）。

步骤 3 点击**端口排除 (Port Exclusions)** 选项卡。

步骤 4 或者，将端口对象添加到“可用端口”(Available Ports) 列表，如在配置发现规则期间创建端口对象，第 1215 页中所述。

步骤 5 使用以下任一方法将特定源端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到源 (Add to Source)**。
- 要排除来自特定源端口的流量而不添加端口对象，请在**所选源端口 (Selected Source Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号（从 1 到 65535 的值），然后点击**添加 (Add)**。

步骤 6 使用以下任一方法将特定目标端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到目标 (Add to Destination)**。
- 要排除来自特定目标端口的流量而不添加端口对象，请在**所选目标端口 (Selected Destination Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号，然后点击**添加 (Add)**。

步骤 7 点击**保存 (Save)** 以保存所做的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

在配置发现规则期间创建端口对象

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

将新的端口对象添加到可在 Firepower 系统中任意位置使用的可重用端口对象和对象组列表，即可将其添加到发现规则中显示的可用端口列表中。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 在“网络”(Networks) 选项卡中，点击**添加规则 (Add Rule)**。

步骤 3 点击 **Port Exclusions**。

步骤 4 要将端口添加到 Available Ports 列表，请点击添加对象图标 ( )。

步骤 5 提供**名称 (Name)**。

步骤 6 在 **Protocol** 字段中，指定要排除的流量协议。

步骤 7 在**端口 (Port)** 字段中，输入要排除在监控范围外的端口。
可以指定单个端口、用破折线 (-) 分隔的一系列端口或者用逗号分隔的端口和端口范围列表。允许的端口值介于 1 到 65535 之间。

步骤 8 点击**保存 (Save)**。

步骤 9 如果添加的端口没有立即显示在列表中，请点击刷新图标 ( )。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

网络发现规则中的区域

要提高性能，可以配置发现规则，以便规则中的区域包含物理连接到规则中的待监控网络的受管设备上的传感接口。

但是，系统可能并不总是告知您网络配置的更改情况。网络管理员可以通过路由或主机更改修改网络配置而无需告知您，这可能会导致您难以随时了解正确的网络发现策略配置。如果您不知道受管设备上的传感接口如何物理连接到您的网络，请将区域配置保留为默认设置。此默认设置会导致系

统将发现规则部署到您的部署中的所有区域。（如果未排除任何区域，则系统会将发现策略部署到所有区域。）

配置网络发现规则中的区域

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Add Rule**（添加规则）。

步骤 3 点击**区域 (Zones)** 选项卡。

步骤 4 从**可用区域 (Available Zones)** 列表中选择一个或多个区域。

步骤 5 点击**保存 (Save)** 以保存所做的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

基于流量的检测身份源

基于流量的检测是 Firepower 系统唯一支持的未授权身份源。进行配置后，受管设备会检测您指定的网络上的 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录。从基于流量的检测获取的数据仅可用于用户感知。与授权身份源不同，您可在网络发现策略中配置基于流量的检测，如配置基于流量的用户检测，第 1218 页中所述。

请注意以下限制：

- 基于流量的检测仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。受管设备无法检测使用协议（例如 SSL 或 TLS）的加密 LDAP 身份验证。
- 基于流量的检测只能检测使用 OSCAR 协议的 AIM 登录。无法检测使用 TOC2 的 AIM 登录。
- 基于流量的检测无法限制 SMTP 日志记录。这是因为未根据 SMTP 登录将用户添加到数据库；虽然系统会检测 SMTP 登录，这些登录不会被记录下来，除非数据库中包含已具有匹配邮件地址的用户。

基于流量的检测还会记录失败的登录尝试。如果登录尝试失败，不会将新用户添加到数据库的用户列表中。基于流量的检测功能检测到的登录失败活动的用户活动类型是**登录失败的用户 (Failed User Login)**。

注释 系统无法区分失败和成功的 HTTP 登录。要查看 HTTP 用户信息，您必须在基于流量的检测配置中启用**捕获登录失败尝试 (Capture Failed Login Attempts)**。

基于流量的检测数据

设备使用基于流量的检测功能检测到登录时，它会将以下信息发送到Firepower管理中心（这些信息将被记录为用户活动）：

- 识别出的登录用户名
- 登录时间
- 登录使用的 IP 地址，可能是用户的主机（用于 LDAP、POP3、IMAP 和 AIM 登录）、服务器（用于 HTTP、MDNS、FTP、SMTP 和 Oracle 登录）或会话发起方（用于 SIP 登录）的 IP 地址
- 用户的邮件地址（用于 POP3、IMAP 和 SMTP 登录）
- 检测到登录的设备名称

如果之前已检测到该用户，Firepower 管理中心会更新该用户的登录历史记录。请注意，Firepower 管理中心可以使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 用户 关联。举例来说，这意味着如果 Firepower 管理中心检测到新的 IMAP 登录，且 IMAP 登录中的邮件地址与某个现有 LDAP 用户的邮件地址匹配，则 IMAP 登录不会创建新用户，而是会更新该 LDAP 用户的历史记录。

如果之前从未检测到该用户，Firepower 管理中心会将该用户添加到用户数据库。唯一的 AIM、SIP 和Oracle登录始终会创建新用户记录，因为这些登录事件中没有Firepower管理中心可与其他登录类型关联的数据。

在以下情况下，Firepower 管理中心**不**会记录用户活动或用户身份：

- 网络发现策略被配置为忽略该登录类型。
- 受管设备检测到 SMTP 登录，但用户数据库不包含之前使用匹配的邮件地址检测到的 LDAP、POP3 或 IMAP 用户

用户数据将被添加到用户表中。

基于流量的检测策略

可以限制在其中发现用户活动的协议，以减少检测到的用户的总数，以便将重点放在可能提供最完整用户信息的用户。限制协议检测有助于最大程度地减少用户名混乱以及预留Firepower管理中心上的存储空间。

当选择基于流量的检测协议时，请注意以下事项：

- 如果通过协议（例如 AIM、POP3 和 IMAP）获取用户名，可能会由于承包商、访客及其他访客的网络访问而引入与组织无关的用户名。

- AIM、Oracle 和 SIP 登录可能会创建外来用户记录。之所以会发生这种情况，是因为这些登录类型没有与系统从 LDAP 服务器获取的任何用户元数据关联，也没有与受管设备会检测的其他类型登录中包含的任何信息关联。因此，Firepower 管理中心无法将这些用户与其他类型的用户关联。

配置基于流量的用户检测

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

在网络发现规则中启用基于流量的用户检测时，将会自动启用主机发现。有关基于流量的检测的详细信息，请参阅基于流量的检测身份源，第 1204 页。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 单击“**用户**”。

步骤 3 点击编辑图标 ( )。

步骤 4 选中要检测登录的协议的复选框，或取消选中不希望检测登录的协议的复选框。

步骤 5 或者，要记录在 LDAP、POP3、FTP 或 IMAP 流量中检测的失败登录尝试，或捕获 HTTP 登录的用户信息，请启用 **Capture Failed Login Attempts**。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 配置网络发现规则以发现用户，如配置网络发现规则，第 1209 页中所述。
- 部署配置更改；请参阅部署配置更改，第 254 页。

配置高级网络发现选项

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

可以使用网络发现策略的 Advanced 选项卡来配置策略范围的设置，以指定要检测的事件、发现数据的保留时间长度和更新频率、用于影响关联的漏洞映射，以及如何解决操作系统和服务器身份冲突。此外，还可以添加主机输入源和 NetFlow 导出器，以允许从其他源导入数据。

注释 发现和用户活动事件的数据库事件限制是在系统配置中设置。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击要修改的设置旁边的编辑图标 ( ) 或添加图标 ( ):

- “数据存储设置”(Data Storage Settings) - 更新设置，如配置网络发现数据存储，第 1226 页中所述。
- “事件日志记录设置”(Event Logging Settings) - 更新设置，如配置网络发现事件日志记录，第 1226 页中所述。
- “常规设置”(General Settings) - 更新设置，如配置网络发现常规设置，第 1220 页中所述。
- “身份冲突设置”(Identity Conflict Settings) - 更新设置，如配置网络发现身份冲突解决方法，第 1221 页中所述。
- “危害表现设置”(Indications of Compromise Settings) - 更新设置，如启用危害表现规则，第 1223 页中所述。
- “NetFlow 导出器”(NetFlow Exporters) - 更新设置，如将 NetFlow 导出器添加到网络发现策略，第 1224 页中所述。
- “操作系统和服务器身份源”(OS and Server Identity Sources) - 更新设置，如添加网络发现操作系统和服务器身份源，第 1227 页中所述。
- “用于影响评估的漏洞”(Vulnerabilities to use for Impact Assessment) - 更新设置，如启用网络发现漏洞影响评估，第 1222 页中所述。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

网络发现常规设置

常规设置控制系统更新网络映射的频率以及是否在发现过程中捕获服务器横幅。

Capture Banners

如果希望系统存储来自播发服务器供应商和版本的网络流量的报头信息（“横幅”），请选中此复选框。这些信息可提供有关收集的信息的其他上下文。可以通过访问服务器详细信息来访问为主机收集的服务器横幅。

更新间隔

系统更新信息（例如，上一次显示任何主机的 IP 地址的时间、使用应用的时间或应用的点击次数）的时间间隔。默认设置为 3600 秒（1 小时）。

请注意，为更新超时设置较小的时间间隔可在主机显示中提供更准确的信息，但会生成更多网络事件。

配置网络发现常规设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **General Settings** 旁的编辑图标 ( )。

步骤 4 更新设置，如网络发现常规设置，第 1219 页中所述。

步骤 5 点击**保存 (Save)** 以保存常规设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

网络发现身份冲突设置

系统通过将操作系统和服务器的指纹与流量模式进行匹配，从而确定在主机上运行的操作系统和应用。为了提供最可靠的操作系统和服务器身份信息，系统会核对来自多个源的指纹信息。

系统使用所有被动数据来推导操作系统身份并分配置信度值。

默认情况下，除非存在身份冲突，否则由扫描工具或第三方应用添加的身份数据会覆盖 Firepower 系统检测到的身份数据。可以使用 Identity Sources 设置按优先级对扫描程序和第三方应用指纹源进行评级。系统为每个源保留一个身份，但只有优先级最高的第三方应用或扫描程序源中的数据可用作当前身份。但请注意，用户输入数据会覆盖扫描程序和第三方应用数据，无论后者的优先级如何。

身份冲突是指系统检测到某个身份与来自“身份源”(Identity Sources) 设置中列出的活动扫描工具或第三方应用源或者来自 Firepower 系统用户的现有身份相冲突。默认情况下，身份冲突不会自动解决，必须通过主机配置文件，或者通过重新扫描主机或重新添加新的身份数据覆盖被动身份来解决冲突。但是，可以将系统设置为通过保留被动身份或主动身份来自动解决冲突。

Generate Identity Conflict Event

指定在发生身份冲突时系统是否生成事件。

Automatically Resolve Conflicts

从**自动解决冲突 (Automatically Resolve Conflicts)** 下拉列表中，选择以下选项之一：

- **已禁用 (Disabled)**，如果要强制手动解决身份冲突
- **身份 (Identity)**，如果要在发生身份冲突时让系统使用被动指纹
- **保留主动身份 (Keep Active)**，如果要在发生身份冲突时让系统使用来自最高优先级主动源的当前身份

配置网络发现身份冲突解决方法

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **Identity Conflict Settings** 旁边的编辑图标 ( )。

步骤 4 更新“编辑身份冲突设置”(Edit Identity Conflict Settings) 弹出窗口中的设置，如网络发现身份冲突设置，第 1220 页中所述。

步骤 5 点击**保存 (Save)** 以保存身份冲突设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

网络发现漏洞影响评估选项

可以配置 Firepower 系统如何对入侵事件执行关联影响。您具有以下选择：

- 如果要使用基于系统的漏洞信息执行影响关联，请选中**使用网络发现漏洞映射 (Use Network Discovery Vulnerability Mappings)** 复选框。
- 如果要使用第三方漏洞参考执行影响关联，请选中**使用第三方漏洞映射 (Use Third-Party Vulnerability Mappings)** 复选框。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

可以同时选中这两个复选框或选中其中之一。如果系统生成入侵事件，且该事件涉及的主机所拥有的服务器或操作系统包含所选漏洞映射集中的漏洞，则该入侵事件将带有 Vulnerable（级别 1：红色）影响图标。对于没有供应商或版本信息的任何服务器，需要在 Firepower 管理中心配置中启用漏洞映射。

如果取消选中这两个复选框，入侵事件将**不会**带有 Vulnerable（级别 1：红色）影响图标。

启用网络发现漏洞影响评估

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **Vulnerabilities to use for Impact Assessment** 旁边的编辑图标 ( )。

步骤 4 更新“编辑漏洞设置”(Edit Vulnerability Settings) 弹出窗口中的设置，如网络发现漏洞影响评估选项，第 1221 页中所述。

步骤 5 点击**保存 (Save)** 保存漏洞设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

危害表现

Firepower 系统使用网络发现策略中的 IOC 规则，以确定主机是否可能被恶意手段损害。当主机满足这些系统提供的规则中指定的条件时，系统将使用危害表现 (IOC) 进行标记。相关规则被称为 *IOC* 规则。每条 IOC 规则对应于一种类型的 IOC 标记。*IOC* 标记用于指定可能发生的危害的性质。

当发生以下情况时，Firepower 管理中心可以标记涉及的主机：

- 通过使用入侵、连接、安全情报和文件或恶意软件事件，系统将收集到的关于受监控网络及其流量的数据相关联，并确定潜在 IOC 已发生。

- Firepower 管理中心可通过 AMP 云从面向终端的 AMP 部署导入 IOC 数据。由于这些数据检查主机本身上的活动（例如，单个程序执行的操作），因此，通过这些数据可了解到纯网络数据无法洞察到的可能威胁。为了方便起见，Firepower 管理中心会自动获取思科从 AMP 云开发的任何新 IOC 标记。

要配置此功能，请参阅启用危害表现规则，第 1223 页。

您还可以针对主机 IOC 数据和合规规则（决定 IOC 标记的主机）写入关联规则。

要调查和使用标记的危害表现，请参阅危害表现数据，第 1664 页及其子主题。

启用危害表现规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

要使系统检测和标记危害表现 (IOC)，必须先在网络发现策略中至少激活一个 IOC 规则。每个 IOC 规则对应于一种类型的 IOC 标记，所有 IOC 规则均由思科预定义；您不能创建原始规则。可根据网络和组织需要启用任何或全部规则。例如，如果使用诸如 Microsoft Excel 等软件的主机从未出现在监控网络上，可决定不启用与基于 Excel 的威胁相关的 IOC 。

提示 要禁用个别主机的 IOC 规则，请参阅编辑单台主机的危害表现规则状态，第 1667 页。

开始之前

由于 IOC 规则根据 Firepower 系统的其他组件以及面向终端的 AMP 提供的数据触发，因此必须为要设置 IOC 标记的 IOC 规则正确许可并配置这些组件。启用与您将启用的 IOC 规则相关联的 Firepower 系统功能，例如入侵检测和防御 (IPS) 及高级恶意软件防护 (AMP)。如果未启用 IOC 规则的关联功能，将不会收集相关数据，规则也将无法触发。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **Indications of Compromise Settings** 旁边的编辑图标 ( )。

步骤 4 要关闭或关闭整个 IOC 功能，请点击 **Enable IOC** 旁边的滑块。

步骤 5 要全局启用或禁用个别 IOC 规则，请点击相应规则的**启用 (Enabled)** 列中的滑块。

步骤 6 点击**保存 (Save)** 以保存 IOC 规则设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改， 第 254 页。

将 NetFlow 导出器添加到网络发现策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

开始之前

- 配置计划使用的 NetFlow 导出器，如Firepower 系统中的 Netflow 数据， 第 1127 页中所述。
- 审核其他 NetFlow 必备条件，如使用 NetFlow 数据的要求， 第 1128 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **NetFlow 设备 (NetFlow Devices)** 旁边的添加图标 ( )。

步骤 4 在 **IP 地址 (IP Address)** 字段中，输入要使受管设备从中收集 NetFlow 数据的网络设备的 IP 地址。

步骤 5 或者：

- 重复前两个步骤以添加其他 NetFlow 导出器。
- 通过点击删除图标 ( ) 删除 NetFlow 导出器。请记住，如果在发现规则中使用 NetFlow 导出器，必须先删除该规则，然后才能从“高级”(Advanced) 页面中删除设备。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 配置网络发现规则以监控 NetFlow 流量，如配置网络发现规则， 第 1209 页中所述。
- 部署配置更改；请参阅部署配置更改， 第 254 页。

网络发现数据存储设置

发现数据存储设置包括主机限制和超时设置。

When Host Limit Reached

Firepower管理中心可以监控因而存储在网络映射中的主机数取决于其型号。**当达到主机限制时 (When Host Limit Reached)** 选项控制在达到主机限制后检测到新主机时发生的情况。您可以执行以下操作：

丢弃主机

系统丢弃保持非活动状态时间最长的主机，然后添加新主机。这是默认设置。

不插入新主机

系统不跟踪任何新发现的主机。系统仅在主机计数降至低于限制后跟踪新主机，例如，在管理员增大域的主机限制或从网络映射中手动删除主机后，或者，如果系统因主机不活动而将其识别为已超时。

在多域部署中，枝叶域共享受监控主机的可用池。要确保每个枝叶域都可以填充其网络映射，可以在域的属性中的任何子域级别设置主机限制。由于每个枝叶域具有各自的网络发现策略，因此在系统发现新主机时，每个枝叶域会监管各自的行为，如下表所述。

表 *199*：达到多租户的主机限制

设置	已设置域主机限制？	已达到域主机限制	已达到祖先域主机限制
丢弃主机	yes	丢弃受限制域中的最旧主机。	丢弃配置为丢弃主机的所有后代枝叶域中的最旧主机。 如果无法丢弃任何主机，则不添加主机。
	否	n/a	丢弃配置为丢弃主机以及共享常规池的所有后代枝叶域中的最旧主机。
不插入新主机	是/否	不添加主机。	不添加主机。

Host Timeout

系统在网络映射丢弃进入非活动状态的来自网络映射主机前允许它们存在的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。单个主机 IP 和 MAC 地址可以单独超时，但是，除非主机的所有关联地址都超时，否则该主机不会从网络映射中消失。

要避免主机提前超时，请确保主机超时值大于网络发现策略常规设置中的更新间隔。

Server Timeout

系统在丢弃进入非活动状态的服务器前允许它们存在的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

要避免服务器提前超时，请确保服务超时值大于网络发现策略常规设置中的更新间隔。

Client Application Timeout

系统在丢弃进入非活动状态的客户端前允许它们存在的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

确保客户端超时值大于网络发现策略常规设置中的更新间隔。

配置网络发现数据存储

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **Data Storage Settings** 旁边的编辑图标 ( )。

步骤 4 更新“数据存储设置”(Data Storage Settings) 对话框中的设置，如网络发现数据存储设置，第 1224 页中所述。

步骤 5 点击**保存 (Save)** 以保存数据存储设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

配置网络发现事件日志记录

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

事件日志记录设置控制是否记录发现和主机输入事件。如果不记录事件，将无法在事件视图中检索事件，也不能将事件用于触发关联规则。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **Event Logging Settings** 旁边的编辑图标 ( )。

步骤 4 选中或取消选中要在数据库中记录的发现和主机输入事件类型旁边的复选框，如发现事件类型，第 1650 页和主机输入事件类型，第 1653 页中所述。

步骤 5 点击**保存 (Save)** 以保存事件日志记录设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加网络发现操作系统和服务器身份源

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

在网络发现策略的“高级”(Advanced) 选项卡中，可以添加新的主动源，或更改现有源的优先级或超时设置。

将扫描工具添加到此页面不会添加 Nmap 扫描工具已有的完整集成功能，但允许集成导入的第三方应用或扫描结果。

如果从第三方应用或扫描工具导入数据，请确保将源中的漏洞映射到网络中检测到的漏洞。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击 **Advanced**。

步骤 3 点击 **OS and Server Identity Sources** 旁边的编辑图标 ( )。

步骤 4 要添加新源，请点击 **Add Source**。

步骤 5 输入 **Name**。

步骤 6 从下拉列表中选择输入源**类型 (Type)**：

- 如果打算使用 AddScanResult 函数导入扫描结果，请选择**扫描工具 (Scanner)**。
- 如果不打算导入扫描结果，请选择**应用 (Application)**。

步骤 7 要指示从此源将某个身份添加到网络映射到删除该身份之间的持续时间，请从**超时 (Timeout)** 下拉列表中选择**小时数 (Hours)**、**天数 (Days)** 或**周数 (Weeks)**，并输入适当的持续时间。

步骤 8 或者：

- 要升级某个源并使用操作系统和应用身份以支持列表中该源下面的源，请选择该源并点击向上箭头。
- 要降级某个源并且只有列表中该源上面的源没有提供身份时才会使用操作系统和应用身份，请选择改源并点击向下箭头。
- 要删除某个源，请点击该源旁边的删除图标 ( )。

步骤 9 点击**保存 (Save)** 以保存身份源设置。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

对网络发现策略进行故障排除

在对系统的默认检测功能进行任何更改之前，应分析哪些主机未被正确地识别以及原因，以便可以决定实施哪些解决方案。

受管设备是否正确布置？

如果诸如负载均衡器、代理服务器或NAT 设备的网络设备位于受管设备和未识别或错误识别的主机之间，请将受管设备布置在更靠近错误识别的主机的位置，而不是使用自定义指纹技术。思科不建议在这种情况下使用自定义指纹技术。

未识别的操作系统是否拥有唯一的 TCP 堆栈？

如果系统错误地识别主机，应调查主机为何被错误地识别，以便帮助您做出以下决择：是创建和激活自定义指纹，还是用 Nmap 或主机输入数据替代发现数据。

注意 如果遇到错误识别的主机，请在创建自定义指纹之前联系支持代表。

如果主机正在运行的操作系统未被系统默认检测到而且不与已检测的现有操作系统共享识别性 TCP 堆栈特征，应创建自定义指纹。

例如，如您拥有的 Linux 自定义版本带有系统无法识别的唯一 TCP 堆栈，则创建自定义指纹将让您受益，因为，这可使系统识别并继续监控主机，而不必使用扫描结果或第三方数据，进而无需持续自行主动更新数据。

请注意，许多开源 Linux 发行版本使用相同的内核，同样，系统将使用 Linux 内核名称来识别它们。如为 Red Hat Linux 系统创建自定义指纹，可能会看到识别为 Red Hat Linux 的其他操作系统（如 Debian Linux、Mandrake Linux、Knoppix 等），因为相同的指纹与多个 Linux 发行版本匹配。

不应在每种情况下都使用指纹。例如，可能对主机的 TCP 堆栈做出了修改，以使其与另一操作系统类似或相同。例如，Apple Mac OS X 主机已修改，使其指纹与 Linux 2.4 主机相同，从而导致系统将其识别为 Linux 2.4 而不是 Mac OS X。如果为 Mac OS X 主机创建自定义指纹，可能会导致所有合法

的 Linux 2.4 主机被错误地识别为 Mac OS X 主机。在这种情况下，如果 Nmap 正确地识别主机，应为该主机安排定期的 Nmap 扫描。

如果使用主机输入从第三方系统导入数据，则必须将第三方用于描述服务器和应用协议的供应商、产品和版本字符串映射到这些产品的思科定义。请注意，即使将应用数据映射到Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

系统可以协调来自多个源的数据，以便确定操作系统或应用的当前标识。

对于 Nmap 数据，可安排定期 Nmap 扫描。对于主机输入数据，可定期运行用于导入的 Perl 脚本或命令行实用程序。然而，请注意，主动扫描数据和主机输入数据可能不会随发现数据的频率进行更新。

Firepower 系统能否识别所有应用？

如果主机已由系统正确识别，但有未识别的应用，则可创建用户定义的检测器来向系统提供端口和模式匹配信息以帮助识别应用。

是否已应用可修复漏洞的修补程序？

如果系统已正确识别主机，但未反映已应用的修补，则可使用主机输入功能导入修补程序信息。导入修补程序信息时，必须将修补程序的名称映射至数据库中的修补程序。

是否要跟踪第三方漏洞？

如果拥有要用于影响关联的第三方系统的漏洞信息，则可将服务器和应用协议的第三方漏洞标识符映射到思科数据库中的漏洞标识符，然后使用主机输入功能导入漏洞。有关使用主机输入功能的详细信息，请参阅《《*Firepower* 系统主机输入*API*指南》》。请注意，即使将应用数据映射到Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

第 68 章

领域和身份策略

以下主题介绍领域和身份策略：

简介：领域和身份策略

领域由一个或多个共享相同凭证的 LDAP 或 Microsoft Active Directory 服务器组成。如果要执行用户和用户组查询、用户控制或者配置授权身份源（用户代理、ISE 或强制网络门户），则必须配置领域。配置一个或多个领域后，可以配置身份策略。

身份策略将网络上的流量与授权身份源和领域相关联。配置一个或多个身份策略后，可以将其与访问控制策略相关联，然后将该访问控制策略部署到受设备。

领域基础知识

领域可在Firepower管理中心与用于监控的服务器之间建立连接。它们可指定该服务器的连接设置和身份验证过滤器设置。领域可以：

- 指定要监控其活动的用户和用户组。
- 可供您查询服务器上有关授权用户以及某些非授权用户的用户元数据：通过基于流量的检测检测到的 POP3 和 IMAP 用户以及通过基于流量的检测检测到的用户、用户代理或 ISE。

您可以将多个服务器添加为一个领域内的目录，但它们必须共享相同的基本领域信息。领域内的目录必须为专门的 LDAP 或专门的 AD 服务器。启用领域后，保存的更改将在 Firepower 管理中心下一次查询服务器时生效。

要执行用户感知，必须为任何一种支持的服务器类型配置一个领域。系统使用这些连接查询服务器上与 POP3 和 IMAP 用户关联的数据，并收集有关通过基于流量的检测发现的 LDAP 用户的数据。系统使用 POP3 和 IMAP 登录中的邮件地址与 Active Directory、OpenLDAP 或 Oracle Directory Server Enterprise Edition 服务器上的 LDAP 用户相关联。例如，如果受管设备检测到某个用户使用与某个 LDAP 用户相同的邮件地址登录 POP3，则系统会将 LDAP 用户的元数据与该用户关联。

要执行用户控制，可以配置以下任何项目：

- 配置为支持用户代理或 ISE 的 AD 服务器的领域
- 配置为支持强制网络门户的 AD、Oracle 或 OpenLDAP 服务器的领域

如果您已为下载用户配置领域（用于用户感知或用户控制），则 Firepower 管理中心会定期查询服务器，以获取自上次查询以来检测到其活动的新用户和已更新用户的元数据。

用户活动数据存储在用户活动数据库，而用户身份数据存储在用户数据库。可在访问控制中存储和使用的最大用户数取决于 Firepower 管理中心型号。选择要包含的用户和组时，请确保用户总数小于型号限制。如果访问控制参数范围太宽泛，则 Firepower 管理中心会获取尽可能多的用户的信息，并报告其无法在消息中心的“任务”(Tasks) 选项卡中检索的用户数。

注释 即使您从 LDAP 服务器移除系统检测到的用户，Firepower 管理中心也**不会**从其用户数据库中移除这些用户；您必须手动删除。但是，在 Firepower 管理中心下次更新其授权用户列表时，LDAP 更改**会**反映在访问控制规则中。

领域支持的服务器

可以配置领域以连接到以下类型的服务器（如果这些服务可从 Firepower 管理中心进行 TCP/IP 访问）：

服务器类型	支持用户感知数据检索？	支持用户代理数据检索？	支持 ISE 数据检索？	支持强制网络门户数据检索？
Windows Server 2008 和 Windows Server 2012 上的 Microsoft Active Directory	是	是	是	是
Windows Server 2008 上的 Oracle Directory Server Enterprise Edition 7.0	是	否	是	是

服务器类型	支持用户感知数据检索？	支持用户代理数据检索？	支持 ISE 数据检索？	支持强制网络门户数据检索？
Linux 上的 OpenLDAP	是	否	否	是

请注意以下与服务器组配置有关的事项：

- 如果要对用户组或组内用户执行用户控制，必须在服务器上配置用户组。如果由服务器管理基本对象层次结构中的用户，则 Firepower 管理中心无法执行用户组控制。
- 如果要配置包含或排除属于服务器上的子组成员的用户的 Active Directory 领域，请注意，Active Directory 服务器会限制其报告的用户数：

  在 Windows Server 2008 或 2012 的 Microsoft Active Directory 上，每组 5000 个用户

  如有必要，可以修改 Active Directory 服务器配置以增大此默认限制并容纳更多用户。

支持的服务器字段名称

领域中的服务器**必须**使用下表列出的字段名称，以使 Firepower 管理中心检索服务器的用户元数据。如果服务器中的字段名称不正确，Firepower 管理中心将无法使用该字段中的信息来填充其数据库。

表 *200*：将服务器字段映射到 *Firepower* 管理中心字段

元数据	管理中心字段	Active Directory 字段	Oracle Directory Server 字段	OpenLDAP 字段
LDAP 用户名	用户名	samaccountname	cn uid	cn uid
first name	名字	givenname	givenname	givenname
last name	姓氏	sn	sn	sn
email address	电子邮件	邮件 userprincipalname（如果 mail 没有值）	邮件	邮件
department	部门	department distinguishedname（如果 department 没有值）	department	ou
电话号码	电话	telephonenumber	n/a	telephonenumber

对领域和用户下载问题进行故障排除

如果发现意外的服务器连接行为，请考虑调整领域配置、设备设置或服务器设置。有关其他相关故障排除信息，请参阅对用户身份源问题进行故障排除，第1198页和对用户控制进行故障排除，第289页。

在非正常时间发生用户超时

如果发现系统按非预期间隔执行用户超时，请确认用户代理或ISE服务器上的时间与Firepower管理中心上的时间同步。如果设备不同步，系统可在非预期时间间隔时执行用户超时。

没有按领域配置中的规定不包括或排除用户

如果配置包含或排除属于服务器上的子组成员的用户的 Active Directory 领域，请注意，Microsoft Windows 服务器会限制其报告的用户数：

- 在 Microsoft Windows Server 2008 或 2012 上，每组 5000 个用户

如有必要，可以修改服务器配置以增大此默认限制并容纳更多用户。

先前未发现的 ISE 和用户代理用户的用户数据未显示在 Web 界面上

在系统检测到其数据尚未包含在数据库中的 ISE 或用户代理用户的活动后，系统从服务器检索其有关信息。在某些情况下，系统需要额外时间来从 Active Directory 服务器成功检索此信息。在数据检索成功之前，ISE 或用户代理用户发现的活动**不**显示在 Web 界面中。

请注意，这还可防止系统使用访问控制规则处理用户的流量。

身份策略基础知识

身份策略包含身份规则。身份规则会将流量集与领域和身份验证方法相关联：被动身份验证、主动身份验证或无身份验证。

您必须完全配置计划使用的领域和身份验证方法，然后才能在身份规则中进行调用：

- 在**系统 (System)** > **集成 (Integration)** > **领域 (Realms)**中，配置身份策略外的领域。有关详细信息，请参阅创建领域，第 1235 页。
- 在**系统 (System)** > **集成 (Integration)** > **身份源 (Identity Sources)**中，配置用户代理和 ISE 被动身份验证身份源。有关详细信息，请参阅配置用户代理连接，第 1200 页和配置 ISE 连接，第 1202 页。
- 在身份策略中，配置主动身份验证身份源：强制网络门户。有关详细信息，请参阅配置强制网络门户主动身份验证，第 1241 页。

向一个身份策略添加多个身份规则后，对规则排序。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一个规则是处理该流量的规则。

配置一个或多个身份策略后，必须调用访问控制策略中的一个身份策略。当网络上的流量与身份规则中的条件匹配时，系统会将流量与指定领域相关联并使用指定身份源对流量中的用户进行身份验证。

如果不配置身份策略，则系统不会执行用户身份验证。

创建领域

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**领域 (Realms)**。

步骤 3 点击**新建领域 (New Realm)**。

步骤 4 配置基本领域信息，如配置基本领域信息，第 1238 页中所述。

步骤 5 配置目录，如配置领域目录，第 1238 页中所述。

步骤 6 配置用户和用户组下载（访问控制必需），如配置自动用户下载，第 1239 页中所述。

步骤 7 保存领域设置。

步骤 8 或者，编辑领域并修改默认“用户会话超时”(User Session Timeout) 设置，如配置领域用户会话超时，第 1240 页中所述。

步骤 9 保存领域设置。

接下来的操作

- 启用领域，如启用或禁用领域，第 1255 页中所述。
- 或者，监控任务状态；请参阅查看任务消息，第 239 页。

领域字段

以下字段用于配置领域。

领域配置字段

以下设置适用于领域内的所有服务器（目录）。

AD 主域 (AD Primary Domain)

仅适用于 AD 领域，应在其上进行用户身份验证的 Active Directory 服务器的域。

说明

领域的可选说明。

目录用户名和目录密码 (Directory Username and Directory Password)

为具有检索用户信息的相应权限的用户提供的可分辨名称和密码。

Base DN

Firepower 管理中心应在其上开始搜索用户数据的服务器上的目录树。

通常，基本 DN 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 ou=security,dc=example,dc=com。

组 DN (Group DN)

Firepower 管理中心应在其上搜索具有组属性的用户的服务器上的目录树。

组属性 (Group Attribute)

服务器的组属性：成员 (Member) 或 唯一成员 (Unique Member)。

Name

领域的唯一名称。

Type

领域的类型：AD 或 LDAP。

用户会话超时：通过身份验证的用户 (User Session Timeout: Authenticated Users)

用户会话超时前的最长时间（以分钟为单位）。

如果用户进行被动身份验证且其会话超时，则他们会被识别为未知用户，并且系统会根据访问控制规则设置允许或阻止其当前会话。系统将在用户下次登录时重新识别。如果通过强制网络门户对用户进行主动身份验证且其会话超时，则系统会提示其重新进行身份验证。

用户会话超时：身份验证失败的用户 (User Session Timeout: Failed Authentication Users)

因用户会话超时而尝试强制网络门户主动身份验证失败后的时间（以分钟为单位）。用户身份验证失败且其会话超时时，系统会提示其重新进行身份验证。

用户会话超时：访客用户 (User Session Timeout: Guest Users)

进行主动身份验证的强制网络门户访客用户的会话超时前的最长时间（以分钟为单位）。当他们的会话超时时，系统会提示其重新进行身份验证。

领域目录字段

以下设置适用于领域内的各个服务器（目录）。

加密

要用于 Firepower 管理中心和服务器连接的加密方法。

- STARTTLS - 加密的 LDAP 连接
- LDAPS - 加密的 LDAP 连接
- 无 (None) - 未加密的 LDAP 连接（不安全的流量）

主机名/IP 地址

服务器的主机名或 IP 地址。如果指定**加密 (Encryption)** 方法，则必须在此字段中指定主机名。

端口

要用于 Firepower 管理中心和服务器连接的端口。

SSL 证书 (SSL Certificate)

要用于对服务器进行身份验证的 SSL 证书。必须配置 STARTTLS 或 LDAPS 作为**加密 (Encryption)** 类型才能使用 SSL 证书。

如果使用证书进行身份验证，则证书中的服务器名称必须与服务器**主机名/IP 地址 (Hostname / IP Address)** 匹配。例如，如果将 10.10.10.250 作为 IP 地址，而不是证书中的 computer1.example.com，则连接会失败。

用户下载字段

可用组 (Available Groups)、添加以包含 (Add to Include)、添加以排除 (Add to Exclude)

确定您要下载并可用于用户感知和用户控制的组。

- 如果您将某个组留在**可用组 (Available Groups)** 框中，则不能下载该组。
- 如果您将某个组移动到**添加以包含 (Add to Include)** 框中，则可以下载该组，并将用户数据用于用户感知和用户控制。
- 如果您将某个组移动到**添加以排除 (Add to Exclude)** 框中，则可以下载该组并将用户数据用于用户感知，但不能用于用户控制。

自动下载开始时间 (Begin automatic download at)、重复频率 (Repeat every)

指定自动下载的频率。

下载用户和组（用户访问控制必需）(Download users and groups [required for user access control])

启用用户数据自动下载。

配置基本领域信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在“添加新领域”(Add New Realm) 页面中，输入**名称 (Name)** 和**说明 (Description)**（可选）。

步骤 2 从下拉列表中选择**类型 (Type)**。

步骤 3 如果正在配置 AD 领域，请输入 **AD 主域 (AD Primary Domain)**。

步骤 4 为具有检索用户信息的相应权限的用户输入可分辨**目录用户名 (Directory Username)** 和**目录密码 (Directory Password)**。

步骤 5 输入目录的**基础 DN (Base DN)**。

步骤 6 输入目录的**组 DN (Group DN)**。

步骤 7 或者，从下拉列表中选择**组属性 (Group Attribute)**。

步骤 8 点击 **OK**。

接下来的操作

- 配置领域目录，如配置领域目录，第 1238 页中所述。

配置领域目录

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

有关领域配置字段的详细信息，请参阅领域字段，第 1235 页。

过程

步骤 1 在“目录”(Directory) 选项卡上，点击**添加目录 (Add Directory)**。

步骤 2 为服务器输入**主机名/IP 地址 (Hostname / IP Address)** 和**端口 (Port)**。

步骤 3 选择**加密模式 (Encryption Mode)**。

步骤 4 或者，从下拉列表中选择 **SSL 证书 (SSL Certificate)**。请注意，您可以点击添加图标 () 快速创建对象。

步骤 5 如果要测试连接，请点击**测试 (Test)**。

步骤 6 点击 **OK**。

接下来的操作

- 或者，配置自动用户下载，如配置自动用户下载，第 1239 页中所述。

配置自动用户下载

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

如果未指定要包含的任何组，则系统会检索与所提供的参数相匹配的所有组的用户数据。出于性能方面的考虑，思科建议您仅明确包含代表要在访问控制中使用的用户的组。

有关领域配置字段的详细信息，请参阅领域字段，第 1235 页。

过程

步骤 1 在“用户访问控制”(User Access Control) 选项卡上，选择**下载用户和组（用户访问控制必需）(Download users and groups [required for user access control])** 复选框。

步骤 2 从下拉列表中选择**自动下载开始时间 (Begin automatic download at)**。

步骤 3 从**重复频率 (Repeat Every)** 下拉列表中选择下载时间间隔。

步骤 4 要从下载中包括或排除用户组，请从**可用组 (Available Groups)** 列中选择用户组，然后点击**添加至包括 (Add to Include)** 或**添加至排除 (Add to Exclude)**。
使用逗号分隔多个用户。还可以在此字段中使用星号 (*) 作为通配符。

注释 如果要对该组中的用户执行用户控制，必须**添加至包括 (Add to Include)**。

配置领域用户会话超时

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

有关领域配置字段的详细信息，请参阅领域字段，第 1235 页。

注释 如果系统以意外间隔执行用户超时，请确认用户代理或 ISE 服务器上的时间是否与 Firepower 管理中心上的时间同步。

过程

步骤 1 选择**领域配置 (Realm Configuration)** 选项卡。

步骤 2 为**通过身份验证的用户 (Authenticated Users)**、**身份验证失败的用户 (Failed Authentication Users)** 和**访客用户 (Guest Users)** 输入用户会话超时值。

步骤 3 点击**保存 (Save)** 或继续编辑领域。

创建身份策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

开始之前

- 创建并启用一个或多个领域，如创建领域，第 1235 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**并点击**新建策略 (New Policy)**。

步骤 2 键入**名称 (Name)** 和**说明 (Description)**（可选）。

步骤 3 如果要将规则添加到策略，请点击**添加规则 (Add Rule)**，如创建身份规则，第 1244 页中所述。

步骤 4 如果要添加规则类别，请点击**添加类别 (Add Category)**，如添加身份规则类别，第 1257 页中所述。

步骤 5 如果要配置强制网络门户主动身份验证，请点击**主动身份验证 (Active Authentication)**，如配置强制网络门户主动身份验证，第 1241 页中所述。

步骤 6 点击**保存 (Save)** 保存身份策略。

接下来的操作

- 将身份策略与访问控制策略相关联；请参阅将其他策略与访问控制相关联，第 622 页。
- 部署配置更改；请参阅部署配置更改，第 254 页。

配置强制网络门户主动身份验证

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任意设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

在您的身份策略的“主动身份验证”(Active Authentication) 选项卡上配置强制网络门户设置。有关强制网络门户的详细信息，请参阅强制网络门户主动身份验证身份源，第 1203 页和强制网络门户主动身份验证字段，第 1242 页。

开始之前

- 确认您的 Firepower 管理中心使用已配置的路由接口管理一台或多台设备。
- 将访问控制规则配置为允许流量流向计划用于强制网络门户的端口。
- 如果要对 HTTPS 流量执行强制网络门户主动身份验证，必须创建 SSL 规则以解密源自要使用强制网络门户进行身份验证的用户的流量。
- 如果您计划为强制网络门户使用 ASA FirePOWER 设备（在路由模式且运行 ASA 版本 9.5(2) 或更高版本），请使用 **captive-portal** ASA CLI 命令启用强制网络门户进行主动身份验证并定义端口，如《*ASA* 防火墙配置指南》（版本 9.5(2) 或更高版本）中所述：http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**并创建或编辑身份策略。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 点击**主动身份验证 (Active Authentication)**。

步骤 3 从下拉列表中选择相应的**服务器证书 (Server Certificate)**。或者，点击添加图标 ( ) 快速创建内部证书对象。

步骤 4 键入**端口 (Port)** 并指定**最大登录尝试次数 (Maximum login attempts)**。

步骤 5 或者，选择**主动身份验证响应页面 (Active Authentication Response Page)**，如配置强制网络门户主动身份验证响应页面，第 1243 页中所述。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 配置身份规则，如创建身份规则，第 1244 页中所述。必须配置一个或多个已启用**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)** 选项的主动身份验证规则或被动身份验证规则，以便执行强制网络门户主动身份验证。有关其他主动身份验证设置的详细信息，请参阅在身份规则中配置主动身份验证设置，第 1251 页。

  如果在步骤 5 中选择了响应页面，则必须选择 HTTP 响应页面作为**身份验证类型 (Authentication Type)**。

- 部署配置更改；请参阅部署配置更改，第 254 页。

强制网络门户主动身份验证字段

使用以下字段，在您的身份策略的“主动身份验证”(Active Authentication) 选项卡上配置强制网络门户设置。

服务器证书 (Server Certificate)

强制网络门户后台守护程序显示的服务器证书。

端口

要用于强制网络门户连接的端口号。如果您计划为强制网络门户使用 ASA FirePOWER 设备，此字段中的端口号必须与使用 **captive-portal** CLI 命令在 ASA FirePOWER 设备上配置的端口号相匹配。

最大登录尝试次数 (Maximum login attempts)

系统拒绝用户登录请求前允许的最大失败登录尝试的次数。

主动身份验证响应页面 (Active Authentication Response Page)

要向强制网络门户用户显示的系统提供或自定义HTTP响应页面。在您的身份策略主动身份验证设置中选择**主动身份验证响应页面 (Active Authentication Response Page)**后，还必须配置一个或多个身份规则，将HTTP响应页面 (HTTP Response Page) 作为**身份验证类型 (Authentication Type)**。

配置强制网络门户主动身份验证响应页面

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任意设备，除了NGIPSv	任意	管理员/访问管理员/网络管理员

可以选择向强制网络门户用户显示系统提供的或自定义 HTTP 响应页面。

有关强制网络门户的详细信息，请参阅强制网络门户主动身份验证身份源，第 1203 页和强制网络门户主动身份验证字段，第 1242 页。

开始之前

- 开始配置强制网络门户，如配置强制网络门户主动身份验证，第 1241 页中所述。

过程

步骤 1 在身份策略的“主动身份验证”(Active Authentication) 选项卡上，从下拉菜单中选择**主动身份验证响应页面 (Active Authentication Response Page)**。

- 要使用通用响应，请选择**系统提供 (System-provided)**。可以点击查看图标 () 以查看此页面的 HTML 代码。
- 要创建自定义响应，请选择**自定义 (Custom)...**。系统将显示一个弹出窗口，其中预先填充有系统提供的可以替换或修改的代码。完成时，保存更改。可以通过点击编辑图标()来编辑自定义页面。

步骤 2 点击**保存 (Save)**。

接下来的操作

- 继续配置强制网络门户，如配置强制网络门户主动身份验证，第 1241 页中所述。

创建身份规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

注意 添加或删除**主动身份验证 (Active Authentication)** 规则操作，或者在规则操作为**被动身份验证 (Passive Authentication)** 时选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**。

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击 **Add Rule**（添加规则）。

步骤 4 配置基本身份规则信息，如配置基本身份规则信息，第 1246 页中所述。

步骤 5 或者，添加区域条件，如将区域条件添加到身份规则，第 1249 页中所述。

步骤 6 或者，添加网络或地理位置条件，如将网络或地理位置条件添加到身份规则，第 1247 页中所述。

步骤 7 或者，添加 VLAN 标记条件，如将 VLAN 标记条件添加到身份规则，第 1249 页中所述。

步骤 8 或者，添加端口条件，如将端口条件添加到身份规则，第 1248 页中所述。

系统无法对非 TCP 流量执行主动身份验证。如果身份规则操作为“主动身份验证”(Active Authentication)（使用的是强制网络门户），或者如果您选中选项**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，请仅使用 TCP 端口限制。如果身份规则操作为“被动身份验证”(Passive Authentication) 或“无身份验证”(No Authentication)，则可以根据非 TCP 流量创建端口条件。

步骤 9 将规则与领域相关联，如在身份规则中关联领域，第 1250 页中所述。

步骤 10 或者，配置主动身份验证设置，如在身份规则中配置主动身份验证设置，第 1251 页中所述。

步骤 11 点击 **Add**。

步骤 12 点击 **Save**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

身份规则字段

使用以下字段配置身份规则。

启用

选择此选项可启用身份策略中的身份规则。取消选择此选项可禁用身份规则。

操作

要对指定**领域 (Realm)** 中的用户执行的身份验证类型。您可以选择被动身份验证 (Passive Authentication)、主动身份验证 (Active Authentication) 或无身份验证 (No Authentication)。必须完全配置身份验证方法或身份源，然后再选择其作为身份规则中的操作。

有关您的 Firepower 系统版本支持哪些被动和主动身份验证方法的信息，请参阅概述：用户身份源，第 1197 页。

领域 (Realm)

包含要对其执行指定**操作 (Action)** 的用户的领域。必须在选择作为身份规则中的领域之前，对领域进行完全配置。

在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)

如果被动身份验证无法识别用户，选择此选项可通过主动身份验证对用户进行身份验证。必须在身份策略中配置主动身份验证（强制网络门户），以便选择此选项。

如果禁用此选项，则被动身份验证无法识别的用户会被识别为未知用户。

如果身份验证无法识别用户，则识别为访客 (Identify as Guest if authentication cannot identify user)

通过选择此选项，主动身份验证失败三次的用户可以访客身份访问您的网络。这些用户显示在按其用户名识别（如果 AD 或 LDAP 服务器上存在其用户名）或由**访客**识别（如果其用户名未知）的 Web 界面中。其领域是在身份规则中指定的领域。

仅在身份规则中配置主动身份验证（作为规则**操作**，或者通过选择**在被动身份验证无法识别用户时使用主动身份验证 [Use active authentication if passive authentication cannot identify user]** 选项）时，才会显示此字段。

身份验证类型

要用于执行强制网络门户主动身份验证的方法。选项因领域、LDAP 或 AD 的类型而有所不同。

- 如果要使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证，请选择 HTTP 基本身份验证 (HTTP Basic)。用户使用其浏览器的默认身份验证弹出窗口登录网络。
- 如果要使用 NT LAN Manager (NTLM) 连接对用户进行身份验证，请选择 NTLM。仅在选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。
- 选择 HTTP 协商 (HTTP Negotiate) 可允许强制网络门户服务器选择 HTTP 基本身份验证”(HTTP Basic) 或 NTLM 进行身份验证连接。仅在选择 AD 领域时，此选项才可用。

注释 如果您创建身份规则来执行“HTTP 协商”(HTTP Negotiate) 强制网络门户且配置了 DNS 解析，则必须配置您的 DNS 服务器，以解析强制网络门户设备的主机名。您用于强制网络门户的设备主机名必须与配置 DNS 时提供的主机名相匹配。

- 如果要使用系统提供的或自定义的 HTTP 响应页面对用户进行身份验证，请选择 HTTP 响应页面 (HTTP Response Page)。用户使用配置的响应页面登录网络。

配置基本身份规则信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

注意 添加或删除**主动身份验证 (Active Authentication)** 规则操作，或者在规则操作为**被动身份验证 (Passive Authentication)** 时选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

过程

步骤 1 在身份规则编辑器页面中，键入**名称 (Name)**。

步骤 2 指定规则是否为 **Enabled**。

步骤 3 要将规则添加到规则类别，请参阅添加身份规则类别，第 1257 页。

步骤 4 从下拉列表中选择规则**操作 (Action)**。

步骤 5 点击**添加 (Add)** 或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则，第 1244 页中所述。

将网络或地理位置条件添加到身份规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在身份规则编辑器页面中，选择**网络 (Networks)** 选项卡。

步骤 2 从**可用网络 (Available Networks)** 中查找要添加的网络，如下所示：

- 要即时添加可随后添加到条件中的网络对象，请点击“可用网络”(Available Networks) 列表上方的添加图标 ( )。
- 要搜索要添加的网络或地理位置对象，请点击**可用网络 (Available Networks)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象名称或对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。

步骤 5 添加您想要手动指定的任何源或者目标 IP 地址或地址块。点击 **Source Networks** 或 **Destination Networks** 列表下方的 **Enter an IP address** 提示，然后键入 IP 地址或地址块，并点击 **Add**。

步骤 6 点击**添加 (Add)** 或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则 ， 第 1244 页中所述。

将端口条件添加到身份规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员 访问管理员 网络管理员

系统无法对非 TCP 流量执行主动身份验证。如果身份规则操作为“主动身份验证”(Active Authentication)（使用的是强制网络门户），或者如果您选中选项**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，请仅使用 TCP 端口限制。如果身份规则操作为“被动身份验证”(Passive Authentication) 或“无身份验证”(No Authentication)，则可以根据非 TCP 流量创建端口条件。

过程

步骤 1 在身份规则编辑器中，点击**端口 (Ports)** 选项卡。

步骤 2 从**可用端口 (Available Ports)** 列表中查找并选择要添加的预定义端口。

- 要即时添加可随后添加到条件中的端口对象，请点击添加图标 ( )。
- 要搜索要添加的端口对象和组，请点击**按名称或值搜索 (Search by name or value)** 提示，然后输入对象名称或对象中某一端口的值。列表会在您键入内容时进行更新，以显示匹配的对象。例如，如果键入 443，规则编辑器将显示系统提供的 HTTPS 端口对象。

步骤 3 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**，或进行拖放操作。

步骤 4 添加要手动指定的任何源或目标端口：

- 源 - 选择**协议 (Protocol)**，输入**端口 (Port)**（0 到 65535），然后点击**添加 (Add)**。
- 目标（非 ICMP） - 选择或输入**协议 (Protocol)**。如果不想指定协议，或者如果选择 **TCP** 或 **UDP**，请输入单个**端口 (Port)**（0 到 65535）。点击 **Add**。
- 目标 (ICMP) - 从**协议 (Protocol)** 下拉列表中选择 **ICMP** 或 **IPv6-ICMP**，然后在显示的弹出窗口中选择**类型 (Type)** 和相关**代码 (Code)**。有关 ICMP 类型和代码的详细信息，请参阅互联网编号分配机构 (IANA) 网站。.

步骤 5 保存或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则，第 1244 页中所述。

将 VLAN 标记条件添加到身份规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 在身份规则编辑器页面中，选择 **VLAN 标记 (VLAN Tags)** 选项卡。

步骤 2 从**可用 VLAN 标记 (Available VLAN Tags)** 中查找要添加的 VLAN，如下所述：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击**可用 VLAN 标记 (Available VLAN Tags)** 列表上方的添加图标 ( )。
- 要搜索要添加的 VLAN 标记对象和组，请点击**可用 VLAN 标记 (Available VLAN Tags)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的一个 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 4 点击 **Add to Rule**（**添加至规则**）。

步骤 5 添加要手动指定的任何 VLAN 标记。点击 **Selected VLAN Tags** 列表下方的 **Enter a VLAN Tag** 提示，然后键入 VLAN 标记或范围并点击 **Add**。可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

步骤 6 点击**添加 (Add)** 或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则，第 1244 页中所述。

将区域条件添加到身份规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 在身份规则编辑器页面中，选择**区域 (Zones)** 选项卡。

步骤 2 或者，选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)** 复选框。

步骤 3 从**可用区域 (Available Zones)** 中查找要添加的区域。要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

步骤 4 点击以选择区域。要选择所有区域，请点击右键，然后选择**全选 (Select All)**。

步骤 5 点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。

步骤 6 点击**添加 (Add)** 或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则，第 1244 页中所述。

在身份规则中关联领域

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 在身份规则编辑器页面中，选择**领域和设置 (Realm & Settings)** 选项卡。

步骤 2 从下拉列表中选择**领域 (Realm)**。

步骤 3 点击**添加 (Add)** 或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则，第 1244 页中所述。

在身份规则中配置主动身份验证设置

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任意，NGIPSv 除外	任意	管理员、访问管理员、网络管理员

如果选择了主动身份验证作为身份规则**操作 (Action)**，或如果选择了**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)** 选项，请为主动身份验证配置附加设置。

注意

添加或删除**主动身份验证 (Active Authentication)** 规则操作，或者在规则操作为**被动身份验证 (Passive Authentication)** 时选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)**，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是通过而无需进一步检测取决于受管设备的型号及其处理流量的方式。

开始之前

- 配置强制网络门户，如配置强制网络门户主动身份验证，第 1241 页中所述。强制网络门户是 Firepower 系统唯一支持的主动身份验证方法。

过程

步骤 1 在身份规则编辑器页面中，选择**领域和设置 (Realm & Settings)** 选项卡。

步骤 2 或者，选择**在被动身份验证无法识别用户时使用主动身份验证 (Use active authentication if passive authentication cannot identify user)** 复选框。请注意，仅在配置被动验证规则时会显示此复选框。

步骤 3 如果选择了步骤 2 中的复选框，或者如果这是主动身份验证规则，请继续执行步骤 4。否则，请跳至步骤 7。

步骤 4 或者，选择**如果身份验证无法识别用户，则识别为访客 (Identify as Guest if authentication cannot identify user)** 复选框。

步骤 5 从下拉列表中选择**身份验证类型 (Authentication Type)**。

步骤 6 或者，**排除 HTTP 用户代理 (Exclude HTTP User-Agents)** 以将特定应用流量排除在主动身份验证范围之外，如将应用排除在主动身份验证范围之外，第 1252 页中所述。

步骤 7 点击**添加 (Add)** 或继续编辑规则。

接下来的操作

- 继续创建身份规则，如创建身份规则，第 1244 页中所述。

将应用排除在主动身份验证范围之外

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任意，NGIPSv 除外	任意	管理员、访问管理员、网络管理员

您可以选择应用（通过其 HTTP 用户代理字符串识别）并使其免除主动身份验证。这允许所选应用的流量在未经身份验证的情况下通过身份策略。

注释 此列表中仅显示具有用户代理排除**标记**的应用。

过程

步骤 1 在身份规则编辑器页面的**领域和设置 (Realm & Settings)** 选项卡上，使用**应用过滤器 (Application Filters)** 列表中思科提供的过滤器缩小要添加到过滤器中的应用列表的范围。

- 点击每种过滤器类型旁边的箭头可展开和折叠列表。
- 右键单击某种过滤器类型并点击 **Check All** 或 **Uncheck All**。请注意，列表会指示已选择的每种类型的过滤器数目。
- 要减少显示的过滤器，请在 **Search by name** 字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击清除图标 ( )。
- 要刷新过滤器列表并清除所有选定的过滤器，请点击重新加载图标 ( )。
- 要清除所有过滤器和搜索字段，请点击 **Clear All Filters**。

注释 该列表每次显示 100 个应用。

步骤 2 从 **Available Applications** 列表中选择要添加到过滤器的应用：

- 选择 **All apps matching the filter** 可添加满足在上一步骤中指定的限制条件的所有应用。
- 要减少显示的应用，请在 **Search by name** 字段中键入搜索字符串。要清除搜索，请点击清除图标 ( )。
- 使用位于列表底部的页码图标可浏览可用应用的列表。
- 要刷新应用列表并清除所有选定的应用，请点击重新加载图标 ( )。

步骤 3 添加所选应用以免除外部身份验证。可以点击并拖动，也可以点击 **Add to Rule**。结果是以下项的组合：

- 所选的应用过滤器

- 所选的各个可用应用，或者 **All apps matching the filter**

接下来的操作

- 继续配置身份规则，如创建身份规则，第 1244 页中所述。

管理领域

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**领域 (Realms)**。

步骤 3 如果要删除领域，请点击删除图标()。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如果要编辑领域，请点击领域旁边的编辑图标()并进行更改，如创建领域，第 1235 页中所述。如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 5 如果要启用或禁用领域，请点击要启用或禁用的领域旁边的**状态 (State)**滑块，如启用或禁用领域，第 1255 页中所述。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 6 如果要按需下载用户和用户组，请点击下载图标()，如按需下载用户和用户组，第 1254 页中所述。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 如果要复制领域，请点击复制图标 ()。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 8 如果要比较领域，请参阅比较领域，第 1253 页。

比较领域

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、安全审批人、访问管理员、网络管理员

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**领域 (Realms)**。

步骤 3 点击**比较领域 (Compare Realms)**。

步骤 4 从**比较对象 (Compare Against)** 下拉列表中选择**比较领域 (Compare Realm)**。

步骤 5 从**领域 A (Realm A)** 和**领域 B (Realm B)** 下拉列表中选择要比较的领域。

步骤 6 点击 **OK**。

步骤 7 如果要逐一浏览更改，请点击标题栏上方的**上一个 (Previous)**或**下一个 (Next)**。

步骤 8 或者，点击**比较报告 (Comparison Report)** 以生成领域比较报告。

步骤 9 或者，点击**新增比较 (New Comparison)** 以生成新的领域比较视图。

按需下载用户和用户组

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

如果更改领域中的用户或组下载参数，或者如果更改服务器上的用户或组且希望更改立即可用于用户控制，则可强制 Firepower 管理中心从服务器执行按需用户下载。

Firepower 管理中心可从服务器检索的最大用户数取决于 Firepower 管理中心型号。如果领域中的下载参数范围太宽泛，Firepower管理中心会尽可能获取有关更多用户的信息，并报告无法在消息中心的“任务”(Task) 选项卡中检索的用户数。

开始之前

- 启用领域，如以下章节所述 启用或禁用领域，第 1255 页

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**领域 (Realms)**。

步骤 3 点击要下载用户和用户组的领域旁边的下载图标 ( )。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

接下来的操作

- 或者，监控任务状态；请参阅查看任务消息，第 239 页。

启用或禁用领域

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

如果禁用领域，则系统会停止在服务器上查询用户下载并阻止您在身份规则中使用领域。

过程

步骤 1 选择**系统 (System)** > **集成 (Integration)**。

步骤 2 点击**领域 (Realms)**。

步骤 3 点击要启用或禁用的领域旁边的**状态 (State)** 滑块。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

接下来的操作

- 或者，监控任务状态；请参阅查看任务消息，第 239 页。

管理身份策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**。

步骤 2 如果要删除策略，请点击删除图标(🗑)。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 如果要编辑策略，请点击策略旁边的编辑图标 (✎) 并进行更改，如创建身份策略，第 1240 页中所述。如果改为显示查看图标 (🔍)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如果要复制策略，请点击复制图标 (⧉)。

步骤 5 如果要生成该策略的报告，请点击报告图标 (📄)，如生成当前策略报告，第 262 页中所述。

步骤 6 如果要比较策略，请参阅比较策略，第 261 页。

管理身份规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **身份 (Identity)**。

步骤 2 点击要编辑的策略旁边的编辑图标 (✎)。如果改为显示查看图标 (🔍)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 如果要编辑身份规则，请点击编辑图标 (✎) 并进行更改，如创建身份策略，第 1240 页中所述。

步骤 4 如果要删除身份规则，请点击删除图标 (🗑)。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

添加身份规则类别

智能许可证	经典许可证	支持的设备	支持的域	Access
任意	可控性	任何环境	任何环境	管理员、访问管理员、网络管理员

过程

步骤 1 在身份规则编辑器页面中，您有以下选择：

- 从第一个**插入 (Insert)** 下拉列表中选择**类别上方 (above Category)**，然后从第二个下拉列表中选择要在其上放置规则的类别。
- 从下拉列表中选择**规则下方 (below rule)**，然后输入现有的规则编号。仅当策略中存在至少一个规则时，该选项才有效。
- 从下拉列表中选择**规则上方 (above rule)**，然后输入现有的规则编号。仅当策略中存在至少一个规则时，该选项才有效。

步骤 2 点击 **OK**。

注释 删除的类别中的规则将会添加至以上类别。

步骤 3 点击**添加 (Add)** 或继续编辑规则。

第 XVII 部分

关联和合规性

第 69 章

合规白名单

以下主题介绍如何在将合规白名单添加到关联策略之前对其进行配置。

合规白名单简介

合规白名单，有时缩写为白名单，是指定允许在网络上的主机上运行的操作系统、应用（Web 和客户端）以及协议的一系列标准。即使主机违反白名单，系统也会生成一个事件。

合规白名单有两个主要组件：

- 目标是您选择用于白名单评估的主机。您可以评估所有或部分受监控的主机，按照子网、VLAN 和主机属性进行限制。在多域部署中，您可以将域以及域内或跨域的子网作为目标。
- 主机配置文件指定面向目标的合规标准。全局主机配置文件与操作系统无关。您也可以配置操作系统特定的主机配置文件，主机配置文件为一个白名单独有或跨白名单共享。

Cisco Talos 安全情报和研究小组 (Talos) 提供配有建议设置的默认白名单。您也可以创建自定义白名单。简单的自定义白名单可能只允许主机运行某一操作系统。较复杂的白名单可能允许所有操作系统，但指定主机在特定端口上运行某一应用协议必须使用的操作系统。

注释

系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。此限制可能会影响创建合规白名单的方式。

实施合规白名单

要实施白名单，请将该白名单添加到活动关联策略。系统评估目标并给每个主机分配对应的属性：

- 合规 - 主机没有违反白名单。
- 不合规 - 主机违反白名单。
- 未评估 - 主机不是白名单的目标，主机现在正在接受评估，或者系统没有足够的信息来确定主机是否合规。

注释 要删除主机属性，请删除其对应的白名单。停用、删除或删除关联策略中的白名单**不**会删除主机属性，也不会更改每个主机的属性值。

完成初始评估后，当受监控的主机不再符合活动白名单时，系统会生成白名单事件；它会还记录白名单违规。

您可以使用工作流程、控制面板以及网络映射来监控整个系统的合规活动，并确定个别主机何时、以何种方式违反了您的白名单。您也可以通过补救和警报自动对白名单违规做出响应。

示例：将 HTTP 限制为 Web 服务器

您的安全策略规定只有 Web 服务器可以运行 HTTP。您可以创建一份评估整个网络（不包括 Web 场）的白名单，以确定哪些主机正在运行 HTTP。

通过使用网络映射和控制面板，您可以获取您的网络合规性的概览摘要。只需几秒钟，便可以确定组织内的哪些主机违反了策略正在运行 HTTP，并采取相应的行动。

然后，使用关联功能配置系统，使系统在网络场之外的主机开始运行 HTTP 时发出警报。

合规白名单目标网络

目标网络指定要用于白名单合规性评估的主机。白名单可具有多个目标网络，并且会评估与其任何目标的条件相符的主机。

最初，您可通过 IP 地址或范围限制目标网络。在多域部署中，初始限制还包括一个域。

系统提供的默认白名单针对所有受监控主机：0.0.0.0/0 和 ::/0。在多域部署中，默认白名单限用于（且仅适用于）全局域。

如果修改目标网络或主机，致使该主机不再是白名单的有效目标，则该主机不再通过白名单进行评估，并且既不视为合规，也不视为不合规。

调查和优化目标网络

将目标网络添加到白名单中时，系统会提示您调查网络映射以帮助确定合规主机的特征。调查会将目标添加到表示已调查的主机的白名单中。

您可以调查子网或单个主机。在多域部署中，您可以调查整个域，也可以跨域调查。调查祖先域会导致系统调查该域的后代。

除已添加的目标之外，调查还会对在该调查中检测到的每个操作系统都使用一个主机配置文件填充白名单。这些主机配置文件允许系统在适用操作系统上检测到的所有客户端、应用协议、Web 应用和协议。

在调查目标网络（或跳过调查）后，请优化目标。您可以按 IP 地址排除主机，或者按主机属性或 VLAN 限制目标网络。

使用合规白名单设定目标域

在多域部署中，域和目标网络紧密相连。

- 枝叶域管理员可以创建对其枝叶域内的主机进行评估的白名单。
- 更高级别的域管理员可以创建跨域评估主机的白名单。您可以在同一个白名单中以不同域中的不同子网作为目标。

假设您是全局域管理员，并且要将同一合规性标准应用于整个部署中的 Web 服务器。您可以在全局域中创建用于定义合规性标准的白名单。然后，使用指定各枝叶域中 Web 服务器的 IP 空间（或单个 IP 地址）的目标网络来限制白名单。

注释 除将枝叶域中的 IP 地址和范围设定为目标之外，您还可以使用更高级别的域来限制目标网络。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

合规白名单主机配置文件

在合规白名单中，主机配置文件指定允许在目标主机上运行的操作系统、客户端、应用协议、Web 应用和协议。有三种类型的主机配置文件可在合规白名单中使用；每个类型在合规白名单编辑器中以不同方式显示。

表 *201*：合规白名单主机配置文件类型

主机配置文件类型	外观	说明
global	任何操作系统	指定允许在目标主机上运行的内容，而不考虑操作系统
特定于操作系统	以纯文本列示	指定允许在特定操作系统的目标主机上运行的内容
共享	以斜体形式列示	指定可以在多个白名单中使用的操作系统条件

操作系统特定主机配置文件

在合规白名单中，特定操作系统主机配置文件不仅指定了允许在网络上运行的操作系统，还指定了允许在这些操作系统上运行的应用协议、客户端、Web 应用及通信协议。

例如，可以要求合规主机运行特定版本的 Microsoft Windows。再例如，可以允许 SSH 于端口 22 在 Linux 主机上运行，并进一步限制 SSH 客户端的供应商和版本。

请为允许在网络上运行的各个操作系统创建一个主机配置文件。要禁止网络上的某个操作系统，则不要创建该操作系统的主机配置文件。例如，为了确保网络上的所有主机均运行 Windows，请将白名单配置为只包含该操作系统的主机配置文件。

注释 未识别的主机在被识别之前，一直处于符合所有白名单条件的状态。但是，可以为未知主机创建一份白名单主机配置文件。未识别的主机是指系统尚未收集足够的信息识别其操作系统的主机。未知主机是指其操作系统与已知指纹不匹配的主机。

共享主机配置文件

在合规白名单中，共享主机配置文件绑定到特定操作系统，但是您可以在多个白名单中使用每个共享主机配置文件。

例如，您可能在全球具有多个办事处，其中每个位置对应单独的白名单，但是要对运行 Apple Mac OS X 的所有主机都使用同一配置文件。您可以为该操作系统创建共享配置文件，并将其用于所有白名单中。

默认白名单使用共享主机配置文件的一个特殊类别，即内置主机配置文件。这些配置文件使用内置应用协议、Web 应用、协议和客户端。在合规白名单编辑器中，系统使用内置主机配置文件图标( )标记这些配置文件。

在多域部署中，系统会显示在当前域中创建的共享主机配置文件，您可以对其进行编辑。系统还会显示祖先域中的共享主机配置文件，您不可以对其进行编辑。要查看和编辑在较低域中创建的共享主机配置文件，请切换至该域。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个白名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

白名单违规触发器

当系统出现以下情况时，主机的白名单合规情况会发生变化：

- 检测到主机的操作系统发生变化
- 检测到主机的操作系统或主机上的应用协议存在身份冲突
- 检测到主机上有新的 TCP 服务器端口（例如，SMTP 或网络服务器使用的端口）处于活动状态，或主机上有新的 UDP 服务器正在运行
- 检测到主机上运行的 TCP 或 UDP 服务器发生变化，例如由于升级导致版本发生变化
- 检测主机上有新的客户端或 Web 应用正在运行
- 从其数据库中丢弃不活动的客户端或 Web 应用

- 检测到主机正使用新的网络或传输协议进行通信
- 检测到新的破解移动设备
- 检测到主机上的某个 TCP 或 UDP 端口已关闭或超时

此外，您还可以使用主机输入功能或主机配置文件执行以下操作来触发主机合规性的改变：

- 向主机添加客户端、协议或服务器
- 从主机中删除客户端、协议或服务器
- 设置主机的操作系统定义
- 更改主机的主机属性，这样该主机便不再是一个有效目标

注释 为避免事件数量过多而使系统不堪重负，系统在初始评估时不会为违规主机生成白名单事件，也不会对由于修改了有效白名单或共享主机配置文件而导致违规的主机生成白名单事件。但是，仍会记录违规情况。如果要为所有违规目标生成白名单事件，请清除发现数据。重新发现网络资产可能会触发白名单事件。

示例：操作系统合规性

如果白名单指定只允许在网络上运行 Microsoft Windows 主机，但系统检测到主机正在运行 Mac OS X，则系统会生成白名单事件。此外，该主机与白名单关联的主机属性从“合规”(Compliant) 更改为“违规”(Non-Compliant)。

要将本示例中主机的合规属性恢复为合规，必须发生下列任一情况：

- 您编辑白名单，以允许 Mac OS X 操作系统的运行
- 您手动将主机的操作系统定义更改为 Microsoft Windows
- 系统检测到操作系统已更改回 Microsoft Windows

示例：从网络映射中删除违规资产

如果白名单禁止使用 FTP，并且您从应用协议网络映射或事件视图中删除了 FTP，则运行 FTP 的主机的属性变为合规。但如果系统再次检测到该应用协议，则会生成白名单事件，且该主机的属性变为违规。

示例：仅对完整信息触发

如果白名单仅在端口 21 上允许 TCP FTP 流量，且系统检测到端口 21/TCP 上存在不确定的活动，则白名单不会触发。仅当系统将该流量识别为除 FTP 流量以外的其他流量，或者您使用主机输入功能将该流量指定为非 FTP 流量时，白名单才会触发。系统不会记录仅含部分信息的违规。

创建合规白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

当创建白名单时，系统会提示您调查网络，创建初始目标并帮助确定合规主机的特征。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**白名单 (White List)** 选项卡。

步骤 2 点击 **New White List**。

步骤 3 或者，输入初始目标网络的 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。在多域部署中，在**域 (Domain)** 中选择目标网络所在的域。

提示 要调查整个受监控网络，请使用默认值 0.0.0.0/0 和 ::/0。

注释 在为目标网络选择域之后，不能更改该域。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 添加目标网络：

- 添加 - 要添加目标网络而无需调查，请点击**添加 (Add)**。
- 添加并调查网络 - 要添加并调查目标网络，请点击**添加并调查网络 (Add and Survey Network)**。
- 跳过 - 要创建白名单而不调查网络，请点击**跳过 (Skip)**。

步骤 5 或者，为白名单输入新的**名称 (Name)** 和**说明 (Description)**。

步骤 6 或者，在网络上**允许破解的移动设备 (Allow Jailbroken Mobile Devices)**。禁用此选项会导致破解设备生成白名单违规。

步骤 7 向白名单中至少添加一个**目标网络 (Target Network)**，如为合规白名单创建目标网络，第 1267 页中所述。

步骤 8 使用**允许的主机配置文件 (Allowed Host Profiles)** 确定合规主机的特征：

- 全局主机配置文件 - 要编辑白名单的全局主机配置文件，请点击**任何操作系统 (Any Operating System)**，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 编辑已调查的配置文件 - 要编辑由网络调查创建的现有操作系统特定主机配置文件，请点击其名称，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 创建新配置文件 - 要为此白名单创建新的操作系统特定主机配置文件，请点击**允许的主机配置文件 (Allowed Host Profiles)** 旁边的添加图标 ( )，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。

- 添加共享主机配置文件 - 要向白名单中添加现有共享主机配置文件，请点击**添加共享主机配置文件 (Add Shared Host Profile)**，选择要添加的共享主机配置文件，然后点击**确定 (OK)**。共享主机配置文件以斜体显示。

步骤 9 点击**保存白名单 (Save White List)**。

接下来的操作

- 将白名单添加到活动关联策略中，如配置关联策略，第 1278 页中所述。系统立即开始评估白名单并生成违规。

为合规白名单创建目标网络

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

添加目标网络时，可以对其进行调查以确定合规主机的特征。此调查会对调查中检测到的每个操作系统都使用一个主机配置文件来填充白名单。这些主机配置文件允许系统在适用操作系统上检测到的所有客户端、应用协议、Web 应用和协议。

过程

步骤 1 在合规白名单编辑器中，点击**添加目标网络 (Add Target Network)**。

步骤 2 为目标网络输入 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。

步骤 3 在多域部署中，在**域 (Domain)** 中选择目标网络所在的域。

注释 在为目标网络选择域之后，不能更改该域。将更高级别的域中的子网设定为目标即会以**每个**后代枝叶域中的**同一**子网为目标。系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 4 添加目标网络：

- 添加 - 要在不调查的情况下添加目标网络，请点击**添加 (Add)**。
- 添加并调查网络 - 要添加并调查目标网络，请点击**添加并调查网络 (Add and Survey Network)**。

步骤 5 或者，点击新目标以进一步对其进行配置：

- 名称 - 在**名称 (Name)** 中输入新名称。
- 添加网络 - 要以其他主机为目标，请点击添加图标 ()，然后输入 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)**。要从白名单合规性中排除网络，请选择**排除 (Exclude)**。

- 添加主机属性 - 要以具有特定主机属性的主机为目标，请点击添加图标 ( )，然后指定**属性 (Attribute)** 及其**值 (Value)**。
- 添加 VLAN - 要以 VLAN 为目标，请点击添加图标 ( )，然后键入 VLAN 编号（对于 802.1q VLAN）。
- 删除 - 要删除目标限制，请点击删除图标 ( )。

步骤 6 要立即实施自上次保存以来进行的所有更改，请点击**保存白名单 (Save White List)**。

构建白名单主机配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

主机配置文件指定白名单的合规性标准，即允许在目标主机上运行的操作系统、客户端、应用协议、Web 应用和协议。

每个白名单都有一个与操作系统无关的全局主机配置文件。例如，无需编辑多个 Microsoft Windows 和 Linux 主机配置文件以允许 Mozilla Firefox，可以将全局主机配置文件配置为允许 Firefox，无论检测到该主机使用的是什么操作系统。

您也可以配置操作系统特定的主机配置文件，主机配置文件为一个白名单独有或跨白名单共享。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个白名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

开始之前

- 如编辑合规白名单，第 1272 页中所述在白名单内创建或编辑主机配置文件，或者如管理共享主机配置文件，第 1274 页中所述创建或编辑共享主机配置文件。

过程

步骤 1 在合规白名单主机配置文件编辑器中，配置主机配置文件：

- 名称 - 输入**名称 (Name)**。
- 操作系统 - 要将主机配置文件限制为特定的操作系统，请使用**操作系统供应商 (OS Vendor)**、**操作系统名称 (OS Name)** 和**版本 (Version)** 下拉列表。由于其目的是应用到运行任何操作系统的主机，因此无法限制全局主机配置文件。

- 应用协议 - 要允许应用协议，请点击添加图标 ( )，并如将应用协议列入白名单，第 1269 页中所述继续操作。
- 客户端 - 要允许客户端，请点击添加图标 ( )，并如将客户端列入白名单，第 1270 页中所述继续操作。
- Web 应用 - 要允许 Web 应用，请点击添加图标 ( )，并如将 Web 应用列入白名单，第 1270 页中所述继续操作。
- 协议 - 要允许协议，请点击添加图标 ( )，并如将协议列入白名单，第 1271 页中所述继续操作。
- 删除 - 要禁止之前允许的项目，请点击删除图标 ( )。
- 编辑属性 - 要编辑允许的应用协议、客户端或协议的属性，请点击其名称。进行的更改反映在使用该元素的所有主机配置文件中。

提示 选中相应的**全部允许...(Allow all...)**复选框，以允许与此配置文件匹配的主机的所有应用协议、客户端或 Web 应用。

步骤 2 要立即实施自上次保存后进行的所有更改，请点击**保存白名单 (Save White List)**（或如果您编辑的是共享主机配置文件，则点击**保存所有配置文件 [Save All Profiles]**）。

将应用协议列入白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

使用白名单主机配置文件，您可以在全局范围或在特定操作系统上将应用协议列入白名单。或者，可以按端口、供应商或版本限制应用协议。例如，可以允许特定版本的 SSH 在 Linux 主机的端口 22/TCP 上运行。

过程

步骤 1 创建或修改白名单主机配置文件时，点击**允许的应用协议 (Allowed Application Protocols)** 旁边的添加图标 ( )（或者，如果修改的是全局主机配置文件，则点击**全局允许的应用协议 (Globally Allowed Application Protocols)** 旁边的添加图标）。

步骤 2 此时您有两种选择：

- 如果列出了要允许的应用协议，请选择这些协议。Web 界面列出白名单已允许或当前允许的应用协议。
- 要允许列表中未包含的应用协议，请选择**<新应用协议> (<New Application Protocol>)**，然后点击**确定 (OK)** 显示应用协议编辑器。选择要允许的应用协议**类型 (Type)** 和**协议 (Protocol)**。或者，按**端口 (port)**、**供应商 (Vendor)** 和**版本 (Version)** 限制应用协议。

注释　必须完全按照供应商和版本在应用的表视图中的显示键入该供应商和版本。如果不指定供应商或版本，则只要类型与协议匹配，白名单便允许所有供应商和版本。

步骤 3　点击 **OK**。

步骤 4　要立即实施自上次保存以来进行的所有更改，请点击**保存白名单 (Save White List)**。

将客户端列入白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

使用白名单主机配置文件时，可以在全局或在特定操作系统上将客户端列入白名单。或者，要求客户端的特定版本。例如，可以只允许 Microsoft Internet Explorer 10 在 Microsoft Windows 主机上运行。

过程

步骤 1　创建或修改白名单主机配置文件时，点击**允许的客户端 (Allowed Clients)** 旁边的添加图标 ( )（或者，如果修改的是全局主机配置文件，则点击**全局允许的客户端 [Globally Allowed Clients]** 旁边的添加图标）。

步骤 2　此时您有两种选择：

- 如果要允许的客户端已列出，请选择这些客户端。Web 界面列出已被白名单允许或当前允许的客户端。
- 要允许不在列表中的客户端，请选择**<新建客户端> (<New Client>)** 并点击**确定 (OK)** 以显示客户端编辑器。从下拉列表中选择要允许的**客户端 (Client)**，或者将客户端限制为允许的**版本 (Version)**。

  注释　必须准确地输入版本，因为它会显示在客户端表视图中。如果不指定版本，则白名单会允许所有版本。

步骤 3　点击 **OK**。

步骤 4　要立即实施自上次保存以来进行的所有更改，请点击**保存白名单 (Save White List)**。

将 Web 应用列入白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

使用白名单主机配置文件，您可以全局或在特定操作系统上将 Web 应用列入白名单。

过程

步骤 1 创建或修改白名单主机配置文件时，点击**允许的 Web 应用 (Allowed Web Applications)** 旁的添加图标 ()（或者，如果修改的是全局主机配置文件，则点击**全局允许的 Web 应用 [Globally Allowed Web Applications]** 旁的添加图标）。

步骤 2 选择要允许的 Web 应用。

步骤 3 点击 **OK**

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击**保存白名单 (Save White List)**。

将协议列入白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

使用白名单主机配置文件，您可以在全局范围或在特定操作系统上将协议列入白名单。始终允许在任何主机上运行 ARP、IP、TCP 和 UDP；不能禁用这些协议。

过程

步骤 1 创建或修改白名单主机配置文件时，点击**允许的协议 (Allowed Protocols)** 旁边的添加图标 ()（或者，如果修改的是全局主机配置文件，则点击**全局允许的协议 (Globally Allowed Protocols)** 旁边的添加图标）。

步骤 2 此时您有两种选择：

- 如果列出了要允许的协议，请选择这些协议。Web 界面列出白名单已允许或当前允许的协议。
- 要允许列表中未包含的协议，请选择**<新协议> (<New Protocol>)**，然后点击**确定 (OK)** 显示协议编辑器。从**类型 (Type)** 下拉列表中，选择协议类型（**网络 [Network]** 或**传输 [Transfer]**），然后从下拉列表中选择**协议 (Protocol)**。

  提示 选择 **Other (manual entry)** 以指定不在列表中的通信协议。对于网络协议，请键入 http://www.iana.org/assignments/ethernet-numbers/ 中所列的相应编号。对于传输协议，请键入 http://www.iana.org/assignments/protocol-numbers/ 中所列的相应编号。

步骤 3 点击 **OK**。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击**保存白名单 (Save White List)**。

管理合规白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可以使用“白名单”(White List) 页面管理合规白名单和共享主机配置文件。默认白名单表示建议的设置，并使用共享主机配置文件的一个特殊类别，即内置主机配置文件。

在多域部署中，系统会显示在当前域中创建的合规白名单，您可以对其进行编辑。系统还会显示祖先域中的选定白名单，您不可以对其进行编辑。要查看和编辑在较低域中创建的白名单，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。默认白名单仅在全局域中可用。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**白名单 (White List)** 选项卡。

步骤 2 管理合规白名单：

- 创建 - 要创建新的白名单，请点击**新建白名单 (New White List)**，然后如创建合规白名单，第 1266 页中所述继续操作。
- 删除 - 要删除未使用的白名单，请点击删除图标 ( )，然后确认要删除该白名单。删除白名单还会从网络上所有主机中删除其关联的主机属性。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 编辑 - 要修改现有白名单，请点击编辑图标 ( )，然后如编辑合规白名单，第 1272 页中所述继续操作。如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。
- 共享主机配置文件 - 要管理白名单的共享主机配置文件，请点击**编辑共享配置文件 (Edit Shared Profiles)**，然后如管理共享主机配置文件，第 1274 页中所述继续操作。

编辑合规白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

当修改并保存活动关联策略中包含的合规白名单时，系统会立即重新评估白名单的目标网络中主机的合规性。尽管此重新评估可能会使某些主机合规或不合规，但是系统不会生成任何白名单事件。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**白名单 (White List)** 选项卡。

步骤 2 在要修改的白名单旁，点击编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑合规白名单：

- 名称和说明 - 要更改名称或说明，请点击左侧面板中的白名单名称以显示基本白名单信息，然后键入新信息。
- 允许破解的设备 - 要在网络上允许破解的移动设备，请点击左侧面板中的白名单名称以显示基本白名单信息，然后启用**允许破解的移动设备 (Allow Jailbroken Mobile)**。禁用此选项会导致破解设备生成白名单违规。
- 添加允许的主机配置文件 - 要为此白名单创建操作系统特定主机配置文件，请点击“允许的主机配置文件”(Allowed Host Profiles) 旁边的添加图标 ( )，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 添加共享主机配置文件 - 要向白名单中添加现有共享主机配置文件，请点击**添加共享主机配置文件 (Add Shared Host Profile)**，选择要添加的共享主机配置文件，然后点击**确定 (OK)**。共享主机配置文件以斜体显示。
- 添加目标网络 - 要添加新的目标网络而不调查其主机，请点击“目标网络”(Target Networks) 旁边的添加图标 ( )，然后如为合规白名单创建目标网络，第 1267 页中所述继续操作。
- 删除主机配置文件 - 要从白名单中删除共享主机配置文件或操作系统特定主机配置文件，请点击主机配置文件旁边的删除图标 ( )，然后确认选择。删除共享主机配置文件会从白名单中将其移除，但是不会删除该配置文件，也不会从使用它的任何其他白名单中将其移除。您无法删除白名单的全局主机配置文件。
- 删除目标网络 - 要从白名单中移除目标网络，请点击网络旁边的删除图标 ( )，然后确认选择。
- 编辑全局主机配置文件 - 要编辑白名单的全局主机配置文件，请点击**任何操作系统 (Any Operating System)**，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 编辑其他主机配置文件 - 要编辑共享主机配置文件或操作系统特定主机配置文件，请点击该主机配置文件的名称，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 编辑目标网络 - 要编辑目标网络，请点击网络的名称，然后如为合规白名单创建目标网络，第 1267 页中所述继续操作。

步骤 4 要立即实施自上次保存以来进行的所有更改，请点击**保存白名单 (Save White List)**。

管理共享主机配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在合规白名单中，共享主机配置文件绑定到特定操作系统，但是您可以在多个白名单中使用每个共享主机配置文件。如果创建了多个白名单，但要使用相同的主机配置文件来评估运行白名单中规定的特定操作系统的主机，可使用共享主机配置文件。

在多域部署中，系统会显示在当前域中创建的共享主机配置文件，您可以对其进行编辑。系统还会显示祖先域中的共享主机配置文件，您不可以对其进行编辑。要查看和编辑在较低域中创建的共享主机配置文件，请切换至该域。

注释 如果修改共享主机配置文件（包括内置主机配置文件），或者修改内置应用协议、协议或客户端，则更改会影响使用它的每个白名单。如果无意中更改或删除了这些内置元素，则可以重置为出厂默认设置。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**白名单 (White List)** 选项卡。

步骤 2 点击 **Edit Shared Profiles**。

步骤 3 管理共享主机配置文件：

- 创建共享主机配置文件 - 要创建新的共享主机配置文件而不调查主机，请点击共享主机配置文件旁边的添加图标 ( )，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 通过调查创建共享主机配置文件 - 要通过调查网络创建多个新的共享主机配置文件，请点击**添加目标网络 (Add Target Network)**，然后如为合规白名单创建目标网络，第 1267 页中所述继续操作。
- 删除 - 要删除共享主机配置文件，请点击删除图标 ( )，然后确认您的选择。
- 编辑 - 要修改现有的共享主机配置文件（包括内置共享主机配置文件），请点击其名称，然后如构建白名单主机配置文件，第 1268 页中所述继续操作。
- 重置内置主机配置文件 - 要将所有内置主机配置文件重置为出厂默认设置，请点击**内置主机配置 (Built-in Host Profiles)**，然后点击**重置为出厂默认设置 (Reset to Factory Defaults)** 并确认您的选择。

步骤 4 要立即实施自上次保存后做出的所有更改，请点击**保存所有配置文件 (Save All Profiles)**。

第 70 章

关联策略

以下主题介绍如何配置关联策略和规则。

关联策略和规则简介

您可以通过关联功能，使用关联策略实时应对网络威胁。

当网络活动触发某个活动的关联策略中的关联规则或合规白名单时，会导致关联策略违规的发生。

关联规则

当活动的关联策略中的关联规则触发时，系统会生成关联事件。关联规则可在以下情况下触发：

- 系统生成特定类型的事件（连接、入侵、恶意软件、发现、用户活动等）。
- 网络流量偏离其正常的量变曲线。

可以通过下列方式限制关联规则：

- 添加主机配置文件限定条件以使用涉及触发事件的主机的主机配置文件中的信息限制该规则。
- 将连接跟踪器添加至关联规则，以便在满足规则的初始条件后，系统开始跟踪某些连接。然后，只有在跟踪的连接满足其他标准时，才可生成关联事件。
- 将用户资格添加至关联规则以跟踪某些用户或用户群。例如，您可以限制关联规则，以便只有特定用户的流量或来自特定部门的流量才会触发该关联规则。
- 添加暂停周期。当关联规则触发后，暂停周期会导致该规则在指定时间间隔内不会再次触发。暂停周期过后，该规则可再次触发并开始新的暂停周期。

- 添加非活动周期在非活动周期，关联规则不会触发。

虽然您可以配置关联规则而不对您的部署授予许可，但使用未经许可组件的规则不会触发。

合规白名单

合规白名单指定允许在网络中的主机上运行的操作系统、应用（Web 和客户端）及协议。当主机违反活动的关联策略中使用的白名单时，系统会生成白名单事件。

关联响应

对关联策略违规的响应包括简单的警报以及各种补救（例如扫描主机）。可以将每个关联规则或白名单与单个响应或一组响应相关联。

如果网络流量触发多个规则或白名单，系统将发起与每个规则和白名单相关的所有响应。

关联和多租户

在多域部署中，可以在任意域级别创建关联策略，只要使用的是该级别可用的规则、白名单和响应。高层域管理员可以在域中或跨域执行关联：

- 按域限制关联规则将匹配该域的后代所报告的事件。
- 高层域管理员可以跨域创建评估主机的合规白名单。您可以在同一个白名单中以不同域中的不同子网作为目标。

注释 系统会为每个枝叶域构建单独的网络映射。使用文字配置（例如IP地址、VLAN标记和用户名）限制跨域关联规则可能会出现意外结果。

配置关联策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

使用关联规则、合规白名单、警报响应和补救来构建关联策略。

在多域部署中，可以在任何域级别使用该级别可用的任何构成配置来创建关联策略。

可为每个关联策略以及该策略中使用的每条规则和白名单分配优先级。规则和白名单优先级会覆盖关联策略优先级。如果网络流量违反关联策略，则产生的关联事件会显示策略优先级值，除非违反的规则或白名单有自己的优先级。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**。

步骤 2 点击 **Create Policy**。

步骤 3 输入**策略名称 (Policy Name)** 和**策略说明 (Policy Desription)**。

步骤 4 从**默认优先级 (Default Priority)** 下拉列表中选择策略的优先级。选择**无 (None)** 以便仅使用规则的优先级。

步骤 5 点击**添加规则 (Add Rules)**，选择要在策略中使用的规则和白名单，然后点击**添加 (Add)**。

步骤 6 从每个规则或白名单的**优先级 (Priority)** 列表中选择优先级：

- 优先级值介于 1 到 5 之间。
- **无**
- **Default**，以使用策略的默认优先级

步骤 7 将响应添加到规则和白名单中，如将响应添加到规则和白名单，第 1279 页中所述。

步骤 8 点击**保存 (Save)**。

接下来的操作

- 通过点击滑块来激活策略。

将响应添加到规则和白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

可以将每个关联规则或白名单与单个响应或一组响应相关联。如果网络流量触发多个规则或白名单，系统将发起与每个规则和白名单相关的所有响应。请注意，Nmap 补救在用作对流量量变曲线更改的响应时不会启动。

在多域部署中，可以使用在当前域或祖先域中创建的或响应。

过程

步骤 1 在关联策略编辑器中要添加响应的规则或白名单旁边，点击响应图标 ()。

步骤 2 在“未分配的响应”(Unassigned Responses) 下，选择在规则或白名单触发时要启动的响应，然后点击向上箭头 (^)。

步骤 3 点击**更新 (Update)**。

管理关联策略

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

对活动关联策略进行的更改会立即生效。

激活关联策略时，系统会立即开始处理事件并触发响应。请注意，系统不会在初次、激活后的评估中为不合规主机生成白名单事件。

在多域部署中，系统会显示在当前域中创建的关联策略，您可以对其进行编辑。系统还会显示来自祖先域中的选定关联策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的关联策略，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**。

步骤 2 管理关联策略：

- 激活或停用 - 点击滑块。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 创建 - 点击**创建策略 (Create Policy)**；请参阅配置关联策略，第 1278 页。
- 编辑 - 点击编辑图标 ()；请参阅配置关联策略，第 1278 页。如果改为显示查看图标 ()，则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 点击删除图标 ()。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置关联规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

简单的关联规则仅要求发生特定类型的事件。您不需要提供更具体的条件。例如，基于流量量变曲线变更的关联规则不需要条件。您也可以使用多个条件和添加的限制来创建复杂的关联规则。

当创建关联规则触发条件、主机配置文件限定条件、用户资格或连接跟踪器时，语法发生变化但结构保持不变。

注释 在多域部署中，按祖先域限制关联规则将匹配该域的后代所报告的事件。

开始之前

- 确认您的部署正在收集您要用来触发关联事件的信息类型。例如，任意单个连接或连接摘要事件的可用信息取决于几个因素，包括检测方法、日志记录方法和事件类型。系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**规则管理 (Rule Management)** 选项卡。

步骤 2 点击 **Create Rule**。

步骤 3 输入**规则名称 (Rule Name)** 和**规则说明 (Rule Description)**。

步骤 4 或者，也可为规则选择**规则组 (Rule Group)**。

步骤 5 选择基础事件类型，并为关联规则指定其他触发条件（后者为可选项）。您可以选择以下基础事件类型：

- **发生入侵事件 (an intrusion event occurs)** - 请参阅入侵事件触发条件的语法，第 1282 页。
- **发生恶意软件事件 (a malware event occurs)** - 请参阅恶意软件事件触发条件的语法，第 1285 页。
- **发生发现事件 (a discovery event occurs)** - 请参阅发现事件触发条件的语法，第 1286 页。
- **检测到用户活动 (user activity is detected)** - 请参阅用户活动事件触发条件的语法，第 1289 页。
- **发生主机输入事件 (a host input event occurs)** - 请参阅主机输入事件触发条件的语法，第 1290 页。
- **发生连接事件 (a connection event occurs)** - 请参阅连接事件触发条件的语法，第 1291 页。

- **流量量变曲线更改 (a traffic profile changes)** - 请参阅流量量变曲线更改的语法，第 1294 页。

步骤 6 或者，也可以通过添加以下任一项或全部条件来进一步限制关联规则：

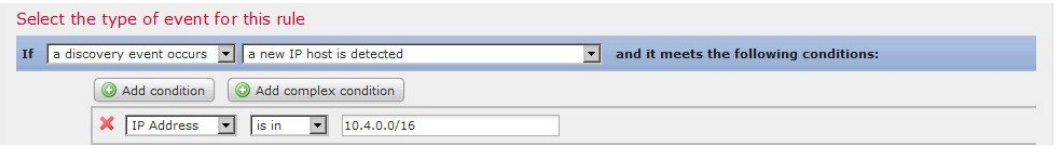
- 主机配置文件限定条件 - 点击**添加主机配置文件限定条件 (Add Host Profile Qualification)**；请参阅关联主机配置文件限定条件的语法，第 1296 页。
- 连接跟踪器 - 点击**添加连接跟踪器 (Add Connection Tracker)**；请参阅连接跟踪器，第 1300 页。
- 用户资格 - 点击**添加用户资格 (Add User Qualification)**；请参阅用户资格的语法，第 1299 页。
- 暂停周期 - 在“规则选项”(Rule Options) 下，使用**暂停 (Snooze)** 文本字段和下拉列表指定在关联规则触发后系统要再次触发该规则应等待的时间间隔。
- 非活动周期 - 在“规则选项”(Rule Options) 下，点击**添加非活动周期 (Add Inactive Period)**。使用文本字段和下拉列表，指定您希望系统停止根据关联规则评估网络流量的时间和频率。

提示 要移除暂停周期，请将时间间隔指定为 0（秒、分钟或小时）。

步骤 7 点击**保存规则 (Save Rule)**。

简单的关联规则示例

如果在特定子网中检测到新的主机，则会触发以下简单的关联规则。请注意，当类别为 IP 地址时，选择 **is in** 或 **is not in** 作为运算符使您可以指定 IP 地址是还是不是在 IP 地址块中，如特殊表示法（例如 CIDR）所述。



接下来的操作

- 使用关联策略中的规则，如配置关联策略，第 1278 页中所述。

入侵事件触发条件的语法

下表介绍将入侵事件选定为基础事件时如何构建关联规则条件。

表 *202*：入侵事件的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择使用生成入侵事件的入侵策略的一个或多个访问控制策略。

如果您指定.....	选择运算符，然后.....
Access Control Rule Name	输入使用生成入侵事件的入侵策略的访问控制规则的全部或部分名称。
应用协议	选择一个或多个与入侵事件关联的应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
分类	选择一个或多个分类。
Client	选择一个或多个与入侵事件关联的客户端。
Client Category	选择一个或多个客户端类别。
Destination Country 或 Source Country	选择一个或多个与入侵事件中的源或目标 IP 地址关联的国家/地区。
目标 IP、源 IP、源 IP 和目标 IP，或者源 IP 或目标 IP	输入单个 IP 地址或地址块。
Destination Port/ICMP Code 或 Source Port/ICMP Type	输入源流量的端口号或 ICMP 类型或目标流量的端口号或 ICMP 代码。
设备	选择一个或多个可能生成事件的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
出口接口或入口接口	选择一个或多个接口。
Egress Security Zone 或 Ingress Security Zone	选择一个或多个安全区域。
Generator ID	选择一个或多个预处理器。
Impact Flag	选择分配给入侵事件的影响级别。 对于从NetFlow数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”(Vulnerable)（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。
Inline Result	选择系统**已丢弃 (dropped)** 还是**应该已丢弃 (would have dropped)** 违反入侵策略的数据包。 在内联、交换或路由部署中，系统可以丢弃数据包。但是在被动部署中，包括当内联集处于分路模式下时，不管入侵规则状态或入侵策略的丢弃行为如何，系统都无法丢弃数据包。
入侵策略	选择一个或多个生成入侵事件的入侵策略。

如果您指定.....	选择运算符，然后.....
IOC Tag	选择危害表现标记是不是因为入侵事件而设置。
优先级	选择规则优先级。 对于基于规则的入侵事件，优先级对应于`priority`关键字的值或`classtype`关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。
协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
Rule Message	输入全部或部分规则消息。
Rule SID	输入由逗号分隔的单个 Snort ID (SID) 或多个 SID。 如果将 **is in** 或 **is not in** 选定为运算符，则无法使用具有多项选择的弹出窗口。必须输入由逗号分隔的 SID 列表。
规则类型	指定规则是否本地规则。 本地规则包括自定义的标准文本入侵规则、经您修改的标准文本规则，以及您在保存包含已修改报头信息时创建的共享对象规则的任何新实例。
SSL Actual Action	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL Certificate Fingerprint	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL Certificate Subject Common Name (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL Certificate Subject Country (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL Certificate Subject Organization (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL Certificate Subject Organizational Unit (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL Flow Status	基于系统尝试解密流量的结果选择一种或多种状态。
用户名	输入登录入侵事件中的源主机的用户的用户名。
VLAN ID	输入与触发入侵事件的数据包关联的最内部的 VLAN ID
Web 应用	选择与入侵事件关联的一个或多个 Web 应用。
Web Application Category	选择一种或多种 Web 应用类别。

恶意软件事件触发条件的语法

要使关联规则基于恶意软件事件，首先得指定要使用的恶意软件事件类型。您的选择决定您可以使用的一组触发条件。您可以选择：

- **通过基于终端的恶意软件检测**（面向终端的 AMP）
- **通过基于网络的恶意软件检测**（面向网络的 AMP）
- **通过基于网络的追溯性恶意软件检测**（面向网络的 AMP）

下表介绍将恶意软件事件选定为基础事件时如何构建关联规则条件。

表 *203*：恶意软件事件的语法

如果您指定.....	选择运算符，然后.....
应用协议	选择一个或多个与恶意软件事件相关的应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Client	选择一个或多个与恶意软件事件相关的客户端。
Client Category	选择一个或多个客户端类别。
Destination Country 或 Source Country	选择一个或多个与恶意软件事件中的源或目标 IP 地址相关的国家/地区。
Destination IP, Host IP, or Source IP	输入单个 IP 地址或地址块。
Destination Port/ICMP Code	输入目标流量的端口号或 ICMP 代码。
处理结果	选择**恶意软件 (Malware)** 或 **自定义检测 (Custom Detection)** 或选择两者。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
事件类型	选择一个或多个与基于终端的恶意软件事件相关的事件类型。
文件名	输入文件的名称。
文件类型	选择文件类型。
File Type Category	选择一个或多个文件类型类别。
IOC Tag	选择危害表现标记**是 (is)** 还是**不是 (is not)** 因为恶意软件事件而设置。

如果您指定.....	选择运算符，然后.....
SHA-256	输入或粘贴文件的 SHA-256 散列值。
SSL Actual Action	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL Certificate Fingerprint	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL Certificate Subject Common Name (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL Certificate Subject Country (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL Certificate Subject Organization (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL Certificate Subject Organizational Unit (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL Flow Status	基于系统尝试解密流量的结果选择一种或多种状态。
Source Port/ICMP Type	输入源流量的端口号或 ICMP 类型。
Web 应用	选择一个或多个与恶意软件事件相关的 Web 应用。
Web Application Category	选择一种或多种 Web 应用类别。

发现事件触发条件的语法

要使关联规则基于发现事件，首先得指定要使用的发现事件类型。您的选择决定您可以使用的一组触发条件。下表列出可以选择的发现事件类型。

在跃点变更上或由于达到主机限制而使系统丢弃新的主机时，不能触发关联规则。然而，当任何类型的发现事件发生时，可选择 **there is any type of event** 来触发该规则。

表 *204*: 关联规则触发条件对比发现事件类型

选择的选项	要使用的发现事件类型
a client has changed	Client Update
a client timed out	Client Timeout
a host IP address is reused	DHCP: IP Address Reassigned
a host is deleted because the host limit was reached	Host Deleted: Host Limit Reached

选择的选项	要使用的发现事件类型
a host is identified as a network device	Host Type Changed to Network Device
a host timed out	Host Timeout
a host’s IP address has changed	DHCP: IP Address Changed
a NETBIOS name change is detected	NETBIOS Name Change
a new client is detected	New Client
a new IP host is detected	New Host
a new MAC address is detected	Additional MAC Detected for Host
a new MAC host is detected	New Host
a new network protocol is detected	New Network Protocol
a new transport protocol is detected	New Transport Protocol
a TCP port closed	TCP Port Closed
a TCP port timed out	TCP Port Timeout
a UDP port closed	UDP Port Closed
a UDP port timed out	UDP Port Timeout
a VLAN tag was updated	VLAN Tag Information Update
an IOC was set	Indication of Compromise
an open TCP port is detected	New TCP Port
an open UDP port is detected	New UDP Port
the OS information for a host has changed	New OS
the OS or server identity for a host has a conflict	Identity Conflict
the OS or server identity for a host has timed out	Identity Timeout
there is any kind of event	任何事件类型
there is new information about a MAC address	MAC Information Change
there is new information about a TCP server	TCP Server Information Update

选择的选项	要使用的发现事件类型
there is new information about a UDP server	UDP Server Information Update

下表介绍将发现事件选定为基础事件时如何构建关联规则条件。

表 *205*: 发现事件的语法

如果您指定.....	选择运算符，然后.....
应用协议	选择一个或多个应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Application Port	输入应用协议端口号。
Client	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
Client Version	输入客户端的版本号。
设备	选择一个或多个可能生成发现事件的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
硬件	输入移动设备的硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 iPhone。
Host Type	选择一个或多个主机类型。可以在一个主机或多种网络设备中的一种之间选择。
“IP 地址”(IP Address) 或“新建 IP 地址”(New IP Address)	输入单个 IP 地址或地址块。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。
MAC Address	输入主机的全部或部分 MAC 地址。 例如，如果知道特定硬件制造商的设备拥有的 MAC 地址以 0A:12:34 开头，则可选择**开头为 (begins with)** 作为运算符，然后输入 0A:12:34 作为值。

如果您指定.....	选择运算符，然后.....
MAC Type	选择 MAC 地址是否是**按 ARP/DHCP 检测 (ARP/DHCP Detected)**。 例如，选择系统是否将 MAC 地址明确识别为属于主机（**按 ARP/DHCP 检测 [is ARP/DHCP Detected]**），或者因为，打个比方，受管设备和主机之间有路由器，因此系统是否可以看见许多具有该 MAC 地址的主机（**不是按 ARP/DHCP 检测 [is not ARP/DHCP Detected}**）。
MAC Vendor	输入触发发现事件的网络流量使用的 NIC 的 MAC 硬件供应商的全部或部分名称。
移动设备	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NETBIOS Name	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
OS Name	选择一个或多个操作系统名称。
操作系统供应商	选择一个或多个操作系统供应商。
OS Version	选择一个或多个操作系统版本。
“协议”(Protocol) 或“传输协议”(Transport Protocol)	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
来源	选择主机输入数据的源（用于操作系统和服务器标识更改与超时）。
Source Type	选择主机输入数据的源的类型（用于操作系统和服务器标识更改与超时）。
VLAN ID	输入涉及事件的主机的 VLAN ID。
Web 应用	选择 Web 应用。

用户活动事件触发条件的语法

要将关联规则以用户活动为基础，请首先选择要使用的用户活动的类型。您的选择决定您可以使用的一组触发条件。您可以选择：

- **检测到的新用户身份**
- **登录到主机的用户**

下表介绍将用户活动选定为基础事件时如何构建关联规则条件。

表 *206*：用户活动的语法

如果您指定.....	选择运算符，然后.....
设备	选择可能检测到用户活动的一个或多个设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
IP 地址	输入单个 IP 地址或地址块。
用户名	输入用户名。

主机输入事件触发条件的语法

要使关联规则基于主机输入事件，首先得指定要使用的主机输入事件类型。您的选择决定您可以使用的一组触发条件。下表列出可以选择的主机输入事件类型。

当添加、删除或更改用户定义的主机属性的定义，或设置漏洞影响限定条件时，不能触发关联规则。

表 *207*：关联规则触发条件与主机输入事件类型

选择的选项	要在该事件类型上触发规则.....
a client is added	Add Client
a client is deleted	Delete Client
a host is added	Add Host
a protocol is added	Add Protocol
a protocol is deleted	Delete Protocol
a scan result is added	Add Scan Result
a server definition is set	Set Server Definition
a server is added	Add Port
a server is deleted	Delete Port
a vulnerability is marked invalid	Vulnerability Set Invalid
a vulnerability is marked valid	Vulnerability Set Valid
an address is deleted	Delete Host/Network

选择的选项	要在该事件类型上触发规则.....
an attribute value is deleted	Host Attribute Delete Value
an attribute value is set	Host Attribute Set Value
an OS definition is set	Set Operating System Definition
host criticality is set	Set Host Criticality

下表介绍将主机输入事件选定为基础事件时如何构建关联规则条件。

表 *208*：主机输入事件的语法

如果您指定.....	选择运算符，然后.....
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
IP 地址	输入单个 IP 地址或地址块。
来源	选择主机输入数据的源。
Source Type	选择主机输入数据的源类型。

连接事件触发条件的语法

要使关联规则基于连接事件，首先指定要使用的连接事件类型。请注意，可用于连接事件的信息可能会根据系统记录连接的方式、原因和时间而异。您可以选择：

- 位于连接开头或末尾
- 位于连接开头
- 位于连接末尾

下表介绍将连接事件选定为基础事件时如何构建关联规则条件。

表 *209*：连接事件的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择记录连接的一个或多个访问控制策略。

如果您指定.....	选择运算符，然后.....
Access Control Rule Action	选择与记录连接的访问控制规则相关的一个或多个操作。 当网络流量与任何监控规则的条件匹配时，不管随后处理连接的规则或默认操作如何，都选择**监控 (Monitor)** 以触发关联事件。
Access Control Rule	输入记录连接的访问控制规则的全部或部分名称。 不管随后处理连接的规则或默认操作如何，您都可以输入其条件与连接匹配的任何监控规则的名称。
应用协议	选择一个或多个与连接相关的应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Client	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
Client Version	输入客户端的版本号。
Connection Duration	输入连接事件的持续时间，单位为秒。
连接类型	指定是否要根据获取连接信息的方式触发关联规则： • 为已导出 NetFlow 数据生成的连接事件选择**是 (is)** 和 **Netflow**。 • 为 Firepower 系统受管设备检测到的连接事件选择**不是 (is not)** 和 **Netflow**。
Destination Country 或 Source Country	选择一个或多个与连接事件中的源或目标 IP 地址相关的国家/地区。
设备	选择一个或多个检测到连接或处理连接（对于已导出 NetFlow 记录的连接数据）的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
出口接口或入口接口	选择一个或多个接口。
Egress Security Zone 或 Ingress Security Zone	选择一个或多个安全区域。
“发起方字节数”(Initiator Bytes)、“响应方字节数”(Responder Bytes) 或“总字节数”(Total Bytes)	输入以下其中一项： • 发送的字节数（**发起方字节数 [Initiator Bytes]**）。 • 接收的字节数（**响应方字节数 [Responder Bytes]**）。 • 发送和接收的字节数（**总字节数 [Total Bytes]**）。

如果您指定.....	选择运算符，然后.....
“发起方 IP”(Initiator IP)、“响应方 IP”(Responder IP)、“发起方和响应方 IP”(Both Initiator and Responder IP) 或“发起方 IP 或响应方 IP 之一”(Either Initiator IP or Responder IP)	指定单个 IP 地址或地址块。
“发起方数据包数”(Initiator Packets)、“响应方数据包数”(Responder Packets) 或“数据包总数”(Total Packets)	输入以下其中一项： • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**）。 • 接收的数据包数量（**响应方数据包数 [Responder Packets]**）。 • 发送和接收的数据包数量（**数据包总数 [Total Packets]**）
Initiator Port/ICMP Type 或 Responder Port/ICMP Code	输入发起方流量的端口号或 ICMP 类型或接收方流量的端口号或 ICMP 类型。
IOC Tag	指定危害表现标记**是 (is)** 还是**不是 (is not)** 因为连接事件而设置。
NetBIOS Name	输入连接中受监控主机的 NetBIOS 名称。
NetFlow Device	选择要用于触发关联规则的 NetFlow 导出器的 IP 地址。如果没有将任何 NetFlow 导出器添加到网络发现策略，则 **NetFlow 设备 (NetFlow Device)** 下拉列表为空。
Reason	选择一个或多个与连接事件关联的原因。
Security Intelligence Category	选择一个或多个与连接事件关联的安全情报类别。 要将安全情报类别用作连接结束事件的条件，请在访问控制策略中该类别设置到**监控 (Monitor)** 而非**阻止 (Block)** 中。
SSL Actual Action	指定指示系统如何处理加密连接的 SSL 规则操作。
SSL Certificate Fingerprint	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书状态	选择一个或多个与用于加密会话的证书关联的状态。
SSL Certificate Subject Common Name (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL Certificate Subject Country (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL Certificate Subject Organization (O)	输入用于加密会话的证书的全部或部分使用者组织名称。

如果您指定.....	选择运算符，然后.....
SSL Certificate Subject Organizational Unit (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL Cipher Suite	选择一个或多个用于加密会话的加密套件。
SSL Encrypted Session	选择**已成功解密 (Successfully Decrypted)**。
SSL Flow Status	基于系统尝试解密流量的结果选择一种或多种状态。
SSL 策略	选择一个或多个记录加密连接的 SSL 策略。
SSL Rule Name	输入记录加密连接的 SSL 规则的全部或部分名称。
SSL Server Name	输入客户端用来建立加密连接的服务器的全部或部分名称。
SSL URL Category	选择一个或多个在加密连接中受访的 URL 的 URL 类别。
SSL Version	选择一个或多个用于加密会话的 SSL 或 TLS 版本。
TCP Flags	选择为了触发关联规则，连接事件必须包含的 TCP 标志。只有 NetFlow 记录生成的连接数据包含 TCP 标志。
传输协议	输入连接使用的传输协议：TCP 或 UDP。
URL	输入在连接中受访的全部或部分 URL。
URL 类别	选择一个或多个在连接中受访的 URL 的 URL 类别。
URL Reputation	选择一个或多个在连接中受访的 URL 的 URL 信誉值。
用户名	输入登录连接中的任一主机的用户的用户名。
Web 应用	选择一个或多个与连接关联的 Web 应用。
Web Application Category	选择一种或多种 Web 应用类别。

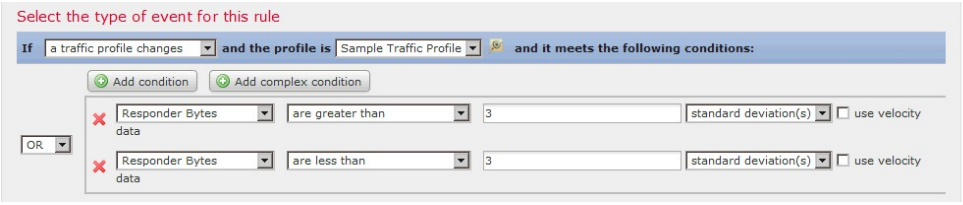
流量量变曲线更改的语法

要使关联规则基于流量量变曲线更改，首先选择要使用的流量量变曲线。当网络流量偏离以您所选量变曲线为特征的模式时，触发此规则。

可以基于原始数据或从计算数据得出的统计结果触发该规则。例如，您可以编写如果通过网络的数据量（单位：字节）突然达到高峰时触发的规则，该高峰可能是由于攻击或其他安全策略违规造成的。如果出现下列两种情况中的一种，可以指定规则触发：

- 通过网络的字节数量激增，超过一定数量的字节
- 通过网络的字节数激增，超过流量平均值上下的一定数量的标准偏差

请注意，要创建在通过网络的字节数超出一定数量的标准偏差（高于或低于）时触发的规则，必须指定上下限，如下图所示。



要创建在通过网络的字节数超过一定数量的高于平均值的标准偏差时触发的规则，请仅使用图中所示的第一个条件。

要创建在通过网络的字节数超过一定数量的低于平均值的标准偏差时触发的规则，请仅使用第二个条件。

选中**使用速度数据 (use velocity data)** 复选框，以基于数据点之间的变化率触发关联规则。如果要使用上例中的速度数据，则可以指定在出现下列任何一种情况时触发规则：

- 通过网络的字节数量变化幅度非常大，高于或低于一定数量的高于平均变化率的标准偏差
- 通过网络的字节数激增，高于一定数量的字节

下表介绍在将流量量变曲线变更选定为基础事件时如何构建关联规则中的条件。

表 *210*：流量量变曲线更改的语法

如果您指定.....	选择运算符，然后输入.....	然后选择以下之一.....
连接数	检测到的连接总数 **或** 高于或低于平均值的标准偏差的数量，检测到的连接数量必须在此范围内以触发该规则	连接 standard deviation(s)
总字节数、发起方字节数或响应方字节数	以下任一项： • 发送的总字节数 (**Total Bytes**) • 发送的字节数 (**Initiator Bytes**) • 接收的字节数 (**Responder Bytes**) **或** 高于或低于平均值的标准偏差的数量，上述标准之一必须在此范围内以触发该规则	字节 standard deviation(s)

如果您指定.....	选择运算符，然后输入.....	然后选择以下之一.....
数据包总数、发起方数据包数或响应方数据包数	以下任一项： • 发送的数据包总数 (**Total Packets**) • 发送的数据包数量 (**Initiator Packets**) • 接收的数据包数量 (**Responder Packets**) **或** 高于或低于为平均值的标准偏差的数量，上述标准之一必须在此范围内以触发该规则	数据包 standard deviation(s)
Unique Initiators	发起会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的独立发起方的数量必须为该平均值以触发该规则	initiators standard deviation(s)
Unique Responders	响应会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的独立响应方的数量必须为该平均值以触发该规则	responders standard deviation(s)

关联主机配置文件限定条件的语法

要根据事件中所涉及的主机的主机配置文件来限制关联规则，请添加主机配置文件限定条件。不能将主机配置文件限定条件添加到在恶意软件事件、流量量变曲线更改或新的 IP 主机的检测上触发的关联规则。

当构建主机配置文件限定条件时，先指定要用于限制关联规则的主机。可选择的主机取决于规则的基础事件类型：

- 连接事件 - 选择**响应方主机 (Responder Host)** 或**发起方主机 (Initiator Host)**。
- 入侵事件 - 选择**目标主机 (Destination Host)** 或**源主机 (Source Host)**。
- 发现事件、主机输入事件或用户活动 - 选择**主机 (Host)**。

下表介绍如何构建关联规则的主机配置文件限定条件。

表 *211*：主机配置文件限定条件的语法

如果您指定.....	选择运算符，然后.....
应用协议 (Application Protocol) > 应用协议 (Application Protocol)	选择应用协议。
应用协议 (Application Protocol) > 应用端口 (Application Port)	输入应用协议端口号。
应用协议 (Application Protocol) > 协议 (Protocol)	选择一个协议。
Application Protocol Category	选择类别。
Client > Client	选择客户端。
Client > Client Version	输入客户端版本。
Client Category	选择类别。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
硬件	输入移动设备的硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 iPhone。
主机重要性	选择主机重要性。
Host Type	选择一个或多个主机类型。您可以在一个常规主机或多种网络设备中的一种之间选择。
IOC Tag	选择一个或多个危害表现标记。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。
MAC Address > MAC Address	输入主机的全部或部分 MAC 地址。
MAC Address > MAC Type	选择 MAC 类型是否为“按 ARP/DHCP 检测”(ARP/DHCP detected)： • 系统是否明确地将 MAC 地址识别为属于主机（**按 ARP/DHCP 检测 [ARP/DHCP Detected]**） • 打个比方，因为设备和主机之间有路由器，所以系统看到许多主机具有该 MAC 地址（**不按 ARP/DHCP 检测 [is not ARP/DHCP Detected]**） • MAC 类型不相关（**为任意 [is any]**）

如果您指定.....	选择运算符，然后.....
MAC Vendor	输入主机使用的硬件的全部或部分 MAC 供应商。
移动设备	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NetBIOS Name	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
Operating System > OS Vendor	选择一个或多个操作系统供应商名称。
Operating System > OS Name	选择一个或多个操作系统名称。
Operating System > OS Version	选择一个或多个操作系统版本。
传输协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
VLAN ID	输入主机的 VLAN ID 号。
Web 应用	选择 Web 应用。
Web Application Category	选择类别。
任何可用的主机属性，包括默认合规性白名单主机属性	根据主机属性类型输入或选择适合的值。

使用隐含或通用客户端来构建主机配置文件限定条件

如果系统报告检测到的客户端使用的应用协议名称后跟 `client`（例如，`HTTPS client`），则该客户端是隐含或通用客户端。在这些情况下，系统未检测到特定客户端，但根据服务器响应流量推断客户端的存在。

要使用隐含或通用客户端创建主机配置文件限定条件，应限制使用在响应方主机上而不是客户端上运行的应用协议。

使用事件数据来构建主机配置文件限定条件

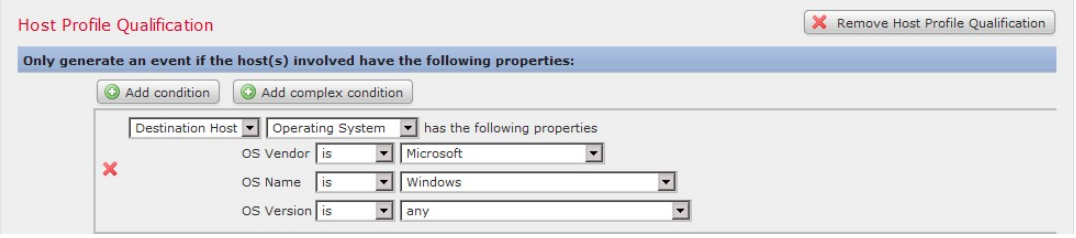
在构建主机配置文件限定条件时，通常可以使用关联规则的基础事件中的数据。

例如，当系统检测到受监控主机之一使用了特定浏览器时，假设触发关联规则。进一步假设，当检测此使用时，如果浏览器版本不是最新版本，则您要生成事件。

您可将主机配置文件限定条件添加到此关联规则，以便只有在**客户端 (Client)** 是**事件客户端 (Event Client)**，但**客户端版本 (Client Version)** 不是最新版本的情况下才会触发规则。

主机配置文件限定条件示例

下列主机配置文件限定条件会限制关联规则，以便该规则仅在涉及作为其基础的发现事件的主机运行一个 Microsoft Windows 版本时才触发。



用户资格的语法

如果您使用连接事件、入侵事件、发现事件或主机输入事件触发关联规则，则您可以基于涉及事件的用户的标识限制该规则。此限制称为用户资格。例如，您可以限制关联规则，以便仅当源用户或目标用户源自销售部门时才会触发关联规则。

不能将用户资格添加到在流量量变曲线发生更改或检测到用户活动时触发的关联规则中。此外，系统还通过在身份领域中建立的 Firepower 管理中心-服务器连接获取用户详细信息。该信息不能提供给数据库中的所有用户。

当构建用户资格时，先指定要用于限制关联规则的身份。可选择的身份取决于规则的基础事件类型：

- 连接事件 - 选择**发起方身份 (Identity on Initiator)** 或**响应方身份 (Identity on Responder)**。
- 入侵事件 - 选择**目标身份 (Identity on Destination)** 或**源身份 (Identity on Source)**。
- 发现事件 - 选择**主机身份 (Identity on Host)**。
- 主机输入事件 - 选择**主机身份 (Identity on Host)**。

下表介绍如何构建关联规则的用户资格。

表 *212*：用户资格的语法

如果您指定.....	选择运算符，然后.....
Authentication Protocol	选择用于检测用户的身份验证协议（或用户类型协议）。
部门	输入部门。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
电子邮件	输入邮箱地址。
名字	输入名字。
姓氏	输入姓氏。

如果您指定.....	选择运算符，然后.....
电话	输入电话号码。
用户名	输入用户名。

连接跟踪器

连接跟踪器限制关联规则，以便在满足规则的初始标准后（包括主机配置文件和用户资格），系统开始跟踪某些连接。如果跟踪的连接满足在指定的时间段内收集到的其他条件，则系统会为规则生成关联事件。

提示 通常，连接跟踪器监控非常具体的流量，而且当被触发时，仅运行指定的一段时间。将连接跟踪器与流量量变曲线进行对比，发现后者一般监控的网络流量范围比较广并且持续运行。

连接跟踪器可以通过两种方法生成事件。

满足条件时，立即触发的连接跟踪器

可以配置连接跟踪器，以便在网络流量满足跟踪器的条件时，立即触发关联规则。如果出现这种情况，即使还没有超过超时周期，系统也为该连接跟踪器实例停止跟踪连接。如果此前触发关联规则的相同类型的策略违规再次发生，则系统可创建新的连接跟踪器。

但是，如果在网络流量满足连接跟踪器中的条件之前时间到期，则系统不会生成关联事件，并且还会停止跟踪该规则实例的连接。

例如，只有在特定类型的连接发生的次数超过一定时间周期内的具体次数时，连接跟踪器才可以通过生成关联事件作为一种事件阈值。或者，只有在初始连接之后，系统检测到其他数据传输时，才可以生成关联事件。

在超时期结束时触发的连接跟踪器

可以配置连接跟踪器，以便连接跟踪器可依靠在整个超时周期内搜集到的数据，因此在超时期末前，您不能触发连接跟踪器。

例如，如果将连接跟踪器配置为在检测到的字节数少于在一定时间周期内传输的一定数量的字节数时即触发，则系统在那段时间周期终止前处于等待状态，然后在网络流量满足该条件时生成事件。

添加连接跟踪器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

开始之前

- 根据连接、入侵、发现、用户身份或主机输入事件创建关联策略。不能将连接跟踪器添加到基于恶意软件事件或流量量变曲线更改的规则。

过程

步骤 1 在关联策略编辑器中，点击**添加连接跟踪器 (Add Connection Tracker)**。

步骤 2 指定要跟踪的连接；请参阅连接跟踪器的语法，第 1301 页。

步骤 3 根据跟踪的连接，指定要生成关联事件的时间；请参阅连接跟踪器事件的语法，第 1303 页。

步骤 4 指定在此期间必须满足跟踪器的条件的时间间隔（单位：秒、分或小时）。

连接跟踪器的语法

下表介绍如何构建指定要跟踪的连接种类的连接跟踪器条件。

表 *213*：连接跟踪器的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择一个或多个处理要跟踪的连接的访问控制策略。
Access Control Rule Action	选择一个或多个与记录要跟踪的连接的访问控制规则关联的访问控制规则操作。 不管随后处理连接的规则或默认操作如何，请选择**监控 (Monitor)** 以跟踪与任何监控规则的条件匹配的连接。
Access Control Rule Name	输入记录要跟踪的连接的访问控制规则的全部或部分名称。 要跟踪匹配监控规则的连接，请输入监控规则的名称。不管随后处理连接的规则或默认操作如何，系统都对连接进行跟踪。
应用协议	选择一个或多个应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Client	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
Client Version	输入客户端的版本。
Connection Duration	输入连接持续时间，以秒为单位。

如果您指定.....	选择运算符，然后.....
连接类型	指定是否要根据获取连接信息的方式触发关联规则： • 为已导出 NetFlow 记录生成的连接事件选择**是 (is)** 和 **Netflow**。 • 为 Firepower 系统受管设备检测到的连接事件选择**不是 (is not)** 和 **Netflow**。
Destination Country 或 Source Country	选择一个或多个国家/地区。
设备	选择一个或多个要跟踪其已检测连接的设备。如果要跟踪NetFlow连接，请选择处理来自已导出 NetFlow 记录的连接数据的设备。
Ingress Interface 或 Egress Interface	选择一个或多个接口。
“入口安全区域”(Ingress Security Zone) 或“出口安全区域”(Egress Security Zone)	选择一个或多个安全区域。
“发起方 IP”(Initiator IP)、“响应方 IP”(Responder IP)、或“发起方/响应方 IP”(Initiator/Responder IP)	输入单个 IP 地址或地址块。
“发起方字节数”(Initiator Bytes)、“响应方字节数”(Responder Bytes) 或“总字节数”(Total Bytes)	输入以下其中一项： • 发送的字节数 (**Initiator Bytes**) • 接收的字节数 (**Responder Bytes**) • 发送和接收的字节数 (**Total Bytes**)
“发起方数据包数”(Initiator Packets)、“响应方数据包数”(Responder Packets) 或“数据包总数”(Total Packets)	输入以下其中一项： • 发送的数据包数量 (**Initiator Packets**) • 接收的数据包数量 (**Responder Packets**) • 发送和接收的数据包数量 (**Total Packets**)。
Initiator Port/ICMP Type 或 Responder Port/ICMP Code	输入发起方流量的端口号或 ICMP 类型或接收方流量的端口号或 ICMP 类型。
IOC Tag	选择危害表现标记是**已设置 (is)** 还是**未设置 (is not)**。
NETBIOS Name	输入连接中受监控主机的 NetBIOS 名称。

如果您指定.....	选择运算符，然后.....
NetFlow Device	选择要跟踪的 NetFlow 导出器的 IP 地址。如果没有将任何 NetFlow 导出器添加到网络发现策略，则“NetFlow 设备”(NetFlow Device) 下拉列表为空。
Reason	选择一个或多个与要跟踪的连接关联的原因。
Security Intelligence Category	选择一个或多个与要跟踪的连接关联的安全情报类别。
TCP Flags	选择为了跟踪连接在连接中必须包含的 TCP 标志。只有导出的 NetFlow 记录生成的连接包含 TCP 标志数据。
传输协议	选择连接使用的传输协议。
URL	输入要跟踪的连接中受访的全部或部分 URL。
URL 类别	选择要跟踪的连接中受访的 URL 的一个或多个 URL 类别。
URL Reputation	选择要跟踪的连接中受访的 URL 的一个或多个 URL 信誉值。
用户名	输入登录要跟踪的连接中的任一主机的用户的用户名。
Web 应用	选择一个或多个 Web 应用。
Web Application Category	选择一个或多个 Web 应用类别。

使用事件数据构建连接跟踪器

在构建连接跟踪器时，通常可以使用关联规则的基础事件中的数据。

例如，假设系统检测到新客户端时会触发关联规则。将连接跟踪器添加到此类型的关联规则时，系统会自动向跟踪器填充指向基础事件的限制：

- **发起方/响应方 IP (Initiator/Responder IP)** 设置为**事件 IP 地址 (Event IP Address)**。
- **客户端 (Client)** 设置为**事件客户端 (Event Client)**。

提示 要跟踪特定 IP 地址或 IP 地址块的连接，请点击**切换至手动输入 (switch to manual entry)** 以手动指定 IP。点击 **switch to event fields** 返回以使用事件中的 IP 地址。

连接跟踪器事件的语法

下表介绍如何构建指定何时基于正在跟踪的连接生成关联事件的连接跟踪器条件。

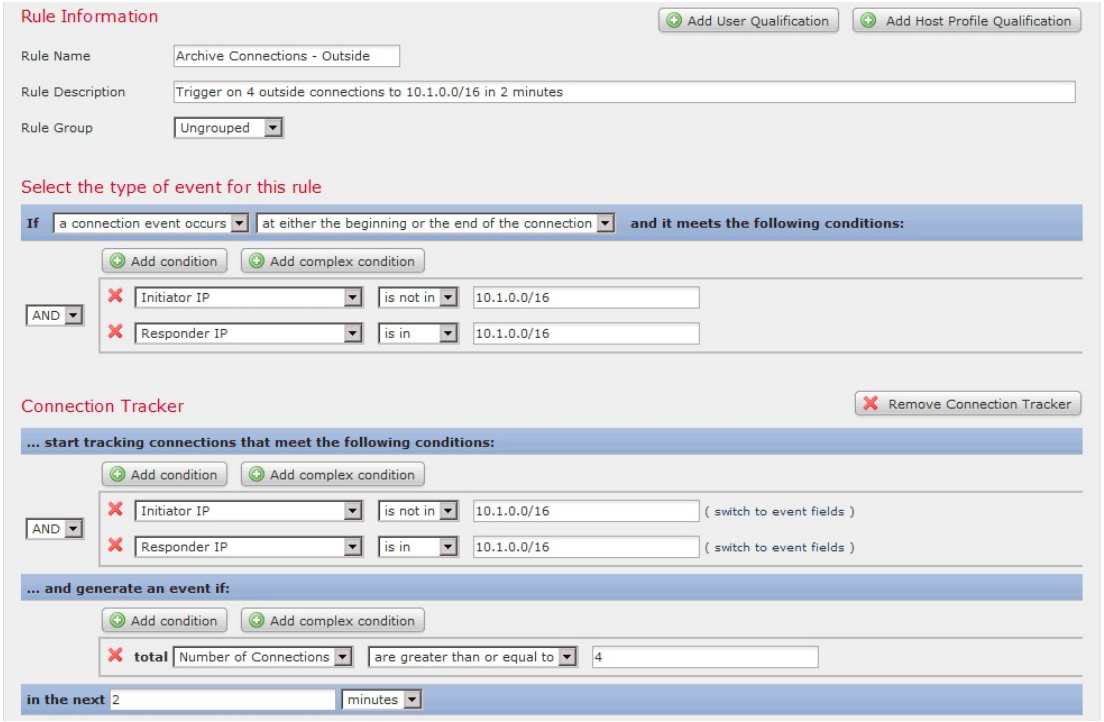
表 *214*：连接跟踪器事件的语法

如果您指定.....	选择运算符，然后输入.....
连接数	检测到的连接总数
Number of SSL Encrypted Sessions	检测到的 SSL 或 TLS 加密会话的总数
总字节数、发起方字节数或响应方字节数	以下任一项： • 发送的总字节数 (**Total Bytes**) • 发送的字节数 (**Initiator Bytes**) • 接收的字节数 (**Responder Bytes**)
数据包总数、发起方数据包数或响应方数据包数	以下任一项： • 发送的数据包总数 (**Total Packets**) • 发送的数据包数量 (**Initiator Packets**) • 接收的数据包数量 (**Responder Packets**)
独立发起方或 独立响应方	以下任一项： • 检测到的发起会话的独立主机的数量 (**Unique Initiators**) • 响应检测到的连接的独立主机的数量 (**Unique Responders**)

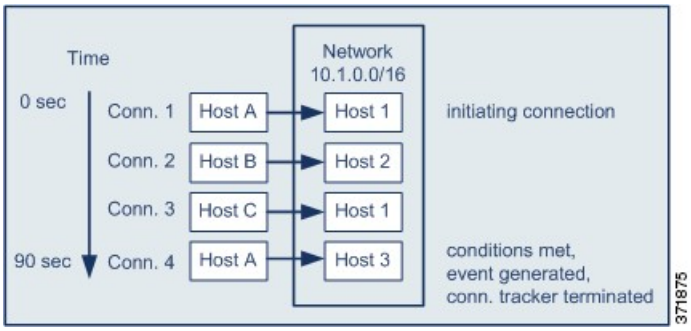
外部主机连接过多的配置示例

考虑这样一个场景：您将敏感文件存档到网络 10.1.0.0/16 上，而且该网络外的主机通常不向网络内的主机发起连接。网络外的主机偶尔会发起连接，但当您确定在两分钟内发起四次或更多次的连接时，则说明有令人担心的问题。

下图所示规则规定 10.1.0.0/16 网络外的主机向网络内的主机发起连接的时间，系统开始跟踪符合该标准的连接。然后，如果系统在两分钟内检测到匹配该签名的四次连接（包括原始连接），系统会生成关联事件。



下图显示网络流量如何触发上述关联规则。



在本示例中，系统检测到满足关联规则的基本条件的连接，即，系统检测到从 10.1.0.0/16 网络外的主机向该网络内的主机及进行的连接。这样创建连接跟踪器。

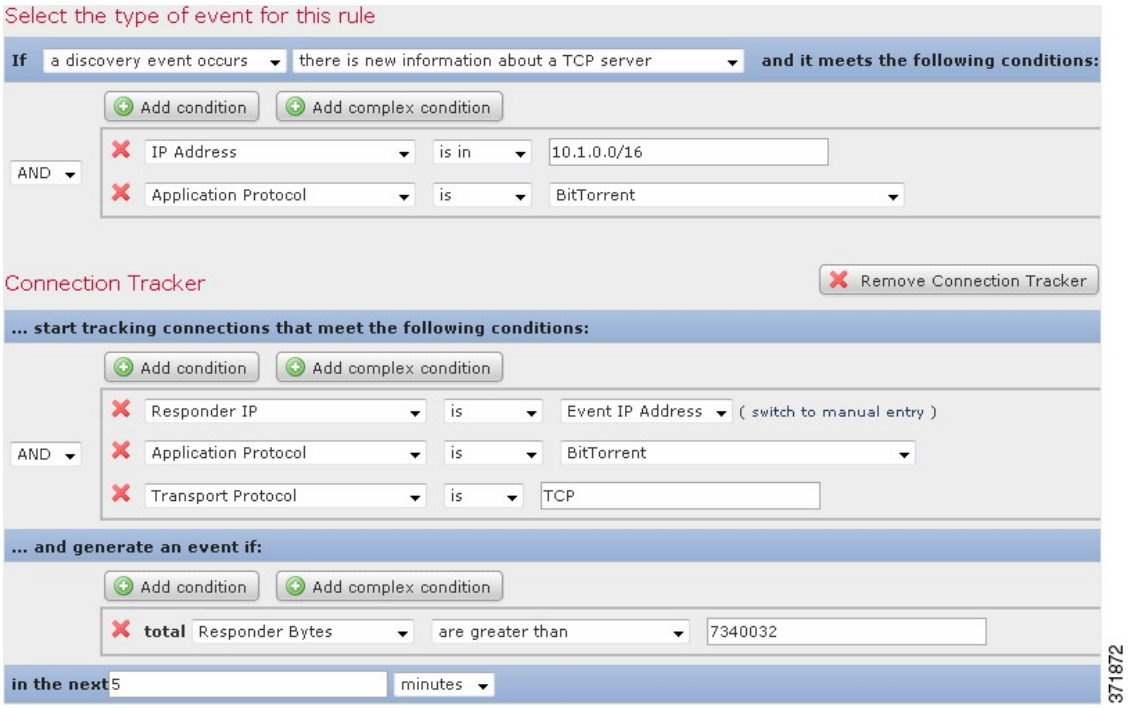
处理连接跟踪器的阶段如下：

- 首先，当系统检测到从网络外的主机 A 向网络内的主机 1 进行的连接时，系统开始跟踪连接。
- 系统检测到符合连接跟踪器特征的两次以上的连接：Host B 至Host 2 和 Host C 至 Host 1。
- 当在两分钟的时间限制内 Host A 连接到 Host 3 时，系统检测到第四次符合特征的连接。满足规则条件。
- 最后，系统生成关联事件，且系统停止跟踪连接。

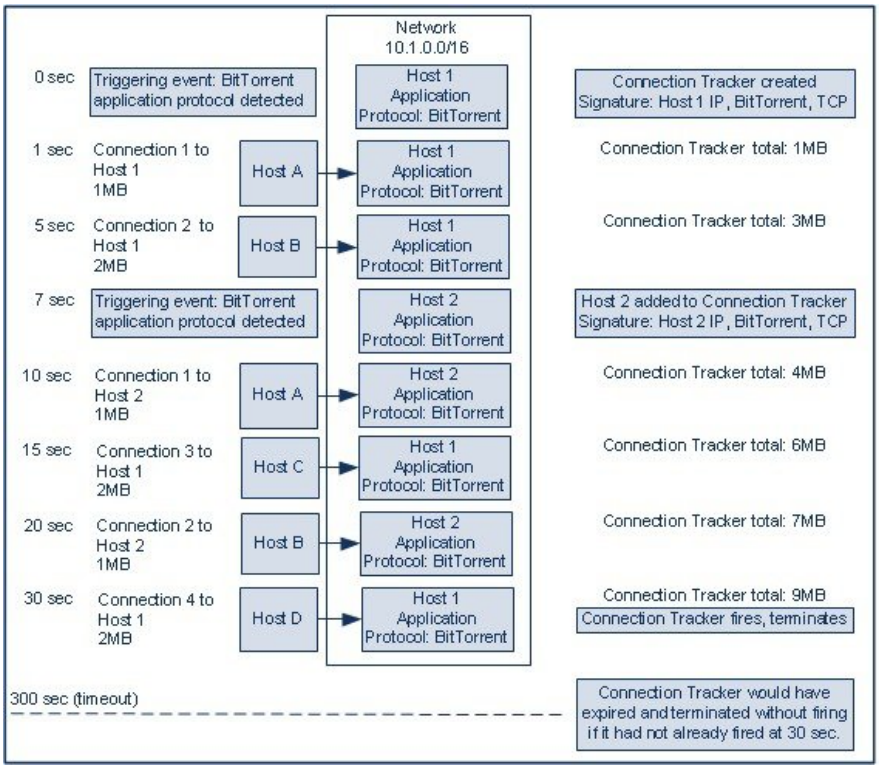
BitTorrent 数据传输过多的配置示例

考虑这样一个场景：要生成关联事件，即使系统检测到在初始连接后其他 BitTorrent 数据传输到受控网络上的任何一台主机。

下图显示当系统检测到受控网络上的 BitTorrent 应用协议时触发的关联规则。该规则具有限制规则的连接跟踪器，以便仅当受控网络（在本例中，受控网络为 10.1.0.0/16）上的主机在出现初始策略违规后的五分钟内通过 BitTorrent 传输的数据共超过 7 MB （7340032 字节）时触发该规则。



下图显示网络流量如何触发上述关联规则。



在本示例中，系统在两个不同的主机上检测到 BitTorrent TCP 应用协议：Host 1 和 Host 2。这两台主机通过 BitTorrent 将数据传输到其他四台主机：Host A、Host B、Host C 和 Host D。

处理该连接跟踪器的阶段如下：

- 首先，当系统检测到 Host 1 上的 BitTorrent 应用协议时，系统开始跟踪 0 秒标记处的连接。请注意，如果系统无法检测到接下来的 5 分钟（按 300 秒标记）内传输的 7 MB 的 BitTorrent TCP 数据，则连接跟踪器将过期。
- 5 秒钟时，Host 1 已经传输符合特征的 3 MB 数据：

  在 1 秒标记处时，从 Host 1 传输至 Host A 的 1 MB 的数据量 （实现连接跟踪器时计算的 1 MB 的 BitTorrent 总流量）

  在 5 秒标记处时，从 Host 1 传输至 Host B 的 2 MB 的数据量（总共 3 MB）

- 在 7 秒种时，系统检测 Host 2 上的 BitTorrent 应用协议，同时也开始跟踪该主机的 BitTorrent 连接。
- 在 20 秒种时，系统已经检测到从 Host 1 和 Host 2 传输的符合特征的其他数据：

  在 10 秒标记处时，从 Host 2 传输至 Host A 的 1 MB 的数据量（总共 4 MB）

  在 15 秒标记处时，从 Host 1 传输至 Host C 的 2 MB 的数据量（总共 6 MB）

  在 20 秒标记处时，从 Host 2 传输至 Host B 的 1 MB 的数据量（总共 7 MB）

- 尽管 Host 1 和 Host 2 目前已经传输 7 MB 的 BitTorrent 综合数据，但因为传输字节总数必须**超过** 7 MB，所以规则不会触发 (**Responder Bytes are greater than 7340032**)。此时，如果系统在跟踪器超时期间余下的 280 秒内没有检测到其他 BitTorrent 数据传输，则跟踪器过期且系统不会生成关联事件。
- 但是，在 30 秒钟时，系统检测到其他 BitTorrent 传输，且满足规则条件：

  在 30 秒标记处时，2 MB 数据从 Host 1 传输至 Host D（总共 9 MB）

- 最后，系统会生成关联事件。此外，尽管 5 分钟的周期尚未过期，但是在该连接跟踪器示例中，系统也停止跟踪连接。如果此时系统检测到使用 BitTorrent TCP 应用协议的新连接，则系统会创建新的连接跟踪器。请注意，在 Host 1 向 Host D 传输总计 2 MB 的数据后，系统生成关联事件，因为其在会话终止后才会计算连接数据。

暂停和非活动周期

您可以在关联规则中配置暂停周期。当关联规则触发时，即使在指定间隔期间违反该规则，暂停周期也会指示系统在该间隔内停止触发该规则。在暂停周期过后，规则可以再次触发（并开始进入新的暂停周期）。

例如，可以将网络上的一个主机设置为永远不产生流量。取决于主机上的网络流量，每当系统检测到涉及该主机的连接时都会触发的简单关联规则可在短时间内创建多个关联事件。要限制披露策略违规的关联事件数量，可以添加暂停周期，以便仅为系统检测到的涉及该主机的第一个连接（在指定的时间周期内）生成关联事件。

此外，还可以在关联规则中设置非活动周期。在非活动周期，关联规则将不会触发。可以将非活动周期设置为每日、每周或每月。例如，可以在内部网络中在夜间扫描Nmap，以寻找主机操作系统的变化情况。在这种情况下，可以在扫描周期在受影响的关联规则上设置每天的非活动周期，以便那些规则不会错误地触发。

关联规则构建机制

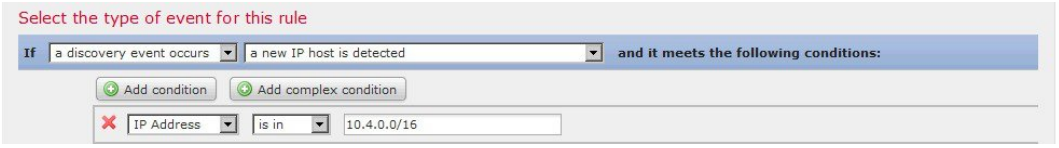
您可通过指定触发条件来构建关联规则。您可以在条件中使用的语法会根据您正在创建的元素而变化，但是机制相同。

大多数条件有三部分：类别、运算符和值。

- 可选择的类别取决于您是在构建关联规则触发器、主机配置文件限定条件、连接跟踪器还是用户资格。在关联规则触发器中，类别的划分进一步取决于规则的基础事件类型。某些条件可能包含多个类别，每个类别都可能有自己的运算符和值。
- 条件的可用运算符取决于类别。
- 可用于指定条件值的语法取决于类别和运算符。有时侯，您可以在文本字段键入值。有时候，您可以从下拉列表中选择一个值（或多个值）。

例如，如果要在每次检测到新主机时都生成关联事件，则可以创建无条件的简单规则。

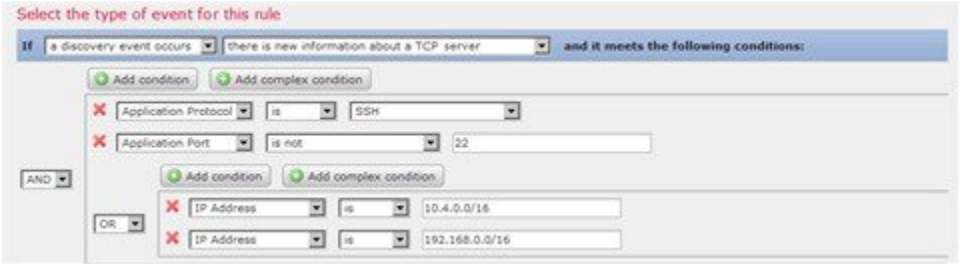
如果要在仅当 10.4.x.x 网络中检测到该新的主机时进一步限制规则并生成事件，则可以添加一个条件。



当构建的结构不止一个条件时，您必须与将这些条件用 **AND** 与 **OR** 操作符结合起来。相同级别的条件会被放在一起评估：

- **AND** 操作符要求必须满足其控制的级别上的所有条件。
- **OR** 操作符要求必须满足其控制的级别上的至少一个条件。

检测 10.4.x.x 网络和 192.168.x.x 网络上的非标准端口的 SSH 活动的以下规则具有四个条件，底部的两个的条件较复杂。



从逻辑上讲，该规则被评估如下：

```
(A and B and (C or D))
```

表 *215*：规则评估

关键字	为陈述以下情况的条件.....
A	Application Protocol 是 SSH
B	Application Port 不是 22
选	IP 地址为 10.0.0.0/8
D	IP Address 为 196.168.0.0/16

注意 评估触发常见事件的复杂关联规则可降低系统的性能。例如，系统必须根据每个已记录的连接评估的多条件规则可能会导致资源超载。

关联规则中的添加和连接条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

过程

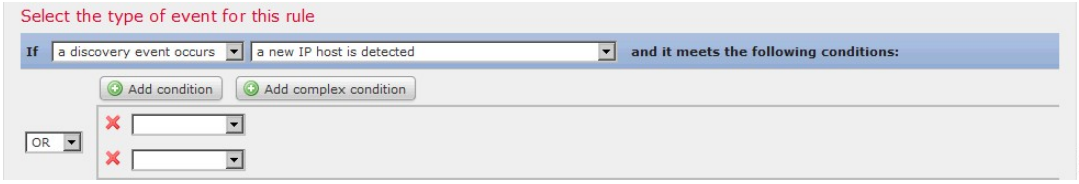
步骤 1 在关联规则编辑器中，添加简单或复杂条件：

- 简单 - 点击**添加条件 (Add condition)**。
- 复杂 - 点击**添加复杂条件 (Add complex condition)**。

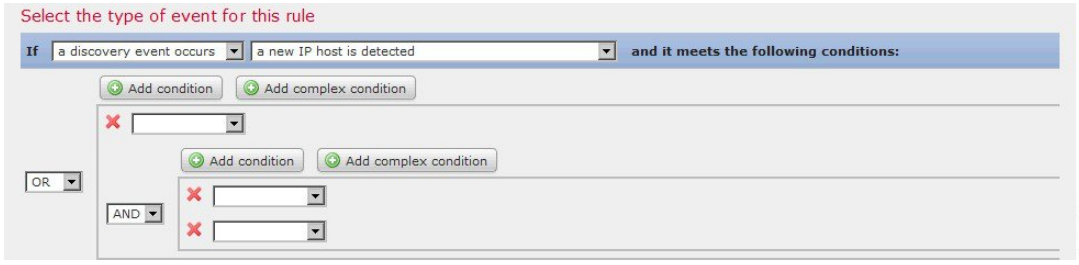
步骤 2 通过从条件左侧的下拉列表中选择 **AND** 或 **OR** 运算符来连接条件。

示例：简单和复杂条件

下图显示具有使用 **OR** 运算符结合的两个简单条件的关联规则。



下图显示具有使用 **OR** 运算符结合的一个简单条件和一个复杂条件的关联规则。复杂条件包括使用 **AND** 运算符结合的两个简单条件。



在关联规则条件中使用多个值

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

在构建关联条件且条件语法允许您从下拉列表中选择值时，通常可以从列表中选择多个值。

过程

步骤 1 在关联条件编辑器中，构建条件，选择 **is in** 或 **is not in** 作为运算符。

步骤 2 点击文本字段或 **Edit** 链接的任意位置。

步骤 3 在**可用 (Available)** 下，选择多个值。也可以点击并拖动以选择多个相邻值。

步骤 4 点击右箭头 (**>**) 将选定条目移动到 **Selected** 中。

步骤 5 点击 **OK**。

管理关联规则

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

在多域部署中，系统会显示在当前域中创建的关联规则和组，您可以对这些关联规则和组进行编辑。它还显示祖先域中的所选关联规则和组，您无法对这些关联规则和组进行编辑。要查看和编辑在较低域中创建的关联规则和组，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。

对活动关联策略中的规则进行的更改会立即生效。

开始之前

- 如果要删除规则，请从所有关联策略中将其删除，如管理关联策略，第 1280 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**规则管理 (Rule Management)** 选项卡。

步骤 2 管理规则：

- 创建 - 点击**创建规则 (Create Rule)**；请参阅配置关联规则，第 1281 页。
- 创建组 - 点击**创建组 (Create Group)**，输入组的名称，然后点击**保存 (Save)**。要向组中添加规则，请编辑该规则。
- 编辑 - 点击编辑图标()；请参阅配置关联规则，第 1281 页。如果改为显示查看图标()，则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除规则或规则组 - 点击删除图标()。删除规则组会对规则取消分组。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置关联响应组

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

您可以创建警报和补救的关联响应组，然后将该组激活并分配到活动关联策略中的关联规则。当网络流量与关联规则相匹配时，系统会启动所有分组的响应。

在活动关联策略中使用时，对活动组或其任何分组响应的更改会立即生效。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**组 (Groups)**。

步骤 2 点击 **Create Group**。

步骤 3 输入 **Name**。

步骤 4 如果在创建后激活组，请选中**活动 (Active)** 复选框。
已停用的组不会启动响应。

步骤 5 选择对组的**可用响应 (Available Responses)**，然后点击向右箭头 (>) 以将其移至**组中的响应 (Responses in Group)**。要向另一边移动响应，请使用向左箭头 (<)。

步骤 6 点击**保存 (Save)**。

接下来的操作

- 如果在创建后未激活组并要立即将其激活，请点击滑块。

管理关联响应组

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

如果关联策略中没有使用响应组，可以删除该组。删除响应组将取消对响应的分组。您也可以在不删除响应组的情况下，暂时停用响应组。这样可以在系统中保留响应组，但在违反策略时不会启动响应组。

在多域部署中，系统会显示在当前域中创建的组，您可以对其进行编辑。系统还会显示在祖先域中创建的组，您不可以对其进行编辑。要查看和编辑在较低域中创建的组，请切换至该域。

对活动的、正在使用的相应组进行的更改会立即生效。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**组 (Groups)**。

步骤 2 管理响应组：

- 激活或停用 - 点击滑块。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 创建 - 点击**创建组 (Create Group)**；请参阅配置关联响应组，第 1312 页。
- 编辑 - 点击编辑图标()；请参阅配置关联响应组，第 1312 页。如果改为显示查看图标()，则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 点击删除图标 ()。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

第 71 章

流量分析

以下主题介绍如何配置流量量变曲线：

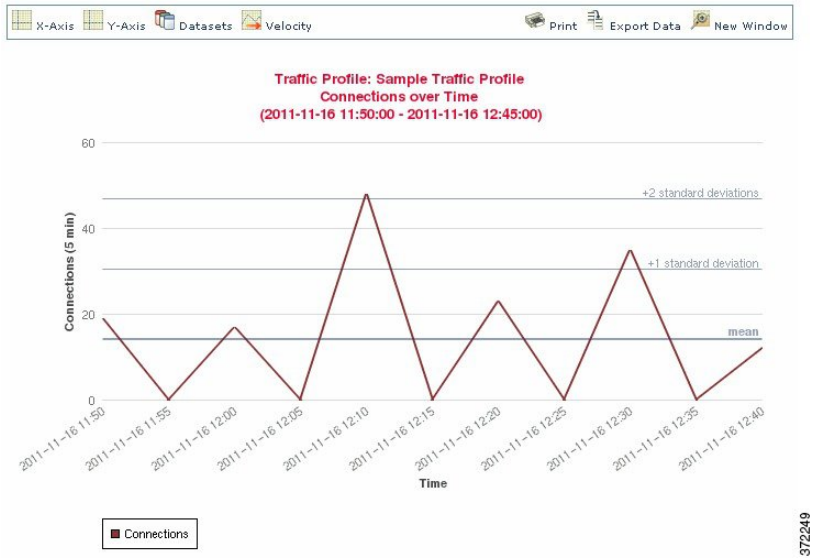
流量量变曲线简介

流量量变曲线是基于在分析时间窗口 (PTW) 收集的连接数据的网络流量图形。此测量可能表示正常网络流量。在学习期后，可以通过对照量变曲线评估新的流量来检测异常网络流量。

默认 PTW 是一周，但是，您可以将其更改为短至 1 小时或长至几周。默认情况下，流量量变曲线会生成系统在五分钟时间区间内生成的连接事件的统计数据。但是，可以将此采样率增加到长达 1 小时。

提示 思科建议 PTW 至少包含 100 个数据点。配置 PTW 和采样率，以便流量量变曲线包含足够的数据以具备统计意义。

下图显示了 PTW 为一天及采样率为五分钟的流量量变曲线。



您也可以在流量量变曲线中设置非活动周期。流量量变曲线在非活动周期内收集数据，但在计算量变曲线统计数据不使用该数据。一段时间内划分的流量量变曲线图可显示非活动周期为阴影区域。

例如，可以考虑所有工作站均在每晚午夜时备份的网络基础设施。备份大约需要30分钟，并将使网络流量达到峰值。可以为流量量变曲线配置周期性非活动周期，以与计划备份相符。

注释 系统使用连接结束数据创建连接图和流量量变曲线。要使用流量量变曲线，请确保将连接结束事件记录到 Firepower 管理中心数据库。

实施流量量变曲线

当激活流量量变曲线时，系统会收集并评估所配置的学习期 (PTW) 的连接数据。在学习期后，系统评估根据流量量变曲线编写的关联规则。

例如，您可写入当通过网络的数据量（单位为数据包、KB或连接数）突然达到平均流量以上三个标准差的峰值时触发的规则，这可能表示出现攻击或其他安全策略违规。然后，您可以包括关联策略中的规则以警告您流量达到峰值或执行补救措施作为响应措施。

以流量量变曲线为目标

量变曲线条件和主机配置文件限定条件限制流量量变曲线。

使用量变曲线条件，可以分析所有网络流量，也可以将流量量变曲线限用于监控域、域内或跨域的子网或者单个主机。在多域部署中：

- 枝叶域管理员可以分析其枝叶域内的网络流量。
- 较高级别的域管理员可以在域内或跨域分析流量。

量变曲线条件还可以使用基于连接数据的条件来限制流量量变曲线。例如，可以设置量变曲线条件，以便流量量变曲线仅使用特定端口、协议或应用来分析会话。

最后，还可以使用有关被跟踪主机的信息来限制流量量变曲线。此类限制被称为主机配置条件限定条件。例如，可以仅收集具有高重要性的主机的连接数据。

注释 将流量量变曲线限于较高级别的域可汇聚并分析**每个**后代枝叶域中**相同**类型的流量。系统会为每个枝叶域构建单独的网络映射。在多域部署中，跨域分析流量可能会出现意外结果。

流量量变曲线条件

您可以创建简单的流量量变曲线条件和主机配置文件限定条件，也可以通过结合和嵌套条件创建较复杂的结构。

条件有三部分：类别、运算符和值。

- 可以使用的类别取决于是构建流量量变曲线条件还是主机配置文件限定条件。
- 可以使用的运算符取决于选择的类别。
- 可用于指定条件值的语法取决于类别和运算符。有时侯，必须在文本字段键入值。有时候，可以从下拉列表中选择一个或多个值。

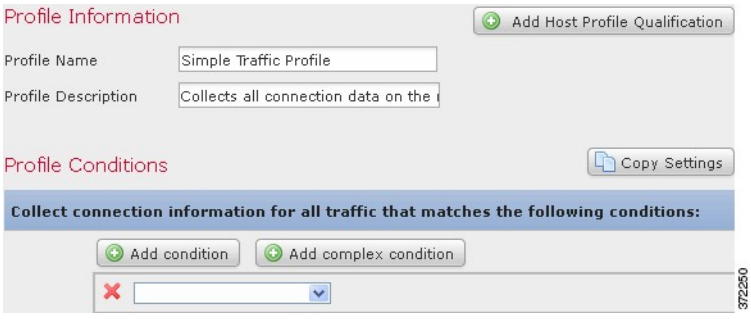
对于主机配置文件限定条件，还必须指定是否使用有关发起或响应主机的信息数据限制流量量变曲线。

当构建的结构不止一个条件时，您必须与将这些条件用 **AND** 与 **OR** 操作符结合起来。相同级别的条件会被放在一起评估：

- **AND** 操作符要求必须满足其控制的级别上的所有条件。
- **OR** 操作符要求必须满足其控制的级别上的至少一个条件。

受限制的流量量变曲线

如果要创建为整个监控网段收集数据的流量量变曲线，可以创建一个非常简单的不带条件的流量量变曲线，如下图所示。

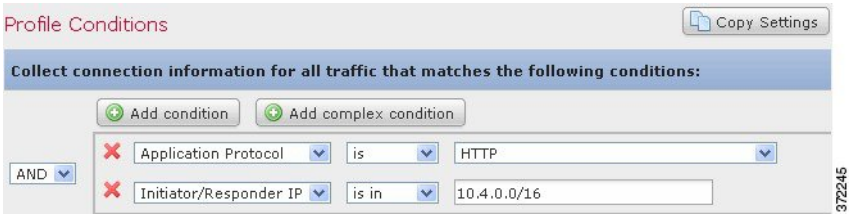


简单流量量变曲线

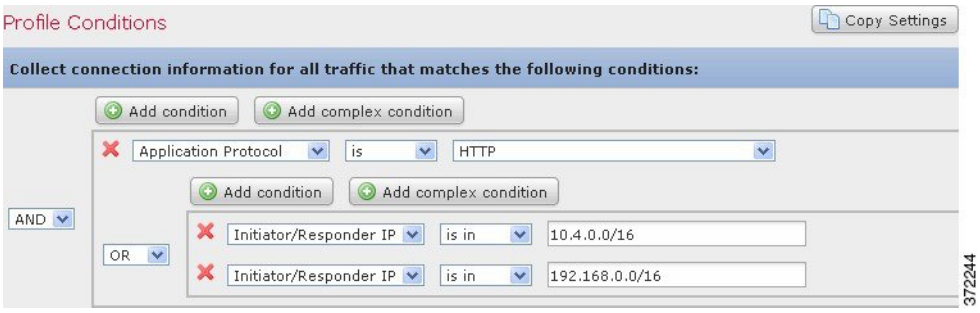
如果要仅为子网限制流量量变曲线和收集数据，可以添加单个条件，如下图所示。

复杂流量量变曲线

以下流量量变曲线包含以**AND**连接的两个条件。这意味着流量量变曲线仅会在两种条件均为真时收集连接数据。在本示例中，它会收集所有 IP 地址在特定子网中的主机的 HTTP 连接。



相反，在任意一个子网中收集 HTTP 活动连接数据的以下流量量变曲线有三个条件，最后一个构成复杂条件。



从逻辑上讲，上述流量量变曲线应如下进行评估：

```
(A and (B or C))
```

关键字	为陈述以下情况的条件.....
A	应用协议名称是 HTTP
B	IP 地址为 10.4.0.0/16
选	IP 地址为 192.168.0.0/16

管理流量量变曲线

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

只有对处于活动状态的完整流量量变曲线写入的规则才可触发关联策略违规。每个流量量变曲线旁边的滑块图标表示该配置文件是否处于活动状态并正在收集数据。进度条显示流量量变曲线学习期的状态。

在多域部署中，系统会显示在当前域中创建的流量量变曲线，您可以对其进行编辑。系统还会显示祖先域中的选定流量量变曲线，您不可以对其进行编辑。要查看和编辑在较低域中创建的流量量变曲线，请切换至该域。

注释 如果祖先域中的流量量变曲线的条件可透露无关域的信息（包括名称、受管设备等），则系统不会显示该配置文件。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**流量量变曲线 (Traffic Profiles)** 选项卡。

步骤 2 管理流量量变曲线：

- 激活/停用 - 要激活或停用流量量变曲线，请点击滑块。停用流量量变曲线会删除其关联的数据。如果重新激活该配置文件，必须等待 PTW 时长后，对其写入的规则才会触发。
- 创建 - 要创建新的流量量变曲线，请点击**新建配置文件 (New Profile)**，然后如配置流量量变曲线，第 1319 页中所述继续操作。您也可以点击复制图标 ( ) 编辑现有流量量变曲线的副本。
- 删除 - 要删除流量量变曲线，请点击删除图标 ( )，然后确认您的选择。
- 编辑 - 要修改现有流量量变曲线，请点击编辑图标 ( )，然后如配置流量量变曲线，第 1319 页中所述继续操作。如果流量量变曲线处于活动状态，则只能更改其名称和说明。
- 图表 - 要查看图表形式的流量量变曲线，请点击图表图标 ( )。在多域部署中，如果属于祖先域的流量量变曲线的图表可透露无关域的信息，则无法查看该图表。

配置流量量变曲线

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

将流量量变曲线限于较高级别的域可汇聚并分析**每个**后代枝叶域中**相同**类型的流量。系统会为每个枝叶域构建单独的网络映射。在多域部署中，跨域分析流量可能会出现意外结果。

过程

步骤 1 选择**策略 (Policies)** > **关联 (Correlation)**，然后点击**流量量变曲线 (Traffic Profiles)** 选项卡。

步骤 2 点击 **New Profile**。

步骤 3 输入**配置文件名称 (Profile Name)** 和输入**配置文件说明 (Profile Description)**（可选）。

步骤 4 或者，限制流量量变曲线：

- “复制设置”(Copy Settings) - 要复制某个现有流量量变曲线的设置，请点击**复制设置 (Copy Settings)**，选择要使用的流量量变曲线，然后点击**加载 (Load)**。
- “配置文件条件”(Profile Conditions) - 要使用被跟踪连接的信息限制流量量变曲线，请按添加流量量变曲线条件，第 1320 页中所述进行操作。
- “主机配置文件限定条件”(Host Profile Qualification) - 要使用被跟踪主机的信息限制流量量变曲线，请按将主机配置文件限定条件添加到流量量变曲线中，第 1321 页中所述进行操作。
- “分析时间窗口 (PTW)”(Profiling Time Window [PTW]) - 要更改**分析时间窗口 (Profiling Time Window)**，请输入时间单位，然后选择**小时数 (hour[s])**、**天数 (day[s])** 或**周数 (week[s])**。
- “采样率”(Sampling Rate) - 选择**采样率 (Sampling Rate)**（以分钟为单位）。
- “非活动周期”(Inactive Period) - 点击**添加非活动周期 (Add Inactive Period)**，然后使用下拉列表指定希望流量量变曲线保持非活动的时间和频率。非活动流量量变曲线不会触发关联规则。流量量变曲线不包含配置文件统计信息中非活动时期的数据。

步骤 5 保存流量量变曲线：

- 要保存量变曲线并立即开始收集数据，请点击 **Save & Activate**。
- 要保存量变曲线而不激活它，请点击 **Save**。

添加流量量变曲线条件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

过程

步骤 1 在流量量变曲线编辑器中的“量变曲线条件”(Profile Conditions) 下，为要添加的每个条件点击**添加条件 (Add condition)** 或**添加复杂条件 (Add complex condition)**。相同级别的条件会被放在一起评估。

- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。

- 如果需要只有一个条件位于满足操作符控制的级别上，请选择 **OR**。

步骤 2 为每个条件指定类别、运算符和值，如流量量变曲线条件的语法，第 1322 页和流量量变曲线条件，第 1317 页中所述。
如果选择 **is in** 或 **is not in** 作为运算符，则可以在单个条件中选择多个值，如在流量量变曲线条件中使用多个值，第 1325 页中所述。

当类别为某个 IP 地址时，选择 **is in** 或 **is not in** 作为操作符使您可以指定 IP 地址是还是不是在某个 IP 地址范围中。

示例

以下流量量变曲线收集有关特定子网的信息。条件的类别是 **Initiator/Responder IP**，操作符是 **is in**，值为 `10.4.0.0/16`。

将主机配置文件限定条件添加到流量量变曲线中

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

过程

步骤 1 在流量量变曲线编辑器上，点击**添加主机配置文件限定条件 (Add Host Profile Qualification)**。

步骤 2 在“主机配置文件限定条件”(Host Profile Qualification) 下，为要添加的每个条件点击**添加条件 (Add condition)** 或**添加复杂条件 (Add complex condition)**。相同级别的条件会被放在一起评估。

- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。
- 如果需要只有一个条件位于满足操作符控制的级别上，请选择 **OR**。

步骤 3 为每个条件指定主机类型、类别、运算符和值，如流量量变曲线中主机配置文件限定条件的语法，第 1323 页和流量量变曲线条件，第 1317 页中所述。
如果选择 **is in** 或 **is not in** 作为运算符，则可以在单个条件中选择多个值，如在流量量变曲线条件中使用多个值，第 1325 页中所述。

示例

以下主机配置文件限定条件则限制了流量量变曲线以便其只在检测到的连接中的响应主机运行 Microsoft Windows 版本时才会收集连接数据。

流量量变曲线条件的语法

下表介绍了如何构建流量量变曲线条件。请记住，可用于构建流量量变曲线的连接数据取决于多个因素，包括流量特征和检测方法。

表 *216*：流量量变曲线条件的语法

如果选择.....	选择运算符，然后.....
应用协议	选择一个或多个应用协议。
Application Protocol Category	选择一个或多个应用协议类别。
Client	选择一个或多个客户端。
Client Category	选择一个或多个客户端类别。
连接类型	选择配置文件是使用来自 Firepower 系统受管设备监控的流量还是来自已导出的 NetFlow 记录的连接数据。 如果您不指定连接类型，则流量量变曲线会同时包括两者。
Destination Country 或 Source Country	选择一个或多个国家/地区。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。
“发起方 IP”(Initiator IP)、“响应方 IP”(Responder IP) 或“发起方/响应方 IP”(Initiator/Responder IP)	输入 IP 地址或 IP 地址范围。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

如果选择.....	选择运算符，然后.....
NetFlow Device	选择要使用其数据创建流量量变曲线的 NetFlow 导出器。
Responder Port/ICMP Code	输入端口号或 ICMP 代码。
Security Intelligence Category	选择一个或多个安全情报类别。 要将安全情报类别用于流量量变曲线条件，该类别必须在访问控制策略中设置为**监控(Monitor)**而不是**阻止 (Block)**。
SSL Encrypted Session	选择**已成功解密 (Successfully Decrypted)**。
传输协议	输入 TCP 或 UDP 作为传输协议。
Web 应用	选择一个或多个 Web 应用。
Web Application Category	选择一个或多个 Web 应用类别。

流量量变曲线中主机配置文件限定条件的语法

当构建主机配置文件限定条件时，必须首先选择要用于限制流量量变曲线的主机。您可以选择**响应方主机 (Responder Host)** 或**发起方主机 (Initiator Host)**。在选择主机角色之后，请继续构建主机配置文件限定条件。

虽然可以使用 NetFlow 记录将主机添加到网络映射中，但是有关这些主机的可用信息有限。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。此外，如果流量量变曲线使用已导出的 NetFlow 记录中的连接数据，请记住，NetFlow 记录不包含有关连接中的哪台主机是发起方和哪台主机是响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。

要匹配隐含或一般客户端，请根据响应客户端的服务器所用的应用协议创建主机配置文件限定条件。当作为连接发起方或源的主机上的客户端列表包含**客户端**遵循的应用协议名称时，该客户端可能实际上就是一种隐含客户端。换句话说，系统会根据使用该客户端的应用协议的服务器响应流量，而非检测到的客户端流量来报告该客户端。

例如，如果系统将 **HTTPS 客户端**作为主机上的一个客户端进行报告，请为 **Responder Host** 创建主机配置限定条件，其中 **Application Protocol** 被设置为 **HTTPS**，因为 HTTPS 客户端会根据响应方或目标主机发送的 HTTPS 服务器响应流量被报告为一种一般客户端。

表 *217*：主机配置文件限定条件的语法

如果选择.....	选择运算符，然后.....
应用协议 (Application Protocol) > 应用协议 (Application Protocol)	选择一个或多个应用协议。

如果选择.....	选择运算符，然后.....
应用协议 (Application Protocol) > 应用端口 (Application Port)	输入应用协议端口号。
应用协议 (Application Protocol) > 协议 (Protocol)	选择协议。
Application Protocol Category	选择一个或多个应用协议类别。
Client > Client	选择一个或多个客户端。
Client > Client Version	输入客户端版本。
Client Category	选择一个或多个客户端类别。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。
硬件	输入移动设备硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 `iPhone`。
主机重要性	选择主机重要性。
Host Type	选择一个或多个主机类型。您可以在一个常规主机或多种网络设备中的一种之间选择。
IOC Tag	选择一个或多个 IOC 标记。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。
MAC Address > MAC Address	输入主机的全部或部分 MAC 地址。
MAC Address > MAC Type	选择 MAC 类型是否是**按 ARP/DHCP 检测 (ARP/DHCP Detected)**，即， • 系统是否明确地将 MAC 地址识别为属于主机（**按 ARP/DHCP 检测 [ARP/DHCP Detected]**） • 打个比方，因为设备和主机之间有路由器，所以系统看到许多主机具有该 MAC 地址（**不按 ARP/DHCP 检测 [is not ARP/DHCP Detected]**） • MAC 类型不相关（**为任意 [is any]**）
MAC Vendor	输入主机使用的硬件的全部或部分 MAC 供应商。
移动设备	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NETBIOS Name	输入主机的 NetBIOS 名称。

如果选择.....	选择运算符，然后.....
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
Operating System > OS Vendor	选择一个或多个操作系统供应商名称。
Operating System > OS Name	选择一个或多个操作系统名称。
Operating System > OS Version	选择一个或多个操作系统版本。
传输协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
VLAN ID	输入主机的 VLAN ID 号。 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字VLAN标记限制此配置可产生意外结果。
Web 应用	选择一个或多个 Web 应用。
Web Application Category	选择一个或多个 Web 应用类别。
任何可用的主机属性，包括默认合规性白名单主机属性	指定适当的值，这取决于您选择的主机属性类型： • 如果主机属性类型为 Integer，请在针对该属性确定的范围中输入一个整数值。 • 如果主机属性类型为“文本”(Text)，请输入文本值。 • 如果主机属性类型为“列表”(List)，请选择有效的列表字符串。 • 如果主机属性类型是 URL，请输入 URL 值。

在流量量变曲线条件中使用多个值

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/发现管理员

在构建条件，且条件语法允许您从下拉列表中选择值时，您通常可以从列表中选择多个值。

例如，如果想要将主机配置文件限定条件添加到需要主机运行 UNIX 的流量量变曲线，而非构建使用 OR 操作符连接的多个条件，请使用以下步骤。

过程

步骤 1 在构建流量量变曲线或主机配置文件限定条件时，选择 **is in** 或 **is not in** 作为运算符。
下拉列表会更改至文本字段。

步骤 2 点击文本字段或 **Edit** 链接的任意位置。

步骤 3 在**可用 (Available)** 下，选择多个值。

步骤 4 点击右箭头将选定条目移动到**选定项 (Selected)** 中。

步骤 5 点击 **OK**。

第 72 章

补救

以下主题包含有关配置补救的信息：

补救简介

补救是一种 Firepower 系统为响应关联策略违规而启动的程序。

当补救程序运行时，系统会生成补救状态事件。补救状态事件包括详细信息，如补救名称、触发补救的关联策略和规则及退出状态消息。

系统支持多种补救模块：

- 思科 IOS 空路由 - 在出现关联策略违规的情况下，阻止发送到主机或网络的流量（需要思科 IOS 版本 12.0 或更高版本）
- Nmap 扫描 - 扫描主机以确定运行的操作系统和服务器
- 设置属性值 - 在出现关联策略违规的情况下，设置一台主机的属性。

提示 您可以安装执行其他任务的自定义模块；请参阅《《*Firepower* 系统补救 *API* 指南》》。

实施补救

要实施补救，请先为所选模块创建至少一个实例。您可为每个模块创建多个实例，其中每个实例的配置各不相同。例如，要使用思科 IOS 空路由补救模块与多个路由器通信，请为该模块配置多个实例。

然后，您可以为每个实例添加多个补救，这些补救介绍了违反策略时要执行的操作。

最后，将补救与关联策略中的规则相关联，以便系统启动补救以响应关联策略违规。

补救和多租户

在多域部署中，您可以在任何域级别安装自定义补救模块。系统提供的模块属于全局域。

虽然您无法将补救添加到祖先域中创建的实例，但可以在当前域中创建类似配置的实例，并将补救添加到该实例。您也可以使用祖先域中创建的补救作为关联响应。

思科 IOS 空路由补救

借助思科 IOS 空路由补救模块，您可以使用思科的“null route”命令阻止某个 IP 地址或地址范围。这会将发送到某主机或网络的所有流量路由到路由器的 NULL 接口，从而丢弃这些流量。不过，这不会阻止从违规主机或网络发送的流量。

注释 不要使用基于目标的补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

注意 Cisco IOS 补救激活后，就不再有超时期限。要解除阻止 IP 地址或网络，必须从路由器手动清除路由更改。

为思科 IOS 路由器配置补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

注释 不要使用基于目标的补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

注意 Cisco IOS 补救激活后，就不再有超时期限。要解除阻止 IP 地址或网络，必须从路由器手动清除路由更改。

开始之前

- 确认思科路由器运行的是思科 IOS 12.0 或更高版本。
- 确认您对路由器具有 15 级管理访问权限。

过程

步骤 1 在思科路由器上启用 Telnet，如思科路由器或 IOS 软件随附的文档中所述。

步骤 2 在 Firepower 管理中心上，为计划使用的每个思科 IOS 路由器添加思科 IOS 空路由实例；请参阅添加思科 IOS 实例，第 1329 页。

步骤 3 根据在违反关联策略时要在路由器上引发的响应类型，为每个实例创建补救。

- 添加思科 IOS 阻止目标补救，第 1330 页
- 添加思科 IOS 阻止目标网络补救，第 1330 页
- 添加思科 IOS 阻止源补救，第 1331 页
- 添加思科 IOS 阻止源网络补救，第 1332 页

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

添加思科 *IOS* 实例

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

如果具有多个要发送补救的路由器，请为每个路由器创建单独的实例。

开始之前

- 在思科 IOS 路由器上配置 Telnet 访问，如路由器或 IOS 软件随附的文档中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 从**添加新实例 (Add a New Instance)** 列表中，选择**思科 IOS 空路由 (Cisco IOS Null Route)** 并点击**添加 (Add)**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 在 **Router IP** 字段中，输入要用于补救的 Cisco IOS 路由器的 IP 地址。

步骤 5 在 **Username** 字段中，输入路由器的 Telnet 用户名。该用户必须对路由器拥有 15 级管理访问权限。

步骤 6 在 **Connection Password** 字段中，输入 Telnet 用户的用户密码。

步骤 7 在 **Enable Password** 字段中，输入 Telnet 用户的启用密码。该密码用于进入路由器的特权模式。

步骤 8 在**白名单 (White List)** 字段中，输入要免除补救的 IP 地址或范围（每行一个）。

注释　系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。

步骤 9　点击**创建**。

接下来的操作

- 添加要供关联策略使用的特定补救，如添加思科 IOS 阻止目标补救，第 1330 页、添加思科 IOS 阻止目标网络补救，第 1330 页、添加思科 IOS 阻止源补救，第 1331 页和添加思科 IOS 阻止源网络补救，第 1332 页中所述。

添加思科 *IOS* 阻止目标补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

思科 IOS 阻止目标补救可阻止从路由器发送到关联事件违规中涉及的目标主机的流量。不要使用此补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 1329 页中所述。

过程

步骤 1　选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2　在要向其添加补救的实例旁，点击视图图标（  ）。

步骤 3　在**已配置补救 (Configured Remediations)** 部分，选择**阻止目标 (Block Destination)** 并点击**添加 (Add)**。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4　输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5　依次点击 **Create** 和 **Done**。

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

添加思科 *IOS* 阻止目标网络补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

思科 IOS 阻止目标网络补救可阻止从路由器发送到关联事件违规中涉及的目标主机网络的流量。不要使用此补救作为对基于发现或主机输入事件的关联规则的响应。这些事件与源主机关联。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 1329 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 在要向其添加补救的实例旁，点击视图图标（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止目标网络 (Block Destination Network)** 并点击**添加 (Add)**。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 在 **Netmask** 字段中，输入子网掩码或使用 CIDR 表示法说明要阻止流量进入的网络。
例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络（不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 6 依次点击 **Create** 和 **Done**。

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

添加思科 *IOS* 阻止源补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

思科 IOS 阻止源补救可阻止从路由器发送到关联策略违规中涉及的源主机的流量。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 1329 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 在要向其添加补救的实例旁，点击视图图标（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止源 (Block Source)**，然后点击**添加 (Add)**。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 依次点击 **Create** 和 **Done**。

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

添加思科 *IOS* 阻止源网络补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

思科 IOS 阻止源网络补救可阻止从路由器发送到关联事件违规中涉及的源主机网络的流量。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 添加思科 IOS 实例，如添加思科 IOS 实例，第 1329 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 在要向其添加补救的实例旁，点击视图图标（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**阻止源网络 (Block Source Network)** 并点击**添加 (Add)**。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 在 **Netmask** 字段中，输入子网掩码或描述要阻止流量进入的网络 CIDR 表示法。
例如，要在单个主机触发规则时阻止流量进入整个 Class C 网络（不推荐），请使用 `255.255.255.0` 或 `24` 作为子网掩码。

又例如，要阻止流量进入包括触发 IP 地址的 30 条地址，请指定 `255.255.255.224` 或 `27` 作为子网掩码。在这种情况下，如果 IP 地址 `10.1.1.15` 触发补救，则将阻止 `10.1.1.1` 与 `10.1.1.30` 之间的所有 IP 地址。要阻止触发 IP 地址，请将该字段留空，输入 `32` 或 `255.255.255.255`。

步骤 6 依次点击 **Create** 和 **Done**。

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

Nmap 扫描补救

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。您可以通过 Nmap 补救对关联策略违规做出响应，Nmap 补救会触发 Nmap 扫描补救。

有关 Nmap 扫描的详细信息，请参阅Nmap Scanning，第 1156 页。

设置属性值补救

可以响应关联策略违规，只需在触发事件发生的主机上设置主机属性值。对于文本主机属性，可以使用事件说明作为属性值。

配置设置属性补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 创建设置属性实例，如添加设置属性值实例，第 1334 页中所述。

步骤 3 添加设置属性补救，如添加设置属性值补救，第 1334 页中所述。

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

添加设置属性值实例

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 从**添加新实例 (Add a New Instance)** 列表中选择**设定的属性值 (Set Attribute Value)**，然后点击**添加 (Add)**。

步骤 3 输入**实例名称 (Instance Name)** 和**说明 (Description)**。

步骤 4 点击**创建**。

接下来的操作

- 如添加设置属性值补救，第 1334 页中所述，创建设定的属性补救。

添加设置属性值补救

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

设置属性值补救在关联策略违规所涉及的主机上设置主机属性。为要设置的每个属性值创建补救。对于文本属性，可以使用触发事件的说明作为属性值。

在多域部署中，无法将补救添加到祖先域中创建的实例。

开始之前

- 创建设置属性实例，如添加设置属性值实例，第 1334 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 在要向其添加补救的实例旁，点击视图图标（  ）。

步骤 3 在**已配置补救 (Configured Remediations)** 部分，选择**设置属性值 (Set Attribute Value)**，然后点击**添加 (Add)**。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**补救名称 (Remediation Name)** 和**说明 (Description)**。

步骤 5 要使用此补救响应带有源和目标数据的事件，请选择**从事件更新哪些主机 (Update Which Host(s) From Event)** 选项。

步骤 6 对于文本属性，请指定是否要**将事件说明用于属性值 (Use Description From Event For Attribute Value)**：

- 要使用事件说明作为属性值，请点击**打开 (On)** 并在**属性值 (Attribute Value)** 中输入要设置的属性值。
- 要使用补救的**属性值 (Attribute Value)** 设置作为属性值，请点击**关闭 (Off)**。

步骤 7 依次点击 **Create** 和 **Done**。

接下来的操作

- 分配补救以作为对安全策略违规的响应；请参阅将响应添加到规则和白名单，第 1279 页。

管理补救模块

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

在多域部署中，自定义表会显示在当前域中安装的补救模块，您可以对其进行删除。系统还会显示在祖先域中安装的模块，您不可以对其进行删除。要管理较低域中的补救模块，请切换至该域。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **模块 (Modules)**。

步骤 2 管理补救模块：

- 配置 - 要查看模块的“模块详细信息”(Module Detail) 页面并配置其实例和补救，请点击查看图标 ( )。在多域部署中，对于安装在祖先域中的模块，无法在当前域中使用“模块详细信息”(Module Detail) 页面为其添加、删除或编辑实例。相反，请使用“实例”(Instances) 页面 (**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**)；请参阅管理补救实例，第 1336 页。
- 删除 - 要删除未在使用的自定义模块，请点击删除图标 ( )。无法删除系统提供的模块。
- 安装 - 要安装自定义模块，请点击**选择文件 (Choose File)**，浏览至模块，然后点击**安装 (Install)**。有关详细信息，请参阅《*Firepower* 系统补救 *API* 指南》。

管理补救实例

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

“实例”(Instances) 页面列出了所有补救模块的所有已配置实例。

在多域部署中，系统会显示在当前域中创建的补救实例，您可以对其进行编辑。系统还会显示在祖先域中创建的实例，您不可以对其进行编辑。要管理较低域中的补救实例，请切换至该域。

虽然您无法将补救添加到祖先域中创建的实例，但可以在当前域中创建类似配置的实例，并将补救添加到该实例。您也可以使用祖先域中创建的补救作为关联响应。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**。

步骤 2 管理补救实例：

- 添加 - 要添加实例，请选择要为其添加实例的补救模块，然后点击**添加 (Add)**。对于系统提供的模块，请参阅：

  添加思科 IOS 实例，第 1329 页

  添加 Nmap 扫描实例，第 1165 页

  添加设置属性值实例，第 1334 页

  如需获取添加自定义模块的帮助，请参阅该模块的文档（如有）。

- 配置 - 要配置实例详细信息并向实例添加补救，请点击查看图标 ( )。
- 删除 - 要删除未在使用的实例，请点击删除图标 ( )。

管理单个补救模块的实例

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员 发现管理员

“模块详细信息”(Module Detail) 页面显示为特定补救模块配置的所有实例和补救。

在多域部署中，可以访问当前域和祖先域中安装的补救模块的“模块详细信息”(Module Detail) 页面。但是，不能使用“模块详细信息”(Module Detail) 页面为祖先域中安装的模块添加、删除或编辑当前域中的实例。请改用“实例”(Instances) 页面（**策略 (Policies)** > **操作 (Actions)** > **实例 (Instances)**）；请参阅管理补救实例，第 1336 页。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **模块 (Modules)**。

步骤 2 在要管理其实例的补救模块的旁边，点击查看图标 ().

步骤 3 管理补救实例：

- 添加 - 要添加实例，请点击**添加 (Add)**。对于系统提供的模块，请参阅：

  添加思科 IOS 实例，第 1329 页

  添加 Nmap 扫描实例，第 1165 页

  添加设置属性值实例，第 1334 页

  要帮助为自定义模块添加实例，该参阅该模块的文档（如果可用）。

- 配置 - 要配置实例详细信息并添加对实例的补救，请点击查看图标 ()。
- 删除 - 要删除未在使用的实例，请点击删除图标 ()。

第 XVIII 部分

报告和警报

第 73 章

使用报告

以下主题介绍如何在 Firepower 系统中使用报告：

报告简介

Firepower 系统提供一个灵活的报告系统，能够利用 Firepower 管理中心上显示的事件视图或控制面板快速而轻松地生成多部分报告。还可以从头设计自定义报告。

报告是一种采用 PDF、HTML 或 CSV 格式的文档文件，其包含要传达的内容。报告模板指定报告及其各部分的数据搜索和格式。Firepower 系统内有一个功能强大的报告设计器，用于自动执行报告模板的设计。可以复制网络界面中显示的任何活动视图表或控制面板图形的内容。

可以根据需要的数量创建报告模板。每个报告模板分别定义报告中的各个部分并指定创建报告内容的数据库搜索，以及演示文稿格式（表、图表，详细视图等等）和时间范围。模板还指定文档属性，例如封面和目录以及文档页面是否有页眉和页脚（仅适用于 PDF 格式的报告）。可以将报告模板导出到单个的配置包文件中，然后再导入，以便在其他Firepower 管理中心上重复使用。

在模板中可以加入输入参数，以扩展其实用性。使用输入参数，可以对同一报告生成定制的变量。当使用输入参数生成报告时，生成过程会提示输入每个输入参数的值。键入的值仅限报告内容一次。例如，在生成入侵事件报告的搜索的目标 IP 字段中可以放入一个输入参数；当系统提示输入目标 IP 地址时，可以指定部门的网段。生成的报告随后只包含该特定部门的相关信息。

报告模板

使用报告模板定义报告的每个部分中的数据内容和格式，以及报告文件的文档属性（封面、目录及页眉和页脚）。在生成报告之后，模板仍可重复使用，直到将其删除为止。

报告包含一个或多个信息部分。为每个部分分别选择格式（文本、表或图表）。为部分选择的格式可能限制可包含的数据。例如，使用饼图格式，无法显示某些表中基于时间的信息。可以随时更改部分的数据条件或格式，以获得最佳演示效果。

可以在预定义的事件视图基础上完成报告的初始设计，也可以通过从任何定义的控制面板、工作流程或摘要导入内容开始设计。还可以从空的模板开始添加部分并逐一定义其属性。

注释 在多域部署中，可以查看但无法编辑属于祖先域的报告模板。要从这些模板生成报告，必须将它们复制到当前的域。

报告模板字段

表 *218*：报告部分标题栏元素

属性	定义
部分标题	包含部分显示在报告中的名称。在“报告部分”(Report Sections) 页面上查看时，系统会截断长部分标题名称。
部分标题图标	允许您复制部分 (+)，将部分最小化 (−) 或在确认后删除部分 (×)

表 *219*：报告部分字段

字段名称	**Definition**
表	显示一个下拉菜单，用于选择提取部分数据的表。
Preset	显示预定义搜索的下拉菜单。在定义新的搜索时，可以选择合适的预设初始化搜索条件。

字段名称	Definition
Format	提供用于选择部分数据格式的图标。选项包括：  条形图：比较所选变量的数量。  折线图：显示所选变量随时间推移的趋势/更改。仅适用于基于时间的表。  饼形图：将每个所选变量显示为总体的百分比。数量为零的变量不在图表中显示。极少的数量归到标记为 **Other** 的类别。  表视图：显示每个记录的属性值。不适用于摘要或统计数据。  详细视图：显示与特定事件相关联的复杂对象数据，例如数据包（用于入侵事件）和主机配置文件（用于主机事件）。格式仅适用于涉及此类对象的事件类型。如果请求的数量很大，输出可能会降低性能。
Search 或 Filter	显示搜索或应用过滤器的下拉菜单。 对于大多数表，可使用预定义的或保存的 **Search** 限制报告。您还可以通过点击编辑图标 () 来创建新搜索。 对于“应用统计信息”(Application Statistics) 表，使用用户定义的应用**过滤器**限制报告。
X-Axis	为所选图表的 X 轴显示其可用数据列的下拉菜单。只有选择图表格式时才会显示。对于折线图，X 轴值始终是 **Time**。对于条形图和饼图，则不能选择 **Time** 为 X 轴值。
Y-Axis	为所选图表的 Y 轴显示其可用数据列的下拉菜单。
Section Description	定义在部分中的搜索数据前面的描述性文本。输入文本和输入参数组合。新部分的默认值是以下两个输入参数的集合：`$<Time Window>` 和 `$<Constraints>`。
Time Window	为部分中显示的数据定义时间段。如果部分搜索基于时间的表，可以选择复选框以继承报告的全局时间段。或者，可以为部分设置特定时间段。
结果	选择 **Top** 或 **Bottom** 并输入要在部分中包括的最大记录数量。
颜色	定义部分中图形数据的颜色。根据需要选择一个或多个颜色。

报告模板创建

报告模板是各部分的框架，每个部分通过自己的数据库查询独立构建。

您可以通过创建新模板，使用现有模板，将模板基于事件视图，或者导入控制面板或工作流程来构建新的报告模板。

如果不想复制现有报告模板，可以创建一个全新模板。创建模板的第一步是生成用于添加和格式化各部分的框架。然后，按照希望的顺序设计各个模板部分并设置报告文档的属性。

每个模板部分均包括由搜索或过滤器生成的数据集，且具有确定展现方式的格式规格（表，饼图等）。通过选择要在输出中包含的数据记录中的字段，以及要显示的时间范围和记录数量，进一步确定部分内容。

注释 使用部分预览实用程序检查列选择和饼图颜色等输出特性。这并不能可靠地表明配置的搜索是正确的。

从模板生成的报告具有多个覆盖所有部分和控制功能的文档属性，例如封面、页眉和页脚、页码等。

请注意，如果选择 CSV 作为文档格式，则无需设置文档属性。

如果在现有模板中找到理想模型，则可以复制模板并编辑其属性以创建新报告模板。思科还提供一组在模板列表中的**报告 (Reports)** 选项卡上可视的预定义报告模板。

从事件视图中，可以创建报告模板并将其修改为满足您的需求。可以添加更多部分、修改自动包含的部分和删除各部分。

通过导入控制面板、工作流程和统计摘要，可以快速创建新的报告。导入为控制面板中的每个构件图形以及工作流程中的每个事件视图创建一个部分。为重点显示最重要的信息，可以删除任何不必要的部分。

创建自定义报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击**报告模板 (Report Templates)** 选项卡。

步骤 3 点击 **Create Report Template**。

步骤 4 或者，在**报告标题 (Report Title)** 字段中输入新模板的名称，然后点击**保存 (Save)**。

步骤 5 要向报告标题添加输入参数，请将光标置于应显示参数值的标题中，然后点击插入输入参数图标 ( )。

步骤 6 根据需要，使用“报告部分”(Report Sections) 标题栏下的一组添加图标来插入部分。

步骤 7 点击**保存 (Save)**。

步骤 8 配置部分内容，如报告模板配置 ， 第 1348 页中所述。

提示 可以点击部分窗口底部的**预览 (Preview)**，查看所选择的列布局或图形格式。

步骤 9 点击**高级 (Advanced)**，设置 PDF 和 HTML 报告的属性，如报告模板中的文档属性，第 1357 页中所述。

从现有模板创建报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击**报告模板 (Report Templates)** 选项卡。

步骤 3 点击要复制的报告模板旁边的复制图标 ( )。

步骤 4 在**报告标题 (Report Title)** 字段中，输入名称。

步骤 5 点击**保存 (Save)**。

步骤 6 根据需要对模板进行更改。

从事件视图创建报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在事件视图中填入要在报告中显示的事件：

- 使用事件搜索定义要查看的事件。
- 深入查找工作流程，直到在事件视图中获得相应的事件。

步骤 2 从事件视图页面中，点击 **Report Designer**。
“报告部分”(Report Sections) 页面为已捕获工作流程中的每个视图显示一个部分。

步骤 3 或者，在**报告标题 (Report Title)** 字段中输入新名称并点击**保存 (Save)**。

步骤 4 您可以执行以下操作：

- 添加封面、目录、开始页码或页眉和页脚文本 - 点击**高级设置 (Advanced Settings)**。
- 添加分页符 - 点击添加分页符图标 ()，并将新分页符对象从模板底部拖动到应该开始新页面的那个部分的前面。
- 添加文本部分 - 点击添加文本部分图标 ()，并将新文本部分从模板底部拖动到要在报告模板中显示的位置。
- 更改某个部分的标题 - 点击标题栏中该部分的标题，输入部分标题，然后点击**确定 (OK)**。
- 配置报告部分 - 调整每个部分中的字段设置。

  提示 要查看某一部分的当前列布局或图表格式，请点击该部分的 **Preview** 链接。

- 从报告中排除模板部分 - 点击该部分标题栏中的删除图标 ( ) 并确认删除。

  注释 有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响Firepower管理中心的性能。

步骤 5 点击**保存 (Save)**。

通过导入控制面板或工作流程创建报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 确定要在报告中复制的控制面板、工作流程或摘要。

步骤 2 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 3 点击**报告模板 (Report Templates)** 选项卡。

步骤 4 点击 **Create Report Template**。

步骤 5 在**报告标题 (Report Title)** 字段中输入新报告模板的名称。

步骤 6 点击**保存 (Save)**。

步骤 7 点击导入部分图标 ( )。可以选择导入报告部分的数据源选项，第 1347 页中所述的任何数据源。

步骤 8 从下拉菜单中选择控制面板、工作流程或摘要。

步骤 9 对要添加的数据源，点击 **Import**。
对于控制面板，每个构件图形都有自己的部分；对于工作流，每个事件视图都有自己的部分。

步骤 10 根据需要更改部分的内容。

注释 有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响Firepower 管理中心的性能。

步骤 11 点击**保存 (Save)**。

导入报告部分的数据源选项

表 *220*：导入报告部分窗口上的数据源选项

选择此选项…	导入…
Import Dashboard	所选控制面板上的任何自定义分析构件。
Import Workflow	任何预定义或自定义的工作流。 选项具有以下格式： `Table - Workflow name` 例如，`Connection Events - Traffic by Port` 可导入从“连接事件”(Connection Events) 表生成的“按端口划分的流量”(Traffic by Port) 工作流程中的视图。
Import Summary Sections	以下任意一种通用摘要： • 入侵详细摘要 • 入侵简要摘要 • 发现详细摘要 • 发现简要摘要

报告模板配置

创建报告模板后，可以进行修改和自定义。可以通过修改各种报告部分属性调整部分的内容及其数据展示。

报告模板中的各部分通过查询数据库表生成该部分的内容。更改部分的数据格式使用相同的数据查询，但会根据格式类型的分析用途修改部分中显示的字段。例如，入侵事件的表视图在部分中填入每个事件记录的大量数据字段，而饼图部分则显示各个选定属性代表的所有匹配记录的比例，不显示单个事件的详细信息。条形图部分比较具有特定属性的匹配记录总数。折线图就单个属性总结匹配记录随时间推移的变化。折线图仅适用于基于时间的数据，不适用于有关主机、用户和第三方漏洞等信息。

报告部分中的搜索或过滤器指定部分内容所基于的数据库查询。对于大多数表，可以使用预定义或保存的搜索来限定报告，也可以随时创建新的搜索：

- 预定义的搜索作为示例用于搜索特定事件表，并可以对可能想要在报告中包含的重要网络信息提供快速访问。
- 保存的事件搜索包括您或他人已创建的全部公共事件搜索，以及所有保存的私密事件搜索。
- 只有在报告模板本身中才能实现当前报告模板的保存搜索。已保存报告模板搜索的搜索名称以字符串“Custom Search”结尾。用户在设计报告时创建这些搜索。

对于“应用统计信息”(Application Statistics) 表，使用用户定义的应用过滤器限制报告。

如果在部分中包括表数据，则可以选择要显示数据记录中的哪些字段。表中所有字段都可以包括或排除。选择实现报告用途的字段，然后进行相应的排列和排序。

可以向模板添加文本部分以提供自定义文本，例如，整个报告或各部分的简介。

在模板中，可以在任何部分的前面或后面添加分页符。此功能尤其适用于多部分报告，其具有介绍各个部分的文本页面。

报告模板的时间段定义模板的报告周期。

注释 安全分析人员仅可以编辑由其创建的报告模板。在多域配置中，无法从祖先域编辑报告模板，但是可以复制以创建后代版本。

设置报告模板部分的表和数据格式

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板部分，使用**表 (Table)** 下拉菜单选择要查询的表。
适用于所选表的每个输出格式的图标显示在**格式 (Format)** 字段中。

步骤 2 选择相关部分适用的输出格式图标。

步骤 3 要更改搜索限制，请点击 **Search** 或 **Filter** 字段旁边的编辑图标 ( )。

步骤 4 对于图形输出格式（饼图、条形图等），请使用下拉菜单调整 **X-Axis** 和 **Y-Axis** 参数。
当为 X 轴选择值时，只有相对应的值才显示在 Y 轴下拉菜单中，反之亦然。

步骤 5 对于表输出，请在输出中选择列、显示顺序和排序顺序。

步骤 6 点击**保存 (Save)**。

为报告模板部分指定搜索或过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板部分中，从**表 (Table)** 下拉菜单中选择要查询的数据库表：

- 对于大多数表，显示 **Search** 下拉列表。
- 对于 Application Statistics 表，显示 **Filter** 下拉列表。

步骤 2 选择要用于限制报告的搜索或过滤器。
点击编辑图标 ( ) 可查看搜索条件或创建新的搜索。

设置表格式部分中显示的搜索字段

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 对于表格式报告部分，请点击**字段 (Fields)** 参数旁边的编辑图标 ( )。

步骤 2 如果要修改该部分，必须添加和删除字段，并将字段图标拖入到所需的列顺序中。

步骤 3 如果要更改任何列的排序顺序，必须使用每个字段图标上的下拉列表设置排序顺序和优先级。

步骤 4 点击 **OK**。

向报告模板添加文本部分

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

文本部分可包含使用多种字体大小和样式（如粗体、斜体等）的富文本，以及输入参数和导入的图像。

提示 文本部分对于介绍报告或报告各部分非常有用。

过程

步骤 1 在报告模板编辑器中，点击添加文本部分图标 ( )。

步骤 2 将新文本部分拖放到其在报告模板的指定位置。

步骤 3 如果要将文本部分放在页面开始或末尾，请在文本部分之前或之后添加分页符。

步骤 4 如果要更改文本部分的通用名称，请点击标题栏中的部分名称并输入新名称。

步骤 5 在文本部分的正文中添加带格式的文本和图像。
可以包括在生成报告时动态更新的输入参数。

步骤 6 点击**保存 (Save)**。

向报告模板添加分页符

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击添加分页符图标 ()。
分页符显示在模板的底部。

步骤 2 将分页符拖放到部分前面或后面的指定位置。

步骤 3 点击**保存 (Save)**。

全局时间窗口与报告模板部分

包含基于时间的数据的报告模板（例如，入侵或发现事件）具有全局时间段，默认情况下，模板中基于时间的部分创建时会继承该时间段。更改全局时间段会更改配置为继承全局时间段的部分的本地时间段。可以通过清除 **Inherit Time Window** 复选框来禁用单个部分的时间段继承。然后可以编辑本地时间段。

注释 全局时间段继承仅适用于具有基于时间的表数据的报告部分，例如入侵事件和发现事件。对于报告网络资产（主机和设备）和相关信息（如漏洞）的部分，必须分别设置每个时间段。

为报告模板及其部分设置全局时间窗口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

提示 报告的每个部分可以有不同的时间范围。例如，第一部分可能是一个月度摘要，而剩余部分则可深入提供周级别的详细信息。在这些情况下，单独设置部分级别的时间段。

过程

步骤 1 在报告模板编辑器中，点击**生成 (Generate)**。

步骤 2 要修改全局时间段，请点击时间段图标 ()。

步骤 3 在**事件时间窗口 (Events Time Window)** 选显卡中修改时间设置。

步骤 4 点击 **Apply**。

步骤 5 点击**生成 (Generate)** 以生成报告并点击**是 (Yes)** 进行确认。

为报告模板部分设置本地时间窗口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在模板的 Report Sections 页面上，清除部分的 **Inherit Time Window** 复选框（若有）。

步骤 2 要更改部分的本地时间段，请点击时间段图标 ( )。

注释 包含统计表的数据的部分只能有滑动时间窗。

步骤 3 点击“事件时间窗口”(Events Time Window) 上的**应用 (Apply)**。

步骤 4 点击**保存 (Save)**。

重命名报告模板部分

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击部分页眉中的当前部分名称。

步骤 2 为该部分输入新名称。

步骤 3 点击 **OK**。

预览报告模板部分

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

预览功能显示表视图的字段布局和排序顺序以及图形的重要易读特征，如饼图颜色。

过程

步骤 1 在编辑报告模板部分时，可随时点击**预览 (Preview)** 预览该部分。

步骤 2 点击**确定 (OK)** 关闭预览。

报告模板部分中的搜索

生成成功报告的关键在于定义填入报告部分的搜索。Firepower 系统提供搜索编辑器，可查看报告模板中可用的搜索以及定义新的自定义搜索。

在报告模板部分搜索

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板的相关部分中，点击 **Search** 字段旁边的编辑图标 ( )。

步骤 2 如果要根据预定义搜索进行自定义搜索，必须从**已保存搜索 (Saved Searches)** 下拉列表中选择预定义搜索。
此列表包含此表格的所有可用预定义搜索，包括系统范围和报告特定的预定义搜索。

步骤 3 在相应的字段中编辑搜索条件。
对于某些字段，限制可以包含与事件搜索相同的运算符（<、<>等）。如果输入多个条件，则搜索只返回与所有条件匹配的记录。

步骤 4 如果要从下拉菜单插入输入参数，而不是输入限制值，则必须点击输入参数图标 ( )。

注释 在编辑报告搜索的限制时，系统会使用以下名称保存已编辑的搜索：*section* custom search，其中 *section* 是部分标题栏中的名称，后跟字符串 custom search。要使保存的自定义搜索具有有意义的名称，请确保更改部分名称后再保存已编辑搜索。无法重命名已保存的报告搜索。

步骤 5 点击 **OK**。

输入参数

在报告模板中可以使用输入参数，使报告可以在生成时自动更新。输入参数图标 ( ) 指示可处理其的字段。有两种输入参数：

- 预定义的输入参数由内部系统功能或配置信息解析。例如，在生成报告时，系统用当前日期和时间替换 $<Time> 参数。
- 用户定义的输入参数提供部分搜索限制。使用输入参数限制搜索，会指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地定制报告显示特定数据子集，而无需更改模板。例如，可以为报告部分搜索的 **Destination IP** 字段提供输入参数。然后，当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

  还可以定义字符串类型输入参数，在报告的以下特定区域中添加动态文本，例如，邮件（主题或正文）、报告文件名和文本部分。可以为不同部门个性化设置报告，具有自定义的报告文件名、邮件地址和邮件消息，使同一模板适用一切。

预定义输入参数

表 *221*：预定义输入参数

插入此参数…	…在模板中包括此信息：
$<Logo>	所选的上传徽标
$<Report Title>	报告标题
$<Time>	运行报告的日期和时间，粒度为一秒
$<Month>	当前月份
$<Year>	当前年份
$<System Name>	Firepower 管理中心的名称
$<Model Number>	Firepower 管理中心的型号
$<Time Window>	当前应用于报告部分的时间段

插入此参数…	…在模板中包括此信息：
$<Constraints>	当前应用于报告部分的搜索限制

表 222：预定义输入参数的使用

参数	报告模板封面	报告模板报告标题	报告模板部分说明	报告模板文本部分	生成报告文件名	生成报告邮件主题、正文
$<Logo>	是	否	否	否	否	否
$<Report Title>	是	否	是	是	是	是
$<Time>	是	是	是	是	是	是
$<Month>	是	是	是	是	是	是
$<Year>	是	是	是	是	是	是
$<System Name>	是	是	是	是	是	是
$<Model Number>	是	是	是	是	是	是
$<Time Window>	否	否	是	否	否	否
$<Constraints>	否	否	是	否	否	否

用户定义的输入参数

使用输入参数可扩展搜索的实用性。输入参数指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地限制报告显示特定数据子集，而无需更改搜索。例如，可以为深度提供部门级安全事件的报告部分的 **Destination IP** 字段提供输入参数。当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

输入参数的类型确定可以使用其的搜索字段。只能在相应的字段中使用指定类型。例如，定义为字符串类型的用户参数可插入文本字段，但不可插入接受 IP 地址的字段。

定义的每个输入参数均具有名称和类型。

表 223：用户定义的输入参数类型

将此参数类型…...	用于包含此数据的字段…...
Network/IP	CIDR 格式的任何 IP 地址或网段
应用	应用协议、客户端应用或网络应用的名称

将此参数类型……	用于包含此数据的字段……
Event Message	任何事件视图消息
设备	管理中心或受管设备
用户名	用户身份，比如发起者用户和响应者用户
Number (VLAN ID, Snort ID, Vuln ID)	任何 VLAN ID、Snort ID 或漏洞 ID
字符串	文本字段（如应用或操作系统版本、注释或说明）

创建用户定义的输入参数

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击添加输入参数图标 ( )。

步骤 3 输入参数**名称 (Name)**。

步骤 4 从**类型 (Type)** 下拉列表中选择值。

步骤 5 点击**确定 (OK)** 添加参数。

步骤 6 点击**确定 (OK)** 返回到编辑器。

编辑用户定义的输入参数

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

报告模板的**输入参数 (Input Parameters)** 部分列出模板的所有可用用户定义参数。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击要修改的参数旁边的编辑图标 ( )。

步骤 3 在**名称 (Name)** 中输入新名称。

步骤 4 使用**类型 (Type)** 下拉列表来更改参数类型。

步骤 5 点击 **OK**，保存更改。

步骤 6 如果要删除输入参数，请点击输入参数旁边的删除图标 ( ) 并确认。

步骤 7 点击**确定 (OK)** 返回到报告模板编辑器。

使用用户定义的输入参数限制搜索

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

定义的输入参数仅适用于与其参数类型匹配的搜索字段。例如，**Network/IP** 类型的参数仅适用于接受 CIDR 格式的 IP 地址或网段的字段。

过程

步骤 1 在报告模板编辑器中，点击该部分中**搜索 (Search)** 字段旁边的编辑图标 ( )。
可接受输入参数的字段标有输入参数图标 ( )。

步骤 2 点击字段旁边的输入参数图标 ( )，然后从下拉菜单中选择输入参数。
用户定义的输入参数标有图标 ( )

步骤 3 点击 **OK**。

报告模板中的文档属性

在生成报告之前，可以设置影响报告外观的文档属性。这些属性包括可选封面和目录。对一些属性是否支持取决于所选的报告格式：PDF、HTML 或 CSV。

表 *224*：文档属性支持

属性	是否支持 PDF？	是否支持 HTML？	是否支持 CSV？
封面页	是，具有可选徽标和自定义外观	是，具有可选徽标和自定义外观	否
目录	是	是	否
页眉和页脚	是，在任意字段中均具有可选文本或徽标	否	否
自定义开始页码	是	否	否
不显示首页页码的选项	是	否	否

编辑报告模板中的文档属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 有以下选项可供选择：

- 添加封面 - 要添加封面，请选中**包含封面 (Include Cover Page)** 复选框。
- 自定义封面 - 要编辑封面设计，请参阅自定义封面，第 1359 页。
- 添加目录 - 要添加目录，请选中**包含目录 (Include Table of Contents)** 复选框。
- 管理徽标 - 要管理与模板关联的徽标图像，请参阅管理报告模板徽标，第 1359 页。
- 配置页眉和页脚 - 要指定此模板的页眉和页脚的元素，请使用**页眉 (Header)** 和**页脚 (Footer)** 字段中的下拉列表。
- 设置首页码 - 要指定报告首页的页码，请输入**页码开始 (Page Number Start)** 值。

- 显示首页码 - 要显示报告首页的页码，请选中**对首页编号？(Number First Page?)** 复选框。如果选择此选项，则封面未编号。

步骤 3 点击 **OK**，保存更改。

自定义封面

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以自定义报告模板的封面。封面可包含使用多种字体大小和样式（如粗体、斜体等）的富文本，以及输入参数和导入的图像。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **Cover Page Design** 旁边的编辑图标 ( )。

步骤 3 在富文本编辑器中编辑封面设计。

步骤 4 点击 **OK**。

管理报告模板徽标

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以在Firepower管理中心上存储多个徽标，并将其与其他报告模板关联。在设计模板时设置徽标关联。如果导出模板，导出包会包含徽标。

将徽标上传到 Firepower 管理中心时，该徽标可用于：

- Firepower 管理中心上的所有报告模板，或
- 在多域部署中，当前域中的所有报告模板

徽标图像可为 GIF、JPG 或 PNG 格式。

可以将报告中的徽标更改为上传到Firepower管理中心的任何JPG图像。例如，如果重复使用模板，可以将另一个公司的徽标与报告关联。

可以删除任何已上传的徽标。删除徽标会从使用其的所有模板删除徽标。删除操作无法撤消。请注意，不能删除预定义思科徽标。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。
当前与模板相关联的徽标显示在 **General Settings** 中的 **Logo** 下。

步骤 2 点击徽标旁边的编辑图标 ( )。

步骤 3 有以下选项可供选择：

- 添加 - 添加新徽标，如添加新徽标，第 1360 页中所述。
- 更改 - 更改报告模板的徽标，如更改报告模板的徽标，第 1361 页中所述。
- 删除 - 删除徽标，如删除徽标，第 1361 页中所述。

添加新徽标

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击**徽标 (Logo)** 字段旁边的编辑图标 ( )。

步骤 3 点击 **Upload Logo**。

步骤 4 点击**浏览 (Browse)** 按钮，浏览至文件的位置，然后点击**打开 (Open)**。

步骤 5 点击**上传**。

步骤 6 如果要将新徽标与当前模板关联，请选择当前模板，然后点击**确定 (OK)**。

更改报告模板的徽标

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击**徽标 (Logo)** 字段旁边的编辑图标 ( )。

步骤 3 从“选择徽标”(Select Logo) 对话框中，选择要与报告模板关联的徽标。

步骤 4 点击 **OK**。

删除徽标

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击**徽标 (Logo)** 字段旁边的编辑图标 ( )。

步骤 3 从“选择徽标”(Select Logo) 对话框中，选择要删除的徽标。

步骤 4 点击 **Delete Logo**。

步骤 5 点击 **OK**。

管理报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在多域部署中，系统会显示在当前域中创建的报告模板，您可以对其进行编辑。系统还会显示在祖先域中创建的报告模板，您不可以对其进行编辑。要查看和编辑在较低域中创建的报告模板，请切换至该域。系统仅显示在当前域中创建的报告。

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击**报告模板 (Report Templates)** 选项卡。

步骤 3 有以下选项可供选择：

- 删除 - 在要删除的模板旁边，点击删除图标 ( ) 并确认。
  不能删除系统提供的报告模板。安全分析人员仅可删除由其创建的报告模板。在多域部署中，仅可以删除属于当前域的报告模板。
- 编辑 - 要编辑报告模板，请参阅编辑报告模板，第 1362 页。
- 导出 - 要导出报告模板，请参阅导出报告模板，第 1363 页。
  提示 也可以使用标准配置导出过程导出报告模板；请参阅导出配置，第 151 页。
- 导入 - 要导入报告模板，请参阅导入配置，第 151 页。

编辑报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，系统会显示在当前域中创建的报告模板，您可以对其进行编辑。系统还会显示在祖先域中创建的报告模板，您不可以对其进行编辑。要查看和编辑在较低域中创建的报告模板，请切换至该域。

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击**报告模板 (Report Templates)** 选项卡。

步骤 3 点击要编辑的模板的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 有以下选项可供选择：

- 添加分页符；请参阅向报告模板添加分页符，第 1350 页。
- 添加文本部分；请参阅向报告模板添加文本部分，第 1350 页。
- 配置部分内容，如报告模板配置，第 1348 页中所述。
- 创建输入参数；请参阅创建用户定义的输入参数，第 1356 页。
- 编辑输入参数；请参阅编辑用户定义的输入参数，第 1356 页。
- 编辑文档属性；请参阅编辑报告模板中的文档属性，第 1358 页。
- 搜索模板部分；请参阅在报告模板部分搜索，第 1353 页。
- 通过点击**高级 (Advanced)** 来设置文档属性，如报告模板中的文档属性，第 1357 页中所述。
- 设置全局时间窗口；请参阅为报告模板及其部分设置全局时间窗口，第 1351 页。
- 设置本地时间窗口；请参阅为报告模板部分设置本地时间窗口，第 1352 页。
- 设置搜索字段；请参阅设置表格式部分中显示的搜索字段，第 1349 页。
- 设置表和数据格式；请参阅设置报告模板部分的表和数据格式，第 1348 页。
- 指定搜索和过滤器；请参阅为报告模板部分指定搜索或过滤器，第 1349 页。

导出报告模板

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 选择**报告模板 (Report Templates)** 选项卡。

步骤 3 点击要导出的模板的导出图标 ( )。

步骤 4 点击**保存文件 (Save file)**和**确认 (OK)** 以将文件保存到本地计算机。

使用模板生成报告

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

创建并自定义报告模板后便可生成报告了。在生成过程中，可以选择报告格式（HTML、PDF 或 CSV）。还可以调整报告的全局时间段，它对所有部分应用一致的时间范围，但您排除的时间范围除外。

在 PDF 报告中不支持使用 Unicode (UTF - 8) 字符的文件名。如果生成 PDF 格式的报告，包含特殊 Unicode 文件名（例如，文件或恶意活动中显示的那些文件名）的任何报告部分以转换形式显示这些文件名。

如果报告模板的搜索规格中包括用户输入参数，生成过程会提示输入值，将报告的这次运行定制为数据的一个子集。

如已配置 DNS 服务器且启用 IP 地址解析，则当解析成功时，报告包含主机名。

在多域部署中，如果在祖先域中生成报告，该报告可包括来自所有后代域的结果。要为特定叶域生成报告，请切换至该域。

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击**报告模板 (Report Templates)** 选项卡。

步骤 3 点击要用于生成报告的模板旁边的报告图标 ( )。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

提示 要从祖先模板生成报告，请将该模板复制到当前域。

步骤 4 或者，也可以配置报告名称：

- 输入新的**文件名 (File Name)**。如果不输入新名称，系统将使用报告模板中指定的名称。
- 使用输入参数图标 ( ) 向文件名添加一个或多个输入参数。

步骤 5 点击相应的图标，选择报告的输出格式：HTML、PDF 或 CSV。

步骤 6 如果要更改全局时间段，请点击时间段图标 ( )。

注释 只有当单个报告部分配置为继承全局设置时，设置全局时间段才会影响单个报告的内容。

步骤 7 为**输入参数 (Input Parameters)** 部分中显示的任何字段输入值。

提示 通过在字段中键入 * 通配符，可以忽略用户参数。这会消除对搜索的用户参数限制。

注释　系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址或 VLAN 标记限制报告结果可能会出现意外结果。

步骤 8　如果在 Firepower 管理中心配置中启用了邮件中继主机，点击**邮件 (Email)** 可在报告生成时自动通过邮件传送报告。

步骤 9　点击**确定 (OK)**，并在显示提示时进行确认。

步骤 10　有以下选项可供选择：

- 点击报告链接以在新窗口中显示该报告。
- 点击**确定 (OK)** 返回到报告模板编辑器。

报告生成选项

可以配置报告生成选项来执行以下操作：

- 使用 Firepower 系统调度程序自动执行报告生成。可以在每日、每周和每月等全程时间范围上自定义计划。
- 使用调度程序分发邮件报告。必须在计划任务**之前**配置报告模板和邮件中继主机。
- 当生成报告时，将报告作为邮件附件自动发送到收件人列表。必须具有适当配置的邮件中继主机，才能通过邮件传送报告。
- 将新生成的报告文件保存到所配置的远程存储位置。要使用远程存储，必须先配置远程存储位置。

注释　如果在远程存储后又切换回本地存储，则远程存储中的报告不在 Reports 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

在生成时通过邮件分发报告

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击**报告模板 (Report Templates)** 选项卡。

步骤 3 点击要用于生成报告的模板旁边的报告图标 ( )。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

提示 要从祖先模板生成报告，请将该模板复制到当前域。

步骤 4 展开窗口的**邮件 (Email)** 部分。

步骤 5 在**邮件选项 (Email Options)** 字段中，选择**发送邮件 (Send Email)**。

步骤 6 在**收件人列表 (Recipient List)**、**CC** 和 **BCC** 字段中，输入逗号分隔列表形式的收件人邮箱地址。

步骤 7 在**主题 (Subject)**字段中，输入邮件主题。

提示 可以在 **Subject** 和邮件正文中提供输入参数，以动态生成邮件中的信息，例如时间戳或 Firepower 管理中心名称。

步骤 8 根据需要在邮件正文中输入附函。

步骤 9 点击**确定 (OK)** 并确认。

关于使用生成的报告

在“报告”(Reports) 选项卡页面上访问和使用之前生成的报告。

查看报告

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

Reports选项卡列出所有以前生成的报告，提供报告名称、生成日期和时间、生成用户以及报告是在本地还是远程存储的信息。状态栏指示报告是已生成，处于生成队列中（例如，对于计划任务）还是无法生成（例如，由于磁盘空间不足）。

请注意，具有管理员访问权限的用户可以查看所有报告；其他用户只能查看自己所生成的报告。

在多域部署中，只能查看在当前域中生成的报告。

Reports选项卡页面显示所有本地存储的报告。如果当前配置了远程存储，该页面也显示远程存储的报告。远程存储的报告的**位置 (Location)** 列数据为 `Remote`。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在 Reports 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

过程

步骤 1 选择概述 (Overview) > 报告 (Reporting)。

步骤 2 点击 **Reports** 选项卡。

步骤 3 点击要查看的报告。

下载报告

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以将任何报告文件下载到本地计算机。由此，可以通过邮件发送报告，或者通过其他可用的手段以电子方式分发。

在多域部署中，只能下载在当前域中生成的报告。

过程

步骤 1 选择概述 (Overview) > 报告 (Reporting)。

步骤 2 点击 **Reports** 选项卡。

步骤 3 选中要下载的报告旁边的复选框，然后点击下载 (Download)。

提示 点击页面左上方的复选框以下载页面上的所有报告。如果有多个报告页面，则系统会再显示一个复选框，可以点击该复选框以下载所有页面上的所有报告。

步骤 4 根据浏览器提示下载报告。如果选择多个报告，则以单个 `.zip` 文件形式对其进行下载。

远程存储报告

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

当前配置的报告存储位置显示在“概述”(Overview) > “报告”(Reporting) > “报告”(Reports) 页面的底部，提供本地、NFS 和 SMB 存储的磁盘使用率。如果使用 SSH 访问远程存储，则不提供磁盘使用量的数据。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在 Reports 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

开始之前

- 配置远程存储位置，如远程存储管理， 第 446 页中所述。

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 选择**报告 (Reports)** 选项卡。

步骤 3 选中页面底部的**启用报告的远程存储 (Enable Remote Storage of Reports)** 复选框。

接下来的操作

- 将报告从本地存储移至远程存储；请参阅将报告移至远程存储器， 第 1368 页。

将报告移至远程存储器

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以按批量处理模式或单个地将本地存储的报告转移到远程存储位置。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在 Reports 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

开始之前

- 配置远程存储位置，如远程存储管理，第 446 页中所述。

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 选择**报告 (Reports)** 选项卡。

步骤 3 选中要移动的报告旁边的复选框，然后点击**移动 (Move)**。

提示 选中页面左上方的复选框以移动页面上的所有报告。如果报告有多页，则会再显示一个复选框，可以选中该复选框来移动所有页面上的全部报告。

步骤 4 确认要转移报告。

删除报告

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以随时删除报告文件。此步骤会完全删除文件，并且无法恢复。尽管仍然有生成了报告的报告模板，但如果时间段已扩展或滑动，就可能难以重新生成特定报告文件。如果模板使用输入参数，重新生成可能也很困难。

在多域部署中，只能删除在当前域中生成的报告。

过程

步骤 1 选择**概述 (Overview)** > **报告 (Reporting)**。

步骤 2 点击 **Reports** 选项卡。

步骤 3 有以下选项可供选择：

- 删除所选项 - 选中要删除的报告旁边的复选框，然后点击**删除 (Delete)**。

- 删除所有 - 选中页面左上方的复选框以删除页面上的所有报告。如果报告有多页，则会再显示一个复选框，可以选中该复选框来删除所有页面上的全部报告。

步骤 4 确认删除。

第 74 章

Firepower 管理中心的外部警报

以下主题介绍如何配置 Firepower 管理中心的警报响应和外部警报：

Firepower 管理中心警报响应

通过 SNMP、系统日志或邮件发送外部事件通知有助于重要系统监控。Firepower 管理中心使用可配置的警报响应与外部服务器交互。各种事件日志记录和警报配置使用这些警报响应发送外部警报，并且/而非（有时）将事件记录到 Firepower 系统数据库。

注释 使用警报响应的任何警报均从 Firepower 管理中心发送。受管设备还可以基于单个入侵规则触发发送外部警报。有关详细信息，请参阅配置入侵规则的外部警报， 第 1379 页。

在大多数情况下，外部警报与相关数据库记录的事件中的信息相同。但是，无论是何种基础事件类型，对于关联规则中包含连接跟踪器的关联事件警报，您收到的信息都与流量量变曲线更改警报相同。

可在“警报”(Alerts) 页面（**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**）上创建和管理警报响应。新的警报响应自动启用。要暂停警报生成，可以禁用警报响应，而非将它们删除。

如果您使用警报响应将连接日志发送到 SNMP 陷阱或系统日志服务器（连接事件不支持外部邮件警报），则必须在编辑这些警报响应之后部署配置更改。否则，对警报响应所做的更改会立即生效。

在多域部署中，当您创建警报响应时，它属于当前域。后代域也可能使用此警报响应。

支持警报响应的配置

创建警报响应后，可以使用它从 Firepower 管理中心发送以下外部警报。

警报/事件类型	有关详细信息，请参阅
按影响标志划分的入侵事件	配置影响标志警报，第 1377 页
按类型划分的发现事件	配置发现事件警报，第 1377 页
基于网络的恶意软件和追溯性恶意软件事件	配置面向 Firepower 的 AMP 警报，第 1378 页
按关联策略违规划分的关联事件	将响应添加到规则和白名单，第 1279 页
按日志记录规则或默认操作（不支持邮件警报）划分的连接事件	可配置的连接日志记录，第 1502 页
按运行状况模块和严重性级别划分的运行状况事件	创建运行状况监控器警报，第 212 页

创建 SNMP 警报响应

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任意，除外	任意	管理

可使用 SNMPv1、SNMPv2 或 SNMPv3 创建 SNMP 警报响应。

注释 为 SNMP 协议选择 SNMP 版本时，请注意 SNMPv2 仅支持只读社区，SNMPv3 仅支持只读用户。此外，SNMPv3 还支持使用 AES128 加密。

如果想要使用 SNMP 监控 64 位值，则必须使用 SNMPv2 或 SNMPv3。SNMPv1 不支持 64 位监控。

开始之前

- 如果网络管理系统需要 Firepower 管理中心的管理信息库 (MIB) 文件，则可在 `/etc/sf/DCEALERT.MIB` 处获取该文件。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建 SNMP 警报 (Create SNMP Alert)**。

步骤 3 输入**名称 (Name)** 指定 SNMP 响应。

步骤 4 在**陷阱服务器 (Trap Server)** 字段中，输入 SNMP 陷阱服务器的主机名或 IP 地址。

注释 如果在此字段中输入了无效的 IPv4 地址（例如 192.169.1.456），则系统**不会**发出警告。相反，无效地址会被视为主机名。

步骤 5 从**版本 (Version)** 下拉列表中，选择要使用的 SNMP 版本。SNMP v3 是默认值。

步骤 6 根据使用的 SNMP 版本，执行以下任一操作:

- 对于 SNMP v1 或 SNMP v2，在**社区字符串 (Community String)** 字段中输入 SNMP 社区名称，并跳至步骤 12。
- 对于 SNMP v3，在**用户名 (User Name)** 字段中，输入要使用 SNMP 服务器对其进行身份验证的用户的名称并继续下一步。

步骤 7 从**身份验证协议 (Authentication Protocol)** 下拉列表中，选择要用于身份验证的协议。

步骤 8 在**身份验证密码 (Authentication Password)** 字段中，输入使用 SNMP 服务器进行身份验证所需的密码。

步骤 9 从**隐私协议 (Privacy Protocol)** 列表中，选择**无 (None)** 以不使用隐私协议，或选择 **DES** 以使用数据加密标准作为隐私协议。

步骤 10 在**隐私密码 (Privacy Password)** 字段中，输入 SNMP 服务器所需的隐私密码。

步骤 11 在**引擎 ID (Engine ID)** 字段中，使用偶数数字（十六进制表示法）输入 SNMP 引擎的标识符。使用 SNMPv3 时，系统使用引擎 ID 值对消息进行编码。SNMP 服务器需要使用该值对消息进行解码。

思科建议您使用十六进制版本的 Firepower 管理中心 IP 地址的。例如，如果Firepower 管理中心的 IP 地址是 `10.1.1.77`，请使用 `0a01014D0`。

步骤 12 点击**保存 (Save)**。

创建系统日志警报响应

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

配置系统警报响应时，可指定与系统日志消息相关联的严重性和设备，以确保它们得到系统日志服务器的正确处理。设备指明创建消息的子系统，严重性界定消息的严重性。设备和严重性不显示在系统日志中的实际消息中，而是告知接收系统日志消息的系统如何对消息进行归类。

提示 有关系统日志如何运行及如何对其进行配置的更多详细信息，请参阅系统文档。在 UNIX 系统上，`syslog` 和 `syslog.conf` 的 `man` 页面提供了概念信息和配置说明。

虽然在创建系统日志警报响应时可选择任何类型的设施，但是应根据系统日志服务器选择合适的设施；并非所有系统日志服务器都支持所有设施。对于 UNIX 系统日志服务器，`syslog.conf` 文件应指示哪些设备保存到了服务器的哪些日志文件上。

开始之前

- 确认系统日志服务器可接受远程消息。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建系统日志警报 (Create Syslog Alert)**。

步骤 3 输入警报的**名称 (Name)**。

步骤 4 在**主机 (Host)** 字段中，输入系统日志服务器的主机名或 IP 地址。

注释 如在此字段中输入了无效的 IPv4 地址（例如 192.168.1.456），则系统不会发出警告。相反，无效地址会被视为主机名。

步骤 5 在**端口 (Port)** 字段中，输入服务器用于系统日志消息的端口。默认情况下，此值为 514。

步骤 6 从**设施 (Facility)** 列表中，选择系统日志警报设施，第 1374 页中所述的设施。

步骤 7 从**严重性 (Severity)** 列表中，选择系统日志严重性级别，第 1375 页中所述的严重性。

步骤 8 在**标记 (Tag)** 字段中，输入要与系统日志消息一起显示的标记名称。

例如，如果要在发送到系统日志的所有消息前加上 `FromMC`，请在字段中输入 `FromMC`。

步骤 9 点击**保存 (Save)**。

系统日志警报设施

下表列出了可选择的系统日志设施。

表 *225*: 可用的系统日志设施

设施	说明
ALERT	警报消息。
审计	审计子系统生成的消息。

设施	说明
AUTH	与安全和授权相关的消息。
AUTHPRIV	与安全和授权相关的访问限制消息。在很多系统上，这些消息会转发至一个安全文件。
CLOCK	时钟守护程序生成的消息。 请注意，运行 Windows 操作系统的系统日志服务器将使用 CLOCK 设备。
CRON	时钟守护程序生成的消息。 请注意，运行 Linux 操作系统的系统日志服务器将使用 CRON 设备。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
MAIL	邮件系统生成的消息。
新闻	网络新闻子系统生成的消息。
NTP	NTP 守护程序生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志严重性级别

下表列出可选择的标准系统日志严重性级别。

表 *226*：系统日志严重性级别

Level	说明
ALERT	应立即更正的状况。
CRIT	临界状况。

Level	说明
DEBUG	包含调试信息的消息。
EMERG	向所有用户广播的紧急状况。
ERR	错误状况。
信息	信息性消息
请注意！	需要注意但非错误的状况。
警告	警告消息。

创建邮件警报响应

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

开始之前

- 确认 Firepower 管理中心可反向解析其自身的 IP 地址。
- 配置邮件中继主机，如配置邮件中继主机和通知地址，第 458 页中所述。

注释 不可以使用邮件警报记录连接。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 从**创建警报 (Create Alert)** 下拉菜单中，选择**创建邮件警报 (Create Email Alert)**。

步骤 3 为警报响应输入**名称 (Name)**。

步骤 4 在**收件人 (To)** 字段中，输入要将警报发送到其中的邮箱地址（用逗号分隔）。

步骤 5 在**发件人 (From)** 字段中，输入要显示为警报发件人的邮箱地址。

步骤 6 在 **Relay Host** 旁，验证列出的邮件服务器是要用于发送警报的服务器。

提示 要更改邮件服务器，请点击编辑图标 ()。

步骤 7 点击**保存 (Save)**。

配置影响标志警报

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理

可将系统配置为只要出现带有特定影响标志的入侵事件就会发出警报。影响标记可通过将入侵数据、网络发现数据和漏洞信息相关联来帮助评估入侵对网络的影响。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 点击**影响标志警报 (Impact Flag Alerts)** 选项卡。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**影响配置 (Impact Configuration)** 部分中，选中相应复选框为每个影响标志指定要接收的警报。

步骤 5 点击**保存 (Save)**。

配置发现事件警报

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可将系统配置为只要出现特定类型的发现事件就会发出警报。

开始之前

- 将网络发现策略配置为记录要为其配置警报的发现事件类型，如配置网络发现事件日志记录，第 1226 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 点击**发现事件警报 (Discovery Event Alerts)** 选项卡。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**事件配置 (Events Configuration)** 部分中，选中与要为每种发现事件类型接收的警报对应的复选框。

步骤 5 点击**保存 (Save)**。

配置面向 Firepower 的 AMP 警报

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件	恶意软件	任何环境	任何环境	管理

可将系统配置为只要生成任何基于网络的恶意软件事件（包括回溯性事件）就发出警报。但是，不能对基于终端的（面对终端的 AMP）恶意软件事件发送警报。

开始之前

- 配置文件策略以执行恶意软件云查找并将该策略与访问控制规则相关联，如使用入侵和文件策略的访问控制，第 637 页中所述。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 点击**高级恶意软件防护警报 (Advanced Malware Protections Alerts)** 选项卡。

步骤 3 在**警报 (Alerts)** 部分中，选择要用于每种警报类型的警报响应。

提示 要创建新警报响应，请从任何下拉列表中选择**新建 (New)**。

步骤 4 在**事件配置 (Event Configuration)** 部分中，选中与要为每种恶意软件事件类型接收的警报对应的复选框。

请注意，**All network-based malware events** 包括 **Retrospective Events**。

步骤 5 点击**保存 (Save)**。

第 75 章

配置入侵规则的外部警报

以下主题介绍如何配置入侵规则的外部警报：

概述：配置入侵规则的外部警报

虽然 Firepower 系统在 Web 界面内提供各种入侵事件视图，但一些企业更喜欢通过定义外部入侵事件通知对关键系统实施持续监控。如果想要立即通知关键事件的特定联系人，可以设置邮件警报进行操作。也可以记录日志到系统日志设施或将事件数据发送到 SNMP 陷阱服务器。

您可以为每个入侵策略指定入侵事件通知限制、设置发送到外部日志记录设施的入侵事件通知，也可以配置入侵事件的外部响应。

一些分析师并不希望收到同一入侵事件的多个警报，但却希望控制收到特定入侵事件通知的频率。您可以为规则创建事件阈值，限制在某个时段生成事件的频率，还可以抑制规则的事件生成。

在多域部署中，可以配置任何域中的外部警报。在祖先域中，系统会为后代域中的入侵事件生成通知。

提示

在 Firepower 系统中，除了入侵策略，还可以执行另一种警报。对于其他类型事件，可以配置邮件、SNMP 和系统日志警报响应活动。这些事件包括带有特定影响标记的入侵事件或采用特定访问控制规则记录的连接事件。

SNMP 响应

SNMP 陷阱是一种网络管理通知。将设备配置为以 SNMP 陷阱（又称为 *SNMP* 警报）的形式发送入侵事件通知。每个 SNMP 警报都包括以下内容：

- 生成陷阱的服务器的名称
- 检测到入侵事件的设备的 IP 地址
- 检测到入侵事件的设备的名称
- 事件数据

可以设置 SNMP 警报的多种参数。可设定的参数因所用的 SNMP 版本而有所不同。

SNMP 响应配置选项

提示 如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从Firepower管理中心中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

对于 SNMP v2，您可指定下表中介绍的选项。

表 *227*：*SNMP v2* 选项

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则可以选择 **as Binary**。否则，应选择 **as String**。例如，HP Openview 就需要选择字符串类型。
Trap Server	收到 SNMP 陷阱通知的服务器。 可指定一个唯一的 IP 地址或主机名。
Community String	社区名称。

SNMP v3 选项

对于 SNMP v3，您可指定下表中介绍的选项。

注释 当您使用 SNMP v3 时，设备会使用一个 Engine ID 值编码消息。SNMP 服务器需要使用该值解码消息。目前，该 Engine ID 值始终采用设备 IP 地址的十六进制形式，且该字符串的末尾为 `01`。例如，如果发送 SNMP 警报的设备有一个 IP 地址为 `172.16.1.50`，则 Engine ID 为 `0xAC10013201`，而如果设备有一个 IP 地址为 `10.1.1.77`，则 `0x0a01014D01` 就用作 Engine ID。

表 *228*：*SNMP v3* 选项

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则可以选择 **as Binary**。否则，应选择 **as String**。例如，HP Openview 就需要选择字符串类型。
Trap Server	收到 SNMP 陷阱通知的服务器。 可指定一个唯一的 IP 地址或主机名。
Authentication Password	用于身份验证的密码。SNMP v3 使用消息摘要 5 (MD5) 哈希函数或安全哈希算法 (SHA) 哈希函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
Private Password	用于保护隐私的 SNMP 密钥。SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。 如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。
用户名	SNMP 用户名。

配置 SNMP 响应

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以配置入侵策略中的 SNMP 警报。部署访问控制策略中的入侵策略后，一旦系统检测到任何入侵事件，就会通过 SNMP 陷阱发送通知。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**外部响应 (External Responses)** 下面的 **SNMP 警报 (SNMP Alerting)** 已禁用，则点击**启用 (Enabled)**。

步骤 5 点击 **SNMP 警报 (SNMP Alerting)** 旁边的编辑图标 ( )。

提示 页面底部消息会识别包含配置的入侵策略层。

步骤 6 指定在警报中显示的 IP 地址所用的陷阱类型格式，可选择 **as Binary** 或 **as String**。

注释 如果网络管理系统正常显现 INET_IPV4 地址类型，则使用**二进制形式 (as Binary)** 选项。否则，应使用 **String** 选项。例如，HP Openview 需要选择 **as String** 选项。

步骤 7 在 **SNMP 版本 (SNMP Version)** 旁边，为 SNMP v2 点击**版本 2 (Version2)**，或为 SNMP v3 点击**版本 3 (Version 3)**。

步骤 8 输入配置选项，如SNMP 响应配置选项，第 1380 页中所述。

步骤 9 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

系统日志响应

系统日志 (*syslog*) 是网络事件记录的标准记录机制。您可以将系统配置为将入侵事件通知发送到设备上的系统日志设施。这些通知称为系统日志警报。

设备按以下因素对系统日志中收到的信息分类：

- 优先级 - 指定警报的严重性
- 设施 - 指定生成警报的子系统

请注意，接收主机不会在系统日志的实际消息中显示设施和优先级值；它仅使用它们进行分类。

系统日志警报在入侵策略中配置。

系统日志响应配置选项

系统日志警报包含以下信息：

- 生成警报的日期和时间
- 事件消息
- 事件数据
- 触发事件的生成器 ID (GID)
- Snort ID 触发事件的 (SID)
- revision

根据所用远程系统日志服务器的配置情况来合理配置设备。远程系统中的 `syslog.conf` 文件（如果将系统日志消息记录到基于UNIX或Linux的系统）指示哪些设施保存在服务器的哪些日志文件中。

表 *229*：可用的系统日志设施

设施	说明
AUTH	与安全和授权相关的消息。
AUTHPRIV	与安全和授权相关的访问限制消息。很多系统会将这些消息转发到一个安全的文件中。
CRON	时钟后台守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
MAIL	邮件系统生成的消息。
新闻	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

选择标准系统日志优先级之一，显示在该警报生成的所有通知中：

表 *230*：系统日志优先级

Level	说明
EMERG	紧急状况，向所有用户广播
ALERT	需要立即更正的状况
CRIT	严重的状况
ERR	错误状况
警告	警告消息
请注意！	并未出现错误，但需引起注意的状况
信息	参考消息
DEBUG	包含调试信息的消息

有关系统日志工作方式和配置方法的详细信息，请参阅系统随附的文档。如果您在基于 UNIX 或 Linux 的系统日志中记录数据，`syslog.conf` man 文件（在命令行键入 `man syslog.con`）和系统日志 man 文件（在命令行键入 `man syslog`）提供有关系统日志工作方式和配置方法的信息。

配置系统日志响应

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

您可以配置入侵策略中的系统日志警报。部署之后，如果检测到入侵事件，系统会发送系统日志警报给策略中指定的本地主机或日志记录主机上的系统日志设备。

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)** > **入侵 (Intrusion)**

步骤 2 点击要编辑的策略旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**外部响应 (External Responses)** 下的**系统日志警报 (Syslog Alerting)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**系统日志警报 (Syslog Alerting)** 旁边的编辑图标 ( )。

提示 页面底部消息会识别包含配置的入侵策略层。

步骤 6 如果要指定日志记录主机，请在**日志记录主机 (logging hosts)** 字段中输入远程访问 IP 地址。用逗号分隔多个主机。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 7 从下拉列表中选择设施和优先级，如系统日志响应，第 1382 页中所述。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。
如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

邮件警报

邮件警报是通过邮件发送的入侵事件通知。可以为每个规则或规则组启用或禁用入侵事件邮件警报。不论设备部署了访问控制策略中的哪项入侵策略，都会使用邮件警报设置。

邮件警报配置选项

邮件警报包括以下信息：

- 数据库中的警报总数
- 上一邮件时间（系统生成上一次邮件报告的时间）
- 当前时间（系统生成当前邮件报告的时间）
- 新警报总数
- 与指定邮件过滤器相匹配的事件数量（根据指定规则配置事件的情况下）
- （Summary Output 关闭时）每个事件的时间戳、协议、事件消息和会话信息（源和目标 IP 地址及端口，显示流量方向）

注释 如果多个入侵事件源自同一源 IP，事件下方会出现一则通知，显示其他事件的总数。

- 每个目标端口的事件总数
- 每个源 IP 的事件总数

On/Off

启用或禁用邮件通知。

From Address

指定系统发送入侵事件的一个或多个邮件地址。

To Address

指定系统接收入侵事件的邮件地址。要发送邮件给多个收件人，请使用逗号分隔邮件地址。例如：

```
user1@example.com, user2@example.com
```

Max Alerts

指定系统在按 Frequency (seconds) 计算的指定时间段内通过邮件发送的入侵事件最大数量。

Frequency (seconds)

指定系统发送入侵事件的频率。Frequency 设置也可以指定保存邮件设置的频率。

最低频率：300 秒 最高频率：40 亿秒

Coalesce Alerts

启用或禁用按照源 IP 和事件对入侵事件分组，这样如果同一个源 IP 生成多个相同的入侵事件，页面只会显示一个事件。

请注意，事件过滤后才会执行警报组合（分组）。因此，如果按照特定规则配置邮件警报，只会接收与 Mail Alerting Configuration 中指定规则相匹配的事件列表。

Summary Output

启用或禁用简要邮件警报，适用于有文字数量限制的设备，例如传呼机。简要邮件警报包含以下内容：

- 事件时间戳
- 对于Firepower 管理中心，生成事件设备的 IP 地址
- 事件协议
- 源 IP 和端口

- 目标 IP 和端口
- 事件消息
- 同一个源 IP 生成的入侵事件数量

例如：

```
2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0

snort_decoder: Unknown Datagram decoding problem! (116:108)
```

Email Alerting on Specific Rules Configuration

指定将事件发送到一个或多个指定邮件地址的规则或规则组。

配置邮件警报

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

配置邮件警报后，特定规则或规则组下的入侵事件一旦发生，设备就会发出通知。

开始之前

- 配置邮件主机以接收邮件警报；请参阅配置邮件中继主机和通知地址，第 458 页。
- 确保受管设备和 Firepower 管理中心均可反向解析各自的 IP 地址。

过程

步骤 1 选择**策略 (Policies)** > **操作 (Actions)** > **警报 (Alerts)**。

步骤 2 点击**入侵邮件 (Intrusion Email)** 选项卡。

步骤 3 在**状态 (State)** 旁边，选择**打开 (on)**。

步骤 4 输入**发件人地址 (From Address)**。

步骤 5 输入**收件人地址 (To Address)**。

步骤 6 在**最大警报数 (Max Alerts)** 字段中，输入要在一封邮件中包含的最大事件数。

步骤 7 在**最小频率 (Min Frequency)** 字段中，输入要接收邮件警报的最小频率（以秒为单位）。

步骤 8 要按 IP 地址将事件分组，请在**合并警报 (Coalesce Alerts)** 旁边，选择**打开 (on)**。

步骤 9 要发送简短邮件警报，请在**摘要输出 (Summary Output)** 旁边，选择**打开 (on)**。

提示 如果启用了 **Summary Output**，为了减少生成的警报数量，可以考虑启用 **Coalesce Alerts**。也可以考虑将 **Max Alerts** 设置为 1，从而避免设备文本消息缓冲区溢出。

步骤 10 选择**时区 (Time Zone)**。

步骤 11 要按规则启用邮件警报，请点击 **Email Alerting per Rule Configuration**。

提示　要接收所有类别中所有规则的邮件警报，请选择**全选 (Select All)**。

步骤 12 执行下列一项或两项操作：

- 如果想要接受某个类别规则的所有邮件警报，点击规则类别旁边的 **All**。
- 如果想要指定该类别单个规则下的邮件警报，点击类别文件夹，然后启用接收邮件警报的规则。

步骤 13 点击**保存 (Save)**。

第 XIX 部分

事件和资产分析工具

第 76 章

使用情景管理器

以下主题介绍如何在 Firepower 系统中使用情景管理器：

情景管理器

Firepower 系统情景管理器在情景中显示有关受监控网络状态的详细、交互图形信息，包括有关应用、应用统计、连接、地理位置、危害表现、入侵事件、主机、服务器、安全情报、用户、文件（包括恶意软件文件）和相关URL的数据。不同部分以生动的曲线图、条形图、饼状图和环状图方式显示这些数据，附有详细列表。第一部分是随着时间推移的流量和事件计数曲线图，提供网络活动的最新趋势一览图。

可轻松创建和应用自定义过滤器以微调分析，此外，还可更详细地查看各数据部分，只需点击图形区域或将光标悬停在图形区域上方。还可配置资源管理器的时间范围，以反映短至前一小时或长至上一年的时间段。只有具备管理员、安全分析师或安全分析师（只读）用户角色的用户才能访问 Context Explorer。

Firepower 系统控制面板可自定义、分区且可实时更新。相反，Context Explorer 需手动更新，以便为其数据提供更广泛的上下文，而且拥有单一且一致的布局，以供活跃用户浏览。

可根据自己的特定需求使用控制面板监控网络上的实时活动和设备。相反，可用情景管理器在特别详细和清晰的情景中调查一组预定义的最新数据：例如，如果注意到网络中只有 15% 的主机在使用 Linux，但却占据了几乎所有的 YouTube 流量，则可快速应用过滤器查看仅适合 Linux 主机的数据和/或 YouTube 关联的应用数据。与紧凑、狭小的控制面板构件不同，情景管理器部分旨在以对 Firepower 系统的专家和普通用户均有效的格式醒目再现的系统活动。

显示的数据取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。也可以应用过滤器限制所有情景管理器部分中显示的数据。

在多域部署中，在祖先域中查看数据时，情景管理器会显示所有子域的汇聚数据。在枝叶域中，只能查看特定于该域的数据。

控制面板和情景管理器之间的区别

下表概述控制面板与情景管理器之间的一些主要区别。

表 *231*：比较：控制面板与情景管理器

特性	控制面板	Context Explorer
可显示数据	Firepower 系统监控的任何内容	应用、应用统计、地理定位、危害表现、入侵事件、文件（包括恶意软件文件）、主机、安全情报事件、服务器、用户和 URL
可自定义性	• 控制面板构件的选择可自定义 • 可按不同程度自定义各个构件	• 不能改变基本布局 • 应用的过滤器显示在资源管理器URL中且可标上书签供以后使用
数据更新频率	自动（默认）；用户配置的	手动
数据过滤	可用于某些构件（必须编辑构件首选项）	可用于资源管理器的所有部分，可支持多个过滤器
图形上下文	某些构件（特别是 Custom Analysis）可以图形方式显示数据	所有数据的广泛图形上下文，包括特别详细的环状图
链接到相关网络界面页面	在某些构件中	在每个部分
已显示数据的时间范围	用户配置	用户配置

“流量和入侵事件计数时间”图形

Context Explorer 顶部有一个随时间推移的流量和入侵事件曲线图。X 轴标绘时间间隔（从五分钟到一个月不等，取决于选定的时窗）。Y 轴以千字节标绘流量（蓝线）和入侵事件计数（红线）。

请注意，最小的 X 轴间隔为五分钟。为满足此要求，系统将在选定的时间范围内将起点和终点四舍五入至最近的五分钟间隔。

在默认情况下，此部分显示选定时间范围内的所有网络流量和所有生成的入侵事件。如果应用过滤器，该图表会转而仅显示与过滤器中指定条件相关联的流量和入侵事件。例如，过滤 `Windows` 的 **OS Name** 导致时间图形仅显示与使用 Windows 操作系统的主机相关联的流量和事件。

如用 Context Explorer 过滤入侵事件数据（例如高**优先级**），蓝色流量曲线将隐藏，以便单独突出入侵事件。

将鼠标指针悬停在图形线条的任何点上方，即可查看有关流量和事件计数的确切信息。将鼠标指针悬停在其中一个彩色线条上方，也可将该线条拖至图形前沿，提供更清晰的上下文。

此部分主要从“入侵事件”和“连接事件”表提取数据。

危害表现部分

Context Explorer 的 Indications of Compromise（危害表现）部分包含两个交互部分，提供受监控网络上可能受损主机的全局视图：已触发最常用 IOC 类型的比例视图，以及按已触发指示数量显示的主机视图。

“按表现划分的主机”图形

“按指示划分的主机”图形以环状图形式显示受监控网络中主机触发的危害表现 (IOC) 的比例视图。内环按 IOC 类别划分的（例如，`CnC Connected` 或 `Malware Detected`），同时，外环进一步按特定事件类型划分数据（例如，`Impact 2 Intrusion Event - attempted-admin` 或 `Threat Detected in File Transfer`）。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”(Hosts) 和“主机危害表现”(Indications of Compromise) 表中提取数据。

“按主机划分的表现”图形

“按主机划分的指示”图形以条形图形式显示受监控网络中 15 个 IOC 最活跃的主机触发的独特危害表现 (IOC) 的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”(Hosts) 和“主机危害表现”(Indications of Compromise) 表中提取数据。

网络信息部分

情景管理器的“网络信息”(Network Information) 部分包含六个交互图形，这六个交互图显示受监控网络中连接流量的全局视图：源、目标、用户、与流量关联的安全区域、网络主机使用的操作系统故障细分，以及 Firepower 系统对网络流量执行的访问控制措施的比例视图。

“操作系统”图形

“操作系统”图形以环状图形式显示在受监控网络中主机上检测到的操作系统的比例再现。内环按 OS 名称划分（例如，`Windows` 或 `Linux`），而外环按特定操作系统版本进一步划分该数据（例如，`Windows Server 2008` 或 `Linux 11.x`）。一些密切相关的操作系统（例如，Windows 2000、Windows XP 和 Windows Server 2003）组合在一起。非常罕见或无法识别的操作系统在 **Other** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改资源管理器的时间范围，图形不变。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”表提取数据。

“按源 IP 划分的流量”图形

“按源 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按源用户划分的流量”图形

“按源用户划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源用户的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。它显示从 ISE、用户代理或强制网络门户获取的授权用户数据。

“按访问控制操作划分的连接”图形

“按访问控制操作划分的连接”图形以饼图形式显示 Firepower 系统部署已对受监控流量采取的访问控制操作（例如阻止 [Block] 或允许 [Allow]）的比例视图。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按目标 IP 划分的流量”图形

“按目标 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃目标 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个目标 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按目标 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按入口/出口安全区域划分的流量”图形

“按入口/出口安全区域划分的流量”图形以条形图形式显示受监控网络上配置的每个安全区域的传入或传出网络流量（千字节每秒）和独特连接的计数。可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

对于列出的每个安全区域，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击 **Egress**。点击 **Ingress** 返回默认视图。请注意，离开 Context Explorer 也会使图形返回默认 Ingress 视图。

注释 如果过滤入侵事件信息，“按入口/出口安全区域划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

应用信息部分

Context Explorer 的 Application Information 部分包含三个交互图形和一个表格式列表，它们显示受监控网络中应用活动的全局视图：流量、入侵事件以及与应用相关联且进一步按分配给每个应用的预估风险或业务相关性排列的主机。“应用详情”列表列出了每个应用及其风险、业务相关性、类别和主机计数的交互列表。

对于此部分的所有“应用”实例，“应用信息”图形集默认对应用协议（例如 DNS 或 SSH）进行具体检查。还可配置 Application Information 部分，具体检查客户端应用（例如 PuTTY 或 Firefox）或网络应用（例如 Facebook 或 Pandora）。

关注应用信息部分

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 将鼠标指针悬停在 **Application Protocol Information** 部分的上方。

注释 如果之前在同一个情景管理器会话中更改了此设置，该部分标题可能改为显示**客户端应用信息 (Client Application Information)** 或 **Web 应用信息 (Web Application Information)**。

步骤 3 点击 **Application Protocol**、**Client Application** 或 **Web Application**。

“按风险/业务关联性和应用划分的流量”图形

“按风险/业务相关性和应用划分的流量”图形以环状图形式显示在受监控网络上检测到的应用流量的比例再现，这些受监控网络按应用的预估风险（默认值）或预估业务相关性进行排列。内环按预估的风险/业务相关性水平（例如，`Medium` 或 `High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。很少检测到的应用在 **Other** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改资源管理器的时间范围，图形不变。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务关联性和应用显示流量，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务关联性 (Business Relevance)**。点击 **Risk** 返回默认视图。请注意，离开 Context Explorer 也会此图形返回默认 Risk 视图。

注释 如果过滤入侵事件信息，“按风险/业务和应用划分的流量”图形将隐藏。

此图形主要从“连接事件”和“应用统计数据”表提取数据。

“按风险/业务关联性和应用划分的入侵事件”图形

“按风险/业务相关性和应用划分的入侵事件”图形以环状图形式显示受监控网络上检测到的入侵事件以及与这些入侵事件相关联的应用的比例再现，这些事件按应用的预估风险（默认值）或预估业务相关性进行排列。内环按预估的风险/业务相关性水平（例如，Medium 或 High）划分，而外环按特定应用对数据进行进一步的划分（例如，SSH 或 NetBIOS）。很少检测到的应用在 **Other** 下分组。

将鼠标指针悬停在环状图形任何部分的上方，即可查看详细信息。点击图形中的任何部分，可过滤或向下展开该信息或（如适用）查看应用信息。

提示 要限制此图形，使其按业务关联性和应用显示入侵事件，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务关联性 (Business Relevance)**。点击 **Risk** 返回默认视图。请注意，离开 Context Explorer 也会此图形返回默认 Risk 视图。

此图形主要从“入侵事件”和“应用统计数据”表提取数据。

“按风险/业务关联性和应用划分的主机”图形

“按风险/业务相关性和应用划分的主机”图形以环状图形式显示受监控网络上检测到的主机以及与这些主机相关联的应用的比例化再现，这些主机按应用的预估风险（默认值）或预估业务相关性进行排列。内环按预估的风险/业务相关性水平（例如，Medium 或 High）划分，而外环按特定应用对数据进行进一步的划分（例如，SSH 或 NetBIOS）。非常罕见的应用在 **Other** 下分组。

将鼠标指针悬停在环状图形任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务关联性和应用显示主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务关联性 (Business Relevance)**。点击 **Risk** 返回默认视图。请注意，离开 Context Explorer 也会此图形返回默认 Risk 视图。

此图形主要从“应用”表提取数据。

应用详细信息列表

Application Information 部分底端为“应用详细信息”列表，该表格提供受监控网络上检测到的每个应用的预估风险、预估业务相关性、类别和主机计数信息。应用按关联主机计数的降序列出。

“应用详细信息”列表不能排序，但是，可以点击任何表条目过滤或向下展开该信息或（如适用）查看应用信息。此表主要从“应用”表提取数据。

请注意，无论日期和时间限制如何，此列表均反映所有可用数据。如果更改资源管理器的时间范围，列表保持不变。

安全情报部分

Context Explorer 的 Security Intelligence 部分包含三个交互条形图，这些图显示被安全情报拉入黑名单或监控的受监控网络上流量的全局视图。这些图形按类别、源 IP 地址和目标 IP 地址分别对此类流量进行排序；流量数量（以千字节每秒）和适用的连接数均将显示。

“按类别划分的安全情报流量”图形

“按类别划分的安全情报流量”图形以条形图形式显示受监控网络上的网络流量（千字节每秒）和顶级安全情报类别流量的独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按类别划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

“按源 IP 划分的安全情报流量”图形

“按源IP划分的安全情报流量”视图以条形图形式显示受监控网络中安全情报监控流量的顶级源IP地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按源 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

“按目标 IP 划分的安全情报流量”图形

“按目标IP划分的安全情报流量”视图以条形图形式显示受监控网络中安全情报监控流量的顶级源IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按目标 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

入侵信息部分

Context Explorer 的 Intrusion Information 部分包含六个交互图形和一个表格式列表，它们显示受监控网络中入侵事件的全局视图：影响级别、攻击源、目标、用户、优先级、与入侵事件关联的安全区域，以及入侵事件分类、优先级和计数的详细列表。

“按影响划分的入侵事件”图形

“按影响划分的入侵事件”图形以饼状图形式显示受监控网络上入侵事件的比例视图，按预估的影响级别（从 0 - 4）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“IDS 统计数据”和“入侵事件”表提取数据。

“主要攻击者”图形

“主要攻击者”图形以条形图形式显示受监控网络中主要攻击性主机 IP 地址（导致这些事件的地址）的入侵事件的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要用户”图形

“主要用户”图形以条形图形式按事件计数显示与最高入侵事件计数关联的受监控网络上的用户。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“IDS 用户统计数据”和“入侵事件”表提取数据。它显示从 ISE、用户代理或强制网络门户获取的授权用户数据。

“按优先级划分的入侵事件”图形

“按优先级划分的入侵事件”图形以饼状图形式显示受监控网络中入侵事件的比例视图，按预估的优先级（例如，`High`、`Medium` 或 `Low`）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要目标”图形

“主要目标”图形以条形图形式显示受监控网络中主要目标主机 IP 地址（导致这些事件的连接中的目标）的入侵事件计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要入口/出口安全区域”图形

“主要入口/出口安全区域”图形以条形图形式显示与受监控网络上配置的每个安全区域（入口或出口，取决于图形设置）关联的入侵事件计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击 **Egress**。点击 **Ingress** 返回默认视图。请注意，离开 Context Explorer 也会使图形返回默认 Ingress 视图。

此图形主要从“入侵事件”表提取数据。

可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

入侵事件详细信息列表

Intrusion Information 部分的底端为“入侵事件详细信息”列表，该表格提供了受监控网络上检测到的每个入侵事件的分类、预估优先级和事件计数信息。这些事件按事件计数的降序列出。

“入侵事件详细信息”列表不能排序，但是，可点击任何表条目过滤或向下展开该信息。此表主要从“入侵事件”表提取数据。

文件信息部分

Context Explorer 的 Files Information 部分包含六个交互图形，它们显示受监控网络上的文件和恶意事件的全局视图。

五个图形显示面向 Firepower 的 AMP 数据：网络流量中检测到的文件的文件类型、文件名和恶意软件处置情况，以及发送（上传）和接收（下载）这些文件的主机。最终图形显示在您的组织中检测到的所有恶意软件威胁，无论是由面向 Firepower 的 AMP 还是面向终端的 AMP 检测到。

注释 如果过滤入侵信息，整个 Files Information 部分将隐藏。

“主要文件类型”图形

“主要文件类型”图形以饼状图形式显示网络流量中检测到的文件类型的比例视图（外环），按文件类别（内环）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有恶意软件许可证才能使此图形显示面向 Firepower 的 AMP 数据。

此图形主要从“文件事件”表提取数据。

“主要文件名”图形

“主要文件名”图形以条形图形式显示网络流量中检测到的主要独特文件名的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有恶意软件许可证才能使此图形显示面向 Firepower 的 AMP 数据。

此图形主要从“文件事件”表提取数据。

“按处置情况划分的文件”图形

“主要文件类型”图形以饼状图形式显示面向 Firepower 的 AMP 检测到的文件恶意软件处置情况的比例视图。请注意，只有Firepower管理中心对其执行恶意软件云查找的文件才具有处置情况。未触发云查找的文件性质为 `N/A。Unavailable` 性质表示Firepower 管理中心无法执行恶意软件云查找。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有恶意软件许可证才能使此图形显示面向 Firepower 的 AMP 数据。

此图形主要从“文件事件”表提取数据。

“发送文件的主要主机”图形

“发送文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件发送主机IP地址的文件数量计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示发送恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**Malware**。点击**Files**以返回默认文件视图。请注意，离开Context Explorer也会此图形返回默认文件视图。

请注意，您必须具有恶意软件许可证才能使此图形显示面向 Firepower 的 AMP 数据。

此图形主要从“文件事件”表提取数据。

“接收文件的主要主机”图形

“接收文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件接收主机IP地址的文件数量计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Malware**。点击 **Files** 以返回默认文件视图。请注意，离开 Context Explorer 也会此图形返回默认文件视图。

请注意，您必须具有恶意软件许可证才能使此图形显示面向 Firepower 的 AMP 数据。

此图形主要从“文件事件”表提取数据。

“主要恶意软件检测”图形

“主要恶意软件检测”图形以条形图形式显示在您的组织中检测到的主要恶意软件威胁的计数，无论是由面向 Firepower 的 AMP 还是由面向终端的 AMP 进行检测。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有恶意软件许可证才能使此图形显示面向 Firepower 的 AMP 数据。

此图形主要从“文件事件”和“恶意软件事件”表提取数据。

地理位置信息部分

Context Explorer 的 Geolocation Information 部分包含三个交互环状图形，它们显示与受监控网络上主机交换数据的国家/地区的全局视图：发起方或响应方国家/地区的独特连接、按源或目标国家/地区划分的入侵事件以及按发送或接收国家/地区划分的文件事件。

“按发起方/响应方国家/地区划分的连接”图形

“按发起方/响应方国家/地区划分的连接”图形以环状图形式显示作为发起方（默认值）或响应方的网络连接涉及国家/地区的比例视图。内环将这些国家/地区按大陆分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为连接响应方的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击 **Responder**。点击 **Initiator** 返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认 Initiator 视图。

此图形主要从“连接摘要数据”表提取数据。

“按源/目标国家/地区划分的入侵事件”图形

“按源/目标地国家/地区划分的入侵事件”图形以环状图形式显示作为事件（默认值）或目标来源的网络上入侵事件涉及的国家/地区的比例视图。内环将这些国家/地区按大陆分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为入侵事件目标的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击 **Destination**。点击 **Source** 以返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认 Source 视图。

此图形主要从“入侵事件”表提取数据。

“按发送/接收国家/地区划分的文件事件”图形

“按发送/接收国家/地区划分的文件事件”图形以环状图形式显示网络上文件事件中检测到作为发送（默认值）或接收文件的国家/地区的比例视图。内环将这些国家/地区按大陆分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收文件的国家/地区，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击 **Receiver**。点击 **Sender** 返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认 Sender 视图。

此图形主要从“文件事件”表提取数据。

URL 信息部分

Context Explorer 的 URL Information 部分包含三个交互条形图形，它们显示与受监控网络上主机交换数据的 URL 的全局视图：与 URL 相关联、按单个 URL、 URL 类别和 URL 声誉排序的流量和独特连接。不能过滤 URL 信息。

注释 如果过滤入侵事件信息，整个 RL Information 部分将隐藏。

请注意，您必须具有 URL 过滤许可证才能使此图形包含 URL 类别和信誉数据。

“按 URL 划分的流量”图形

“按 URL 划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 15 个 URL 的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤许可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“连接事件”表提取数据。

“按 URL 类别划分的流量”图形

“按 URL 类别划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 URL 类别 （例如，`Search Engines` 和 `Streaming Media`）的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL 类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 类别划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤许可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

“按 URL 信誉划分的流量”图形

“按URL声誉划分的流量”图形以条形图形式显示受监控网络中请求最频繁的URL声誉组（例如，`Well known` 或`Benign sites with security risks`）的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL 声誉组，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 声誉划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤许可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

刷新情景管理器

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

Context Explorer 不会自动更新显示的信息。要更新数据，必须手动刷新资源管理器。

请注意，虽然重新加载Context Explorer（通过刷新资源管理器程序或离开，然后返回Context Explorer）可刷新所有显示的信息，但此操作不会保留对部分配置做出的任何更改（例如“入口/出口”图形和 Application Information 部分）且可能导致加载延迟。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 点击右上角的**重新加载 (Reload)**。
在刷新完成之前，**重新加载 (Reload)** 按钮呈灰色显示。

设置情景管理器时间范围

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

可配置 Context Explorer 的时间范围，以反映短至前一小时或长至上一年的时间段。请注意，如果更改时间范围，Context Explorer 无法自动更新反映所做的更改。要应用新的时间范围，必须手动刷新资源管理器。

即使离开 Context Explorer 或终止登录会话，对时间范围所做的更改也会持续。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 从**显示最后时间 (Show the last)** 下拉列表，选择时间范围。

步骤 3 或者，要从新时间范围查看数据，请点击 **Reload**。

提示 点击 **Apply Filters** 也可应用任何时间范围更新。

最小化和最大化情景管理器部分

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

可最小化和隐藏 Context Explorer 的一个或多个部分。如要仅重点关注某些部分，或如果想要更简单的视图，此操作很有用。不能最小化“流量和入侵事件计数时间”图形。

即使刷新页面或注销设备，情景管理器部分仍会保持处于配置的最小化或最大化状态。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 要最小化某个部分，请点击部分的标题栏中的最小化图标 ( )。

步骤 3 要最大化某个部分，请点击最小化部分的标题栏中的最大化图标 ( )。

向下展开情景管理器数据

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

如果想要超出 Context Explorer 允许的范围，更详细地检查图形和列表数据，可向下展开相关数据的表视图。（请注意，不能向下展开“随时间推移的流量和入侵事件”[Traffic and Intrusion Events over Time] 图形。）例如，向下展开“按源 IP 划分的流量”(Traffic by Source IP) 图形中的 IP 地址可显示“连接事件”(Connection Events) 表的“具有应用详细信息的连接”(Connections with Application Details) 视图，仅包括与所选源 IP 地址关联的数据。

视乎要检查的数据类型，上下文菜单中会显示其他选项。与特定 IP 地址相关联的数据点提供的选项可用于查看所选 IP 地址上的主机或域名信息。与特定应用相关联的数据点提供的选项可用于查看所选应用中的应用信息。与特定用户相关联的数据点提供的选项可用于查看用户的用户配置文件页。与入侵事件消息相关联的数据点提供的选项可用于查看规则文档，了解该事件的关联入侵规则，而与特定 IP 地址相关联的数据点提供的选项可用于将该地址列为黑名单和白名单。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 在除**随时间推移的流量和入侵事件 (Traffic and Intrusion Events over Time)** 以外的任何部分中，点击要调查的数据点。

步骤 3 视乎所选数据点，系统提供多个选项：

- 要在表视图中查看此数据的更多详细信息，请选择**深入分析 (Drill into Analysis)**。

- 如果选择了与特定IP地址相关联的数据点并要查看有关关联主机的详细信息，请选择**查看主机信息 (View Host Information)**。
- 如果选择了具有特定 IP 地址的数据点并要对该地址执行 whois 搜索，请选择 **Whois**。
- 如果选择了与特定应用相关联的数据点并要查看有关该应用的详细信息，请选择**查看应用信息 (View Application Information)**。
- 如果选择了与特定用户相关联的数据点并要查看有关该用户的详细信息，请选择**查看用户信息 (View User Information)**。
- 如果选择了与特定入侵事件消息相关联的数据点并要查看有关关联入侵规则的详细信息，请选择**查看规则文档 (View Rule Documentation)**。
- 如果选择了与特定 IP 地址相关联的数据点并要将该 IP 地址添加到安全情报全局黑名单或白名单，请选择相应的选项：**立即列入黑名单 (Blacklist Now)** 或**立即列入白名单 (Whitelist Now)**。

情景管理器中的过滤器

除了 Context Explorer 初始显示的基本、广泛数据外，可选择为网络中活动的更精细的上下文照片过滤该数据。过滤器包含除 URL 信息外的所有类型 Firepower 系统数据，支持排除和纳入，点击情景管理器图形数据点即可快速应用，并影响整个管理器。可以一次应用最多 20 个过滤器。

过滤器可以通过多种方式添加至 Context Explorer 数据：

- 从“添加过滤器”(Add Filter) 对话框添加
- 在管理器中选择一个数据点时，从情景菜单添加
- 从特定详细信息视图页面（“应用详细信息”[Application Detail]、“主机配置文件”[Host Profile]、“规则详细信息”[Rule Detail] 和“用户配置文件”[User Profile]）显示的文本链接添加。点击这些链接，根据详细信息视图页面的相关数据自动打开并过滤 Context Explorer。例如，点击一个用户详细信息页面上的 Context Explorer 以便用户 `jenkins` 限制资源管理器仅显示与该用户相关的数据。

某些过滤器类型与其他类型不兼容：例如，与入侵事件相关的过滤器（例如，**设备 [Device]** 和**内联结果 [Inline Result]**）无法与连接事件相关的过滤器（例如，**访问控制操作 (Access Control Action)**）同时应用，因为系统无法按入侵事件数据对连接事件数据进行排序。系统将自动阻止同时应用不兼容过滤器；只要存在不兼容性，当一个过滤器类型最近被激活时，不兼容的过滤器会被隐藏。

当多个过滤器活跃时，同一种数据类型的值被视为 OR 搜索条件：将出现至少与其中一个值相匹配的所有数据。不同数据类型的值被视为 AND 搜索条件：显示至少与每种过滤数据类型相匹配的数据。例如，为 `Application: 2channel`、`Application: Reddit` 和 `User: edickinson` 的过滤器集显示的数据必须与用户 `edickinson` **和**应用 `2channel` **或**应用 `Reddit` 相关联。

在多域部署中，当查看祖先域中的情景管理器时，可以通过多个后代域来过滤。在这种情况下，还添加 **IP 地址 (IP Address)** 过滤器时，要特别注意。系统会为每个枝叶域构建单独的网络映射。使用文字 IP 地址限制此配置可能会出现意外结果。

请注意，显示的数据取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。

注释 过滤器用作一种简单、灵活的工具，可在任何指定时间获取准确的 Firepower 数据情景。过滤器不用作永久性配置设置，在离开 Context Explorer 或结束会话时会消失。要保留过滤器设置供以后使用，可用已应用的首选过滤器创建 Context Explorer 的浏览器书签。由于已应用的过滤器已纳入 Context Explorer 页面 URL，加载该页面的书签也会加载相应的过滤器。

数据类型字段选项

下表列出可用作过滤器的数据类型，并带有每种类型的示例和简要定义。

表 *232*：过滤器数据类型

Type	示例值	Definition
Access Control Action	`Allow`, `Block`	访问控制策略为允许或阻止流量而采取的操作。
Application Category	`web browser`, `email`	应用的最基本功能的一般分类。
应用名称	`Facebook`, `HTTP`	应用的名称。
Application Risk	`Very High`, `Medium`	应用的预计安全风险
Application Tag	`encrypts communications`, `sends mail`	有关应用的其他信息；应用可以具有任意数量的标记，包括无任何标记。
应用类型	`Client`, `Web Application`	应用的类型：应用协议、客户端或 Web 应用。
业务相关性	`Very Low`, `High`	应用与业务活动的预计关联性（与娱乐相对）。
Continent	`North America`, `Asia`	与受监控网络上检测到的可路由IP地址相关联的大陆。
国家/地区	`Canada`, `Japan`	与受监控网络上检测到的可路由 IP 地址相关联的国家/地区。
设备	`device1.example.com`, `192.168.1.3`	受监控网络上的设备的名称或 IP 地址。
域	`Asia Division`、`Europe Division`	要绘制网络活动图表的设备的域。此数据类型只存在于多域部署中。

Type	示例值	Definition
Event Classification	`Potential Corporate Policy Violation`, `Attempted Denial of Service`	入侵事件的概要说明，由触发该事件的规则、解码器或预处理器的分类确定。
Event Message	`dns response`, `P2P`	事件生成的消息，由触发该事件的规则、解码器或预处理器确定。
File Disposition	`Malware`, `Clean`	Firepower 管理中心对其执行了恶意软件云查找的文件的处置情况。
文件名	`Packages.bz2`	网络流量中检测到的文件的名称。
File SHA256	任何 32 位字符串	Firepower 管理中心对其执行了恶意软件云查找的文件的 SHA-256 散列值。
文件类型	`GZ`, `SWF`, `MOV`	网络流量中检测到的文件类型。
File Type Category	`Archive`, `Multimedia`, `Executables`	网络流量中检测到的文件类型的一般类别。
IP 地址	`192.168.1.3`, `2001:0db8:85a3::0000/24`	IPv4 或 IPv6 地址、地址范围或地址块。 请注意，搜索 IP 地址时可返回事件，其中，该地址是事件的源或目标。
Impact Level	`Impact Level 1`, `Impact Level 2`	受监控网络上的事件的预计影响。
Inline Result	`dropped`, `would have dropped`	流量是已丢弃、应已丢弃还是未由系统处理
IOC Category	`High Impact Attack`, `Malware Detected`	已触发的危害表现 (IOC) 事件的类别。
IOC Event Type	`exploit-kit`, `malware-backdoor`	与特定危害表现 (IOC) 相关联的标识符，指代触发该标识符的事件。
Malware Threat Name	`W32.Trojan.a6b1`	恶意软件威胁的名称。
OS Name	`Windows`, `Linux`	操作系统的名称。
OS Version	`XP`, `2.6`	操作系统的特定版本。
优先级	`high`, `low`	事件的预计紧急程度。
Security Intelligence Category	`Malware`, `Spam`	危险流量的类别，由安全情报确定。
安全区域	`My Security Zone`, `Security Zone X`	接口集，流量通过其进行分析，并在内联部署中传递

Type	示例值	Definition
SSL	`yes, no`	SSL 或 TLS 加密流量。
User	`wsmith, mtwain`	登录到受监控网络上的主机的用户的身份。

从“添加过滤器”(Add Filter) 窗口新建过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

使用此程序，通过“添加过滤器”(Add Filter) 窗口从头开始创建过滤器。（也可以使用情景菜单创建快速过滤器。）

点击情景管理器左上方的**过滤器 (Filters)** 下的加号图标 ( ) 即可访问的“添加过滤器”(Add Filter) 窗口，该窗口仅包含两个字段：

- **数据类型 (Data Type)** 下拉列表包含许多可用于限制情景管理器的不同类型的 Firepower 系统数据。选择一个数据类型后，在 **Filter** 字段为该类型输入一个特定的值（例如，为类型 **Continent** 输入一个值 `Asia`）。为了便于操作，Filter 字段将所选数据类型提供多个灰显示例值。（在该字段中输入数据时，这些示例值将被擦除。）
- 在**过滤器 (Filter)** 字段中，可以输入特殊搜索参数，例如，`*` 和 `!`，本质上与事件搜索中一致。可以通过为过滤器参数加上 `!` 符号作为前缀来创建排斥过滤器。

注释 添加的过滤器不会自动应用；必须点击**应用过滤器 (Apply Filters)** 才能查看情景管理器中的过滤内容。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 在左上角的**过滤器 (Filters)** 项下，点击加号图标 (+)。

步骤 3 从**数据类型 (Data Type)** 下拉列表中，选择要过滤的数据类型。

步骤 4 在**过滤器 (Filter)** 字段中，输入要过滤的数据类型值。

步骤 5 点击 **OK**。

步骤 6 或者，请重复以上步骤添加更多的过滤器，直至添加完所需的过滤器集。

步骤 7 点击 **Apply Filters**。

从情景菜单创建快速过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

浏览 Context Explorer 图形和列表数据时，可点击数据点，然后使用上下文菜单根据该数据快速创建一个过滤器（包容性或排除性）。如用上下文菜单过滤“应用”、“用户”或“入侵事件消息”数据类型的信息，或任何单个主机，则过滤器构件包括一个构件信息图标，该图标链接至该数据类型（例如应用数据的“应用详细信息”）的相关详细信息页面。请注意，不能过滤 URL 数据。

上下文菜单还可用于更详细地调查特定图形或列表数据。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 在资源管理器的任何部分（“随时间推移的流量和入侵事件”部分或包含URL数据的部分除外），点击要过滤的数据点。

步骤 3 此时您有两种选择：

- 要为该数据添加一个过滤器，请点击 **Add Filter**。
- 要为该数据添加一个排除过滤器，请点击 **Add Exclude Filter**。应用的过滤器显示与排除值不关联的所有数据。排除过滤器的过滤器值之前显示一个感叹号 (!)。

查看过滤器数据

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 在任何符合条件的过滤器构件上，点击信息图标 ( )。

删除过滤器

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**分析 (Analysis)** > **情景管理器 (Context Explorer)**。

步骤 2 在左上方的**过滤器 (Filters)** 下，点击任何过滤器构件上的清除图标 ( )。

提示 如果要一次性删除所有过滤器，可点击 **Clear** 按钮。

第 77 章

使用网络映射

以下主题介绍如何使用网络映射：

网络映射

Firepower 系统监控通过网络传输的流量，解码流量数据，然后将该数据与既有的操作系统和指纹进行比较。系统之后会使用该数据构建网络的详细表示，称为网络映射。在多域部署中，系统为每个枝叶域都创建单个网络映射。

系统从标识用于在网络发现策略中监控的受管设备收集数据。受管设备直接从受监控流量和间接从已处理的 NetFlow 记录检测网络资产。如果多台设备检测到同一网络资产，则系统会将信息合并成资产的复合表示。

要通过被动检测扩充数据，请执行以下操作：

- 使用开源扫描工具 Nmap™ 主动扫描主机，并将扫描结果添加到网络映射。
- 使用主机输入功能从第三方应用手动添加主机数据。

网络映射显示根据检测到的主机和网络设备显示网络拓扑。

网络映射可用于：

- 获取网络的快速整体视图。
- 选择不同的视图，以适应要执行的分析。网络映射的每个视图都有相同的格式：具有可扩展的类别和子类别的分层树。点击类别时，该类别展开显示其下方的子类别。
- 通过自定义拓扑功能组织并识别子网。例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能将熟悉的标签分配到这些子网。
- 通过深入了解任何受监控主机的主机配置文件查看详细信息。
- 如果对于调查资产不再感兴趣，请将其删除。

注释 如果系统检测到与已从网络映射中删除的主机关联的活动，则其会将该主机重新添加到网络映射。同样，如果系统检测到应用发生更改（例如，如果 Apache Web 服务器升级到新版本），则会将已删除的应用重新添加到网络映射。如果系统检测到使主机易受攻击的更改，则表明在特定主机上重新激活了漏洞。

提示 如果要从网络映射永久排除主机或子网，请修改网络发现策略。如果您发现负载均衡器和 NAT 设备生成额外或不相关的事件，则可能希望从监控中将其排除。

主机网络映射

“主机”(Hosts) 选项卡上的网络映射将显示主机计数以及主机 IP 地址和 MAC 地址的列表。每个地址或部分地址都是一条指向下一级的链接。此网络映射视图提供系统检测到的所有唯一主机的计数，无论主机有一个 IP 地址还是多个 IP 地址。

使用主机网络映射查看网络上按分层树中子网排列的主机，以及向下钻取到特定主机的主机配置文件。

系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

通过为网络创建自定义拓扑，可向主机网络映射中显示的子网分配有意义的标签，例如，部门名称。也可根据在自定义拓扑中指定的公司查看主机网络映射。

可从主机网络映射中删除整个网络、子网或个别主机。例如，如果知道主机不再连接到网络，则可将其删除以简化分析。如果系统此后检测到与已删除主机关联的活动，则会将该主机重新添加至网络映射。如果要从网络映射永久排除主机或子网，请修改网络发现策略。

注意 请勿从网络映射删除网络设备。系统会使用它们来确定网络拓扑。

网络设备网络映射

“网络设备”(Network Devices) 选项卡上的网络映射显示将一个网段连接到另一个网段的网络设备（网桥、路由器、NAT 设备和负载平衡器）。该映射包含两个部分，分别列出按IP地址识别的设备和按 MAC 地址识别的设备。

该映射还提供系统检测到的所有唯一网络设备的计数，无论设备具有一个IP地址还是多个IP地址。

如果为网络创建自定义拓扑，则网络设备网络映射中会显示分配给子网的标签。

系统可用下列方法区分网络设备：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型（仅限思科设备）
- 检测生成树协议 (STP)，可识别作为交换机或网桥的设备
- 检测使用同一 MAC 地址的多台主机，可用于识别 MAC 地址为属于路由器

- 检测客户端 TTL 值变化，或检测比典型启动时间变化更频繁的 TTL 值，可识别 NAT 设备和负载均衡器

如果网络设备使用 CDP 进行通信，则其可能有一个或多个 IP 地址。如果它使用 STP 进行通信，则它可能仅有 MAC 地址。

由于系统使用其位置来确定网络拓扑，因此不能从网络映射中删除网络设备。

网络设备的主机配置文件具有“系统”(System) 部分而不是“操作系统”(Operating Systems) 部分，其中包括反映网络设备后检测到的任何移动设备的硬件平台的“硬件”(Hardware) 列。如果 Systems 下列出硬件平台值，该系统是网络设备后检测出的一个或多个移动设备。请注意，移动设备可能有，也可能没有硬件平台信息，但不会检测到非移动设备系统的硬件平台信息。

移动设备网络映射

“移动设备”(Mobile Devices) 选项卡上的网络映射显示连接到网络的移动设备。此网络映射视还提供系统检测到的所有唯一移动设备的计数，无论设备有一个 IP 地址还是多个 IP 地址。

每个地址或部分地址都是一条指向下一级的链接。您也可以删除子网或 IP 地址；如果系统重新发现设备，则会将该设备重新添加到网络映射。

您还可以向下展开以查看移动设备的主机配置文件。

要识别移动设备，系统应执行以下操作：

- 分析来自移动设备的移动浏览器的 HTTP 流量中的用户代理字符串
- 监控特定移动应用的 HTTP 流量

如为网络创建自定义拓扑，则移动设备网络映射中会显示分配给子网的标签。

危害表现网络映射

“危害表现”(Indications of Compromise) 选项卡上的网络映射显示网络上按 IOC 类别组织的受损主机。受影响主机列在每个类别下方。每个地址或部分地址都是一条指向下一级的链接。

系统使用来自多个源的数据确定主机的受损状态，包括入侵事件、安全情报和思科高级恶意软件防护 (AMP)。

从危害表现网络映射中，可查看通过特定方式确定为已受损的每个主机的主机配置文件。也可删除（标记为已解析）任何 IOC 类别或任何特定主机，这会从相关主机中移除 IOC 标记。例如，如已确定问题得到解决且不可能复发，即可从网络映射中删除 IOC 类别。

标记从网络映射解析的主机或 IOC 类别不会将其从网络中移除。如果系统最近检测到触发该 IOC 的信息，则网络映射中会重新显示已解析的主机或 IOC 类别。

应用协议网络映射

“应用协议”(Application Protocols) 选项卡上的网络映射显示您的网络上运行的应用，按应用名称、供应商、版本并最终按运行每个应用的主机在分层树中排列。

系统检测到的应用可能随系统软件和VDB更新而变化，并且在导入任何附加探测器的情况下也会变化。每个系统或VDB更新的版本说明或咨询文本均包含有关任何新的和已更新的探测器的信息。有关探测器的全面最新列表，请参阅思科支持网站 (http://www.cisco.com/cisco/web/support/index.html)。

在此网络映射中，您可查看运行特定应用的每台主机的主机配置文件。

还可以删除任何应用类别、在所有主机上运行的任何应用或在特定主机上运行的任何应用。例如，如果知道应用在主机上已禁用并要确保系统不使用它进行影响级别限定，即可从网络映射中删除该应用。

从网络映射中删除应用不会将其从网络中移除。如果系统检测到应用发生变化（例如，如果Apache网络服务器升级到新版本），或者如果重新启动系统的发现功能，则网络映射中会重新显示已删除的应用。

视乎删除的内容，行为有所不同：

- 应用类别 - 删除应用类别会将其从网络映射中移除。驻留在该类别下的所有应用都会从包含应用的任何主机配置文件中移除。

  例如，如果删除**http**，则会从所有主机配置文件中移除标识为**http**的所有应用，并且网络映射的应用视图中不再显示**http**。

- 特定应用、供应商或版本 - 删除特定应用、供应商或版本会从网络映射中以及从包含该网络映射的任何主机配置文件中移除受影响的应用。

  例如，如果展开**http**类别并删除**Apache**，则会从包含列为Apache的所有应用（具有Apache下列出的任何版本）的任何主机配置文件中移除这些应用。同样，如果删除特定版本（例如**1.3.17**）而不是删除**Apache**，则仅会将所选版本从受影响主机配置文件中删除。

- 特定IP地址 - 删除IP地址会将其从应用列表中移除，并从所选IP地址的主机配置文件中移除应用本身。

  例如，如果展开**http**、**Apache**、**1.3.17 (Win32)**，然后删除**172.16.1.50:80/tcp**，则会从IP地址172.16.1.50的主机配置文件中删除Apache 1.3.17 (Win32)应用。

漏洞网络映射

“漏洞”(Vulnerabilities)选项卡上的网络映射显示系统在网络上检测到的漏洞，按旧版漏洞ID (SVID)、Bugtraq ID、CVE ID或Snort ID排列。默认情况下，漏洞按SVID显示。漏洞按标识号排列，并且每个漏洞下会列出受影响主机。

从此网络映射中，可查看特定漏洞的详细信息；还可查看受特定漏洞影响的任何主机的主机配置文件。此信息有助于评估该漏洞对特定受影响主机造成的威胁。

如果确定特定漏洞不适用于网络上的主机（例如，已应用补丁），则可停用漏洞。已停用的漏洞仍显示在网络映射中，但是其先前受影响主机的IP地址以灰色斜体显示。那些主机的主机配置文件将已停用的漏洞显示为无效，不过可以手动将其标记为对于个别主机有效。

如果主机上的应用或操作系统存在身份冲突，则系统会列出两种潜在身份的漏洞。解决身份冲突后，漏洞保持与当前身份关联。

默认情况下，仅当数据包包含应用的供应商和版本时，网络映射才会显示检测到的应用的漏洞。但是，可将系统配置为列出缺少供应商和版本数据的应用的漏洞，只需在Firepower管理中心配置中为应用启用漏洞映射设置。

漏洞 ID（或漏洞 ID 的范围）旁边的数字表示两个计数：

受影响的主机

第一个数字是受漏洞影响的非唯一主机的计数。如果主机受多个漏洞影响，则会多次对其进行计数。因此，计数可能高于网络上的主机数。停用漏洞会按可能受该漏洞影响的主机数减小此计数。如果尚未面向漏洞或漏洞范围停用任何潜在受影响主机的任何漏洞，则不显示此计数。

可能受影响的主机

第二个数字是系统已确定为潜在受漏洞影响的非唯一主机的总数的计数。

停用漏洞致使其仅对指定的主机处于非活动状态。可停用已判定为易受攻击的所有主机或指定的个别易受攻击主机的漏洞。漏洞停用之后，适用的主机IP地址以灰色斜体显示在网络映射中。此外，这些主机的主机配置文件将已停用的漏洞显示为无效。

如果系统随后在主机上检测到未尚未停用的漏洞（例如，在网络映射中的新主机上），则系统会激活该主机的漏洞。必须明确停用最近发现的漏洞。此外，如果系统检测到主机的操作系统或应用变化，则可能重新激活关联的已停用漏洞。

主机属性网络映射

“主机属性”(Host Attributes) 选项卡上的网络映射显示按用户定义的主机属性或合规白名单主机属性组织的主机。您不能使用此显示中的预定义主机属性组织主机。

选择要用于组织主机的主机属性时，Firepower管理中心列出该属性在网络映射中的可能值并根据其分配值将主机分组。例如，如果选择按白名单主机属性组织主机，则系统会在类别“合规”(Compliant)、“不合规”(Non-Compliant) 和“未评估”(Not Evaluated) 中显示这些主机。

还可查看为其分配了特定主机属性值的任何主机的主机配置文件。

查看网络映射

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/任何安全分析师

过程

步骤 1 选择**分析 (Analysis)** > **主机 (Hosts)** > **网络映射 (Network Map)**。

步骤 2 点击要查看的网络映射的选项卡。

步骤 3 根据情况继续操作：

- 选择域 - 在多域部署中，从**域 (Domain)** 下拉列表中选择枝叶域。
- 过滤主机 - 如果要按 IP 或 MAC 地址过滤，请在搜索字段中输入地址。要清除搜索，请点击清除图标 ( )。
- 向下展开 - 如果要调查类别或主机配置文件，请向下展开映射中的类别或子网。如果已定义自定义拓扑，请点击**主机 (Host)** 选项卡中的（**拓扑**）**([topology])** 以查看该拓扑，然后在要切换回默认视图时点击（**主机**）**([hosts])**。
- 删除 - 点击相应元素旁边的删除图标 ( )，以执行下列操作：

  从**主机 (Hosts)**、**网络设备 (Network Devices)**、**移动设备 (Mobile Devices)** 或**应用协议 (Application Protocols)** 选项卡上的映射中删除元素。

  标记**危害表现 (Indications of Compromise)** 选项卡上解析的 IOC 类别、受损主机或受损主机组。

  停用**漏洞 (Vulnerabilities)** 选项卡上所有主机或单个主机的漏洞。

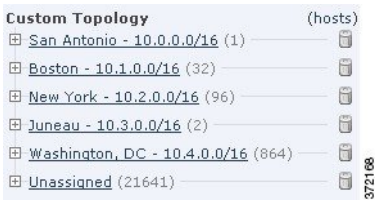
- 指定漏洞类 - 在**漏洞 (Vulnerabilities)** 选项卡上，从**类型 (Type)** 下拉列表中选择要查看的漏洞的类。
- 指定组织属性 - 在**主机属性 (Host Attributes)** 选项卡上，从**属性 (Attribute)** 下拉列表中选择属性。

自定义网络拓扑

使用自定义拓扑功能帮助排列和识别主机及网络设备网络映射中的子网。

例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能标示这些子网。

也可根据在自定义拓扑中指定的公司查看主机网络映射。



您可以使用以下任何或所有策略指定自定义拓扑的网络：

- 您可以从网络发现策略导入网络，以添加您将系统配置为要监控的网络。
- 您可以手动向拓扑中添加网络。

“自定义拓扑”(Custom Topology) 页面列出自定义拓扑及其状态。如果策略名称旁边的灯泡图标亮起，表明拓扑处于活动状态并影响网络映射。如果该图标呈灰色显示，则表明拓扑处于不活动状态。

创建自定义拓扑

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击工具栏中的**自定义拓扑 (Custom Topology)**。

步骤 3 点击 **Create Topology**。

步骤 4 输入 **Name**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 向拓扑添加网络。可使用以下任何或所有策略：

- 从网络发现策略导入网络，如从网络发现策略导入网络，第 1419 页中所述。
- 手动添加网络，如手动向自定义拓扑添加网络，第 1420 页中所述。

步骤 7 点击**保存 (Save)**。

接下来的操作

- 激活拓扑，如激活和停用自定义拓扑，第 1421 页中所述。

从网络发现策略导入网络

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 访问要将网络导入到的自定义拓扑：

- 创建自定义拓扑；请参阅创建自定义拓扑，第 1419 页。

- 编辑现有自定义拓扑；请参阅编辑自定义拓扑，第 1421 页。

步骤 2 点击**导入策略网络 (Import Policy Networks)**。

步骤 3 点击**加载 (Load)**。系统显示网络发现策略的拓扑信息。

步骤 4 优化拓扑：

- 通过点击网络旁边的编辑图标 ( )，键入名称并点击**重命名 (Rename)** 来对拓扑中的网络进行重命名。
- 通过点击删除图标 ( )，然后点击**确定 (OK)** 以确认来从拓扑中删除网络。

步骤 5 点击**保存 (Save)**。

接下来的操作

- 激活拓扑，如激活和停用自定义拓扑，第 1421 页中所述。

手动向自定义拓扑添加网络

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

过程

步骤 1 访问您要添加网络的自定义拓扑：

- 创建自定义拓扑；请参阅创建自定义拓扑，第 1419 页。
- 编辑现有自定义拓扑；请参阅编辑自定义拓扑，第 1421 页。

步骤 2 点击 **Add Network**。

步骤 3 如果要将网络的自定义标签添加到主机和网络设备网络映射中，请键入**名称 (Name)**。

步骤 4 输入用于表示待添加网络的 **IP 地址 (IP Address)** 和**网络掩码 (Netmask)** (IPv4)。

步骤 5 点击 **Add**。

步骤 6 点击 **Save**。

接下来的操作

- 激活拓扑，如激活和停用自定义拓扑，第 1421 页中所述。

激活和停用自定义拓扑

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

注释 只有一个自定义拓扑可以随时处于活动状态。如已创建多个拓扑，则激活一个拓扑会自动停用当前活动的拓扑。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 选择**自定义拓扑 (Custom Topology)**。

步骤 3 点击拓扑旁边的滑块以激活或停用该拓扑。

编辑自定义拓扑

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅限枝叶	管理员/发现管理员

对活动拓扑进行的更改会立即生效。

过程

步骤 1 选择**策略 (Policies)** > **网络发现 (Network Discovery)**。
在多域部署中，如果您不在枝叶域中，则系统会提示您进行切换。

步骤 2 点击**自定义拓扑 (Custom Topology)**。

步骤 3 点击要编辑的拓扑旁边的编辑图标 ( )。

步骤 4 编辑拓扑，如创建自定义拓扑，第 1419 页中所述。

步骤 5 点击**保存 (Save)**。

第 78 章

突发事件

以下主题介绍如何配置事故处理：

事故处理基础知识

事故处理是指一个组织在怀疑存在违反组织安全策略的情况下做出的响应。Firepower 系统包含在您收集和处理与事故调查相关的信息时为您提供支持的功能。您可以使用这些功能收集可能与事故相关的入侵事件和数据包数据。您还可以将事故用作在 Firepower 系统外采取的用于缓解攻击造成的影响的任何活动的有关备注的存储库。例如，如果安全策略要求隔离来自您网络的受危害主机，您就可以注意到事故中这种情况。

Firepower 系统还支持事故生命周期，使您能够在对攻击做出响应的过程中修改事故状态。处理完事故时，您可以注意到根据所学到的经验已经对安全策略进行的任何修改。

事故的定义

通常，事故指您怀疑可能涉及违反安全政策的一个或多个入侵事件。在 Firepower 系统中，该术语也描述可用于跟踪您对事故的响应的功能。

对网络资产可用性、机密性和完整性而言，某些入侵事件比其他入侵事件更加重要。例如，端口扫描检测功能可让您了解网络上的端口扫描活动。但是，您的安全策略可能未明确禁止端口扫描或将其视为高优先级威胁，因此，您可能不会采取任何直接行动，而只想保留全部端口扫描的日志以供日后调查研究之用。

另一方面，如果系统生成表明您网络中的主机已受到危害并且正在参与分布式拒绝服务(DDoS)攻击的事件，那么这个活动就可能明显违反安全策略，您应在Firepower系统中创建事故来帮助跟踪对这些事件的调查。

常见事故处理流程

准备

您可以通过两种方式为事故做准备：

- 落实明确和全面的安全策略以及强化这些策略的硬件和软件资源
- 制定一个清晰明确的事故响应计划，并配备一个可以实施此计划的训练有素的团队

事故处理的关键部分在于了解网络的哪些部分面临最大的风险。在这些网段部署 Firepower 系统组件，可以提高对于事故发生时间和状况的了解。此外，花时间仔细调整每个受管设备的入侵策略，可以确保生成的事件具有最高的质量。

检测和通知

您必须能检测到事故，才能响应事故。事故处理流程应注意您可以检测到的安全相关事件的类型以及您可用于检测这些类型事件的软件和硬件机制。您还应该注意会在何处检测到违反安全策略的活动。如果网络包括没有被主动或被动监控的网段，则需要特别注意。

您在网络中部署的受管设备负责分析安装了这些设备的网段的流量、检测入侵以及生成描述入侵的事件。记住：您在每个受管设备上部署的访问控制策略可控制这些设备可以检测哪些类型的活动以及如何确定其优先级。您还可以设置特定类型入侵事件的通知选项，从而让事故团队无需筛查数百个事件。您可以指定在检测到特定高优先级、高敏感性事件时自动获得通知。

调查和资格审批

您的事故处理流程应指定检测到安全事故之后如何执行调查。某些组织中，初级团队成员负责将所有事故分类并处理严重性或优先级较低的事故，而更高级的团队成员处理严重性和优先级较高的事故。您应该认真确定升级流程，让每个团队成员都了解提高事故重要性的标准。

升级流程的一部分在于了解检测到的事件会如何影响网络资产的安全性。例如，运行 Microsoft SQL Server 的主机的攻击对于使用不同数据库服务器的组织来说优先级并不高。同样，如果网络中使用的是 SQL Server，但是您确信所有服务器都已打补丁并且不容易受到攻击，那么这种攻击对您来说重要性也会降低。但是，如果有人最近安装了一个易受攻击的版本的软件（可能是为了进行测试），您所遇到的问题可能会比粗略调查反映的问题更严重。

Firepower系统特别适合支持调查和资格审批流程。您可以创建自己的事件分类，然后以最充分描述网络漏洞的方式应用这些分类。网络上的流量触发事件时，系统将自动划分事件的优先级和类别，并向您提供表明哪些攻击是针对已知易受攻击的主机的具体指标。

Firepower 系统中的事故跟踪功能还包括状态标记，您可以修改此状态标记，指出哪些事故已经升级。

沟通

所有事故处理流程都应指定事故处理团队和内外受众之间进行事故沟通的方式。例如，您应该考虑哪些类型的事故需要管理人员干涉以及需要哪个级别的管理人员干涉。此外，流程应该规定如何及何时与外部组织沟通。请考虑以下方面：

- 某些事故是否需要通知执法机构？
- 如果您的主机正在参加针对远程站点的分布式拒绝服务 (DDoS)，您是否要通知它们？
- 您是否希望与计算机紧急事故响应小组协调中心 (CERT/CC) 或事故响应与安全组织论坛 (FIRST) 共享信息？

Firepower 系统具备可用于收集诸如 HTML、PDF、CSV（逗号分隔值）等标准格式入侵数据的功能，让您能够轻松与他人共享入侵数据。

例如，CERT/CC 在其网站上收集有关安全事故的标准信息。CERT/CC 寻找可以从 Firepower 系统轻松提取的各类型的信息，例如：

- 有关受影响的机器的信息，包括：

  主机名和 IP 地址

  时区

  主机的用途或功能

- 有关攻击源的信息，包括：

  主机名和 IP 地址

  时区

  您是否与攻击者有任何接触

  处理事故的估算成本

- 事故的描述，包括：

  日期

  入侵方法

  涉及的入侵者工具

  软件版本和补丁级别

  任何入侵者工具输出

  被利用的漏洞的详细信息

  攻击源

  任何其他相关信息

您还可以使用事故的备注部分记录您何时以及与谁沟通了这些问题。

控制和恢复

您的事故处理流程应明确指出主机或其他网络组件受到危害时采取哪些措施。控制范围和恢复选项包括从向易受攻击的主机应用补丁到关闭目标并将其从网络移除。您还应该按照攻击的性质和严重性考虑保留证据的重要性，以备提出刑事指控。

您可以使用 Firepower 系统的事故功能记录您在事故的控制和恢复阶段采取的行动。

学习到的经验

每个安全事故，无论是否攻击成功，都是一个审核安全策略的机会。您是否需要更新防火墙规则？您是否需要采取更加结构化的补丁管理方法？未授权无线接入点是否构成新的安全问题？每个学到的经验都应反馈到安全策略中并帮助您更好地准备处理下一事故。

Firepower 系统中的事故类型

您可以为创建的每个事故指定一个事故类型。Firepower 系统中默认支持以下类型：

- 入侵
- 拒绝服务
- 未经授权的管理员访问权限
- 网站篡改
- 系统完整性危害
- 欺诈
- 失窃
- 损坏
- 未知

您还可以创建自己的事故类型。

创建自定义事故类型

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事故 (Incidents)**。

步骤 2 点击 **Create Incident**。

步骤 3 在 **Type** 区域，点击 **Types**。

默认事故类型列在页面底部。

步骤 4 在**事故类型名称 (Incident Type Name)** 字段中，输入新的事故类型名称。

步骤 5 点击 **Add**。

步骤 6 点击 **Done**。
下次创建或编辑事故时，您就可以使用新的事故类型。

创建事故

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，只能查看和修改在当前域中创建的事故。在祖先域中，可以从任何后代域将事件添加到事故。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事故 (Incidents)**。

步骤 2 点击 **Create Incident**。

步骤 3 从**类型 (Type)** 下拉菜单中，选择可最好地描述事故的选项。

步骤 4 在 **Time Spent** 字段中，按照 #d #h #m #s 格式输入您在此事故上花费的时间，其中 # 代表天数、小时数、分钟数或秒数。

步骤 5 在**摘要 (Summary)** 文本框中，输入事故的简要说明（最多 255 个字母数字字符、空格和符号）。

步骤 6 在**添加注释 (Add Comment)** 文本框中，输入事故的更完整说明（最多 8191 个字母数字字符、空格和符号）。

步骤 7 将事件添加到事故：

- 要添加事件选项，请选择剪贴板上的事件，然后点击**添加到事故 (Add to Incident)**。
- 要从剪贴板添加所有事件，请点击**全部添加到事故 (Add All to Incident)**。

注释 如果想要添加来自剪贴板上多个页面的各个事件，您必须单独添加来自一个页面的事件，再添加来自其他页面的事件。

步骤 8 点击**保存 (Save)**。

编辑事故

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，只能查看和修改在当前域中创建的事故。在祖先域中，可以从任何后代域将事件添加到事故。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事故 (Incidents)**。

步骤 2 点击要编辑的事故旁的编辑图标 ( )。

步骤 3 您可以编辑事故的以下任何方面：

- 更改状态
- 更改类型
- 从剪贴板添加事件
- 删除事件

步骤 4 在 **Time Spent** 字段中，输入在事故上额外花费的时间量。

步骤 5 在 **Add Comment** 文本框中，指出您对事故的更改（至多 8191 个字母数字字符、空格和符号）。

步骤 6 或者，您可以给事故添加或删除事件：

- 要从剪贴板添加事件，请选择剪贴板上的事件，然后点击**添加到事故 (Add to Incident)**。
- 要添加剪贴板上的全部事件，请点击 **Add All to Incident**。
- 要删除事故的特定事件，请选择事件并点击**删除 (Delete)**。
- 要删除事故的所有事件，请点击 **Delete All**。
- 要更新事故而不添加或删除事件，请点击 **Save**。

生成事故报告

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以使用Firepower系统生成事故报告。这些报告可包含事故摘要、事故状态和注释以及您添加到事故上的事件的信息。您还可以指定是否要在报告中包括事件摘要信息。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事故 (Incidents)**。

步骤 2 点击您想要包含在报告中的事故旁的编辑图标 ()。

步骤 3 此时您有两种选择：

- 要将事故的所有事件都包括在报告中，请点击 **Generate Report All**。
- 要将事故的特定事件包含在报告中，请选中要包含的事件旁的复选框并点击**生成报告 (Generate Report)**。

步骤 4 输入报告名称。

步骤 5 在**事故报告部分 (Incident Report Sections)** 中，选中要包含在报告中的事故部分的复选框：**状态 (status)**、**摘要 (summary)** 和**注释 (comments)**。

步骤 6 如果要在报告中包含事件信息，请选择要使用的工作流程，然后在**报告部分 (Report Sections)** 中指定是否要包含事件摘要信息。

步骤 7 选中报告中要包含的工作流程页面旁边的复选框。

步骤 8 选中要用于报告的输出格式旁边的复选框：**PDF**、**HTML** 和 **CSV**。

注释 基于 CSV 的事故报告仅包括事件信息。它们不包括事故的状态、摘要或备注。

步骤 9 点击 **Generate Report** 并确认您要更新报告配置文件。

第 XX 部分

工作流程

第 79 章

工作流程

以下主题介绍如何使用工作流程：

概述：工作流程

工作流程是Firepower管理中心网络界面中可供分析师用于评估系统生成的事件的定制系列的数据页面。

Firepower 管理中心提供以下类型的工作流程：

预定义工作流程

随系统交付的预设工作流程。您无法编辑或删除预定义工作流程。但是，可以复制预定义工作流程，将其用作自定义工作流程的基础。

已保存的自定义工作流程

基于随 Firepower 管理中心交付的已保存自定义表的自定义工作流程。您可以编辑、删除和复制这些工作流程。

自定义工作流程

您为特定需求创建和自定义的工作流程，或者在您创建自定义表时系统自动生成的工作流程。您可以编辑、删除和复制这些工作流程。

工作流程中显示的数据通常取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。

预定义工作流程

以下部分介绍的预定义工作流程随系统一同交付。您无法编辑或删除预定义工作流程，但是您可以复制预定义工作流程，并将其用作自定义工作流程的基础。

预定义入侵事件工作流程

下表描述 Firepower 系统随附的预定义入侵事件工作流程。

表 *233*：预定义入侵事件工作流程

工作流程名称	说明
目标端口	由于目标端口通常绑定到应用，因此该工作流程可以帮助检测遭遇异常高的警报量的应用。Destination Port 列可以帮助识别不应存在于网络上的应用。
Event-Specific	此工作流程提供两个有用的功能。频繁发生的事件可能指示： • 误报 • 蠕虫 • 配置错误的网络 偶尔发生的事件很可能指示针对性攻击和特别关注事项。
Events by Priority and Classification	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。
Events to Destinations	此工作流程提供受攻击主机 IP 地址和攻击性质的高级视图；在适用情况下，还可查看有关攻击中涉及的国家/地区的信息。
IP-Specific	此工作流程显示哪些主机 IP 地址生成最多警报。事件数最多的主机面向公众并接收蠕虫类型流量（指示适合进行调整的位置），或者需要进一步调查以确定警报原因。具有最低计数的主机也有必要进行调查，因为它们可能是针对性攻击的对象。低计数还可指示主机可能不属于该网络。
Impact and Priority	通过此工作流程，可以快速查找重大影响复发事件。报告的影响级别通过事件已发生的次数进行显示。使用此信息，可以识别复发最频繁的重大影响事件，此类事件可能指示攻击在网络上范围广泛。
Impact and Source	此工作流程可帮助识别进行中的攻击的源。报告的影响级别通过事件的关联源 IP 地址进行显示。例如，如果具有 1 级影响的事件重复来自同一源 IP 地址，则这些事件可能指示攻击者已识别易受攻击的系统并在针对这些系统。
Impact to Destination	可以使用此工作流程识别在易受攻击计算机上重复发生的事件，从而能够处理这些系统上的漏洞并停止进行中的任何攻击。

工作流程名称	说明
源端口	此工作流程指示哪些服务器生成最多警报。可以使用此信息标识需要调整的方面，以及决定需要注意的服务器。
Source and Destination	此工作流程识别共享高级警报的主机IP地址。列表顶部的对可能是误报，并可确定需要调整的方面。可以检查列表底部的对来查找针对性攻击、访问其不应访问的资源的用户或不属于该网络的主机。

预定义恶意软件工作流程

下表描述Firepower管理中心中包含的预定义恶意软件工作流程。所有预定义恶意软件工作流程都使用恶意软件事件表视图。

表 *234*：预定义恶意软件工作流程

工作流程名称	说明
恶意软件摘要	此工作流程提供在网络流量中或由面向终端的 AMP 连接器检测到的恶意软件列表，按个别威胁分组。
Malware Event Summary	此工作流程提供不同恶意软件事件类型和子类型的快速细分。
Hosts Receiving Malware	此工作流程提供已接收恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
Hosts Sending Malware	此工作流程提供已发送恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
Applications Introducing Malware	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义文件工作流程

下表描述Firepower管理中心中包含的预定义文件事件工作流程。所有预定义文件事件工作流程都使用文件事件表视图。

表 *235*：预定义文件工作流程

工作流程名称	说明
File Summary	此工作流程提供不同文件事件类别和类型以及任何关联恶意软件性质的快速细分。
Hosts Receiving Files	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。
Hosts Sending Files	此工作流程提供已发送文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义捕获文件工作流程

下表描述Firepower管理中心中包含的预定义捕获文件工作流程。所有预定义捕获文件工作流程都使用捕获文件表视图。

表 *236*：预定义捕获文件工作流程

工作流程名称	说明
捕获的文件摘要	此工作流程根据类型、类别和威胁评分提供捕获文件的细分。
Dynamic Analysis Status	此工作流程根据是否已提交捕获文件进行动态分析来提供此类文件的计数。

预定义连接数据工作流程

下表描述Firepower管理中心中包含的预定义连接数据工作流程。所有预定义连接数据工作流程都使用连接数据表视图。

表 *237*：预定义连接数据工作流程

工作流程名称	说明
连接事件	此工作流程提供基本连接和检测到的应用信息的摘要视图，然后可以使用该视图向下钻取到事件表视图。
Connections by Application	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃应用的图形。
Connections by Initiator	此工作流程包含从连接数来看监控网段上 10 个最活跃的发起了连接事务的主机 IP 地址的图形。
Connections by Port	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃端口的图形。
Connections by Responder	此工作流程包含从连接数来看监控网段上 10 个最活跃的主机 IP 为连接事务中的响应方的主机 IP 地址的图形。
Connections over Time	此工作流程包含某个时间跨度的监控网段上的连接总数的图形。
Traffic by Application	此工作流程包含从传输的数据量来看监控网段上 10 个最活跃应用的图形。
Traffic by Initiator	此工作流程包含从每个地址传输的总数据量来看监控网段上 10 个最活跃主机 IP 地址的图形。
Traffic by Port	此工作流程包含从传输的数据量来看监控网段上 10 个最活跃端口的图形。

工作流程名称	说明
Traffic by Responder	此工作流程包含从每个地址接收的总数据量来看监控网段上 10 个最活跃主机 IP 地址的图形。
Traffic over Time	此工作流程包含某个时间跨度的监控网段上传输的总数据量的图形。
Unique Initiators by Responder	此工作流程包含从已联系每个地址的唯一发起方数量来看监控网段上 10 个最活跃响应主机 IP 地址的图形。
Unique Responders by Initiator	此工作流程包含从已联系地址的唯一响应方数量来看监控网段上 10 个最活跃发起主机 IP 地址的图形。

预定义安全情报工作流程

下表描述 Firepower 管理中心 中包含的预定义安全情报工作流程。所有预定义安全情报工作流程都使用安全情报事件表视图。

表 *238*：预定义安全情报工作流程

工作流程名称	说明
Security Intelligence Events	此工作流程提供基本安全情报和检测到的应用信息的摘要视图，然后可以使用该视图向下钻取到事件表视图。
Security Intelligence Summary	此工作流程与 Security Intelligence Events 工作流程相同，但是以其中仅按类别和计数列出了安全情报事件的 Security Intelligence Summary 页面开头。
具有 DNS 详细信息的安全情报 (Security Intelligence with DNS Details)	此工作流程与“安全情报事件”(Security Intelligence Events) 工作流程相同，但是从其中仅按类别和 DNS 相关特性列出安全情报事件的“具有 DNS 详细信息的安全情报”(Security Intelligence with DNS Details) 页面开始。

预定义主机工作流程

下表描述可与主机数据配合使用的预定义工作流程。

表 *239*：预定义主机工作流程

工作流程名称	说明
主机数	此工作流程包含主机表视图，后跟主机视图。通过基于 Hosts 表的工作流程视图可轻松查看与主机关联的所有 IP 地址上的数据。

工作流程名称	说明
Operating System Summary	可以使用此工作流程分析网络上正在使用中的操作系统。

预定义危害表现工作流程

下表描述可与 IOC（危害表现）数据配合使用的预定义工作流程。

表 *240*：预定义危害表现工作流程

工作流程名称	说明
危害表现	此工作流程以按计数和类别分组的 IOC 数据的摘要视图开头，提供按事件类型进一步细分摘要数据的详细视图。 通过**分析 (Analysis) > 主机 (Hosts)** 菜单访问此工作流程。
Indications of Compromise by Host	可以使用此工作流衡量网络上哪些主机最可能受损（基于 IOC 数据）。 通过**分析 (Analysis) > 主机 (Hosts)** 菜单访问此工作流程。

预定义应用工作流程

下表描述可与应用数据配合使用的预定义工作流程。

表 *241*：预定义应用工作流程

工作流程名称	说明
Application Business Relevance	可以使用此工作流程分析网络上正在运行的各估算业务相关性级别的应用，从而能够监控网络资源的相应使用。
Application Category	可以使用此工作流程分析网络上正在运行的各类别的应用（如邮件、搜索引擎或社交网络），从而能够监控网络资源的相应使用。
Application Risk	可以使用此工作流程分析网络上正在运行的各估算安全风险级别的应用，从而能够估算用户活动的潜在风险并采取相应措施。
Application Summary	可以使用此工作流程获取有关网络上的应用和关联主机的详细信息，从而能够仔细检查主机应用活动。
应用	可以使用此工作流程分析网络上正在运行的应用，从而能够大致了解网络的使用方式。

预定义应用详细信息工作流程

下表描述可与应用详情和客户端数据配合使用的预定义工作流程。

表 *242*：预定义应用详细信息工作流程

工作流程名称	说明
应用详情	可以使用此工作流程更详细地分析网络上的客户端应用。然后，工作流程提供客户端应用表视图，后跟主机视图。
客户端	此工作流程包含客户端应用表视图，后跟主机视图。

预定义服务器工作流程

下表描述可与服务器数据配合使用的预定义工作流程。

表 *243*：预定义服务器工作流程

工作流程名称	说明
Network Applications by Count	可以使用此工作流程分析网络上最频繁使用的应用。
Network Applications by Hit	可以使用此工作流程分析网络上最活跃的应用。
Server Details	可以使用此工作流程详细分析检测到的服务器应用协议的供应商和版本。
服务器	此工作流程包含应用表视图，后跟主机视图。

预定义主机属性工作流程

下表描述可与主机属性数据配合使用的预定义工作流程。

表 *244*：预定义主机属性工作流程

工作流程名称	说明
属性	可以使用此工作流程监控网络上主机的 IP 地址和主机状态。

预定义发现事件工作流程

下表介绍可用于查看发现和身份数据的预定义工作流程。

表 *245*：预定义发现事件工作流程

工作流程名称	说明
Discovery Events	此工作流程以表视图形式提供发现事件的详细列表，后跟主机视图。

预定义用户工作流程

下表介绍可用于查看用户发现和用户身份数据的预定义工作流程。

表 *246*：预定义用户工作流程

工作流程名称	说明
用户	此工作流程提供用户身份源收集的用户信息列表。

预定义漏洞工作流程

下表描述Firepower 管理中心中包含的预定义漏洞工作流程。

表 *247*：预定义漏洞工作流程

工作流程名称	说明
漏洞	可以使用此工作流程审查数据库中的漏洞，包括仅含应用于网络上检测到的主机的活动漏洞的表视图。此工作流程提供漏洞详细视图，其中包含满足限制的每个漏洞的详细描述。

预定义第三方漏洞工作流程

下表描述Firepower 管理中心中包含的预定义第三方漏洞工作流程。

表 *248*：预定义第三方漏洞工作流程

工作流程名称	说明
Vulnerabilities by IP Address	可以使用此工作流程快速了解监控网络上每个主机 IP 地址检测到的第三方漏洞数量。

工作流程名称	说明
Vulnerabilities by Source	可以使用此工作流程快速了解每个第三方漏洞源（如 QualysGuard 扫描程序）检测到的第三方漏洞数量。

预定义关联和白名单工作流程

各类型的相关性数据、白名单事件、白名单违例和修复状态事件具有对应的预定义工作流程。

表 *249*：预定义关联工作流程

工作流程名称	说明
相关事件	此工作流程包含关联事件表视图。
White List Events	此工作流程包含白名单事件表视图。
Host Violation Count	此工作流程提供列出了违反至少一个白名单的所有主机 IP 地址的一系列页面。
White List Violations	此工作流程包含列出了所有违例的白名单违例表视图，其中最新检测到的违例位于列表顶部。表中的每一行都包含一个检测到的违例。
状态	此工作流程包含修复状态表视图，其中包括违反的策略的名称以及应用的修复的名称和状态。

预定义系统工作流程

Firepower 系统随附一些其他工作流程，包括系统事件（例如审核事件和运行状况事件），以及列出了规则更新导入和活动扫描的结果的工作流程。

表 *250*：其他预定义工作流程

工作流程名称	说明
审核日志	此工作流程包含列出了审核事件的审核日志表视图。
Health Events	此工作流程显示运行状况监控策略所触发的事件。
Rule Update Import Log	此工作流程包含列出了有关成功和失败规则更新导入的信息的表视图。
Scan Results	此工作流程包含列出了已完成的各扫描的表视图。

自定义表工作流程

可以使用自定义表功能创建使用来自两种或多种类型的事件的数据的表。这有所帮助，因为可以例如创建将入侵事件数据与发现数据关联的表和工作流程，从而允许对影响关键系统的事件进行简单搜索。

创建自定义表时，系统会自动创建可用于查看与表关联的事件的工作流程。工作流程中的功能根据所使用的表类型而异。例如，基于入侵事件表的自定义表工作流程始终以数据包视图结尾。但是，基于发现事件的自定义表工作流程以主机视图结尾。

与基于预定义事件表的工作流程不同，基于自定义表的工作流程不具有指向其他类型的工作流程的链接。

使用工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

步骤 1 选择适当的菜单路径和选项，如工作流程选择，第 1444 页表中所述。

步骤 2 在当前工作流程中导航：

- 要查看已选事件数据类型中的所有可用列，请使用表视图页面；请参阅使用表视图页面，第 1450 页。
- 要查看已选事件数据类型中的一部分可用列，请使用向下钻取页面；请参阅使用向下钻取页面，第 1450 页。
- 要显示工作流程下一页中的相应行，请点击蓝色向下箭头图标 ()。
- 要在多页工作流程的页面之间移动，请使用每页底部的工具；请参阅工作流程页面遍历工具，第 1447 页。
- 要查看不同类型的事件的工作流程中应用的相同限制，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。

步骤 3 修改当前工作流程的显示：

- 选中页面上一行或多行的复选框以指示要影响的行，然后点击该页面底部的按钮之一（例如，**查看 [View]** 按钮），以对所有选中行执行该操作。

- 选中行顶部的复选框以选择该页面上的所有行，然后点击该页面底部的按钮之一（例如，**查看 [View]** 按钮），以对页面上的所有行执行该操作。
- 通过在要隐藏的列标题中点击关闭图标 ( ) 来限制显示的列。在显示的弹出窗口中，点击 **Apply**。

  提示 要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击 Disabled Columns 下的列名称。
- 通过所选字段的选定值限制数据视图。有关信息，请参阅事件视图限制，第 1464 页和复合事件视图限制，第 1465 页。
- 更改事件视图上的时间限制。位于页面右上角的日期范围为工作流程中要包含的事件设置时间范围；有关详细信息，请参阅事件时间限制，第 1458 页。

  注释 如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间窗口（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。
- 要按列对数据进行排序，请点击该列的名称。要反向排序，请再次点击该列的名称。方向图标指示数据按哪一列排序，以及排序是升序 ( ) 还是降序 ( )。
- 点击工作流程页面链接，以使用任何活动限制显示该页面。工作流程页面链接显示在预定义工作流程表视图和向下展开页面左上角，位于事件上方和工作流程名称下方。

步骤 4 查看当前工作流程中的其他数据：

- 要在新窗口中查看文件的轨迹映射，请点击文件名和 SHA-256 散列值列中的网络文件轨迹图标。该图标因文件状态而异；请参阅文件轨迹图标，第 1447 页。
- 要显示与 IP 地址相关的主机配置文件的弹出窗口，请点击任何 IP 地址列中的主机配置文件图标。该图标因文件状态而异；请参阅主机配置文件图标，第 1448 页。
- 要查看与文件相关的最高威胁评分的动态分析摘要报告，请点击任何威胁评分列中的威胁评分图标。该图标因文件的最高威胁评分而异；请参阅威胁评分图标，第 1449 页。
- 要查看用户配置文件信息，请点击任何用户身份列中的用户图标（ ，对于与危害表现关联的用户，图标为 ）。如果用户无法在数据库中（即，是面向终端的 AMP 连接器用户），则用户图标呈灰色显示。
- 要查看第三方漏洞的漏洞详细信息，请点击任何第三方漏洞 ID 列中的漏洞图标 ( )。
- 查看汇聚的数据点时，将指针悬停在标志图标上方可查看国家/地区名称。
- 查看个别数据点时，可以点击标志图标以进一步查看Geolocation，第 1451 页中所述的地理位置详细信息。

步骤 5 导航到不同的工作流程：

要使用不同的工作流程查看同一事件类型，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])**，然后选择要使用的工作流程。请注意，**不能**将不同的工作流程用于扫描结果。

按用户角色划分的工作流程访问

对工作流程的访问由用户角色确定。有关详细信息，请参阅下表。

用户角色	可访问的工作流程
管理员	可以访问任何工作流程，并且是仅有的可访问审核日志、扫描结果和规则更新导入日志的用户。
Maintenance User	可以访问运行状况事件。
“安全分析师”(Security Analyst) 和“安全分析师 [只读]”(Security Analyst [Read Only])	可以访问入侵、恶意软件、文件、连接、发现、漏洞、相关性和运行状况工作流程。

工作流程选择

Firepower 系统提供下表中所列数据类型的预定义工作流程。

表 *251*：使用工作流程的功能

特性	菜单路径	选项
入侵事件	Analysis > Intrusions	活动 Reviewed Events 剪贴板 突发事件
恶意事件	Analysis > Files	Malware Events
文件事件	Analysis > Files	File Events
Captured files	Analysis > Files	捕获的文件
连接事件	Analysis > Connections	活动
安全情报事件	Analysis > Connections	Security Intelligence Events

特性	菜单路径	选项
主机事件	Analysis > Hosts	Network Map 主机数 危害表现 应用 应用详情 服务器 Host Attributes Discovery Events
用户事件	Analysis > Users	用户活动 用户
漏洞事件	Analysis > Vulnerabilities	漏洞 Third-Party Vulnerabilities
关联事件	Analysis > Correlation	相关事件 White List Events White List Violations 状态
审核事件	System > Monitoring	审计
运行状况事件	运行状况 (Health) > 事件 (Events)	n/a
规则更新导入日志	System > Updates	n/a
扫描结果	Policies > Actions > Scanners	n/a

查看上表中描述的任何种类的数据时，事件显示在该数据的默认工作流程的第一页上。您可通过配置事件视图设置来指定不同的默认工作流程。请注意，工作流程访问取决于用户角色。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

工作流程页面

虽然各类型的工作流程中的数据不同，但是所有工作流程都共享公共的功能集。工作流程可以包含若干类型的页面。可以在工作流程页面上执行的操作取决于页面类型。

通过工作流程中的向下钻取页面和表视图页面，您可以快速缩小数据视图的范围，从而能够专注于对分析至关重要的事件。表视图页面和向下钻取页面都支持许多可用于限制要查看的事件集或浏览

工作流程的功能。当查看工作流程中的向下钻取页面或表视图中的数据时，可以基于任何可用列对数据进行升序或降序排序。如果数据库包含的事件数超过单个工作流程页面上可显示的事件数，则可点击页面底部的链接以显示更多事件。点击其中一个链接时，时间段自动暂停，以便不会重复显示相同事件；当您准备就绪时，可以取消暂停时间段。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

表视图

表视图对应于工作流程所基于的数据库中的每个字段包含一列（如果默认情况下启用了该页面）。

例如，发现事件的表视图包含 Time、Event、IP Address、User、MAC Address、MAC Vendor、Port、Description 和 Device 列。

相反，服务器的表视图包含 Last Used、IP Address、Port、Protocol、Application Protocol、Vendor、Version、Web Application、Application Risk、Business Relevance、Hits、Source Type、Device 和 Current User 列。

请注意，禁用表视图中的列时，如果禁用该列会创建两个或多个相同的行，则Firepower系统将向事件视图中添加“计数”(Count)列。点击表视图页面中的某个值时，即受该值限制。创建自定义工作流程时，通过点击 **Add Table View** 向其中添加表视图。

向下钻取页面

通常，向下钻取页面是在移至表视图页面之前用于将调查范围缩小到若干事件的中间页面。向下钻取页面包含数据库中可用的列的子集。

例如，发现事件的向下钻取页面可能仅包含 IP Address、MAC Address 和 Time 列。另一方面，入侵事件的向下钻取页面可能包含 Priority、Impact Flag、Inline Result 和 Message 列。

通过向下钻取页面，可以缩小所查看的事件范围并在工作流程中前进。例如，如果点击向下钻取页面中的某个值，即受该值限制并会移至工作流程中的下一页，从而更密切关注与所选值匹配的事件。点击向下钻取页面中的值并不会禁用该值所在的列，即使前进到的页面是表视图也如此。请注意，预定义工作流程的向下钻取页面始终具有 Count 列。创建自定义工作流程时，通过点击 **Add Page** 向其中添加向下钻取页面。

图

基于连接数据的工作流程可以包含图页面，也称为连接图。

例如，连接图可能会显示列出了随时间推移系统检测到的连接数的曲线图。通常，连接图是类似于向下钻取页面的中间页面，用于缩小调查范围。

最终页面

工作流程的最终页面取决于工作流程所基于的事件的类型。

- 主机视图是基于应用、应用详细信息、发现事件、主机、危害表现 (IOC)、服务器、白名单违规事件、主机属性或第三方漏洞的工作流程的最终页面。通过从此页面查看主机配置文件，可以轻松查看与具有多个地址的主机关联的所有 IP 地址上的数据。
- 用户详细信息视图是基于用户和用户活动的工作流程的最终页面。

- 漏洞详细视图是基于思科漏洞的工作流程的最终页面。
- 数据包视图是基于入侵事件的工作流程的最终页面。

基于其他类型的事件（例如，审核日志事件和恶意软件事件）的工作流程没有最终页面。

在工作流程的最终页面上，可以展开详细信息部分以查看有关该工作流程期间所关注的集合中各对象的特定信息。尽管网络界面没有在工作流程的最终页面上列出限制，但是先前设置的限制会保留并应用到数据集。

工作流程页面导航工具

工作流程页面提供视觉提示，以方便在各页面之间导航并选择要在事件分析过程中显示的信息。

工作流程页面遍历工具

如果工作流程包含多个页面的数据，则每个页面的底部会显示工作流程中的页数，以及下表中所列的可用于在页面间导航的工具：

表 *252*：工作流程页面遍历工具

页面遍历工具	操作
页码 （要查看其他页面，请输入希望查看的页码，然后按 Enter 键。）	查看其他页面
>	查看下一页
<	查看上一页
>|	跳至最后一页
|<	跳至第一页

文件轨迹图标

当工作流程页面提供机会在新窗口中查看文件的轨迹映射时，将会显示网络轨迹图标。此图标根据文件状态而异。

表 *253*：文件轨迹图标

文件轨迹图标	文件状态
	清洁

文件轨迹图标	文件状态
	恶意软件
	自定义检测
	未知
	不可用

主机配置文件图标

当工作流程页面为您提供机会在弹出式窗口中查看与某个 IP 地址关联的主机配置文件时，将会显示主机配置文件图标。如果主机配置文件图标呈灰色显示，则无法查看主机配置文件，因为该主机不能位于网络映射中（例如，`0.0.0.0`）。根据主机的状态，此图标看起来会有所不同。

表 *254*：主机配置文件图标

主机配置文件图标	主机状态
	主机未被标记为可能受到危害。
	通过已触发的危害表现 (IOC) 规则，主机被标记为可能受到危害。
	列入黑名单（仅当根据安全情报数据执行流量过滤时才会显示。）
	列入黑名单，设置为监控（仅当根据安全情报数据执行流量过滤时才会显示。）

威胁评分图标

在工作流程页面为您提供机会查看与文件的最高威胁评分关联的动态分析摘要报告时，会显示威胁评分图标。该图标因文件的最高威胁评分而异。

表 *255*：威胁评分图标

威胁评分图标	威胁评分级别
	低
	中等
	高
	极高

工作流程工具栏

工作流程中的每个页面包含用于提供对相关功能的快速访问的工具栏。下表描述工具栏上的每个链接

表 *256*：工作流程工具栏链接

特性	说明
Bookmark This Page	将当前页面加入书签，以便稍后可以返回到该页面。加入书签可捕获所查看的页面上已生效的限制，以便稍后能够返回到同一数据（假设数据仍然存在）。
Report Designer	以当前受限工作流程作为选择标准打开报告设计器。
控制面板	打开与当前工作流程相关的控制面板。例如，Connection Events 工作流程链接到 Connection Summary 控制面板。
View Bookmarks	显示可从中进行选择的已保存书签列表。
搜索	显示可在其中对工作流程中的数据执行高级搜索的 Search 页面。也可以点击向下箭头图标以选择并使用已保存的搜索。

使用向下钻取页面

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如表 251：使用工作流程的功能中所述。

步骤 2 在任何工作流程中，您有以下选择：

- 要向下展开到限制某个特定值的下一个工作流程页面，请点击某一行中的一个值。请注意，此操作仅适用于向下钻取页面。在表视图中点击一行中的一个值仅限于表视图，不能钻取到下一页面。
- 要向下展开到限制某些事件的下一个工作流程页面，请选中要在下一个工作流程页面上查看的事件旁边的复选框，然后点击**查看 (View)**。
- 要向下钻取到保留当前限制的下一个工作流程页面，请点击 **View All**。

提示 表视图的页面名称中始终包含“Table View”。

使用表视图页面

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

表视图页面提供在向下钻取、主机视图、数据包视图或漏洞详细信息页面上不可用的某些功能。按如下所述使用这些功能：

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 1444 页中所述。

步骤 2 从工作流程名称下方显示的工作流程路径中选择表视图。

步骤 3 根据需要使用下列功能在表视图中排列和导航：

- 要显示已禁用列的列表，请点击“搜索限制”(Search Constraints) 展开箭头 ( )。
- 要隐藏已禁用列的列表，请点击“搜索限制”(Search Constraints) 折叠箭头 ( )。
- 要将已禁用列重新添加到事件视图中，请点击 Search Constraints 展开箭头 ( ) 以展开搜索限制，然后点击 Disabled Columns 下的列名。
- 要显示或隐藏（禁用）列，请点击任何列名称旁边的清除图标( )。在显示的弹出窗口中，选中或清除相应的复选框以指示要显示哪些列，然后点击**应用 (Apply)**。

Geolocation

地理定位功能提供有关可路由IP地址的地理源的数据（国家/地区和大洲等）。此信息在事件、资产配置文件、情景管理器、控制面板和其他分析工具中可用。

注释 对于检测到在不同国家/地区之间移动的移动设备和其他主机，系统可能会报告大洲而不是具体的国家/地区。

您可以使用地理定位数据来过滤网络流量。例如，您可以确定连接是否起源于或终止于与您的公司无关联的国家/地区。在内联部署中，您可以对这些连接进行阻止。

系统在其地理定位数据库(GeoDB)中存储地理定位数据。思科定期发布GeoDB更新。“关于”(About)页面（**帮助 (Help)** > **关于 (About)**）显示当前 GeoDB 更新版本。

如果您接受 GeoDB 更新，可以在 Firepower 管理中心 Web 界面上点击国家/地区的小旗帜图标和 ISO 国家/地区代码，以获取有关特定 IP 地址的地理定位详细信息；请参阅地理位置详细信息，第 1451 页。还可以使用第三方映射工具精确定位检测到的位置。如果不更新GeoDB，这些详细信息将不可用。

无法在“连接摘要”(Connection Summary)之类的控制面板上查看地理定位详细信息来获取汇聚的地理定位信息。

地理位置详细信息

根据可用性，“地理位置详细信息”(Geolocation Details) 页面上可能会显示多个字段。下表包含有关这些字段的信息。（无信息的字段不显示。）

表 *257*：地理位置详细信息字段

字段	目录
国家/地区	与主机的 IP 地址关联的国家/地区，伴有国家/地区的旗帜。在括号中列出了大陆。示例：`United States (North America)` 和 `Equatorial Guinea (Africa)`
地区	主机所在的国家/地区的州、省或其他子区域。示例：`VA` 和 `35`
城市	主机所在的城市。示例：`Seattle` 和 `Fukuoka`
邮政编码	主机所在区域的邮政编码。示例：`361000` 和 `90210`
Latitude/Longitude	主机位置的精确坐标。示例：`40.0375, -76.1053`；`53.4050, -0.5484`
地图	指向外部映射站点的链接（谷歌地图、雅虎地图、必应地图和OpenStreetMap）。点击任意链接以查看主机的大致位置的情景地图。
Timezone	主机位置的时区，在适用情况下会标注夏令时。示例：`GMT+8:00` 和 `GMT-4:00 (In DST)`
ASN	与主机 IP 地址关联的自治系统编号 (ASN)，以及与该 ASN 有关的任何其他信息。示例：`14618 (Amazon.com Inc.)`；`4837 (Cncgroup China169 Backbone)`
ISP	与主机 IP 地址关联的互联网服务提供商 (ISP)。示例：`Atlantic Broadband`；`China Unicom Ip Network`
Home/Business	主机的连接是用于 `Home` 还是 `Business` 用途。
Organization	与主机 IP 地址关联的公司。示例：`Amazon.com` 和 `Bank of America`
域名	与主机 IP 地址关联的域名。示例：`amazonaws.com` 和 `xmcnc.net`
连接类型	与主机 IP 地址关联的连接类型。示例：`Broadband` 和 `DSL`
代理类型	使用的代理类型。示例：`Anonymous` 和 `Corporate`

连接事件图形

除使用表格向下钻取页面的工作流程和事件的最终表格视图之外，系统可以用在五分钟间隔内汇聚的数据以图形方式展示某些连接数据。请注意，您只可以用图形显示用于汇聚数据的信息：源和目标 IP 地址（以及那些主机的关联用户）、目标端口、传输协议以及应用协议。

提示 您无法将安全情报事件与其关联连接事件分开单独用图形展示。有关安全情报过滤活动的图形概述，请使用控制面板和情景管理器。

有三种不同类型的连接图形：

- 饼形图，显示按各种类别分组的一个数据集中的数据。
- 条形图，显示按各种类别分组的一个或多个数据集中的数据。
- 曲线图，用标准或速度（更改速率）视图图示一个或多个数据集随着时间推移的数据。

注释 系统用曲线图显示流量量变曲线，您可以操作其他任何连接图的方式操作这些图形，但会有一些限制。要查看流量量变曲线，您必须具有管理员访问权限。

与工作流程表一样，您可以向下钻取并限制工作流程图，以重点关注您的分析。

条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方和响应方的总数。饼形图只能显示一个数据集。

通过改变 x 轴、y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据和数据集。在饼形图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。

使用连接事件图形

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

在 Firepower 管理中心上，可以查看连接事件图形并根据要查找的信息操纵这些图形。

访问连接图时看到的页面因所用的工作流程而有所不同。可以使用预定义的工作流程，最终会产生连接事件表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis) > 连接 (Connections) > 事件 (Events)**。

注释 如果显示的是连接事件表而非图形，或者要查看不同图形，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**，然后选择包括图形的预定义工作流程或选择自定义工作流程。请注意，所有预定义连接事件工作流程（包括连接图）最终都会产生连接的表视图。

步骤 2 您有以下选择：

- 时间范围 - 要调整时间范围（如果是空图形会非常有用），请参阅更改时间窗口，第 1461 页。
- 字段名称 - 要详细了解可以用图形表示的数据，请参阅连接和安全情报事件字段，第 1515 页。
- 主机配置文件 - 要查看某个 IP 地址的主机配置文件，请在按发起方或响应方显示连接数据的图形上，点击条形图的某一条或饼形图的某一块，然后选择**查看主机配置文件 (View Host Profile)**。
- 用户配置文件 - 要查看用户配置文件信息，请在按发起方用户显示连接数据的图形上，点击条形图的某一条或饼形图的某一块，然后选择**查看用户配置文件 (View User Profile)**。
- 其他信息 - 要了解有关绘图数据的详细信息，请将光标移动至曲线图的某一点上、条形图的某一条上或饼形图的某一块上。
- 限制 - 要按任意 x 轴（自变量）条件限制连接图形而不前进到工作流程中的下一页，请点击曲线图的某一点、条形图的某一条或饼形图的某一块，然后选择**查看依据... (View by...)** 选项。
- 数据选择 - 要更改图形中显示的数据，请点击 **X 轴 (X-Axis)** 或 **Y 轴 (Y-Axis)**，然后选择要用图形表示的新数据。请注意，将 x 轴更改为**时间 (Time)** 或反之，还会更改图形类型；改变 y 轴会影响显示的数据集。
- 数据集 - 要更改图形的数据集，请点击**数据集 (Datasets)**，然后选择新的数据集。
- 分离 - 要分离连接图形以便在不影响默认时间范围的情况下执行进一步分析，请点击**分离 (Detach)**。

  提示 在分离图中点击**新建窗口 (New Window)** 可创建副本。然后，您可以在每个分离图上进行不同分析。请注意，流量剖面图是分离图形。
- 向下展开 - 要向下展开到工作流程中的下一页，请点击曲线图上的某一点、条形图上的某一条或饼形图上的某一块，然后选择**向下展开 (Drill-down)**。点击曲线图上的某个点可将下一个页面的时间范围更改为以所点击点为中心的 10 分钟时间区间。点击条形图上的某一条或饼形图上的某一块，可基于该条或该块表示的标准限制下一个页面。
- 导出 - 要将图形的连接数据导出为 CSV（逗号分隔值）文件，请点击**导出数据 (Export Data)**。然后，点击**下载 CSV 文件 (Download CSV File)**，并保存文件。
- 图形类型：曲线图 - 要在标准曲线图与速度（变化率）曲线图之间切换，请点击**速度 (Velocity)**，然后选择**标准 (Standard)** 或**速度 (Velocity)**。
- 图表类型：条形图和饼形图 - 要在条形图与饼形图之间切换，请点击**切换为条形图 (Switch to Bar)** 或**切换为饼形图 (Switch to Pie)**。因为不能在饼形图上显示多个数据集，如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，Firepower 管理中心会首选显示总统计信息，而不是发起方和响应方的统计信息；在显示发起方统计信息和响应方统计信息时，会首选显示发起方统计数据。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “重定中心”(Recenter) - 要围绕某个时间点重定曲线图的中心而不更改时间范围的长度，请点击该点，然后选择**重定中心 (Recenter)**。

- “缩放”(Zoom) - 要围绕某个时间点重定曲线图的中心，同时进行放大或缩小，请点击该点，选择**缩放 (Zoom)**，然后选择新的时间区间。

注释 除非使用分离图，否则限制、重定中心和缩放会改变 Firepower 管理中心的默认时间范围。

示例：限制连接图形

思考一个长时间区间连接的图形。如果在按端口图形上应用时间点限制，系统会显示一个条形图，列出基于检测到的连接事件数目、同时受以所点击点为中心的 10 分钟时间区间限制的 10 个最活跃的端口。

如果通过点击条形图中的一条并选择**按发起方 IP 查看 (View by Initiator IP)** 进一步限制该图形，系统将显示一个新的条形图。该条形图不仅受到与之前相同的10分钟时间区间的限制，还受到所点击条柱表示的端口的限制。

示例：更改饼形图上的 X 轴和 Y 轴

考虑一个图形化显示各端口数据量的饼形图。在这种情形下，x 轴是 **Responder Port**，y 轴是 **KBytes**。该饼图表示在一定时间区间内由监控网络发送的总数据量。该饼图的楔块表示在每端口上检测到的数据百分比。

- 如果将该饼图 x 轴变更为 **Application Protocol**，该饼图仍然表示已传输的总数据量，但该饼图的楔块表示为每个已检测到应用协议传输的数据百分比。
- 如果将该图形的 y 轴改为**数据包数 (Packets)**，该饼形图表示在一定时间区间内监控网络传输的数据包总数，而形饼图的楔块表示每个端口上检测到的数据包在数据包总数中所占的百分比。

连接图形数据选项

通过改变 x 轴、y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据。在饼形图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。

表 *258*：*X* 轴选项

X 轴选项	图表类型	绘制此数据的方式
应用协议	条形图或饼形图	通过 10 个最活跃的应用协议
设备	条形图或饼形图	通过 10 个最活跃的受管设备
Initiator IP	条形图或饼形图	通过 10 个最活跃的发起方主机 IP 地址
Initiator User	条形图或饼形图	通过 10 个最活跃的发起方用户

X 轴选项	图表类型	绘制此数据的方式
Responder IP	条形图或饼形图	通过 10 个最活跃的响应方主机 IP 地址
响应方端口 (Responder Port)	条形图或饼形图	通过 10 个最活跃的响应方端口
Source Device	条形图或饼形图	通过 10 个最活跃的 NetFlow 数据导出器，以及 Firepower 系统受管设备检测到的所有连接的名为 `Firepower` 的源设备。
Time	线路	在一段时间内 在**时间 (Time)** 中更改 y 轴的结束和起始时间也会更改图形类型，并可能更改数据集。

表 *259*: *Y* 轴选项

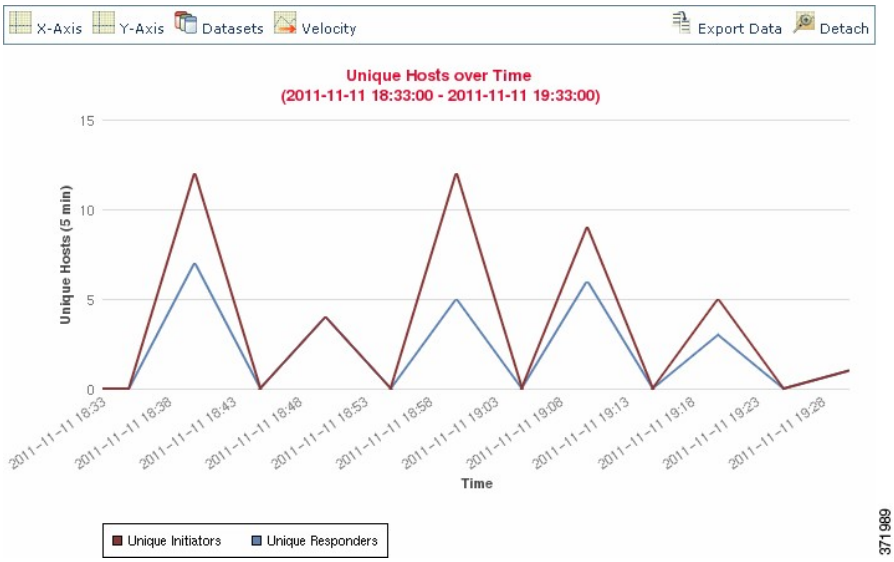
Y 轴选项	使用 X 轴标准绘制此数据
字节	传输的字节数
连接	连接数量
KBytes	传输的千字节数
KBytes Per Second	每秒的千字节数
数据包	传输的数据包数量
Unique Hosts	检测到的独立主机数量
Unique Application Protocols	独立应用协议数量
唯一用户	独立用户数量

具有多个数据集的连接图形

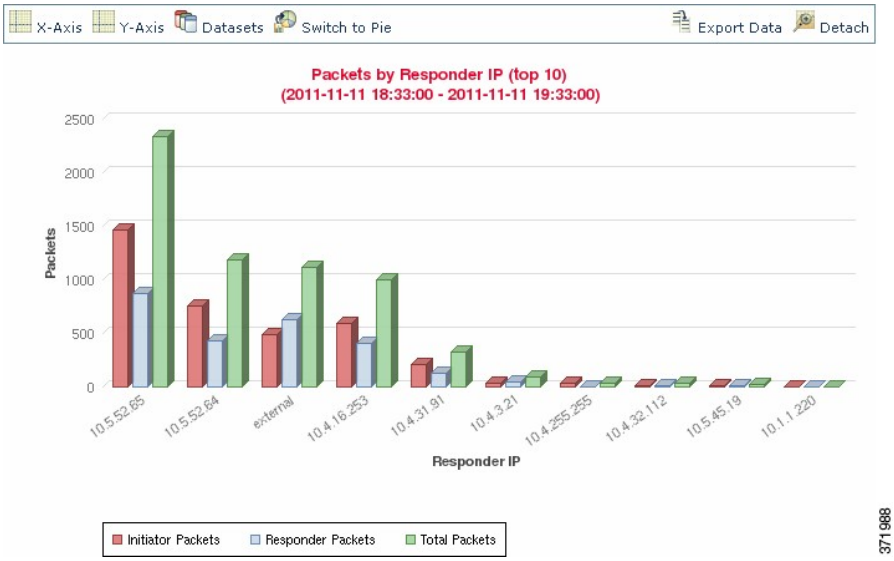
条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方和响应方的总数。

注释 饼形图**不能**显示多个数据集。如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，Firepower 管理中心会首选显示总统计数据，而不是发起方和响应方的统计数据；在显示发起方统计数据和响应方统计数据时，会首选显示发起方统计数据。

在曲线图上，多个数据集显示为多条线，每条线颜色不同。例如，下面的图形显示了在一个小时的时间区间内监控网络上检测到的独立发起方总数和独立响应方总数。



在条形图上，与 x 轴的各个数据点对应的多个数据集显示为一组彩色条形柱。例如，下面的条形图显示监控网络上传输的数据包总数、发起方传输的数据包总数以及响应方传输的数据包总数。



连接图形数据集选项

下表介绍了在连接图 x 轴上可以显示的数据集。

表 *260*：数据集选项

如果 y 轴显示.....	可以选为数据集的对象为.....
连接	仅默认数量，即在受监控网络上检测到的连接数（**连接数 [Connections]**）这是流量剖面图的唯一选项。
KBytes	组合： • 监控网络上传输的总数据量 (**Total KBytes**) • 监控网络上的主机 IP 地址传输的数据量 (**Initiator KBytes**) • 监控网络上的主机 IP 地址收到的数据量 (**Responder KBytes**)
KBytes Per Second	仅默认数量，指在监控网络上每秒传输的总数据量 (**Total KBytes Per Second**)
数据包	组合： • 在监控网络上传输的数据包总数 (**Total Packets**) • 在监控网络上从主机 IP 地址传输的数据包总数 (**Initiator Packets**) • 在监控网络上主机 IP 地址收到的的数据包总数 (**Responder Packets**)
Unique Hosts	组合： • 在监控网络上独立会话发起方的数量 (**Unique Initiators**) • 在监控网络上独立会话响应方的数量 (**Unique Responders**)
Unique Application Protocols	仅默认数量，指监控网络上的独立应用协议的数量 (**Unique Application Protocols**)
唯一用户	仅默认数量，指登录到监控网络上会话发起方的独立用户的数量 (**Unique Initiator Users**)

事件时间限制

每个事件具有指示事件发生时间的时间戳。可以通过设置时间段（有时称为时间范围）限制某些工作流程中显示的信息。

基于可按时间限制的事件的工作流程在页面顶部具有一条时间范围线。默认情况下，思科设备上的工作流程使用设置为前一小时的扩展式时间窗口。例如，如果您在上午 11:30 登录，将会看到发生在上午 10:30 和上午 11:30 之间的事件。随着时间的推进，时间段进行扩展。在中午 12:30，您将会看到发生在上午 10:30 和中午 12:30 之间的事件。

可以通过在事件视图设置中设置自己的默认时间窗口来更改此行为：该时间窗口管理三个属性：

- 时间段类型（静态、扩展式或滑动式）
- 时间段长度
- 时间段数量（多个时间段或单个全局时间段）

无论默认时间段设置如何，都可以在事件分析期间手动更改时间段，方法是点击页面顶部的时间范围，该页面会显示 Date/Time 弹出窗口。根据配置的时间段数量和使用的设备类型，还可以使用 Date/Time 窗口更改所查看的事件类型的默认时间段。

最后，您可以暂停时间窗口，从而能够检查工作流程提供的数据，而无需进行时间窗口更改，以及删除或添加您不感兴趣的事件。请注意，为避免在不同的工作流程页面上显示相同事件，时间窗口会在您点击页面底部的链接以显示事件的另一个页面时自动暂停；在您准备就绪后，可以取消暂停时间窗口。

事件的时间窗口自定义

无论默认时间段设置如何，都可以在事件分析期间手动更改时间段。

注释 手动时间段设置仅对当前会话有效。在注销然后重新登录时，时间段会重置为默认值。

根据配置的时间段数量，更改一个工作流程的时间段可能会影响设备上的其他工作流程。例如，如果具有单个全局时间段，则更改一个工作流程的时间段会更改设备上所有其他工作流程的时间段。另一方面，如果使用的是多个时间段，则更改审核日志或运行状况事件工作流程时间段对于任何其他时间段没有影响，而更改其他种类的事件的时间段则会影响可按时间限制的所有事件（审核事件和运行状况事件除外）。

请注意，由于并非所有工作流程都可按时间限制，因此时间段设置对基于主机、主机属性、应用、应用详情、漏洞、用户或白名单违例的工作流程没有影响。

使用 Date/Time 窗口上的 Time Window 选项卡手动配置时间段。根据在默认时间段设置中配置的时间段数量，选项卡的标题为以下之一：

- **Events Time Window**（如果配置了多个时间段，并且是为除审核日志和运行状况事件工作流程以外的工作流程设置时间段）
- **Health Monitoring Time Window**（如果配置了多个时间段，并且是为运行状况事件工作流程配置时间段）
- **Audit Log Time Window**（如果配置了多个时间段，并且是为审核日志配置时间段）
- **Global Time Window**（如果配置了单个时间段）

配置时间段时必须首先决定要使用的时间段的类型。

- 静态时间段显示从特定开始时间到特定结束时间生成的所有事件。
- 扩展式时间段显示从特定开始时间到目前生成的所有事件；随着时间的推进，时间段进行扩展，并会将新事件添加到事件视图中。

- 滑动式时间段显示从特定开始时间（例如，一周前）到目前生成的所有事件；随着时间的推进，时间段会“滑动”，以便仅显示已配置的范围（在此示例中是上周）的事件。

根据选择的类型，Date/Time 窗口会更改以提供不同配置选项。

注释 Firepower 系统根据在时区首选项中指定的时间使用 24 小时制时钟。

时间窗口设置

下表说明可在 Time Window 选项卡上配置的各种设置。

表 *261*：时间窗口设置

设置	时间段类型	说明
时间段类型下拉列表	n/a	选择要使用的时间段类型：静态、扩展式或滑动式。 请注意，如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间段（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。
Start Time 日历	静态和扩展式	指定时间段的开始日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 可以使用 Presets 选项而不是使用日历，如下所述。
End Time 日历	静态	指定时间段的结束日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 请注意，如果使用的是扩展式时间段，则“结束时间”(End Time) 日历会灰显并指定结束时间为“现在”(Now)。 可以使用 Presets 选项而不是使用日历，如下所述。
显示 Last 字段和下拉列表	滑动式	配置滑动式时间段的长度。
Presets: Last	all	根据设备的本地时间，点击列表中的其中一个时间范围以更改时间段。例如，点击 **1 week** 会将时间段更改为反映上周。点击预设会将日历更改为反映选择的预设。
Presets: Current	静态和扩展式	根据设备的本地时间和日期，点击列表中的其中一个时间范围以更改时间段。点击预设会将日历更改为反映选择的预设。 请注意： • 当日在午夜开始 • 当周在星期天午夜开始 • 当月在月份第一日午夜开始

设置	时间段类型	说明
Presets: Synchronize with	所有（如果使用的是全局时间段则不适用）	点击其中一项： • **Events Time Window** 将当前时间段与事件时间段同步 • **Health Monitoring Time Window** 将当前时间段与运行状况监控时间段同步 • **Audit Log Time Window** 将当前时间段与审核日志时间段同步

更改时间窗口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

步骤 1 在按时间限制的工作流程中，点击时间范围图标 (🕒) 以转至“日期/时间”(Date/Time) 窗口。

步骤 2 在**事件时间窗口 (Events Time Window)** 选项卡上，设置时间窗口，如时间窗口设置，第 1460 页中所述。

提示 点击 **Reset** 以将时间段重新更改为默认设置。

步骤 3 点击 **Apply**。

事件的默认时间窗口

在事件分析期间，可以使用“日期/时间”(Date/Time) 窗口上的“首选项”(Preferences) 选项卡更改所查看的事件类型的默认时间窗口，而不必使用事件视图设置。

请记住，以此方式更改默认时间段仅会更改所查看的事件类型的默认时间段。例如，如果配置了多个时间段，则更改 Preferences 选项卡上的默认时间段会更改事件、运行状况监控或审核日志窗口的设置，换句话说，以第一个选项卡指示的时间段为准。如果配置了单个时间段，则更改 Preferences 选项卡上的默认时间段会更改所有事件类型的默认时间段。

事件类型的默认时间窗口选项

下表说明可在 Preferences 选项卡上配置的各种设置。

表 *262*：时间窗口首选项

偏好	说明
刷新间隔	设置事件视图的刷新间隔（以分钟为单位）。输入零会禁用刷新选项。
Number of Time Windows	指定要使用的时间段数量： • 选择 **Multiple** 以根据可按时间限制的事件为审核日志、运行状况事件和工作流程配置单独的默认时间段。 • 选择**单个 (Single)** 以使用适用于所有事件的全局时间窗口。
Default Time Window: Show the Last - Sliding	此设置允许配置指定长度的滑动式默认时间段。 设备显示从特定开始时间（例如，1 小时前）到目前生成的所有事件。更改事件视图时，时间段会“滑动”，以便始终显示前一小时的事件。
Default Time Window: Show the Last - Static/Expanding	此设置允许配置指定长度的静态或扩展式默认时间段。 对于**静态**时间段（启用 **Use End Time** 复选框），设备显示从特定开始时间（例如，1 小时前）到首次查看事件时生成的所有事件。更改事件视图时，时间段保持固定，以便仅显示静态时间段期间发生的事件。 对于**扩展式**时间段（禁用 **Use End Time** 复选框），设备显示从特定开始时间（例如，1 小时前）到目前生成的所有事件。更改事件视图时，时间段扩展到当前时间。
Default Time Window: Current Day - Static/Expanding	此设置允许配置当日的静态或扩展式默认时间段。根据当前会话的时区设置，当日在午夜开始。 对于**静态**时间段（启用 **Use End Time** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件视图时，时间段保持固定，以便仅显示静态时间段期间发生的事件。 对于**扩展式**时间段（禁用 **Use End Time** 复选框），设备显示从午夜到目前生成的所有事件。更改事件视图时，时间段扩展到当前时间。请注意，如果在您注销之前，分析持续 24 小时以上，则此时间段可以超过 24 小时。
Default Time Window: Current Week - Static/Expanding	此设置允许配置当周的静态或扩展式默认时间段。根据当前会话的时区设置，当周在上个星期天的午夜开始。 对于**静态**时间段（启用 **Use End Time** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件视图时，时间段保持固定，以便仅显示静态时间段期间发生的事件。 对于**扩展式**时间段（禁用 **Use End Time** 复选框），设备显示从星期天午夜到目前生成的所有事件。更改事件视图时，时间段扩展到当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间段可以超过 1 周。

更改事件类型的默认时间窗口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师

过程

步骤 1 在按时间限制的工作流程中，点击时间范围图标 () 以转至“日期/时间”(Date/Time) 窗口。

步骤 2 点击**首选项 (Preferences)** 选项卡并更改您的首选项，如事件类型的默认时间窗口选项，第 1461 页表中所述。

步骤 3 点击**保存首选项**。

步骤 4 此时您有两种选择：

- 要将新的默认时间段设置应用于所使用的事件视图，请点击 **Apply** 以关闭 Date/Time 窗口并刷新事件视图。
- 要继续分析而不应用默认时间段设置，请关闭 Date/Time 窗口而不点击 **Apply**。

时间窗口进度

可以暂停时间段，从而能够检查工作流程提供的数据快照。这会有所帮助，因为已取消暂停的工作流程在更新时，可能会移除要检查的事件，或者添加无关的事件。

请注意，不能暂停静态时间段。此外，暂停事件时间段对控制面板没有影响，而暂停控制面板对暂停事件时间段也没有任何影响。

完成分析后，可以取消暂停时间段。取消暂停时间段将根据您的喜好对其进行更新，并且还更新事件视图以反映已取消暂停的时间段。

如果数据库包含的事件数超过单个工作流程页面上可显示的事件数，则可点击页面底部的链接以显示更多事件。执行此操作时，时间段自动暂停，以便不重复显示相同的事件。

暂停/取消暂停时间窗口

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

在受时间限制的工作流程上，选择所需的时间范围控件：

- 要暂停时间窗口，请点击时间范围控件暂停图标 ( )。
- 要取消暂停时间窗口，请点击时间范围控件播放图标 ( )。

事件视图限制

工作流程页面上显示的信息由实施的限制来确定。例如，最初打开事件工作流程时，信息限制为前一小时生成的事件。

要前进到工作流程中的下一页并通过特定值限制所查看的数据，请选择页面上具有这些值的行，然后点击 **View**。要前进到工作流程中的下一页并保留当前限制和传递所有事件，请选择 **View All**。

注释 如果选择含有多个非计数值的行并点击 **View**，则会创建复合限制。

限制工作流程中的数据有第三种方法。要将页面限制为含有选定值的行，并且还将选定值添加到页面顶部的限制列表中，请点击页面上某一行中的值。例如，如果查看的是已记录连接的列表，并要使用访问控制将该列表仅限于允许的连接，请点击 **Action** 列中的 **Allow**。又例如，如果查看的是入侵事件，并要将列表仅限于目标端口为 80 的事件，请点击**目标端口/ICMP 代码 (Destination Port/ICMP Code)** 列中的 **80 (http)/tcp**。

提示 根据监控规则条件来限制连接事件的过程略有不同，可能需要采取一些额外步骤。此外，不能按关联文件或入侵信息来限制连接事件。

还可以使用搜索来限制工作流程中的信息。要再次限制一列中的多个值时，请使用此功能。例如，如果要查看与两个 IP 地址相关的事件，请点击 **Edit Search**，然后修改 Search 页面上相应的 IP 地址字段以将两个地址均包含在内，然后点击 **Search**。

在搜索页面上输入的搜索条件会列为页面顶部的限制，并且产生的事件相应地受限制。在 Firepower 管理中心中，除非当前限制是复合限制，否则导航到其他工作流程时也会应用这些限制。

在搜索时，必须特别注意搜索限制是否适用于所搜索的表。例如，客户端数据在连接摘要中不可用。如果根据连接中检测到的客户端搜索连接事件，然后在连接摘要事件视图中查看结果，则Firepower 管理中心会显示连接数据，如同其完全未受限制一样。无效限制会标示为不适用 (N/A)，并以删除线进行标记。

限制事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 1444 页中所述。

步骤 2 在任何工作流程中，您有以下选择：

- 要将视图限于与单个值相匹配的事件，请点击页面上行中的所需值。
- 要将视图限于与多个值相匹配的事件，请选中具有这些值的事件的对应复选框，然后点击**视图 (View)**。

  注释 如果行包含多个非计数值，则会添加复合限制。

- 要删除限制，请点击“搜索限制”(Search Constraints) 展开箭头 ( )，然后点击展开的“搜索限制”(Search Constraints) 列表中的限制名称。
- 要使用“搜索”(Search) 页面编辑限制，请点击**编辑搜索 (Edit Search)**。
- 要将限制另存为已保存的搜索，请点击**保存搜索 (Save Search)** 并指定查询名称。

  注释 不能保存包含复合限制的查询。

- 要对其他事件视图使用相同限制，请点击**跳至 (Jump to)** 并选择事件视图。

  注释 当切换到其他工作流程时，不会保留复合限制。

- 要切换限制的显示，请点击“搜索限制”(Search Constraints) 展开箭头 ( ) 或“搜索限制”(Search Constraints) 折叠箭头 ( )。这在限制列表较大并占据大部分屏幕时有用。

复合事件视图限制

复合限制基于特定事件的所有非计数值。选择含有多个非计数值的行时，需要设置复合限制，该限制仅检索与该页面上的该行中所有非计数值都匹配的事件。例如，如果选择源 IP 地址为 `10.10.31.17`

且目标 IP 地址为 10.10.31.15 的行以及源 IP 地址为 172.10.10.17 且目标 IP 地址为 172.10.10.15 的行，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 的事件

  或

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 的事件

将复合限制与简单限制组合时，简单限制分布在各复合限制集合中。例如，如果在以上所列的复合限制中为协议值 tcp 添加了一条简单限制，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 且协议为 tcp 的事件

  或

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 且协议为 tcp 的事件

不能对复合限制执行搜索或保存搜索操作。您也不能在使用事件视图链接或点击（**切换工作流程**）**([switch workflow])** 以切换到其他工作流程时保留复合限制。如果将应用了复合限制的事件视图加入书签，则不使用书签保存限制。

使用复合事件视图限制

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 1444 页中所述。

步骤 2 要管理复合限制，您有以下选择：

- 要创建复合限制，请选择一个或多个具有多个非计数值的行，然后点击**查看 (View)**。
- 要清除复合限制，请点击“搜索限制”(Search Constraints) 展开箭头 ( ) 并点击**复合限制 (Compound Constraints)**。

工作流程间导航

可以使用工作流程页面上的 **Jump to...** 下拉列表中的链接导航到其他工作流程。选择下拉列表以查看并选择其他工作流程。

选择新工作流程时，所选行共享的属性和所设置的限制用于新工作流程中（如果其适用）。如果配置的限制或事件属性没有映射到新工作流程中的字段，则表明其已丢弃。此外，从一个工作流程切换到另一个工作流程时未保留复合限制。此外，捕获的文件工作流程中的限制仅传输到文件和恶意软件事件工作流程。

注释

查看某个时间范围的事件计数时，事件的总数可能无法反映为其提供了更详细数据的事件的数量。因为系统有时会删掉较旧的事件详情以管理磁盘空间使用情况，所以会发生这种情况。要将事件详情删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。

请注意，除非已暂停时间段或已配置静态时间段，否则在更改工作流程时时间段会更改。

此功能可增强您调查可疑活动的能力。例如，如果查看的是连接数据并发现内部主机在向外部站点传送异常大量的数据，则可以选择响应方 IP 地址和端口作为限制，然后跳至 **Applications** 工作流程。应用工作流程将使用响应方 IP 地址和端口作为 IP Address 和 Port 限制，并显示有关应用的其他信息，如应用的种类。也可以点击页面顶部的 **Hosts** 以查看远程主机的主机配置文件。

在找到有关应用的详细信息后，可以选择**关联事件 (Correlation Events)** 以返回到连接数据工作流程，从限制中删除响应方 IP，向限制中添加发起方 IP，然后选择**应用详细信息 (Application Details)** 以了解发起主机上的用户在将数据传输到远程主机时使用了哪个客户端。请注意，Port 限制未转移到 Application Details 页面。保持本地主机作为限制时，也可以使用其他导航按钮查找其他信息。

- 要发现本地主机是否已违反任何策略，请保持 IP 地址作为限制并从 **Jump to** 下拉列表中选择 **Correlation Events**。
- 要了解是否对主机触发了指示危害的入侵规则，请从 **Jump to** 下拉列表中选择 **Intrusion Events**。
- 要查看本地主机的主机配置文件并确定主机是否易受可能已被利用的任何漏洞的攻击，请从 **Jump to** 下拉列表中选择 **Hosts**。

书签

如果要在事件分析中快速返回到特定位置和时间，请创建书签。书签保留以下有关信息：

- 使用的工作流程
- 查看的工作流程部分
- 工作流程中的页码
- 任何搜索限制
- 任何已禁用列
- 使用的时间范围

创建的书签可供具有书签访问权限的所有用户帐户使用。这意味着，如果发现需要深入分析的事件集，则可以轻松创建书签并将调查移交给具有相应特权的其他用户。

注释 如果删除书签中显示的事件（直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

创建书签

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

在多域部署中，只能查看在当前域中创建的书签。

过程

步骤 1 在事件分析期间，显示了有关事件的情况下，点击 **Bookmark This Page**。

步骤 2 在**书签名称 (Bookmark Name)** 字段中，输入名称。

步骤 3 点击**保存书签 (Save Bookmark)**。

查看书签

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

在多域部署中，只能查看在当前域中创建的书签。

过程

从任何事件视图中，您有两个选项：

- 将指针悬停在**查看书签 (View Bookmarks)** 上方，然后点击下拉菜单中的所需书签。
- 点击**查看书签 (View Bookmarks)**，然后在“查看书签”(View Bookmarks) 页面上，点击所需的书签名称或其旁边的查看图标 ( )。

注释　如果删除书签中最初显示的事件（直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

第 80 章

搜索事件

以下主题介绍如何在工作流程中搜索事件：

事件搜索

Firepower 系统生成的信息作为事件存储在数据库表中。事件包含多个字段，描述导致设备生成事件的活动。您可以创建并保存面向您的环境为任何不同事件类型自定义的搜索，并将其保存以供今后重复使用。

保存搜索时，请为其命名，并指定此搜索仅供您自己使用还是供设备的所有用户使用。如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。如果先前保存了一个搜索，则可加载该搜索，做出任何必要更改，然后开始搜索。自定义分析控制面板构件、报告模板和自定义角色也可以使用保存的搜索。如有已保存的搜索，可从 Search 页面删除这些搜索。

对于某些事件类型，Firepower 系统会提供预定义搜索，既可将其用作示例，又可借助其快速访问有关网络的重要信息。可针对网络环境修改预定义搜索中的字段，然后保存搜索，以供日后重复使用。

可使用的搜索条件取决于搜索类型，但搜索技巧相同。搜索仅返回与所有字段的指定搜索条件匹配的记录。

注释 搜索自定义表所需的程序略有不同。

搜索限制

每个数据库表都有自己的搜索页面，您可以在此页面中输入搜索限制值以应用于为该表定义的字段。根据字段的类型，可使用专用语法来指定条件，例如通配符或数值范围。

搜索结果显示在工作流程页面，以柱状布局显示每个表字段。某些数据库表还可使用未在工作流程页面显示为列的字段进行搜索。查看工作流程页面中的结果时，要确定此类限制是否适用于搜索结果，请点击展开图标 ( )，查看活动的搜索限制。

通用搜索限制

搜索事件时，请遵循以下通用准则：

- 所有字段接受协商 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。

  对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A, B, "C, D, E"` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C, D, E"` 的指定字段。这允许与可能的值中包含逗号的字段匹配。

  对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。

  对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。

- 在任何字段中指定 `n/a` 表示无字段相关信息的事件；使用 `!n/a` 表示该字段已填充的事件。
- 您可以在众多数字字段前面加上大于 (>)、大于或等于 (>=)、小于 (<)、小于或等于 (<=) 、等于 (=) 或不等于 (<>) 运算符。

提示 当搜索具有较长复杂值的字段（例如 SHA-256 散列值）时，可以从原材料复制搜索条件值，并将其粘贴到搜索页面上的合适字段中。

搜索中的通配符和符号

在搜索页面的许多文本字段中，可使用星号 (*) 匹配字符串中的字符。例如，指定 `net*` 匹配 `network`、`netware`、`netscape` 等等。

如果想要搜索非字母数字字符（包括星号字符），请用引号将搜索字符串引起来。例如，要搜索字符串：

```
Find an asterisk (*)
```

输入：

```
"Find an asterisk (*)"
```

请注意，在允许输入通配符的文本字段中，如要匹配部分字符串，则**必须**使用通配符。 例如，如在审核日志中搜索所有涉及页面视图（即，消息为“页面视图”[Page View]) 的审核记录，则搜索 `Page` 不会返回结果。相反，应该指定 `Page*`。

在某些字段中，可以搜索全部或部分字段内容而无需使用星号。在这些情况下，必须用引号将搜索字符串引起来进行完全匹配，否则系统将执行部分匹配。例如，如果要使用不带引号的字符串 `Scan Completed with Detection` 搜索此类字段，系统会返回字段包含以下字符串的记录以及字段与搜索字符串完全匹配的记录：

```
Scan Completed, No Detections
Scan completed With Detections
```

搜索中的对象和应用过滤器

Firepower 系统可用于创建可用作网络配置一部分的已命名对象、对象组和应用过滤器。执行或保存搜索时，可使用这些对象、组和过滤器作为搜索条件。

执行搜索时，对象、对象组和应用过滤器以 `${object_name}` 格式显示。例如，有对象名称 `ten_ten_network` 的网络对象在搜索中显示为 `${ten_ten_network}`。

在可使用对象作为搜索条件的搜索字段旁边，可点击添加对象图标 ( )。

搜索中的时间限制

下表显示了采用时间值的搜索条件字段接受的格式。

表 *263*：搜索字段中的时间规范

时间格式	示例
`today [at HH:MMam|pm]`	`today` `today at 12:45pm`
*YYYY-DD*MM- *HH*:*MM*:*SS*	`2006-03-22 14:22:59`

可在时间值前输入下列运算符之一。

表 *264*：时间规范运算符

Operator	示例	说明
<	`< 2006-03-22 14:22:59`	返回时间戳早于 2006 年 3 月 22 日下午 2:23 的事件。
>	`> today at 2:45pm`	返回时间戳晚于今天下午 2:45 的事件。

搜索中的 IP 地址

在搜索中指定 IP 地址时，可输入单个 IP 地址、用逗号隔开的地址列表、地址块或者一系列用连字符 (-) 隔开的 IP 地址。也可使用求反。

对于支持 IPv6 的搜索（例如，入侵事件、连接数据和关联事件搜索），可输入 IPv4 和 IPv6 地址与 CIDR/前缀长度地址块的任意组合。按 IP 地址搜索主机时，结果包括至少有一个 IP 地址与搜索条件匹配的所有主机，即搜索 IPv6 地址可能会返回原地址是 IPv4 的主机。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，Firepower 系统**只**使用掩码或前缀长度指定的那部分网络 IP 地址。例如，如果键入 `10.1.2.3/8`，则 Firepower 系统使用 `10.0.0.0/8`。

因为 IP 地址可以用网络对象表示，所以，也可点击 IP 地址搜索字段旁边的添加网络对象图标 (⁺)，使用网络对象作为 IP 地址搜索条件。

表 *265*：可接受的 *IP* 地址语法

指定的对象	键入的内容	示例
单个 IP 地址	IP 地址。	`192.168.1.1` `2001:db8::abcd`
多个 IP 地址，使用列表	用逗号隔开的 IP 地址列表。请**不要**在逗号前后添加空格。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
可以使用 CIDR 块或前缀长度指定的一系列 IP 地址	采用 IPv4 CIDR 或 IPv6 前缀长度表示法的 IP 地址块。	`192.168.1.0/24` 这可在子网掩码为 255.255.255.0 的 192.168.1.0 网络中指定任意 IP，即 192.168.1.0 至 192.168.1.255。
不能使用 CIDR 块或前缀指定的 IP 地址范围	使用连字符的 IP 地址范围。请**不要**在连字符前后添加空格。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

用于指定 IP 地址或 IP 地址范围的任何其他方法的求反	在 IP 地址、块或范围前面输入感叹号。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

搜索中的受管设备

在使用受管设备作为限制创建搜索时，您可以在 **Device** 搜索条件字段指定以下任一项：

- 受管设备名称、IP 地址或主机名
- 设备组名称
- 设备堆栈名称

- 7000 或 8000 系列设备高可用性对名称

如果系统找到组、设备高可用性对或堆栈的一个匹配项，则系统会用用于执行搜索的相应成员设备名称替换组、设备高可用性对或堆栈名称。在设备字段保存使用了设备组、设备高可用性对或堆栈的搜索时，系统会保存设备字段中指定的名称，并且每次执行搜索时都会再次执行设备名称替换。

搜索中的端口

Firepower 系统接受搜索中端口号的特定语法。可输入：

- 单个端口号
- 用逗号隔开的端口号列表。
- 两个用连字号隔开的端口号，代表端口号范围
- 后接协议缩写、并用正斜杠隔开的端口号（仅限搜索入侵事件时）
- 一个端口号或端口号范围，前面带有感叹号，表示指定端口的求反

注释 指定端口号或范围时，请**不要**使用空格。

表 *266*：端口语法示例

示例	说明
`21`	返回端口 21 上的所有事件，包括 TCP 和 UDP 事件。
`!23`	返回除端口 23 上的事件以外的所有事件。
`25/tcp`	返回端口 25 上的所有与 TCP 相关的入侵事件。
`21/tcp,25/tcp`	返回端口 21 和 25 上所有与 TCP 相关的入侵事件。
`21-25`	返回端口 21 到 25 上的所有事件。

搜索中的事件字段

当搜索事件时，可以使用以下字段作为搜索条件：

- 审核日志工作流程字段，第 1709 页
- 应用数据字段，第 1673 页
- 应用详细信息数据字段，第 1675 页
- 捕获文件字段，第 1605 页

- 白名单事件字段， 第 1700 页
- 连接和安全情报事件字段， 第 1515 页
- 关联事件字段， 第 1696 页
- 发现事件字段， 第 1655 页
- 运行状况事件表， 第 223 页
- 主机属性数据字段， 第 1663 页
- 主机数据字段， 第 1657 页
- 文件和恶意软件事件字段， 第 1586 页
- 入侵事件字段， 第 1541 页
- 规则更新导入日志详细视图， 第 134 页
- 补救状态表字段， 第 1704 页
- Nmap 扫描结果字段， 第 1174 页
- 服务器数据字段， 第 1669 页
- 第三方漏洞数据字段， 第 1682 页
- 用户数据字段， 第 1686 页
- 用户活动数据字段， 第 1691 页
- 漏洞数据字段， 第 1676 页
- 白名单违规事件字段， 第 1702 页

执行搜索

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**分析 (Analysis)** > **搜索 (Search)**。

提示 也可以点击工作流程中任何页面上的**搜索 (Search)**。

步骤 2 从表下拉列表中，选择要搜索的事件或数据的类型。

步骤 3 在相应字段中输入搜索条件；请参阅搜索限制，第 1471 页。

步骤 4 如果要在以后再次使用搜索，请保存搜索，如保存搜索，第 1477 页中所述。

步骤 5 点击**Search**开始搜索。搜索结果出现在正在搜索的表的默认工作流程中，受时间约束（如适用）。

接下来的操作

- 要使用工作流程分析搜索结果，请参阅使用工作流程，第 1442 页。

保存搜索

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，系统会显示在当前域中创建的已保存搜索，您可以对其进行编辑。系统还会显示在祖先域中创建的已保存搜索，您不可以对其进行编辑。要查看和编辑在较低域中创建的搜索，请切换至该域。

开始之前

- 建立搜索条件（如执行搜索，第 1476 页中所述）或加载已保存的搜索（如加载已保存的搜索，第 1478 页中所述）。

过程

步骤 1 从“搜索”(Search)页面中，如果要将搜索另存为专用，以便只有您才能对搜索进行访问，请选中**专用 (Private)** 复选框。

提示 如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 2 此时您有两种选择：

- 如果要保存已加载搜索的新版本，请点击**另存为新项目 (Save As New)**。
- 如果要保存新搜索或使用同一名称覆盖自定义搜索，请点击**保存(Save)**。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

加载已保存的搜索

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，系统会显示在当前域中创建的已保存搜索，您可以对其进行编辑。系统还会显示在祖先域中创建的已保存搜索，您不可以对其进行编辑。要查看和编辑在较低域中创建的搜索，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **搜索 (Search)**。

提示 也可以点击工作流程中任何页面上的**搜索 (Search)**。

步骤 2 从表下拉列表中，选择要搜索的事件或数据的类型。

步骤 3 从**自定义搜索 (Custom Searches)** 列表或**预定义搜索 (Predefined Searches)** 列表中选择要加载的搜索。

步骤 4 如果要使用其他搜索条件，请更改搜索限制。

步骤 5 如果要在以后再次使用更改的搜索，请保存搜索，如保存搜索，第 1477 页中所述。

步骤 6 点击 **Search**。

通过外壳查询覆盖

系统管理员可以使用基于外壳的查询管理工具找到和停止长期查询。

借助于查询管理工具，可找到并停止运行时间超过指定分钟数的查询。停止查询时，此工具会将事件记入审计日志和系统日志。

请注意，只有在本地创建并且在Firepower 管理中心上拥有外壳访问权限的用户才是 `admin` 用户。如果使用授予外壳访问权限的外部身份验证对象，匹配外壳访问过滤器的用户也可以登录外壳。

注释 退出网络界面的搜索页面不会停止查询。需要很长时间才返回结果的查询在运行时会影响总体系统性能。

基于外壳的查询管理语法

使用以下语法管理长期运行的查询：

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 267：*query_manager* 选项

选项	说明
`-h, --help`	打印简短的帮助消息。
`-l, --list [minutes]`	列出所有运行时间超过已用分钟数的查询。默认情况下，将显示所有运行时间超过 1 分钟的查询。
`-k, --kill query_id [...]`	通过传入 ID 终止查询。该选项可使用多个 ID。
`--kill-all minutes`	终止所有运行时间超过已用分钟数的查询。
`-v, --verbose`	包含完整 SQL 查询的详细输出。

注意 外壳访问权应仅限于系统管理员。

停止长期查询

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	`admin` 或其他用户授予的外壳访问权限

过程

步骤 1 通过 `ssh` 连接至Firepower 管理中心。

步骤 2 使用基于外壳的查询管理语法，第 1479 页中所述的语法在 `sudo` 下运行 `query_manager`。

第 81 章

自定义工作流程

以下主题介绍如何使用自定义工作流程：

自定义工作流程简介

如果预定义工作流程和思科提供的自定义工作流无法满足需求，则可以创建并管理自定义工作流程。

自定义工作流程是为满足贵公司的特有需求而创建的工作流程。创建自定义工作流程时，请选择工作流程所基于的事件（或数据库表）类型。在Firepower管理中心中，可以将自定义工作流程基于自定义表。还可以选择自定义工作流程包含的页面；自定义工作流程可以包含向下钻取页面、表视图页面和主机页面或数据包视图页面。

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

提示 可以将自定义工作流程设置为任何事件类型的默认工作流程。

已保存的自定义工作流程

除无法修改的预定义工作流程以外，Firepower管理中心还包含若干已保存的自定义工作流程。其中每个工作流程基于自定义表，并且可以修改。

在多域部署中，这些已保存的工作流程属于全球域，并且不能在较低的域中进行修改。

表 *268*：已保存的自定义工作流程

工作流程名称	说明
Events by Impact, Priority, and Host Criticality	可以使用此工作流程快速选取并关注对于网络重要、当前易受攻击和当前可能受攻击的主机。 此工作流程基于 Intrusion Events with Destination Criticality 自定义表。
Events by Priority and Classification	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。 此工作流程基于 Intrusion Events 自定义表。
Events with Destination, Impact, and Host Criticality	可以使用此工作流程查找对于网络重要且当前易受攻击的主机上的最新攻击。 此工作流程基于 Intrusion Events with Destination Criticality 自定义表。
Hosts with Servers Default Workflow	可以使用此工作流程快速查看 Hosts with Servers 自定义表中的基本信息。 此工作流程基于 Hosts with Servers 自定义表。
Intrusion Events with Destination Criticality Default Workflow	可以使用此工作流程快速查看 Intrusion Events with Destination Criticality 自定义表中的基本信息。 此工作流程基于 Intrusion Events with Destination Criticality 自定义表。
Intrusion Events with Source Criticality Default Workflow	可以使用此工作流程快速查看 Intrusion Events with Source Criticality 自定义表中的基本信息。 此工作流程基于 Intrusion Events with Source Criticality 自定义表。
Server and Host Details	可以使用此工作流程确定哪些服务器在网络上使用最频繁以及哪些主机在运行这些服务器。 此工作流程基于 Hosts with Servers 自定义表。

自定义工作流程的创建

如果预定义工作流程和思科提供的自定义工作流程无法满足需求，则您可以创建自定义工作流程。

提示 可以从其他设备导出自定义工作流程，然后将其导入到设备上，而不是创建新的自定义工作流程。然后，可以编辑已导出工作流程来满足需求。

创建自定义工作流程时，请执行以下操作：

- 选择要作为工作流程源的表
- 提供工作流程名称
- 向工作流程中添加向下钻取页面和表视图页面

对于工作流程中的各向下钻取页面，可以：

- 提供显示在 Web 界面中页面顶部的名称
- 每页包含最多五列
- 指定默认排序顺序（升序或降序）

可以在工作流程页面序列中的任何位置添加表视图页面。它们不具有任何可编辑属性，如页面名称、排序顺序或用户可定义的列位置。

注释 必须向自定义工作流程中添加至少一个向下钻取页面或事件表视图。

注释 如果您选择**漏洞 (Vulnerabilities)** 作为表类型，然后添加 **IP 地址 (IP Address)** 作为表列，则除非使用搜索功能限制工作流程以查看特定 IP 地址或地址块，否则在使用自定义工作流程查看漏洞时不会显示 IP 地址列。

自定义工作流程的最终页面取决于工作流程所基于的表，如下表所述。创建工作流程时，默认情况下会添加这些最终页面。

表 *269*：自定义工作流程最终页面

事件/资产类型	最终页面
发现事件	主机数
漏洞	漏洞详细信息
第三方漏洞	主机数
用户	用户
威胁表现	主机
入侵事件	数据包

系统不是根据其他种类的事件（例如，审核日志或恶意软件事件）向自定义工作流程中添加最终页面。

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同之处在于其中可包括具备连接摘要数据的向下钻取页面、连接数据图形页面、具备单独连接数据的向下钻取页面和表视图页面。

根据非连接数据创建自定义工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义工作流程 (Custom Workflows)**。

步骤 2 点击 **Create Custom Workflow**。

步骤 3 在**名称 (Name)** 字段中输入工作流程的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 从**表 (Table)** 下拉列表中选择要包含的表。

步骤 6 如果要向工作流程中添加一个或多个向下展开页面，请点击**添加页面 (Add Page)**。

步骤 7 在**页面名称 (Page Name)** 字段中输入页面的名称。

步骤 8 在“列 1”(Column 1) 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

示例：
例如，要创建显示所针对的目标端口的页面，并要按计数对页面进行排序，请从**排序优先级 (Sort Priority)** 下拉列表中选择 **2**，并从**字段 (Field)** 下拉列表中选择**目标端口/ICMP 代码 (Destination Port/ICMP Code)**。

步骤 9 继续选择要包含的字段并设置其排序优先级，直至指定要在页面上显示的所有字段。

步骤 10 如果要向工作流程中添加表视图页面，请点击**添加表视图 (Add Table View)**。

步骤 11 点击**保存 (Save)**。

创建自定义连接数据工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同在于可以包含连接数据图形页面以及向下钻取页面和表视图页面。可以按任意顺序在工作流程中包含尽可能多的各类型的页面。每个连接数据图形页面包含单个图形，可以是折线图、条形图或饼图。在折线图和条形图中，可以包含多个数据集。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义工作流程 (Custom Workflows)**。

步骤 2 点击 **Create Custom Workflow**。

步骤 3 在**名称 (Name)** 字段中输入工作流程的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 从**表 (Table)** 下拉列表中，选择**连接事件 (Connection Events)**。

步骤 6 如果要向工作流程中添加一个或多个向下钻取页面，您有两个选择：

- 点击**添加页面 (Add Page)** 以添加包含有关个别连接的数据的向下钻取页面。
- 点击**添加摘要页面 (Add Summary Page)** 以添加包含连接摘要数据的向下钻取页面。

步骤 7 在**页面名称 (Page Name)** 字段中输入页面的名称。

步骤 8 在**列 1 (Column 1)** 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

步骤 9 继续选择要包含的字段并设置其排序优先级，直至指定要在页面上显示的所有字段。

示例：
例如，要创建显示通过受监控网络传输的流量的页面，并要按传输最多流量的响应方对页面进行排序，请从**排序优先级 (Sort Priority)** 下拉列表中选择 **1**，并从**字段 (Field)** 下拉列表中选择**响应方字节数 (Responder Bytes)**。

步骤 10 如果要向工作流程中添加一个或多个图形页面，请点击**添加图形 (Add Graph)**。

步骤 11 在**图形名称 (Graph Name)** 字段中输入页面的名称。

步骤 12 选择要包含在页面上的图形的类型：

- 曲线图 ()
- 条形图 ()
- 饼形图 ()

步骤 13 通过选择图形的 x 轴和 y 轴指定要图形化的数据种类。
在饼图中，x 轴表示独立变量，y 轴表示因变量。

步骤 14 选择要包含在图形中的数据集。
请注意，饼形图只能包含一个数据集。

步骤 15 如果要添加连接数据的表视图，请点击**添加表视图 (Add Table View)**。
表视图不可配置。

步骤 16 点击**保存 (Save)**。

自定义工作流程使用和管理

用于查看工作流程的方法取决于工作流程是基于其中一个预定义事件表还是基于自定义表。

如果自定义工作流程基于预定义事件表，请以与访问设备随附的工作流程相同的方式对其进行访问。例如，要根据“主机”(Hosts) 表访问自定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **主机 (Hosts)**。另一方面，如果自定义工作流程基于自定义表，则必须从 Custom Tables 页面对其进行访问。

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

提示 可以将自定义工作流程设置为任何事件类型的默认工作流程。

根据预定义表查看自定义工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员/任何安全分析师（根据工作流程而定）

过程

步骤 1 为自定义工作流程所基于的表选择适当的菜单路径和选项，如工作流程选择，第 1444 页中所述。

步骤 2 要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的**切换工作流程 (switch workflow)**。

步骤 3 如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅事件时间限制，第 1458 页。

根据自定义表查看自定义工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，系统会显示在当前域中创建的自定义工作流程，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义工作流程，您不可以对其进行编辑。要查看和编辑较低域中的自定义工作流程，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 2 点击要查看的自定义表旁边的查看图标 ( )，或者点击自定义表的名称。

步骤 3 要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的 **(switch workflow)**。

步骤 4 如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅事件时间限制，第 1458 页。

编辑自定义工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，系统会显示在当前域中创建的自定义工作流程，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义工作流程，您不可以对其进行编辑。要查看和编辑较低域中的自定义工作流程，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义工作流程 (Custom Workflows)**。

步骤 2 点击要编辑的工作流程名称旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 对工作流程进行所需的任何更改。

步骤 4 点击**保存 (Save)**。

第 82 章

自定义表格

以下主题介绍如何使用自定义表：

自定义表简介

Firepower 系统收集有关网络的信息时，Firepower 管理中心 会将这些信息存储在一系列数据库表中。当您使用工作流程查看生成的信息时，Firepower 管理中心会从其中一个表提取数据。例如，Network Applications by Count 工作流程的每个页面的列取自 Applications 表中的字段。

如果您确定通过组合不同表中的字段会增强对网络上活动的分析，则可创建自定义表。例如，可以将预定义 Host Attribute 表中的主机重要性信息与预定义 Connection Data 表中的字段进行组合，然后在新的上下文中检查连接数据。

请注意，您可以为预定义表或自定义表创建自定义工作流程。

预定义的自定义表

自定义表包含两个或多个预定义表中的字段。Firepower 系统随附多个系统定义的自定义表，但是，您可以创建其他仅包含符合自身特定需求的信息的自定义表。

例如，Firepower 系统随附用于将入侵事件数据与主机数据相关联的系统定义的自定义表，因此，您可以搜索会影响关键系统的事件并在一个工作流程中查看搜索结果。

在多域部署中，预定义的自定义表属于全局域，不能在低层域中进行修改。

下表介绍系统随附的自定义表。

表 *270*：系统定义的自定义表

表	说明
Hosts with Servers	包含 Hosts 和 Servers 表中的字段，提供有关检测到的在网络上运行的应用的信息，以及有关运行这些应用的主机的基本操作系统信息。
Intrusion Events with Destination Criticality	包含 Intrusion Events 表和 Hosts 表中的字段，提供有关入侵事件的信息，以及每个入侵事件涉及的目标主机的主机重要性。 使用此表可搜索涉及主机重要性高的目标主机的入侵事件。
Intrusion Events with Source Criticality	包含 Intrusion Events 表和 Hosts 表中的字段，提供有关入侵事件的信息，以及每个入侵事件涉及的源主机的主机重要性。 使用此表可搜索涉及主机重要性高的源主机的入侵事件。

可能的表组合

创建自定义表时，可以组合具有相关数据的预定义表中的字段。下表列出了可以组合创建新的自定义表的预定义表。请记住，您可以创建将两个以上的预定义自定义表中的字段进行组合的自定义表。

表 *271*：自定义表组合

可以将这些表中的字段...	与这些表中的字段进行组合...
应用	• 相关事件 • 入侵事件 • Connection Summary Data • Host Attributes • 应用详情 • Discovery Events • 连接事件 • 主机数 • 服务器 • White List Events
相关事件	• 应用 • Host Attributes • 主机数

可以将这些表中的字段...	与这些表中的字段进行组合...
入侵事件	• 应用 • Host Attributes • 主机数 • 服务器
Connection Summary Data	• 应用 • Host Attributes • 主机数 • 服务器
危害表现	• 应用 • 应用详情 • 捕获的文件 • 连接事件 • Connection Summary Data • 相关事件 • Discovery Events • Host Attributes • 主机数 • 入侵事件 • Security Intelligence Events • 服务器 • White List Events

可以将这些表中的字段...	与这些表中的字段进行组合...
Host Attributes	• 应用 • 相关事件 • 入侵事件 • Connection Summary Data • 应用详情 • Discovery Events • 连接事件 • 主机数 • 服务器 • White List Events
应用详情	• 应用 • Host Attributes • 主机数
Discovery Events	• 应用 • Host Attributes • 主机数
连接事件	• 应用 • Host Attributes • 主机数 • 服务器
Security Intelligence Events	• 应用 • Host Attributes • 主机数 • 服务器

可以将这些表中的字段...	与这些表中的字段进行组合...
主机数	• 应用 • 相关事件 • 入侵事件 • Connection Summary Data • Host Attributes • 应用详情 • Discovery Events • 连接事件 • 服务器 • White List Events
服务器	• 应用 • 入侵事件 • Connection Summary Data • Host Attributes • 连接事件 • 主机数
White List Events	• 应用 • Host Attributes • 主机数

有时，一个表中的字段会映射到另一个表中的多个字段。例如，预定义的 **Intrusion Events with Destination Criticality** 自定义表将 Intrusion Events 表和 Hosts 表中的字段进行组合。Intrusion Events 表中的每个事件具有两个与其关联的 IP 地址：源 IP 地址和目标 IP 地址。但是，Hosts 表中的每个“事件”表示单个主机 IP 地址（主机可能有多个 IP 地址）。因此，根据“入侵事件”(Intrusion Events) 表和“主机”(Hosts) 表创建自定义表时，必须选择从“主机”(Hosts) 表显示的数据适用于“入侵事件”(Intrusion Events) 表中的主机源 IP 地址还是主机目标 IP 地址。

创建新的自定义表时，会自动创建显示表中所有列的默认工作流程。此外，如同预定义表一样，您可以搜索自定义表来获取要在网络分析中使用的数据。您还可以根据自定义表生成报告，就像使用预定义表时一样。

用户定义的自定义表

提示 可以从另一个Firepower 管理中心导出自定义表，然后将其导入到您的Firepower 管理中心，而不是创建新的自定义表。

要创建自定义表，请确定 Firepower 系统随附的哪些预定义表含有要在自定义表中包含的字段。然后，可以选择要包含的字段，如有必要，请为所有公共字段配置字段映射。

提示 借助涉及 Hosts 表的数据，可以查看与来自一台主机的所有 IP 地址而不是一个特定 IP 地址相关的数据。

例如，不妨考虑将 Correlation Events 表和 Hosts 表中的字段组合起来以创建自定义表。通过这样的自定义表，您可以获取有关涉及任何关联策略违例的主机的详细信息。请注意，您必须决定从Hosts 表显示与 Correlation Events 表中的源 IP 地址还是目标 IP 地址匹配的数据。

如果查看此自定义表的事件表视图，则它会显示相关性事件（每行一个）。可以将自定义表配置为包含以下信息：

- 事件的生成日期和时间
- 违例的关联策略的名称
- 触发违例的规则的名称
- 与相关性事件中涉及的源主机（又称为发起主机）相关的 IP 地址
- 源主机的 NetBIOS 名称
- 源主机运行的操作系统和版本
- 源主机的关键性

提示 可以创建类似的自定义表来显示目标主机（又称为响应主机）的以上信息。

创建自定义表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何角色/管理员

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 2 点击 **Create Custom Table**。

步骤 3 在**名称 (Name)** 字段中，输入自定义表的名称。

示例：
例如，您可输入 `Correlation Events with Host Information (Src IP)`。

步骤 4 从**表 (Tables)** 下拉列表中，选择**关联事件 (Correlation Events)**。

步骤 5 在**字段 (Fields)** 下，选择**时间 (Time)** 并点击**添加 (Add)** 以添加生成关联事件的日期和时间。

步骤 6 重复第 5 步以添加**策略 (Policy)** 和**规则 (Rule)** 字段。

提示 按住 Ctrl 或 Shift 键并点击可选择多个字段。也可以点击并拖动以选择多个相邻值。但是，如果要指定字段在与表关联的事件表视图中的出现顺序，请一次添加一个字段。

步骤 7 从**表 (Tables)** 下拉列表中，选择**主机 (Hosts)**。

步骤 8 向自定义表添加 **IP 地址 (IP Address)**、**NetBIOS 名称 (NetBIOS Name)**、**OS 名称 (OS Name)**、**OS 版本 (OS Version)** 和**主机重要性 (Host Criticality)** 字段。

步骤 9 在**通用字段 (Common Fields)** 下的**关联事件 (Correlation Events)** 旁边，选择**源 IP (Source IP)**。这样，自定义表即配置为显示在第 8 步中选择的有关相关性事件中涉及的源主机（又称为发起主机）的主机信息。

提示 可以按照以上步骤创建显示有关相关性事件中涉及的目标主机（又称为响应主机）的主机详细信息的自定义表，但在操作过程中应选择**目标 IP (Destination IP)** 而不是**源 IP (Source IP)**。

步骤 10 点击**保存 (Save)**。

修改自定义表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何角色/管理员

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义表，您不可以对其进行编辑。要查看和编辑较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 2 点击要编辑的表旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 或者，点击要删除的字段旁边的删除图标 ( )，从表中删除字段。

注释 如果删除报告中当前正在使用的字段，则系统将提示您确认是否要删除使用这些报告中的这些字段的部分。

步骤 4 根据需要进行其他更改。

步骤 5 点击**保存 (Save)**。

删除自定义表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何角色/管理员

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行删除。系统还会显示在祖先域中创建的自定义表，您不可以对其进行删除。要删除较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 2 点击要删除的自定义表旁边的删除图标 ( )。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

根据自定义表查看工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何角色/管理员

创建自定义表时，系统会自动为其创建默认工作流程。默认工作流程的第一页显示事件表视图。如果在自定义表中包含入侵事件，则工作流程的第二页是数据包视图。否则，工作流程的第二页是主机页面。您也可以根据自定义表创建自己的自定义工作流程。

提示 根据某个自定义表创建自定义工作流程后，可以将创建的自定义工作流程指定为该自定义表的默认工作流程。

您可以使用相同方法查看自定义表中根据预定义表用于事件视图的事件。

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义表，您不可以对其进行编辑。要查看和编辑较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 2 点击与要查看的工作流程有关的自定义表旁边的查看图标 ( )。

搜索自定义表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任何角色/管理员

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义表，您不可以对其进行编辑。要查看和编辑较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 2 点击要搜索的自定义表旁边的查看图标 ( )。

提示 要使用不同的工作流程（包括自定义工作流程），请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])**。

步骤 3 点击 **Search**。

提示 要在数据库中搜索不同类型的事件或数据，请从表下拉列表中进行选择。

步骤 4 在相应的字段中输入搜索条件。
如果您输入多个字段的条件，搜索只返回符合所有字段指定搜索条件的记录。

提示 点击搜索字段旁边的对象图标 ( ) 可将对象用作搜索条件。

步骤 5 如果您计划保存搜索，也可以选中**私有 (Private)** 复选框将搜索另存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示 如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 6 或者，您可以保存搜索，以备以后使用。您有以下选择：

- 点击 **Save**，保存搜索条件。如果选中**私有 (Private)** 复选框，则该搜索只对您的帐户显示。

- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。如果选中**私有 (Private)** 复选框，则该搜索保存成功并只对您的帐户显示。

步骤 7 点击 **Search** 开始搜索。

搜索结果显示在自定义表的默认工作流程中，通过当前时间范围（如适用）进行约束。

第 XXI 部分

事件和资产

第 83 章

连接日志记录

以下主题介绍如何配置 Firepower 系统以记录由受监控网络上的主机进行的连接：

连接日志记录简介

系统可以生成其受管设备检测到的连接的日志。这些日志称为连接事件。规则和策略中的设置可供您精细控制记录的连接、记录连接的时间以及存储数据的位置。特殊连接事件称为安全情报事件，代表被基于信誉的安全情报功能列入黑名单（阻止）的连接。

连接事件包含关于检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等
- 有关连接记录原因的元数据：哪个配置处理流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等

注释 您可以用导出的 NetFlow 记录生成的连接数据补充您的受管设备收集的连接日志。这在 Firepower 系统受管设备无法监控的网络上部署支持 NetFlow 的路由器或其他设备时尤为有用。

连接日志记录策略

根据您的组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

提示 要对连接数据执行详细分析，思科建议您将关键连接的结束事件记录到 Firepower 管理中心数据库中。

由于系统可能会因为多种原因记录连接，因此禁用某一处的日志记录不能确保匹配连接不会被记录。此外，除非禁用连接事件存储，否则系统将自动记录某些连接；例如，与检测到的文件、恶意软件、入侵和智能应用绕行 (IAB) 关联的连接。

您无法记录使用 8000 快速路径规则实现快速路径的连接。

可配置的连接日志记录

要仅记录关键连接，可以逐条规则启用连接日志记录。如果为某条规则启用连接日志记录，则系统会记录该规则处理的所有连接。

您还可以记录策略默认操作处理的连接。根据规则或默认策略操作（以及针对访问控制的规则检查配置），您的日志记录选项可能有所不同。

SSL 策略：规则和默认操作

您可以记录匹配 SSL 规则或 SSL 策略默认操作的连接。

对于受阻连接，系统会立即结束会话并生成事件。对于受监控连接以及您将其传递到访问控制规则的连接，系统会在会话结束时生成事件。

访问控制策略：安全情报决策

只要基于信誉的安全情报功能阻止连接或将其接列入黑名单，您就可以对该连接进行记录。

或者，您可以像被动部署中建议的那样，使用仅监控设置进行安全情报过滤。这使得系统可以进一步分析本应列入黑名单的连接，并仍将匹配项记录至黑名单。安全情报监控还允许您使用安全情报信息创建流量配置文件。

当系统由于安全情报过滤而记录连接事件时，它也会记录匹配的安全情报事件，这是一种您可以单独查看和分析的特殊类型连接事件，而且可以单独存储和删除。因此，您可以确定连接中列入黑名单的 IP 地址，列入黑名单和受监控的 IP 地址旁边的主机图标在事件查看器中看上去稍有不同。

访问控制策略：规则和默认操作

您可以记录匹配访问控制规则或访问控制策略默认操作的连接。

自动连接日志记录

除非禁用连接事件存储，否则系统会将以下连接结束事件自动保存到Firepower管理中心数据库，不考虑任何其他日志记录配置。

与入侵关联的连接

除非通过访问控制策略的默认操作处理连接，否则系统会自动记录与入侵事件关联的连接。

当与访问控制默认操作关联的入侵策略生成入侵事件时，系统**不会**自动记录相关连接终止事件。相反，您必须明确启用默认操作连接日志记录。对于不想记录任何连接数据的仅入侵防御部署，这十分有用。

如果启用了默认操作的连接开始日志记录，这一规则将不适用。在这种情况下，当关联的入侵策略触发时，除了记录连接开始事件外，系统还**会**日志记录连接结束事件。

与文件和恶意软件事件关联的连接

系统会自动记录与文件和恶意软件事件关联的连接。

注释 通过检查 NetBIOS-ssn (SMB) 流量生成的文件事件不会立即生成连接事件，因为客户端和服务器建立持久连接。系统在客户端或服务器结束会话后生成连接事件。

与智能应用绕行关联的连接

系统会自动记录与 IAB 关联的已绕行和将绕行的连接。

连接开始和连接结束日志记录

您可以在连接开始或结束时记录该连接，对于受阻流量，下列情况除外：

- 受阻流量 - 由于会立即拒绝受阻流量而不进一步检查，因此通常您只能记录受阻流量或列入黑名单的流量的连接开始事件。没有要记录的唯一连接结束。
- 受阻加密流量 - 当在 SSL 策略中启用连接日志记录时，系统会记录连接结束而不是连接开始事件。这是因为，系统无法确定连接是否使用会话中第一个数据包加密，因此无法立即阻止已加密会话。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。出于任何原因监控连接都会强制执行连接结束日志记录。对于单个未被阻止的连接，连接终止事件包含连接开始事件中的所有信息，以及在会话期间收集到的信息。

下表详细列出了连接开始和连接终止事件之间的差异，包括相比于记录每种事件的优势。

表 *272*：比较连接开始和连接结束事件

	连接开始事件	连接终止事件
生成时间…	当系统检测到连接开始（或者在前几个数据包之后，如果事件生成取决于应用或 URL 识别）	当系统： • 检测到连接关闭 • 在一段时间后未检测到连接结束 • 由于内存限制，无法再跟踪会话
记录对象...	除受到 SSL 策略阻止以外的所有连接	所有连接，不过您可能无法在所有位置都配置连接结束日志记录
包含...	仅在第一个数据包中可以确定的信息（或者前几个数据包，如果事件生成取决于应用或 URL 识别）	连接开始事件中的所有信息，以及在会话期间通过检测流量确定的信息，例如，传输的总数据量或者连接中最后一个数据包的时间戳
十分有用…	如果您想要记录： • 受阻连接 • 仅连接的开始，因为连接结束信息对您无关紧要	如果要： • 记录由 SSL 策略处理的加密连接 • 使用在会话期间收集的信息执行任何类型的详细分析或者触发关联规则 • 查看自定义工作流程中的连接摘要（汇聚连接数据），查看图形格式的连接数据，或者创建并使用流量量变曲线

Firepower 管理中心与外部日志记录

您可以将连接和安全情报事件记录到Firepower管理中心数据库中（在Web界面的**事件查看器 [Event Viewer]**中）。Firepower管理中心可以存储的事件数取决于其型号。您还可以使用所配置的连接（称为警报响应）将事件记录到外部系统日志或 SNMP 陷阱服务器。

通过记录到 Firepower 管理中心数据库，您可以利用 Firepower 系统的很多报告、分析和数据关联功能。例如：

- 控制面板和情景管理器为您提供由系统记录的连接的图形化概览视图。
- 事件视图显示有关系统记录的连接的详细信息，您可以用图形或表格格式显示这些信息，也可以在报告中将其汇总。
- 流量分析使用连接数据创建正常网络流量的配置文件，然后您可以将其用作检测和跟踪异常行为的基准。

- 通过关联策略，您可以生成事件并触发对特定类型的连接或流量量变曲线更改的响应（例如警报或外部补救）。

注释 要使用这些功能，**必须**将连接记录到Firepower 管理中心数据库（而且在大多数情况下，必须记录连接结束而非开始事件）。这就是为什么系统自动记录关键连接，即与记录的入侵、受禁文件和恶意软件关联的那些链接。

操作与连接日志记录

配置连接日志记录时，规则操作和策略默认操作不仅可以确定系统如何检查和处理匹配流量，而且可以确定您何时及如何记录匹配流量的相关详细信息。连接事件包含有关连接记录原因的元数据，包括哪些配置处理流量。

受监控连接的日志记录

系统始终记录与以下配置匹配的流量的连接结束事件，即使流量与其他规则都不匹配且您没有启用默认操作日志记录：

- 安全情报 - 设为监控的黑名单（也生成安全情报事件）
- SSL 规则 - **监控 (Monitor)** 操作
- 访问控制规则 - **监控 (Monitor)** 操作

系统不会在每次单个连接匹配“监控”(Monitor) 规则时都成一个单独的事件。由于单一连接可能与多条“监控”(Monitor) 规则相匹配，每个连接事件均可能包含和显示关于该连接匹配的前八条监控访问控制规则，以及第一条匹配的 SSL 监控规则的信息。

同样，如果您将连接事件发送至外部系统日志或 SNMP 陷阱服务器，则每当单一连接与监控规则相匹配时，系统均不会发送单独的警报。相反，系统在连接终止时发送的警报包含有关连接匹配的监控规则的信息。

受信任连接的日志记录

您可以记录受信任连接的开始和结束，包括匹配以下规则和操作的流量：

- 访问控制规则 - **信任 (Trust)** 操作
- 访问控制默认操作 - **信任所有流量 (Trust All Traffic)**

受信任的连接不会受到深入检查或发现，因此受信任连接的连接事件包含的信息有限。

系统以不同方式记录“信任”(Trust) 访问控制规则处理的 TCP 连接，具体取决于检测到相关连接的设备：

- 对于 7000 和 8000 系列设备，Trust 规则在第一个数据包中检测到的 TCP 连接会根据是否存在之前启用的 Monitor 规则生成不同的事件。如果 Monitor 规则处于活动状态，则系统评估数据

包并生成连接开始和结束事件。如果没有 Monitor 规则处于活动状态，则系统仅生成连接结束事件。

- 对于所有其他型号，Trust 规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统会在最终会话数据包之后一小时生成事件。

受阻连接的日志记录

您可以记录受阻连接，这包括与以下规则和操作匹配的流量：

- 安全情报 - 设为阻止的黑名单（也生成安全情报事件）
- SSL 规则 - **阻止 (Block)** 和**阻止并重置 (Block with reset)**
- SSL 默认操作 - **阻止 (Block)** 和**阻止并重置 (Block with reset)**
- 访问控制规则 - **阻止 (Block)**、**阻止并重置 (Block with reset)** 和**交互式阻止 (Interactive Block)**
- 访问控制默认操作 - **阻止所有流量 (Block All Traffic)**

仅内联部署的设备（即使用已路由、已交换或透明接口或内联接口对）可以阻止流量。因为阻止的连接实际上在被动部署中并未被阻止，所以系统可能针对每个被阻止的连接报告多个连接开始事件。

注意 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。对 Block 规则启用日志记录之前，考虑此规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口的流量。

受阻连接的连接开始和连接结束的日志记录

当您记录受阻连接时，系统如何进行记录该连接取决于其受阻原因；当根据连接日志配置关联规则时，必须记住这一点：

- 对于阻止已加密流量的SSL规则和SSL策略默认操作，系统记录连接**结束**事件。这是因为系统无法确定连接是否使用会话中的第一个数据包加密。
- 对于其他阻止操作，系统会记录连接**开始**的事件。匹配流量会被拒绝，无需进一步检测。

绕行交互式阻止的日志记录

当用户浏览受禁网站时，交互式阻止访问控制规则导致系统显示警告页面，该等规则可供您配置连接结束日志记录。这是因为，如果用户点击浏览警告页面，该连接会被视为系统可以监控和记录并且允许访问的新连接。

因此，对于与交互式阻止或包含重置规则的交互式阻止相匹配的数据包，系统可以生成以下连接事件：

- 用户的请求最初被阻止且显示警告页面时的连接开始事件；该事件的关联操作为 `Interactive Block` 或 `Interactive Block with reset`

- 当用户点击警告页面并加载最初请求的页面时生成的多个连接开始或连接终止事件；这些事件的关联操作为 `Allow`，原因为 `User Bypass`

允许连接的日志记录

您可以记录允许连接，这包括与以下规则和操作匹配的流量：

- SSL 规则 - **解密 (Decrypt)** 操作
- SSL 规则 - **不解密 (Do not Decrypt)** 操作
- SSL 默认操作 - **不解密 (Do not Decrypt)**
- 访问控制规则 - **允许 (Allow)** 操作
- 访问控制默认操作 - **仅限网络发现 (Network Discovery Only)** 以及任何入侵防御选项

为这些配置启用日志记录可确保连接已记录，同时也允许（或指定）下一阶段的检查和流量处理。SSL 日志记录始终在连接结束时进行；访问控制配置也允许在连接开始时进行日志记录。

当您通过访问控制规则或默认操作允许流量时，可以使用相关入侵策略进一步检查流量和阻止入侵。对于访问控制规则，您也可以使用文件策略检测和阻止被禁止的文件，包括恶意软件。除非禁用连接事件存储，否则系统将自动记录大多数与入侵、文件和恶意软件事件关联的允许连接。有关详细信息，请参阅自动连接日志记录，第 1503 页。请注意，具有加密负载的连接不进行深度检查，因此加密连接的连接事件包含有限信息。

允许连接的文件和恶意软件事件日志记录

当文件策略检测或阻止文件时，它会将以下事件之一记录到 Firepower 管理中心数据库：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件
- 可追溯的恶意软件事件，其在之前检测到的文件的恶意软件性质变更时生成

您可以以每个访问控制规则为基础禁用此日志记录。或者完全禁用文件和恶意软件事件存储。

注释 思科建议您保持启用文件和恶意软件日志记录。

使用 SSL 规则记录可解密连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何设备，除了 NGIPSv	任意	管理员/访问管理员/网络管理员

过程

步骤 1 在 SSL 策略编辑器中，点击要配置日志记录的规则旁边的编辑图标 ( )。
如果改为显示查看图标 ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 点击**日志记录 (Logging)** 选项卡。

步骤 3 选中**在连接结束时记录 (Log at End of Connection)**。
对于受监控流量，需要连接结束日志记录。

步骤 4 指定将连接事件发送至何处。
如果要对这些连接事件执行基于Firepower管理中心的分析，请将事件发送到事件查看器。对于受监控流量，需要执行此操作。

步骤 5 点击 **Save** 保存规则。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

使用安全情报记录连接

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/访问管理员/网络管理员

过程

步骤 1 在访问控制策略编辑器中，点击**安全情报 (Security Intelligence)** 选项卡。

步骤 2 点击日志记录图标 ( ) 以使用以下条件启用安全情报日志记录：

- 按 IP 地址 - 点击**网络 (Networks)** 旁边的日志记录图标。
- 按 URL - 点击 **URL** 旁边的日志记录图标。
- 按域名 - 点击 **DNS 策略 (DNS Policy)** 下拉列表旁边的日志记录图标。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 3 选中**记录连接 (Log Connections)** 复选框。

步骤 4 指定要将连接和安全情报事件发送到何处。
如果要执行基于Firepower管理中心的分析，或者如果要将列入黑名单的对象设置为仅监控，请将事件发送到事件查看器。

步骤 5 点击**确定 (OK)** 以设置日志记录选项。

步骤 6 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

使用访问控制规则记录连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

根据您选择的规则操作和深度检查选项，您的日志记录选项会有所不同；请参阅操作与连接日志记录，第 1505 页。

过程

步骤 1 在访问控制策略编辑器中，点击要配置日志记录的规则旁边的编辑图标 ()。
如果改为显示查看图标 ()，则表明配置从祖先策略继承或属于祖先域，或者您没有修改配置的权限。

步骤 2 点击**日志记录 (Logging)** 选项卡。

步骤 3 指定您是否想要选择 **Log at Beginning of Connection** 还是选择 **Log at End of Connection**。
要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。

步骤 4 （可选）选中**记录文件 (Log Files)** 复选框以记录与连接关联的文件和恶意软件事件。
思科建议您将此选项保留为已启用。

步骤 5 指定将连接事件发送至何处。
如果要对这些连接事件执行基于管理中心的分析，或者如果规则操作为**监控 (Monitor)**，则将事件发送到 Firepower 管理中心。

步骤 6 点击 **Save** 保存规则。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

使用策略默认操作记录连接

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

策略的默认操作确定系统如何处理与策略中所有规则均不匹配的流量（“监控”[Monitor]规则除外，这些规则匹配和记录流量，但不处理或检测流量）。

SSL 策略默认操作的记录设置还监管系统如何记录无法解密的会话。

过程

步骤 1 在策略编辑器中，点击**默认操作 (Default Action)** 下拉列表旁边的记录图标 ( )。

步骤 2 指定要记录匹配连接的时间：

- “在连接开始时记录”(Log at Beginning of Connection) - SSL 默认操作不支持。
- “在连接结束时记录”(Log at End of Connection) - 如果选择访问控制**阻止所有流量 (Block All Traffic)** 默认操作，则不受支持。

要优化性能，请记录所有连接的开始或终止，而不是同时记录两者。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。在访问控制策略中，也可从祖先策略继承配置。

步骤 3 指定将连接事件发送至何处。
如果要对这些连接事件执行基于 Firepower 管理中心的分析，请将事件发送到事件查看器。

步骤 4 点击 **OK**。

步骤 5 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

限制长 URL 的日志记录

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/访问管理员/网络管理员

HTTP 流量的连接结束事件会记录受监控主机所请求的 URL。禁用或限制存储的 URL 字符数可提高系统性能。禁用 URL 日志记录（存储零字符）不会影响 URL 过滤。尽管系统不会记录流量，但会根据请求的 URL 过滤流量。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)** 选项卡，然后点击**常规设置 (General Settings)** 旁边的编辑图标 ( )。

如果改为显示查看图标 ( )，则表明配置从祖先策略继承或属于祖先域，或者您没有修改配置的权限。如果配置已解锁，请取消选中**从基本策略继承 (Inherit from base policy)** 以启用编辑。

步骤 2 输入**要在连接事件中存储的最大 URL 字符数 (Maximum URL characters to store in connection events)**。

步骤 3 点击 **OK**。

步骤 4 点击 **Save** 保存策略。

接下来的操作

- 部署配置更改；请参阅部署配置更改，第 254 页。

第 84 章

连接事件和安全情报事件

以下主题介绍如何使用连接事件和安全事件表。

关于连接事件

系统可以生成其受管设备检测到的连接的日志。这些日志称为连接事件。规则和策略中的设置可供您精细控制记录的连接、记录连接的时间以及存储数据的位置。特殊连接事件称为安全情报事件，代表被基于信誉的安全情报功能列入黑名单（阻止）的连接。有关详细信息，请参阅连接日志记录，第 1501 页。

连接事件和安全情报事件

安全情报事件是一个当会话被列入黑名单（加以阻止）或被基于信誉的安全情报功能监控时生成的连接事件。

但是，对于每个安全情报事件，会存在可单独查看和分析安全情报事件的相同连接事件。系统还会单独地存储和删除安全情报事件。

注释 在本指南中，除非另行说明，否则有关连接事件的信息也与安全情报事件有关。

NetFlow 连接

要补充受管设备收集到的连接数据，可以使用 NetFlow 导出器广播的记录来生成连接事件。这在 NetFlow 导出器监控的网络不同于受管设备监控的网络时尤为有用。

系统会将NetFlow记录记录为Firepower管理中心数据库中的单向连接结束事件。这些连接的可用信息与访问控制策略检测到的连接略有不同；请参阅NetFlow和受管设备数据之间的差异，第1128页。

连接摘要（图形的汇聚数据）

Firepower系统会将在五分钟间隔内收集到的数据汇聚为连接摘要，供系统用于生成连接图形和流量量变曲线。或者，您可以基于连接摘要数据创建自定义工作流程，并以与基于单个连接事件的工作流程相同的方式来使用此类工作流程。

请注意，尽管相应的连接结束事件可以汇总到连接摘要数据中，但安全情报事件无任何特定的连接摘要。

多个连接必须满足以下条件才能汇总到连接摘要：

- 表示连接结束
- 具有相同的源 IP 地址和目标 IP 地址，并在响应方（目标）主机上使用相同的端口
- 使用相同的协议（TCP 或 UDP）
- 使用相同的应用协议
- 由同一 Firepower 系统受管设备或由同一 NetFlow 导出器检测

每份连接摘要都包括总流量统计信息，以及摘要中连接的数量。由于NetFlow导出器生成单向连接，因此对于基于 NetFlow 数据的每个连接而言，摘要的连接计数按 2 递增。

请注意，连接摘要中并未包含与摘要中汇总的连接相关联的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

长期运行连接

如果汇总连接数据的受控会话跨越两个或多个 5 分钟时间间隔，那么该连接可视为长期运行连接。当计算连接摘要中的连接数时，系统仅累加启动长期运行连接的 5 分钟间隔内的连接数。

此外，当计算由长期运行连接中的发起方和响应方传输的数据包和字节数时，系统并不会报告每 5 分钟间隔中实际传输的数据包和字节数。相反，系统会假定一个固定传输比率，并基于传输的数据包和字节总数、连接长度及每 5 分钟间隔内发生的连接部分计算预估数字。

源于外部响应方的组合连接摘要

要减少存储连接数据所需的空间并加快连接图的绘制，系统将在下列情况下合并连接摘要：

- 连接中涉及的其中一台主机并不在监控网络中
- 除外部主机的 IP 地址以外，摘要中的连接还满足摘要汇聚条件

当在事件查看器中查看连接摘要并使用连接图时，系统将显示外部 IP 地址而非未监控主机的 IP 地址。

由于执行汇总的缘故，如果您尝试从涉及外部响应方的连接摘要或连接图钻取到连接数据的表视图（即，访问单个连接的数据），该表视图将不包含任何信息。

连接和安全情报事件字段

可以使用表格和图形工作流程查看及搜索的连接和安全情报事件包含下述字段。请记住，可用于任何单个事件的信息可能会根据系统记录连接的方式、原因和时间而异。

注释 对于每个安全情报事件，都有相同、独立存储的连接事件。所有安全情报事件都具有已填充的**安全情报类别 (Security Intelligence Category)** 字段。

由于连接图基于连接摘要，因此，约束连接摘要的相同标准也约束连接图。搜索页面上标有星号 (*) 的字段会限制连接图形和连接摘要。如果使用无效搜索限制来搜索连接摘要，并在自定义工作流程中使用连接摘要页面查看结果，则无效限制会标记为不适用 (N/A)，并标有删除线。

一般信息

访问控制策略

监控连接的访问控制策略。

Access Control Rule

处理连接的访问控制规则或默认操作，以及最多 8 条该连接匹配的监控规则。

如果连接与一个监控规则匹配，则 Firepower 管理中心显示已处理连接的规则的名称，后跟监控规则名称。如果连接匹配多个监控规则，则事件查看器显示所匹配的监控规则数量，例如，`Default Action + 2 Monitor Rules`。

要显示包含与连接匹配的前 8 个监控规则的列表的弹出窗口，请点击***N*个监控规则 (N Monitor Rules)**。

操作

与已记录连接的配置关联的操作。

对于受安全情报监控的连接，该项操作即为由连接触发的第一个非监控访问控制规则的操作，或者为默认操作。同样，由于与监控规则匹配的流量始终由后续规则或通过默认操作进行处理，因此与因监控规则而记录的连接相关联的操作绝不会是“监控”(Monitor)。不过，您仍然可以在与监控规则匹配的连接上触发关联策略违规。

操作	描述
允许	通过访问控制明确允许或者由于用户绕过交互式阻止而允许的连接。
阻止、阻止并重置	受阻连接，包括： • 被安全情报列入黑名单的连接 • 按 SSL 策略阻止的加密连接 • 漏洞按入侵策略阻止的连接 • 文件（包括恶意软件）按文件策略阻止的连接 对于系统阻止入侵或文件的连接，即使使用访问控制“允许”(Allow) 规则调用深度检查，系统也将显示 `Block`。
交互式阻止、交互式阻止并重置	在系统最初使用“交互式阻止”(Interactive Block) 规则阻止用户的 HTTP 请求时记录的连接。如果用户点击浏览系统显示的警告页面，则为会话记录的其他连接会执行操作“允许”(Allow)。
信任	访问控制信任的连接。系统根据设备型号以不同方式记录受信任 TCP 连接；请参阅受信任连接的日志记录，第 1505 页。
默认操作	访问控制策略的默认操作处理的连接。

连接

连接摘要中的连接数。对于长期运行连接，即跨越多个连接摘要间隔的连接，只有第一个连接摘要间隔可递增。要使用**连接 (Connections)** 条件查看有意义的搜索结果，请使用具有连接摘要页面的自定义工作流程。

计数

与每行显示的信息相匹配的连接数。请注意，仅当您应用创建了两个或多个相同行的约束之后，系统才显示**Count**字段。如果创建了自定义工作流程，但未在向下钻取页面中添加**Count**列，则每个连接都将单独列出，且数据包和字节并不汇总。

终端位置 (Endpoint Location)

使用 ISE 对用户进行身份验证的网络设备的 IP 地址，如 ISE 所识别。

Endpoint Profile

用户的终端设备类型，如 ISE 所识别。

First Packet or Last Packet

查看会话的第一个或最后一个数据包的日期和时间。

发起方/响应方字节数 (Initiator/Responder Bytes)

由会话发起方或会话响应方发送的总字节数。

发起方/响应方数据包数 (Initiator/Responder Packets)

会话发起方发送的数据包总数。

发起方用户 (Initiator User)（限制摘要和图形）

登录到会话发起方的用户。

IOC

事件是否针对连接中涉及的主机触发了危害表现 (IOC)。

Network Analysis Policy

与事件生成相关的网络分析策略 (NAP)（如果有）。

Reason

在许多情况下记录连接的一个或多个原因。有关完整列表，请参阅连接事件原因，第 1527 页。

原因为“IP 阻止”(IP Block)、“DNS 阻止”(DNS Block) 和“URL 阻止”(URL Block) 的连接在每个唯一发起方-响应方对中的阈值都为 15 秒。系统在阻止其中一个连接后，无论端口或协议如何，在接下来的 15 秒内都不会为这两个主机之间的其他受阻连接生成连接事件。

安全情景

对于在多情景模式下由 ASA FirePOWER 处理的连接，是指识别流量通过的虚拟防火墙组的元数据。

安全组标签

连接中涉及的数据包的安全组标记 (SGT) 属性。SGT 指定受信任网络中的流量源的权限。安全组访问（思科 TrustSec 和思科 ISE 的功能）在数据包进入网络时应用该属性。

Security Intelligence Category

表示或包含连接中被列为黑名单的 IP 地址的黑名单对象名称。安全情报类别可以是网络对象或组、黑名单、自定义安全情报列表或源、或者情报源中其中一个类别的名称。

TCP Flags

对于从 NetFlow 数据生成的连接，是指在连接中检测到的 TCP 标志。当搜索此字段时，输入逗号分隔的 TCP 标志列表以查看至少具有其中一个标志的所有连接。

Time

系统用来在连接摘要中汇总连接的 5 分钟时间间隔的结束时间。此字段不可搜索。

流量 (KB) (Traffic [KB])（仅限搜索）

在连接中传输的总数据量（以千字节为单位）。

数据包总数 (Total Packets)（仅限搜索）

在连接中传输的数据包的总数。

网络

目标端口/ICMP 代码 (Destination Port/ICMP Code)（限制摘要和图形）

会话响应方使用的端口或 ICMP 代码。

DNS 查询

在与名称服务器的连接中提交的用于查找域名的 DNS 查询。

DNS 记录类型 (DNS Record Type)

用于解析连接中提交的 DNS 查询的 DNS 资源记录的类型。

DNS 响应

查询时在与名称服务器的连接中返回的 DNS 响应。

DNS Sinkhole 名称 (DNS Sinkhole Name)

系统将连接重定向的 Sinkhole 服务器的名称。

DNS TTL

DNS 服务器缓存 DNS 资源记录的秒数。

HTTP 响应代码 (HTTP Response Code)

在对客户端的 HTTP 请求的响应中通过连接发送的 HTTP 状态代码。

Ingress/Egress Security Zone

与连接相关的入口或出口安全区。

发起方/响应方 IP (Initiator/Responder IP)（限制摘要和图形）

会话发起方或响应方的 IP 地址（如果启用 DNS 解析，则还包括主机名）。黑名单 IP 地址旁边的主机图标会略有不同，因此，您可以在被列入黑名单的连接中识别黑名单 IP 地址。

Original Client IP

提取自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。要填充此字段，必须在网络分析策略中启用HTTP 预处理器的**提取原始客户端 IP 地址 (Extract Original Client IP Address)** 选项。在网络分析策略中，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择“原始客户端 IP 事件”(Original Client IP event) 字段值的优先顺序。

协议 (Protocol)（限制摘要和图形，仅限搜索）

连接中使用的传输协议。要搜索特定协议，请使用 http://www.iana.org/assignments/protocol-numbers 中所列的名称或编号协议。

源端口/ICMP 类型 (Source Port/ICMP Type)（限制摘要和图形）

会话发起方使用的端口或 ICMP 类型。

VLAN ID

与触发连接的数据包关联的最内部的 VLAN ID。

Geolocation

Initiator/Responder Country

当检测到可路由 IP 时，与会话发起方或响应方的 IP 地址关联的国家/地区。系统显示国家/地区的旗帜图标和国家/地区的 ISO 3166-1 alpha-3 国家/地区代码。将鼠标指针悬停在旗帜图标上可以查看该国家/地区的全名。

Initiator/Responder Continent

当检测到可路由 IP 时，与会话发起方或响应方的 IP 地址关联的大洲。

设备

设备 (Device)（限制摘要和图形）

检测到连接的受管设备，或者对于从 NetFlow 数据生成的连接，是指处理数据的受管设备。

域

检测到连接的受管设备的域，或者对于从NetFlow数据生成的连接，是指处理数据的受管设备的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

入口/出口接口 (Ingress/Egress Interface)

与连接相关的入口或出口接口。如果部署包括异步路由配置，则入口和出口接口可能属于同一接口集。

SSL

SSL 实际操作 (SSL Actual Action)（仅限搜索）

系统应用于 SSL 策略中的加密流量的操作。系统显示搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中的字段值。

操作	描述
阻止/阻止并重置	表示阻止的加密连接。
Decrypt (Resign)	表示使用重新签名的服务器证书解密的传出连接。
Decrypt (Replace Key)	表示使用具有替代公钥的自签名服务器证书解密的传出连接。
Decrypt (Known Key)	表示使用已知私钥解密的传入连接。
默认操作	表示连接采用默认操作处理。
不解密 (Do not Decrypt)	表示系统未解密的连接。

SSL 证书状态

仅在配置了证书状态规则条件时，此字段才适用。如果加密流量与 SSL 规则匹配，则此字段显示以下一个或多个服务器证书状态值：

- Self Signed
- 有效
- 无效签名
- Invalid Issuer
- Expired
- 未知
- Not Valid Yet
- Revoked

如果无法解密的流量与 SSL 规则相匹配，则此字段显示未检查 `(Not Checked)`。

SSL 证书信息 (SSL Certificate Information)（仅限搜索）

用于加密流量的公钥证书上存储的信息，包括：

- Subject/Issuer Common Name
- Subject/Issuer Organization
- Subject/Issuer Organization Unit
- Not Valid Before/After
- Serial Number
- Certificate Fingerprint
- Public Key Fingerprint

SSL Cipher Suite

表示用于加密连接的密码套件的宏值。有关密码套件值指定的信息，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。

应用于连接的 SSL 加密 (SSL Encryption applied to the connection)（仅限搜索）

在 **SSL** 字段中输入 yes 或 no 以查看 SSL 加密或非加密连接。

SSL 预期操作 (SSL Expected Action)（仅限搜索）

在 SSL 规则生效的情况下，系统预期会应用于加密流量的操作。输入为 **SSL 实际操作 (SSL Actual Action)** 列出的任何值。

SSL 失败原因 (SSL Failure Reason)

系统无法解密已加密流量的原因：

- 未知
- No Match
- 成功
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- 内部错误
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL Flow Error

当在 SSL 会话期间发生错误时，为错误名称和十六进制代码，如果未发生错误，则为 `Success`。

SSL Flow Flags

已加密连接的前十大调试级别标记。在工作流程页面上，要查看所有标志，请点击省略号 **(...)**。

SSL Flow Messages

下面的关键字表示加密流量与在 SSL 握手期间客户端和服务器之间交换的指定消息类型相关联。有关详细信息，请参阅http://tools.ietf.org/html/rfc5246。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

SSL 策略

处理连接的 SSL 规则。

SSL Rule

处理连接的 SSL 规则或默认操作，以及与连接匹配的第一个监控规则。如果连接与监控规则匹配，则 Firepower 管理中心显示已处理连接的规则的名称，后跟监控规则名称。

SSL Session ID

在 SSL 握手期间，在客户端与服务器之间协商的十六进制会话 ID。

SSL Status

与记录加密连接的 **SSL 实际操作 (SSL Actual Action)**（SSL 规则、默认操作或无法解密的流量操作）关联的操作。指向SSL证书详细信息的锁定图标()链接。如果证书不可用（例如，对于因 SSL 握手错误而受阻的连接），锁定图标会显示为灰色。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示`Do Not Decrypt (Unknown Cipher Suite)`。

当搜索该字段时，请输入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区 (SSL Subject/Issuer Country)（仅限搜索）

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

SSL Ticket ID

在 SSL 握手期间发送的会话单信息的一个十六进制哈希值。

SSL Version

用于加密连接的 SSL 或 TLS 协议版本。

- 未知
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TSLv1.2

应用

应用协议 (Application Protocol)（限制摘要和图形）

连接中检测到的表示主机之间通信的应用协议。

应用协议类别和标记 (Application Protocol Category and Tag)

展示了应用特征的标准，协助您了解应用功能。

Application Risk

与连接中检测到的应用流量关联的风险：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

业务相关性

与连接中检测到的应用流量关联的业务关联性：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

Client 和 Client Version

在连接中检测到的客户端应用及版本。

如果系统无法识别连接中使用的特定客户端，则该字段会显示附加到应用协议名称的术语“client”，以提供通用名称，例如，FTP client。

客户端类别和标记 (Client Category and Tag)

展示了应用特征的标准，协助您了解应用功能。

HTTP Referrer

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址（例如提供到另一个 URL 的链接或从其导入链接的网站）。

Referenced Host

如果连接中的协议是 HTTP 或 HTTPS，则此字段显示各协议使用的主机名。

用户代理

从连接中检测到的 HTTP 流量提取的用户代理字符串应用信息。

Web 应用

表示连接中检测到的 HTTP流量内容或请求的 URL 的网络应用。

如果网络应用不匹配事件的 URL，该流量大概是推荐流量，例如广告流量。如果系统检测到推荐流量，则会存储该推荐应用（如果有），并将该应用列为网络应用。

如果系统不能在 HTTP 流量中识别特定的网络应用，该字段显示 `Web Browsing`。

Web 应用类别和标记 (Web Application Category and Tag)

展示了应用特征的标准，协助您了解应用功能。

URL

URL、URL Category 和 URL Reputation

会话期间受控主机请求的 URL 以及 URL 类别和信誉（如果有）。

如果系统识别或阻止 SSL 应用，而请求的 URL 位于加密流量中，系统会基于 SSL 证书识别流量。因此，对于 SSL 应用，此字段表示包含在证书中的通用名称。

NetFlow

NetBIOS 域

会话中使用的 NetBIOS 域。

NetFlow 源/目标自治系统 (NetFlow Source/Destination Autonomous System)

对于从 NetFlow 数据生成的连接，是指连接中的流量源或目标的边界网关协议自治系统编号。

NetFlow 源/目标前缀 (NetFlow Source/Destination Prefix)

对于从 NetFlow 数据生成的连接，是指与源或目标前缀掩码用 AND 连接的源或目标 IP 地址。

NetFlow 源/目标 TOS (NetFlow Source/Destination TOS)

对于从 NetFlow 数据生成的连接，是指连接流量进入或退出 NetFlow 导出器时服务类型 (TOS) 字节的设置。

NetFlow SNMP Input/Output

对于从 NetFlow 数据生成的连接，是指连接流量进入或退出 NetFlow 导出器时接口的接口索引。

源设备 (Source Device)（限制摘要和图形）

广播用于为连接生成的数据的 NetFlow 导出器的 IP 地址。如果受管设备检测到连接，则此字段显示 `Firepower`。

关联事件

您不能使用连接/安全情报事件“搜索”(Search) 页面搜索与连接关联的事件。

文件

与连接相关的文件事件（如有）。指向文件列表的查看文件图标 () 链接。图标上的数字表示连接中检测到或阻止的文件数量（包括恶意软件文件）。

入侵事件

与连接相关的入侵事件（如有）。指向事件列表的查看入侵事件图标 () 链接。

连接事件原因

在以下情况下，连接事件中的“原因”(Reason) 字段显示记录连接的原因：

Reason	说明
DNS 阻止 (DNS Block)	系统未经检查就根据域名和安全情报数据拒绝连接。“DNS 阻止”(DNS Block) 原因与“阻止”(Block)、“找不到域”(Domain Not Found) 或 Sinkhole 操作匹配，具体取决于 DNS 规则操作。
DNS 监控 (DNS Monitor)	系统将根据域名和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
File Block	连接中包含系统禁止传输的文件或恶意软件文件。“文件阻止”(File Block) 原因始终与“阻止”(Block) 操作匹配。
文件自定义检测 (File Custom Detection)	连接中包含自定义检测列表上系统禁止传输的文件。
File Monitor	系统在连接中检测到特定类型的文件。
允许继续传输文件 (File Resume Allow)	“阻止文件”(Block Files) 或“阻止恶意软件文件”(Block Malware file) 规则最初阻止文件传输。在新访问控制策略允许文件部署之后，会自动恢复 HTTP 会话。此原因只出现在内联部署中。
阻止继续传输文件 (File Resume Block)	“检测文件”(Detect Files) 或“恶意软件云查找文件”(Malware Cloud Lookup file) 规则最初允许文件传输。在新访问控制策略阻止文件部署之后，会自动停止 HTTP 会话。此原因只出现在内联部署中。
智能应用绕行 (Intelligent App Bypass)	智能应用绕行 (IAB) 模式： • 如果操作是“信任”(Trust)，则 IAB 处于绕行模式。匹配的流量通过，无需进一步检查。 • 如果操作是“允许”(Allow)，则 IAB 处于测试模式。匹配流量可供进一步检查。
Intrusion Block	系统阻止或本可阻止在连接中检测到的漏洞（入侵策略违规）。“入侵阻止”(Intrusion Block) 原因与用于阻止漏洞的“阻止”(Block) 操作和用于本可阻止漏洞的“允许”(Allow) 操作匹配。
入侵监控 (Intrusion Monitor)	系统检测到但并未阻止连接中检测到的漏洞。当触发的入侵规则状态设置为“生成事件”(Generate Events) 时，会发生这种情况。
IP Block	系统未经检查就根据 IP 地址和安全情报数据拒绝连接。“IP 阻止”(IP Block) 原因始终与“阻止”(Block) 操作匹配。

Reason	说明
IP Monitor	系统将根据 IP 地址和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
SSL 阻止 (SSL Block)	系统基于 SSL 检查配置阻止加密连接。“SSL 阻止”(SSL Block) 原因始终与“阻止”(Block) 操作匹配。
URL 阻止 (URL Block)	系统未经检查就根据 URL 和安全情报数据拒绝连接。“URL 阻止”(URL Block) 原因始终与“阻止”(Block) 操作匹配。
URL 监控 (URL Monitor)	系统将根据 URL 和安全情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
User Bypass	系统最初阻止用户的 HTTP 请求，但用户点击浏览警告页面以查看网站。“用户绕行”(User Bypass) 原因始终与“允许”(Allow) 操作匹配。

填充连接事件字段的要求

可用于连接事件、安全情报事件或连接摘要的信息取决于多种因素。

Appliance Model 和 License

许多功能要求您启用目标设备上的特定许可功能，并且许多功能仅在部分型号上可用。

例如，NGIPSv 设备不支持 SSL 检查。它们无法检测加密流量；已记录的连接事件不包含有关加密连接的信息。

流量特征

系统仅报告在网络流量中展示（并且可检测）的信息。例如，可能没有与发起人主机相关联的用户，或者在协议不是 DNS、HTTP 或 HTTPS 的连接中未检测到引用的主机。

源/检测方法：基于流量的检测与 NetFlow

除纯 NetFlow 字段以外，NetFlow 记录中可用的信息比由基于流量的检测生成的信息更有限；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

记录方法：连接的开始或结束

当系统检测到连接时，您可以在其开始还是结束（或两者）时记录该连接取决于如何将系统配置为检测和处理该连接。

开始连接事件不具有必须通过检查会话持续时间内的流量来确定的信息（例如，连接中传输数据的总量或最终数据包的时间戳）。也不保证开始连接事件拥有关于会话中应用或URL流量的信息，且该等事件不包含有关会话加密的任何详细信息。连接开始日志记录通常是受阻连接的唯一选项。

连接事件类型：个别与摘要

连接摘要不包含与汇总连接相关的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

请记住，连接图基于连接摘要数据，并且只使用了结束连接记录。如果系统配置为仅记录连接开始数据，则连接图和连接摘要事件视图不包含任何数据。

其他配置

影响连接日志记录的其他配置包括但不限制：

- 仅当在与通过 Active Directory 域控制器进行身份验证的用户关联的连接中配置 ISE 时，才填充 ISE 相关字段。连接事件不包含通过 LDAP、RADIUS 或 RSA 域控制器进行身份验证的用户的 ISE 数据。
- 仅在由 SSL 策略处理的加密连接中，才会填充 SSL 相关字段。
- 仅在由与文件策略关联的访问控制规则记录的连接中，才会填充文件信息字段。
- 仅在由与入侵策略关联或使用默认操作的访问控制规则记录的连接中，才会填充入侵信息字段。
- 仅在特定情况下（例如，当用户绕过交互式阻止配置时），才会填充“原因”(Reason) 字段。
- 仅当曾经配置 Firepower 管理中心以实现多租户时，才存在“域”(Domain) 字段。
- 访问控制策略中控制系统在连接记录中为 HTTP 会话中受控主机请求的每个 URL 存储的字符数的高级设置。如果使用此设置禁用 URL 记录，系统不会在连接记录中显示每个 URL；但如果连接记录中存在类别和信誉数据，仍然可以查看。

连接事件字段中的可用信息

本主题中的表指示系统何时可以填充连接和安全情报字段。表中的列表示以下事件类型：

- 源：直接 - 代表由 Firepower 系统受管设备检测和处理的连接的事件。
- 源：NetFlow - 代表由 NetFlow 导出器导出的连接的事件。
- 记录：开始 - 代表在开始时记录的连接的事件。
- 记录：结束 - 代表在结束时记录的连接的事件。

表中的“是”并不意味着系统必须填充连接事件字段，而表示它可以填充。系统仅报告在网络流量中展示（并且可检测）的信息。例如，只有由 SSL 策略处理的加密连接的记录，才会填充 SSL 相关字段。

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
访问控制策略	是	否	是	是
Access Control Rule	是	否	是	是

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
操作	是	否	是	是
应用协议	是	是	如果有	yes
应用协议类别和标记(Application Protocol Category & Tag)	是	否	如果有	yes
Application Risk	是	否	如果有	yes
业务相关性	是	否	如果有	yes
Client	是	否	如果有	yes
客户端类别和标记 (Client Category & Tag)	是	否	如果有	yes
Client Version	是	否	如果有	yes
连接	是	是	否	yes
计数	是	是	是	是
Destination Port/ICMP Type	是	是	是	是
设备	是	是	是	是
域	是	是	是	是
DNS 查询	是	否	是	是
DNS 记录类型 (DNS Record Type)	是	否	是	是
DNS 响应	是	否	是	是
DNS Sinkhole 名称 (DNS Sinkhole Name)	是	否	是	是
DNS TTL	是	否	是	是
出口接口	是	否	是	是
Egress Security Zone	是	否	是	是
终端位置 (Endpoint Location)	是	否	是	是

连接事件字段	源：直接	源：**NetFlow**	记录：开始	记录：结束
Endpoint Profile	是	否	是	是
文件	是	否	否	yes
First Packet	是	是	是	是
HTTP Referrer	是	否	否	yes
HTTP 响应代码 (HTTP Response Code)	是	否	是	是
入口接口	是	否	是	是
Ingress Security Zone	是	否	是	是
Initiator Bytes	是	是	不实用	yes
Initiator Country	是	否	是	是
Initiator IP	是	是	是	是
Initiator Packets	是	是	不实用	yes
Initiator User	是	是	是	是
入侵事件	是	否	否	yes
入侵策略	是	否	是	是
IOC（危害表现）	是	否	是	是
Last Packet	是	是	否	yes
NetBIOS 域	是	否	是	是
NetFlow 源/目标自治系统 (NetFlow Source/Destination Autonomous System)	否	是	否	yes
NetFlow 源/目标前缀 (NetFlow Source/Destination Prefix)	否	是	否	yes
NetFlow 源/目标 TOS (NetFlow Source/Destination TOS)	否	是	否	yes
NetFlow SNMP Input/Output	否	是	否	yes

连接事件字段	源：直接	源：**NetFlow**	记录：开始	记录：结束
Network Analysis Policy	是	否	是	是
Reason	是	否	是	是
Referenced Host	是	否	否	yes
Responder Bytes	是	是	不实用	yes
Responder Country	是	否	是	是
Responder IP	是	是	是	是
Responder Packets	是	是	不实用	yes
Security Context (ASA only)	是	否	是	是
安全组标记 (SGT) (Security Group Tag [SGT])	是	否	是	是
Security Intelligence Category	是	否	是	是
Source Device	是	是	是	是
Source Port/ICMP Type	是	是	是	是
SSL Certificate Status	是	否	否	yes
SSL Cipher Suite	是	否	否	yes
SSL Flow Error	是	否	否	yes
SSL Flow Flags	是	否	否	yes
SSL Flow Messages	是	否	否	yes
SSL 策略	是	否	否	yes
SSL Rule	是	否	否	yes
SSL Session ID	是	否	否	yes
SSL Status	是	否	否	yes
SSL Version	是	否	否	yes

连接事件字段	源：直接	源：**NetFlow**	记录：开始	记录：结束
TCP Flags	否	是	否	yes
Time	是	是	否	yes
URL	是	否	如果有	yes
URL 类别	是	否	如果有	yes
URL Reputation	是	否	如果有	yes
用户代理	是	否	否	yes
VLAN ID	是	否	是	是
Web 应用	是	否	如果有	yes
Web 应用类别和标记 (Web Application Category & Tag)	是	否	如果有	yes

使用连接和安全情报事件表

智能许可证	经典许可证	支持的设备	支持的域	**Access**
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower管理中心查看连接或安全情报事件表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问连接图时看到的页面因所用的工作流程而有所不同。可以使用预定义的工作流程，最终会产生事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

使用连接或安全情报工作流程表时，可以执行许多常见操作。

请注意，当您在向下钻取页面上约束连接事件时，来自相同事件的数据包和字节数将累加。然而，如果您正使用自定义工作流程，且没有将 **Count** 列添加到向下钻取页面，则会单独列出事件，数据包和字节将不会累加。

过程

步骤 1 选择以下其中一个选项：

- **分析 (Analysis)** > **连接 (Connections)** > **事件 (Events)**（适用于连接事件）
- **分析 (Analysis)** > **连接 (Connections)** > **安全情报事件 (Security Intelligence Events)**

注释 如果系统显示连接图而不是表，请按工作流程标题点击**切换工作流程 (switch workflow)**，然后选择预定义**连接事件 (Connection Events)** 工作流程，或自定义工作流程。请注意，所有预定义连接事件工作流程（包括连接图）最终都会产生连接的表视图。

步骤 2 有以下选项可供选择：

- “时间范围”(Time Range) - 要调整时间范围（如果未显示事件，则非常有用），请参阅更改时间窗口，第 1461 页。
- “字段名称”(Field Names) - 要了解有关表中各列内容的详细信息，请参阅连接和安全情报事件字段，第 1515 页。

  提示 在事件表视图中，有几个字段是默认隐藏的，包括每种应用类型的类别和标记字段、NetFlow 相关字段、SSL 相关字段和其他字段。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

- “主机配置文件”(Host Profile) - 要查看 IP 地址的主机配置文件，请点击主机配置文件图标 ()，或者对于带有效危害表现 (IOC) 标记的主机，请点击显示在 IP 地址旁边的危害主机图标 ()。
- 用户配置文件 - 要查看用户身份信息，请点击显示在用户身份旁边的用户图标（  ）。
- “文件和恶意软件”(Files and Malware) - 要查看在连接中检测到或阻止的文件（包括恶意软件），请点击查看文件图标()，然后如查看连接中检测到的文件和恶意软件，第 1535 页中所述继续操作。
- “入侵事件”(Intrusion Events) - 要查看与某个连接关联的入侵事件，及其优先级和影响，请点击**入侵事件 (Intrusion Events)** 列中的入侵事件图标 ()，然后如查看与连接关联的入侵事件，第 1536 页中所述继续操作。

  提示 要快速查看与一个或多个连接关联的入侵、文件或恶意软件事件，请使用事件查看器中的复选框选中连接，然后从**跳转至 (Jump to)** 下拉列表中选择合适的选项。请注意，由于它们在访问控制规则评估之前已被阻止，因此可能没有与列入安全情报黑名单的连接关联的文件或入侵。如果已配置安全情报来监控连接（而非将其列入黑名单），则只可以看到安全情报事件的这一信息。

- “证书”(Certificate) - 要查看有关用于解密连接的可用证书的详细信息，请在 **SSL 状态 (SSL Status)** 列中点击已启用的锁定图标 ()。
- “限制”(Constrain) - 要限制显示的列，请在要隐藏的列标题中点击关闭图标 ()。在显示的弹出窗口中，点击 **Apply**。

  提示 要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用列添加回视图中，请展开搜索限制条件，然后点击“已禁用列”(Disabled Columns) 下的列名称。

- “删除事件”(Delete Events) - 要删除当前限制视图中的部分或全部项目，请选中要删除的项目旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。
- 向下展开 - 请参阅使用向下钻取页面，第 1450 页。

  提示 要使用匹配已记录连接的多个监控规则之一向下展开，请点击一个*N* **监控规则 (Monitor Rules)** 值。在出现的弹出窗口中，点击要用于限制连接事件的监控规则。

- “导航此页面”(Navigate This Page) - 请参阅工作流程页面遍历工具，第 1447 页。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “排序”(Sort) - 要对工作流程中的数据排序，请点击列标题。再次点击列标题以反转排列顺序。

查看连接中检测到的文件和恶意软件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁或恶意软件	保护或恶意软件	任何环境	任何环境	管理员/任何安全分析师

如果将一个文件策略与一个或多个访问控制规则相关联，系统可以在匹配的流量中检测文件（包括恶意软件）。通过使用事件查看器，您可以查看与这些规则所记录连接相关的文件事件（如有）。

Firepower 管理中心不显示文件列表，而是在 **Files** 列中显示视图文件图标 ()。图标上的数字表示连接中检测到或阻止的文件数量（包括恶意软件文件）。

并非所有文件和恶意软件事件都与连接有关。具体包括：

- 基于终端的恶意软件事件与连接不相关。这些事件是从面向终端的 AMP 导入。
- 许多启用 IMAP 的邮件客户端使用单个 IMAP 会话，仅当用户退出应用时才结束。尽管长期运行的连接是由系统进行记录，但是在会话结束之前，会话中下载的文件不会与连接关联。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 使用连接事件表时，点击查看文件图标 ()。
系统会显示弹出窗口，其中显示连接中检测到的文件列表及其类型和恶意软件处置情况（如适用）。

步骤 2 有以下选项可供选择：

- 查看 - 要查看文件事件表视图，请点击文件的查看图标 ( )。
- 查看 - 要查看恶意软件事件表视图的详细信息，请点击恶意软件的查看图标 ( )。
- 跟踪 - 要跟踪通过您的网络传输的文件，请点击文件的轨迹图标 ( )。
- 查看 - 要查看连接的所有检测到的文件或基于网络的恶意软件事件的详细信息，请点击**查看文件事件 (View File Events)** 或**查看恶意软件事件 (View Malware Events)**。

查看与连接关联的入侵事件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/任何安全分析师

如果您将入侵策略与访问控制规则或默认操作相关联，系统可以检测匹配流量中的漏洞。通过使用事件查看器，您可以查看与已记录连接相关联的入侵事件（如有），及其优先级和影响。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 使用连接事件表时，点击**入侵事件 (Intrusion Events)** 列中的入侵事件图标 ( )。

步骤 2 在显示的弹出窗口中，您有以下选择：

- 点击所列事件的查看图标 ( )，查看数据包视图中的详细信息。
- 点击**查看入侵事件 (View Intrusion Events)**，查看与连接关联的所有入侵事件的详细信息。

已加密连接的证书详细信息

可以使用事件查看器来显示用于加密系统处理的连接的公钥证书（如有）。该证书包含以下信息。

表 *273*：已加密连接的证书详细信息

属性	说明
Subject/Issuer Common Name	证书主体或证书颁发者的主机名和域名。
Subject/Issuer Organization	证书主体或证书颁发者的组织。

属性	说明
Subject/Issuer Organization Unit	证书主体或证书颁发者的组织单位。
Not Valid Before/After	证书有效日期。
Serial Number	由发行 CA 分配的序列号。
Certificate Fingerprint	用于验证证书的 SHA 哈希值。
Public Key Fingerprint	用于对证书内所含公钥进行身份验证的 SHA 哈希值。

查看连接摘要页面

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	自定义

“连接摘要”(Connection Summary) 页面仅对于满足以下条件的用户才可视：具有受连接事件搜索限制的自定义角色，已被授予对“连接摘要”(Connection Summary) 页面的基于菜单的显式访问权限。此页面提供按不同标准组织的受监控网络上的活动的图形。例如，“随时间推移的连接”(Connections over Time) 图形显示在选择的间隔内受监控网络上的连接总数。

如同连接图，您几乎可以在连接摘要图上执行完全一样的操作。然而，由于 Connection Summary 页面上的图形基于汇总数据，因此，您无法检查图形依赖的单个连接事件。换句话说，您无法从连接摘要图展开到连接数据表视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述 (Overview)** > **摘要 (Summary)** > **连接摘要 (Connection Summary)**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择要查看其摘要的设备，或者选择**所有 (All)** 以查看所有设备的摘要。

步骤 3 要操纵和分析连接图，请如使用连接事件图形，第 1453 页中所述继续操作。

提示 要将连接图分离，以便可以执行进一步分析而不影响默认时间范围，请点击**查看 (View)**。

第 85 章

处理入侵事件

以下主题介绍如何处理入侵事件。

入侵事件

Firepower 系统可以帮助监控网络中可能影响主机及其数据的可用性、完整性和机密性的流量。通过将受管设备放在关键网段，可以检查流经网络的数据包是否包含恶意活动。系统通过使用多个机制查找攻击者开发的众多漏洞。

如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是包含攻击的日期、时间、漏洞类型以及有关攻击的来源和目标的情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。受管设备将其事件传输到Firepower管理中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。

还可以将受管设备部署为内联式、交换式或路由式入侵系统，以便将设备配置为会丢弃或替换已知有害的数据包。

Firepower 系统还为您提供复审入侵事件和评估其在网络环境与安全策略的情景中是否重要所需的工具。这些工具包括：

- 事件摘要页面，提供受管设备上当前活动的概览。
- 基于文本和图表的报告，可以针对所选的任何时间段生成此类报告；还可以自行设计报告并将其配置为按预定的时间间隔运行

- 可用来收集与攻击相关的事件数据的事故处理工具；还可以添加注释以便跟踪调查和响应
- 可以为 SNMP、邮件和系统日志配置的自动警报
- 可用于响应和处理特定入侵事件的自动关联策略
- 预定义和自定义工作流程，可用于向下钻取以识别要进一步调查的事件

查看入侵事件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以查看入侵事件来确定其是否会对网络安全构成威胁。

初始入侵事件视图根据用于访问页面的工作流程而不同。可以使用其中一个预定义工作流程（其中包括一个或更多下钻式页面、入侵事件表视图和一个终止数据包视图），或者也可以创建自己的工作流程。还可以查看基于自定义表的工作流程，该表可能包括入侵事件。

如果事件视图包含大量 IP 地址且已启用**解析 IP 地址 (Resolve IP Addresses)** 事件视图设置，事件视图可能显示得很慢。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事件 (Events)**。

步骤 2 有以下选项可供选择：

- 调整时间范围 - 如更改时间窗口，第 1461 页中所述，调整事件视图的时间范围。
- 更改工作流程 - 如果使用的是不包含入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])** 以选择系统提供的任意工作流程。
- 限制 - 要将视图缩小至对分析非常重要的入侵事件，请参阅使用入侵事件工作流程，第 1555 页。
- 删除事件 - 要从数据库删除事件，请点击**删除 (Delete)** 删除您正查看其数据包的事件，或点击**全部删除 (Delete All)** 删除您之前已选择其数据包的所有事件。
- 标记为“已审核” - 要将入侵事件标记为“已审核”，请参阅将入侵事件标记为“已审核”，第 1551 页。
- 查看连接数据 - 要查看与入侵事件关联的连接数据，请参阅查看与入侵事件关联的连接数据，第 1550 页。
- 查看内容 - 如入侵事件字段，第 1541 页中所述，查看表中各列的内容。

入侵事件字段

如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是包含攻击的日期、时间、漏洞类型以及有关攻击的来源和目标的情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。

搜索入侵事件时，请记住任何单独事件的可用信息视系统记录事件的方式、原因和时间而异。例如，只有加密流量上触发的入侵事件才包含 SSL 信息。

注释 入侵事件表视图内一些字段默认被禁用。要在会话期间启用某个字段，请展开搜索限制条件，然后点击**已禁用列 (Disabled Columns)** 下的列名。

访问控制策略

与启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略相关联的访问控制策略。

Access Control Rule

调用生成事件的入侵策略的访问控制规则。`Default Action` 指示启用了规则的入侵政策未与特定访问控制规则相关联，而是配置为访问控制策略的默认操作。

如果入侵检查既未与访问控制规则关联，也未与默认操作关联，例如数据包由默认入侵策略检查，则该字段留空。

应用协议

表示在触发入侵事件的流量中检测到的主机之间的通信的应用协议（如果可用）。

应用协议类别和标记 (Application Protocol Category and Tag)

展示了应用特征的标准，协助您了解应用功能。

Application Risk

与在触发入侵事件的流量中检测到的应用相关联的风险：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。在连接中检测的各种类型的应用都有相关的风险；此字段显示当中的最高风险。

业务相关性

与在触发入侵事件的流量中检测到的应用相关联的业务关联性：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有相关业务；此字段显示当中最低（相关性最小）的业务相关性。

分类

生成事件的规则所属的分类。

当搜索此字段时，请为生成要查看的事件的规则输入分类编号，或者全部或部分分类名称或说明。也可以输入编号、名称或描述的以逗号分隔列表。最后，如果添加自定义分类，还可以使用其完整或部分的名称或描述进行搜索。

Client

客户端应用（如果有），代表在触发入侵事件的流量中检测到的受监控主机上运行的软件。

客户端类别和标记 (Client Category and Tag)

展示了应用特征的标准，协助您了解应用功能。

计数

与每行中所显示的信息匹配的事件数。注意，Count字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

Destination Continent

入侵事件中涉及的接收主机所在的大洲。

Destination Country

入侵事件中涉及的接收主机所在的国家/地区。

目标 IP

入侵事件中涉及的接收主机使用的 IP 地址。

Destination Port/ICMP Code

接收流量的主机的端口号。对于 ICMP 流量，在没有端口号的情况下，此字段显示 ICMP 代码。

目标用户

登录目标主机的任何已知用户的用户 ID。

设备

已部署访问控制策略的受管设备。

请注意，堆叠配置中的主设备和辅助设备就像独立设备一样报告入侵事件。

域

检测到入侵的设备的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

出口接口

触发事件的数据包的出口接口。对于被动接口，不填充此接口列。

Egress Security Zone

触发事件的数据包的出口安全区域。在被动部署中不填充此安全区域字段。

电子邮件附件

提取自 MIME Content-Disposition 报头的 MIME 附件文件名。要显示附件文件名，必须启用 SMTP 预处理器 **Log MIME Attachment Names** 选项。支持多个附件文件名。

邮件报头 (Email Headers)（仅限搜索）

提取自邮件报头的数据。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器 **Log Headers** 选项。

Email Recipient

提取自 SMTP RCPT TO 命令的邮件收件人的地址。要显示此字段的值，必须启用 SMTP 预处理器 **Log To Addresses** 选项。支持多个收件人地址。

Email Sender

提取自 SMTP MAIL FROM 命令的邮件发件人的地址。要显示此字段的值，必须启用 SMTP 预处理器 **Log From Addresses** 选项。支持多个发件人地址。

发电机

生成事件的组件。

HTTP Hostname

提取自 HTTP 请求主机报头的主机名（如果有）。请注意，请求数据包并非总是包含主机名。

要将主机名与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。

在表视图中，此列显示提取的主机名的前50个字符。将光标悬停在缩写主机名的显示部分上可显示完整名称（最多包含 256 个字节）。还可以在数据包视图中显示完整主机名（最多包含 256 个字节）。

HTTP 响应代码 (HTTP Response Code)

在对客户端的 HTTP 请求的响应中通过触发事件的连接发送的 HTTP 状态代码。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI（如果有）。请注意，请求数据包并非总是包含 URI。

要将 URI 与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log URI** 选项。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。

此列显示提取的 URI 的前五十个字符。将光标悬停在缩略 URI 的显示部分上可显示完整 URI（最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI（最多包含 2048 个字节）。

影响

此字段中的影响级别指示入侵数据、网络发现数据和漏洞信息之间的相关性。

当搜索此字段时，请勿指定影响图标颜色或部分字符串。例如，请勿使用 blue、level 1 或 0。不区分大小写的有效值为：

- 影响 0，影响级别 0
- 影响 1，影响级别 1
- 影响 2，影响级别 2
- 影响 3，影响级别 3
- 影响 4，影响级别 4

对于从 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”(Vulnerable)（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。

入口接口

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。

Ingress Security Zone

触发事件的数据包的入口安全区域。在被动部署中仅填充此安全区域字段。

Inline Result

在工作流程和表视图中，此字段显示以下其中一项：

- 一个黑色向下箭头，表明系统已丢弃触发规则的数据包
- 一个灰色向下箭头，表明如果已启用 **Drop when Inline** 入侵策略选项（在内联部署中），或者在系统进行修剪时一个 Drop and Generate 规则生成了该事件，那么 IPS 应该已丢弃数据包
- 空白，表明触发规则未设置为 Drop and Generate Events

无论入侵策略的规则状态或内联丢弃行为如何，系统在被动部署中都不会丢弃数据包，包括当内联接口处于分流模式时。

当搜索此字段时，请输入以下任一项：

- dropped，用于指定在内联部署中是否丢弃数据包
- would have dropped，用于指定当入侵策略设置为在内联部署中丢弃数据包时是否已丢弃数据包

入侵策略

启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则相关联。

IOC

触发入侵事件的流量是否也触发了危害表现 (IOC)。当搜索此字段时，请指定 triggered 或 n/a。

消息

事件的说明文本。对于基于规则的入侵事件，事件消息提取自规则。对于基于解码器和预处理器的事件，事件消息采用硬编码。

MPLS Label

与触发入侵事件的数据包相关联的多协议标签交换标签。

Network Analysis Policy

与事件生成相关联的网络分析策略（如果有）。

URI

此列显示提取的 URI 的前五十个字符。将光标悬停在缩略 URI 的显示部分上可显示完整 URI（最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI（最多包含 2048 个字节）。

Original Client IP

提取自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。

要显示此字段的值，必须在网络分析策略中启用 HTTP 预处理器 **Extract Original Client IP Address** 选项。或者，在网络分析策略的同一区域，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择原始客户端 IP 事件字段值的优先顺序。

优先级

Cisco Talos 安全情报和研究小组 (Talos) 所确定的事件优先级。优先级对应于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。有效值为“高”(high)、“中”(medium) 和“低”(low)。

协议 (Protocol)（仅限搜索）

连接中使用的传输协议的名称或编号，如 http://www.iana.org/assignments/protocol-numbers 中所列。这是与源端口和目标端口/ICMP 列相关的协议。

Reviewed By

审核事件的用户的名称。当搜索此字段时，可以输入 unreviewed 以搜索尚未审核的事件。

安全情景

识别流量通过的虚拟防火墙组的元数据。系统仅在多情景模式下为 ASA FirePOWER 填充此字段。

Snort ID（仅限搜索）

指定生成事件的规则的 Snort ID (SID)，或者指定规则的生成器 ID (GID) 和 SID 的组合，其中 GID 和 SID 之间用冒号 (:) 隔开，格式为 GID:SID。可指定下表中的任何值：

表 *274*：*Snort ID* 搜索值

值	示例
单个 SID	10000
SID 范围	10000 - 11000
大于某个 SID	>10000
大于或等于某个 SID	>=10000
小于某个 SID	<10000
小于或等于某个 SID	<=10000
以逗号分隔的 SID 值列表	10000,11000,12000
单个 GID:SID 组合	1:10000
以逗号分隔的 GID:SID 组合列表	1:10000,1:11000,1:12000
以逗号分隔的 SID 和 GID:SID 组合列表	10000,1:11000,12000

您查看的事件的 SID 在“消息”(Message) 列中列出。

Source Continent

入侵事件中涉及的发送主机所在的大洲。

Source Country

入侵事件中涉及的发送主机所在的国家/地区。

源 IP

入侵事件中涉及的发送主机使用的 IP 地址。

Source Port/ICMP Type

发送主机上的端口号。对于 ICMP 流量，在没有端口号的情况下，此字段显示 ICMP 类型。

源用户

登录源主机的任何已知用户的用户 ID。

SSL 实际操作 (SSL Actual Action)（仅限搜索）

系统应用于已加密流量的操作：

阻止/阻止并重置 (Block/Block with reset)

表示阻止的加密连接。

Decrypt (Resign)

表示使用重新签名的服务器证书解密的传出连接。

Decrypt (Replace Key)

表示使用具有替代公钥的自签名服务器证书解密的传出连接。

Decrypt (Known Key)

表示使用已知私钥解密的传入连接。

默认操作

表示连接采用默认操作处理。

不解密 **(Do not Decrypt)**

表示系统未解密的连接。

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 证书信息 (SSL Certificate Information)（仅限搜索）

用于加密流量的公钥证书上存储的信息，包括：

- Subject/Issuer Common Name
- Subject/Issuer Organization
- Subject/Issuer Organization Unit
- Not Valid Before/After
- Serial Number
- Certificate Fingerprint
- Public Key Fingerprint

SSL 失败原因 (SSL Failure Reason)（仅限搜索）

系统无法解密已加密流量的原因：

- 未知

- No Match
- 成功
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- 内部错误
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL Status

与记录加密连接的 **SSL 实际操作 (SSL Actual Action)**（SSL 规则、默认操作或无法解密的流量操作）关联的操作。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

点击锁图标 () 可查看证书详细信息。

当搜索该字段时，请输入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区 (SSL Subject/Issuer Country)（仅限搜索）

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

Time

事件的日期和时间。此字段不可搜索。

VLAN ID

与触发入侵事件的数据包相关的最内部的 VLAN ID。

Web 应用

网络应用，代表在触发入侵事件流量中检测到的 HTTP 流量的内容或请求的 URL。

如果系统检测到 HTTP 应用协议，但无法检测特定 Web 应用，则系统会在此处提供通用 Web 浏览指定。

Web 应用类别和标记 (Web Application Category and Tag)

展示了应用特征的标准，协助您了解应用功能。

入侵事件影响级别

为了帮助评估事件对网络的影响，Firepower管理中心在入侵事件的表视图中显示影响级别。对于每一个事件，系统都会添加影响级别图标，其颜色表示入侵数据、网络发现数据和漏洞信息之间的相关性。

注释 对于从NetFlow数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”(Vulnerable)（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。

下表介绍了影响级别的可能值。

表 *275*：影响级别

影响级别	漏洞	颜色	描述
0	未知	灰色	源主机和目标主机都不在由网络发现监控的网络上。
1	较弱	红色	可以为以下任意一项： • 源主机或目标主机在网络映射中，并且漏洞已映射到主机 • 源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。
2	Potentially Vulnerable	橙色	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量，端口正在运行服务器应用协议 • 对于非面向端口的流量，主机使用该协议
3	Currently Not Vulnerable	yellow	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量（例如 TCP 或 UDP），端口不处于打开状态 • 对于非面向端口的流量（例如 ICMP），主机不使用该协议
4	Unknown Target	蓝色	源主机或目标主机在受监控网络上，但网络映射中没有该主机的条目。

查看与入侵事件关联的连接数据

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

系统可以记录在其中检测到入侵事件的连接。虽然会对与访问控制规则关联的入侵策略自动执行这种记录，但必须手动启用连接记录才能查看与默认操作关联的连接数据。

在事件的表视图之间导航时，查看相关数据最有用。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **事件 (Events)**。

步骤 2 使用事件查看器中的复选框选择入侵事件，然后从**跳转至 (Jump to)** 下拉列表中选择**连接 (Connections)**。

提示 可以使用类似方法查看与特定连接相关的入侵事件。有关详细信息，请参阅工作流程间导航，第 1466 页。

将入侵事件标记为“已审核”

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

如果确信入侵事件不是恶意的，可以将其标记为“已审核”。

如果检查了某个入侵事件并确信其不对网络安全构成威胁（例如，因为您知道网络中的所有主机均不易受检测到的漏洞攻击），那么可以将事件标记为“已审核”。已审核事件存储在数据库中并包括在事件摘要统计信息中，但不再显示在默认入侵事件页面中。您的姓名会作为审核者显示。

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

如果执行备份然后删除已审核的入侵事件，恢复备份会恢复已删除的入侵事件，但不能恢复其“已审核”状态。应在**入侵事件 (Intrusion Events)** 下，而不是在**已审核事件 (Reviewed Events)** 下查看这些恢复的入侵事件。

过程

在显示入侵事件的页面上，您有两个选择：

- 要标记事件列表中的一个或多个入侵事件，请选择事件旁边的复选框并点击**审核 (Review)**。
- 要标记事件列表中的所有入侵事件，请点击 **Review All**。

查看之前已审核的入侵事件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **已审核事件 (Reviewed Events)**。

步骤 2 有以下选项可供选择：

- 调整时间范围，如更改时间窗口，第 1461 页中所述。
- 如果使用的是不包含入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])** 以选择系统提供的任意预定义工作流程。
- 要了解有关显示的事件的详细信息，请参阅入侵事件字段，第 1541 页。

将已审核的入侵事件标记为“未审核”

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以将已审核的事件返回到默认入侵事件视图，方法是将该事件标记为“未审核”。

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

过程

在显示已审核事件的页面上，您有两个选择：

- 要删除已审核事件列表中的单个入侵事件，请选中特定事件旁边的复选框并点击**取消审核 (Unreview)**。
- 要从已审核事件列表移除所有入侵事件，请点击 **Unreview All**。

预处理器事件

预处理器提供两项功能：对数据包执行指定操作（例如解码和规范化 HTTP 流量）；一旦数据包触发某个预处理器选项且相关预处理器规则处于启用状态，就会通过生成事件来报告指定预处理器选项的执行情况。例如，您可以用 HTTP 检查生成器 (GID) 119 和 Snort ID (SID) 2 来启用 `Double Encoding` HIIP 检查选项及相关的预处理器规则，以在预处理器遇到 IIS 双编码流量时生成事件。

生成事件来报告预处理器执行情况有助于检测异常协议漏洞。例如，攻击者可以制造重叠的IP片段来对主机进行 DoS 攻击。IP 分片重组预处理器可以检测此类攻击并为之生成入侵事件。

预处理器事件与规则事件的不同之处在于，数据包显示不包含对事件的详细规则说明。相反，数据包显示的是事件消息、GID、SID、数据包报头数据和数据包负载。这让您可以分析数据包的报头信息，确定数据包的报头选项是否正在使用以及它们是否会令系统出现漏洞，并检查数据包负载。预处理器分析每个数据包后，规则引擎对其执行适当的规则（如果预处理器能够整理数据包并将其作为有效会话的一部分），进一步分析潜在内容级别的威胁并提供相关报告。

预处理器生成器 ID

每个预处理器都有自己的生成器ID（即GID），用以指明数据包触发的是哪个预处理器。某些预处理器还具有相关SID，这是用于对潜在攻击进行分类的ID编号。这有助于通过对事件类型进行分类来更有效地分析事件，就像规则的Snort ID (SID) 可以提供数据包触发规则的情景一样。可以在入侵策略“规则”页面的“预处理器”筛选组中按预处理器列出预处理器规则；还可以在“类别”筛选组的预处理器和数据包解码器子组中列出预处理器规则。

注释 由标准文本规则生成的事件具有生成器ID 1。事件的SID指明触发的是哪条具体规则。对于共享对象规则，事件具有生成器 ID 3 和用于指示所触发的具体规则的 SID。

下表介绍了生成每个 GID 的事件的类型。

表 *276*: 生成器 *ID*

ID	组件	说明
1	标准文本规则	在数据包触发标准文本规则时生成事件。
2	标记的数据包	事件由标记生成器生成（标记生成器会根据带标记会话生成数据包）。使用 `tag` 规则选项时会出现这种情况。
3	共享对象规则	在数据包共享对象规则时生成事件。
102	HTTP 解码器	解码器引擎解码数据包中的 HTTP 数据。
105	Back Orifice 检测器	Back Orifice 检测器识别与数据包关联的 Back Orifice 攻击。
106	RPC 解码器	RPC 解码器解码数据包。
116	数据包解码器	事件由数据包解码器生成。
119、120	HTTP 检查预处理器	事件由 HTTP 检查预处理器生成。GID 120 规则与服务器特定 HTTP 流量相关。
122	端口扫描检测器	事件由端口扫描流量检测器生成。
123	IP 分片重组器	分片的 IP 数据报不能正确重组时生成事件。

ID	组件	说明
124	SMTP 解码器	SMTP 预处理器检测到针对 SMTP 谓词的漏洞时生成事件。
125	FTP 解码器	FTP/Telnet 解码器检测到 FTP 流量中有漏洞时生成事件。
126	Telnet 解码器	FTP/Telnet 解码器检测到 Telnet 流量中有漏洞时生成事件。
128	SSH 预处理器	SSH 预处理器检测到 SSH 流量中的漏洞时生成事件。
129	流预处理器	在数据流预处理器对数据流进行预处理期间生成事件。
131	DNS 预处理器	事件由 DNS 预处理器生成。
133	DCE/RPC 预处理器	事件由 DCE/RPC 预处理器生成。
134	规则延迟 数据包延迟	规则延迟暂停 (134:1) 或重新启用 (134:2) 一组入侵规则时，或者由于超出数据包延迟阈值而使系统停止检查数据包 (134:3) 时，生成事件。
135	基于速率的攻击检测器	基于速率的攻击检测器识别到网络上的主机存在过多连接时生成事件。
137	SSL 预处理器	事件由 SSL 预处理器生成。
138、139	敏感数据预处理器	事件由敏感数据预处理器生成。
140	SIP 预处理器	事件由 SIP 预处理器生成。
141	IMAP 预处理器	事件由 IMAP 预处理器生成。
142	POP 预处理器	事件由 POP 预处理器生成。
143	GTP 预处理器	事件由 GTP 预处理器生成。
144	Modbus 预处理器	事件由 Modbus SCADA 预处理器生成。
145	DNP3 预处理器	事件由 DNP3 SCADA 预处理器生成。

入侵事件工作流程页面

如果监控的流量违反策略，当前入侵策略中启用的预处理器规则、解码器规则和入侵规则就会生成入侵事件。

Firepower 系统提供使用事件数据填充的一组预定义工作流程，可用于查看和分析入侵事件。每个这些工作流程都会引导您浏览一系列页面，从而帮助您要确定要评估的入侵事件。

预定义的入侵事件工作流程包含三种不同类型的页面（又称为事件视图）：

- 一个或多个下钻式页面
- 入侵事件的表视图
- 数据包视图

向下钻取页面通常在一个表中包含两列或更多列（对于某些向下钻取视图，有多个表），通过其可查看一种特定类型的信息。

“向下钻取”以查找有关一个或多个目标端口的详细信息时，将会自动选择这些事件，然后显示工作流程中的下一页。这样，下钻式表就能够帮助减少一次分析的事件数。

入侵事件的初始表视图在其各自的行中列出每个入侵事件。表中的各列列出各种信息，例如，时间、源 IP 地址、源端口、目标 IP 地址、目标端口、事件优先级和事件消息，等等。

选择表视图中的事件时，可以先不选择事件并显示工作流程中的下一页，而是为事件添加限制条件。限制条件是对要分析的事件类型施加的限制。

例如，如果点击任何列中的关闭列图标 ( ) 并从下拉列表清除 **Time**，可以将 Time 作为一列移除。要减少分析中事件列表的事件数，可以点击表视图中任何行中某个值的链接。例如，要将分析范围缩小为从其中一个源 IP 地址（假设是潜在攻击者）生成的事件，请点击 **Source IP Address** 列中的 IP 地址。

如果选择表中的一行或多行，然后点击 **View**，将会显示数据包视图。数据包视图提供有关触发生成事件的规则或预处理器的数据包的信息。数据包中的每个部分都包含有关数据包中特定层的信息。可以展开折叠的部分以了解详细信息。

注释 由于每个端口扫描事件均由多个数据包触发，因此，端口扫描事件使用特殊版本的数据包视图。

如果预定义工作流程无法满足您的特定需求，则您可以创建仅显示您感兴趣的信息的自定义工作流程。自定义入侵事件工作流程可以包含向下钻取页面和/或事件表视图；系统自动将数据包视图包含作为最后一页。根据调查事件的需要，您可以轻松地在预定义工作流程和自定义工作流程之间切换。

使用入侵事件工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

事件的下钻式视图和表视图共享一些常见功能，这些功能可用于缩小事件列表，以便将分析焦点集中到一组相关事件上。

为了避免在不同的工作流程页面上显示相同的入侵事件，当您点击位于页面底部的链接显示另一页事件时，事件范围会暂停；当您在后续页面上点击以执行任何其他操作时，事件范围将会继续。

提示 在操作过程中，可以随时将限制条件保存为一组搜索条件。例如，如果您发现几天内您的网络被来自某个 IP 地址的攻击者探测，您可以在调查期间保存限制条件，以供日后再次使用。但是，不能将复合限制条件保存为一组搜索条件。

过程

步骤 1 使用**分析 (Analysis)** > **入侵 (Intrusions)** > **事件 (Events)**访问入侵事件工作流程。

步骤 2 或者，限制事件视图中显示的入侵事件数，如入侵事件向下钻取页面限制，第 1557 页或入侵事件表视图限制，第 1557 页中所述。

步骤 3 有以下选项可供选择：

- 要了解有关显示的列的详细信息，请参阅入侵事件字段，第 1541 页。
- 要查看主机的配置文件，请点击显示在主机 IP 地址旁边的主机配置文件图标 ()。
- 要查看地理位置详细信息，请点击“源国家/地区”(Source Country) 或“目标国家/地区”(Destination Country) 列中显示的旗帜图标。
- 要修改所显示事件的时间和日期范围，请参阅更改时间窗口，第 1461 页。

  提示 如果入侵事件未显示在事件视图中，调整指定的时间范围可能会返回结果。建议不要指定旧的时间范围，因为旧时间范围内的事件可能已被删除。调整规则阈值配置可能生成事件。

  注释 如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间段（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。

- 要在当前工作流程页面排序事件或在当前工作流程页面内导航，请参阅使用工作流程，第 1442 页。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- 要将事件添加到剪贴板，以便可在以后将其传输到事故，请点击**复制 (Copy)** 或**全部复制 (Copy All)**。
- 要从事件数据库中删除事件，选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。
- 要将事件标记为“已审核”以将其从入侵事件页面上移除，但不将其从事件数据库中移除，请参阅将入侵事件标记为“已审核”，第 1551 页。
- 要下载触发每个所选事件的数据包的本地副本（libpcap 格式的数据包捕获文件），请选中由要下载的数据包触发的事件旁边的复选框，然后点击**下载数据包 (Download Packets)** 或点击**下载所有数据包 (Download All Packets)**。捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。
- 要导航至其他事件视图以查看关联事件，请参阅工作流程间导航，第 1466 页。

- 要暂时使用另一个工作流程，请点击**切换工作流 (switch workflow)**。
- 要为当前页面添加书签以便快速返回该页面，请点击**将此页面加入书签 (Bookmark This Page)**。
- 要查看“摘要”(Summary) 控制面板的“入侵事件”(Intrusion Events) 部分，请点击**控制面板 (Dashboards)**。
- 要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。
- 要根据当前视图中的数据生成报告，请参阅从事件视图创建报告模板，第 1345 页。

入侵事件向下钻取页面限制

下表介绍如何使用向下钻取页面。

表 *277*：限制向下钻取页面上的事件

所需的操作…	您可以.....
向下钻取到下一个限制特定值的工作流程页面	点击该值。 例如，在 Destination Port 工作流程中，要将事件限制为目标端口为 80 端口的事件，请点击 **DST Port/ICMP Code** 列中的 **80/tcp**。屏幕上将会显示工作流程的下一页（Events 页面），其中仅包含 80/tcp 端口事件。
向下钻取到下一个限制选定事件的工作流程页面	选择要在下一个工作流程页面上查看的事件旁边的复选框，然后点击 **View**。 例如，在 Destination Port 工作流程中，要将事件限制为目标端口为 20/tcp 和 21/tcp 端口的事件，请选择这些端口对应行旁边的复选框，然后点击 **View**。屏幕上将会显示工作流程的下一页（Events 页面），其中仅包含 20/tcp 和 21/tcp 端口事件。 请注意，如果对多行施加限制，并且表具有多列（不包括“计数”[Count] 列），则会构建复合限制。复合限制条件确保仅将计划内的事件纳入限制中。例如，如果使用 Event and Destination 工作流程，在第一个向下钻取页面上选择的每一行都会创建一个复合限制条件。如果选择目标 IP 地址为 10.10.10.100 的事件 1:100，并且选择目标 IP 地址为 192.168.10.100 的事件 1:200，那么，复合限制条件确保您不会选择事件类型为 1:100 且目标 IP 地址为 192.168.10.100 的事件或事件类型为 1:200 且目标 IP 地址为 10.10.10.100 的事件。
向下钻取到下一个保留当前限制的工作流程页面	点击 **View All**。

入侵事件表视图限制

下表介绍如何使用表视图。

表 *278*：限制事件表视图中的事件

所需的操作…	您可以.....
将视图限制为仅显示具有单个属性的事件	点击该属性。 例如，要将视图限制为仅显示目标端口为 80 端口的事件，请点击 **DST Port/ICMP Code** 列中的 **80/tcp**。
从表中移除列	在要隐藏的列标题中点击关闭图标 ( )。在显示的弹出窗口中，点击 **Apply**。 如果要隐藏或显示其他列，请选择或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用的列重新添加到视图中，请点击展开箭头( )展开搜索条件，然后点击**已禁用的列(Disabled Columns)** 下的列名。
查看与一个或多个事件相关的数据包	执行以下其中一种操作： • 点击要查看的数据包的事件旁边的向下箭头图标 ( )。 • 选择要查看的一个或多个数据包，然后点击页面底部的 **View**。 • 在页面底部，点击**查看全部 (View All)** 以查看与当前限制条件匹配的所有事件。

使用入侵事件数据包视图

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

数据包视图提供有关触发生成入侵事件的规则的数据包的信息。

提示 如果用于检测事件的设备的**传输数据包 (Transfer Packet)** 选项已禁用，则 Firepower 管理中心上的数据包视图不包含数据包信息。

数据包视图通过提供有关数据包触发的入侵事件的信息来指示捕获特定数据包的原因，这些信息包括事件的时间戳、消息、分类和优先级（如果事件由标准文本规则生成，则还包括生成事件的规则）。数据包视图还提供有关数据包的一般信息（例如大小）。

此外，数据包视图还有一个介绍数据包中每一层（数据链路层、网络层和传输层）的部分，以及一个介绍组成数据包的字节的部分。如果系统已解密数据包，可以查看解密的字节。可以展开折叠的部分以显示详细信息。

注释 由于每个端口扫描事件均由多个数据包触发，因此，端口扫描事件使用特殊版本的数据包视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 在入侵事件的表视图中，选择要查看的数据包，如入侵事件表视图限制，第 1557 页中所述。

步骤 2 或者，如果选择多个事件，可以使用页面底部的页码来浏览数据包视图中的数据包。

步骤 3 此时，您还有以下选择：

- 调整 - 要修改数据包视图中的日期和时间范围，请参阅更改时间窗口，第 1461 页。
- 剪贴板 - 要将事件添加到剪贴板，以便可在以后将其传输到事故，请点击**复制 (Copy)** 以复制您正在查看其数据包的事件，或点击**全部复制 (Copy All)** 以复制您之前已选择其数据包的所有事件。
- 配置 - 要配置触发事件的入侵规则，请点击“操作”(Actions) 旁边的箭头，然后如在数据包视图中配置入侵规则，第 1562 页中所述继续操作。
- 删除 - 要从数据库删除事件，请点击**删除 (Delete)** 以删除您正在查看其数据包的事件，或点击**全部删除 (Delete All)** 以删除您之前已选择其数据包的所有事件。
- 下载 - 要下载触发事件的数据包的本地副本（libpcap 格式的数据包捕获文件），请点击**下载数据包 (Download Packet)** 以保存您正在查看的事件的已捕获数据包的副本，或点击**下载所有数据报 (Download All Packets)** 以保存您之前已选择其数据包的所有事件的已捕获数据包的副本。捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。

  注释 不能下载端口扫描数据包，因为单个端口扫描事件基于多个数据包；但端口扫描视图提供所有可用的数据包信息。要下载，必须至少有 15% 的可用磁盘空间。
- 标记为已审核 - 要将事件标记为“已审核”以从事件视图中将其移除，但不从事件数据库中移除，请点击**审核 (Review)** 以标记您正在查看其数据包的事件，或点击**全部审核 (Review All)** 以标记您之前已选择其数据包的所有事件。有关详细信息，请参阅将入侵事件标记为“已审核”，第 1551 页。
- 查看其他信息 - 要展开或折叠页面部分，请点击该部分旁边的箭头。有关详细信息，请参阅事件信息字段，第 1559 页、帧信息字段，第 1565 页和数据链路层信息字段，第 1566 页。
- 查看网络层信息 - 请参阅查看网络层信息，第 1567 页。
- 查看数据包字节信息 - 请参阅查看数据包字节信息，第 1572 页。
- 查看传输层信息 - 请参阅 查看传输层信息，第 1569 页

事件信息字段

在数据包视图上，可以查看有关 Event Information 部分中数据包的信息。

Event

事件消息。对于基于规则的事件，这相当于规则消息。对于其他事件，这取决于解码器或预处理器。

事件 ID 以 (GID:SID:Rev) 格式附加到消息后面。GID 是生成事件的规则引擎、解码器或预处理器的生成器 ID。SID 是规则、解码器消息或预处理器消息的标识符。Rev 是规则的修订号。

Timestamp

捕获数据包的时间。

分类

事件分类。对于基于规则的事件，这相当于规则分类。对于其他事件，这取决于解码器或预处理器。

优先级

事件优先级。对于基于规则的事件，这相当于 `priority` 关键字或 `classtype` 关键字的值。对于其他事件，这取决于解码器或预处理器。

Ingress Security Zone

触发事件的数据包的入口安全区域。在被动部署中仅填充此安全区域字段。

Egress Security Zone

触发事件的数据包的出口安全区域。在被动部署中未填充此字段。

域

受管设备所属的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

设备

已部署访问控制策略的受管设备。

请注意，堆叠配置中的主设备和辅助设备就像独立设备一样报告入侵事件。

安全情景

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 填充此字段。

入口接口

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。

出口接口

对于内联部署，触发事件的数据包的出口接口。

Source/Destination IP

触发事件的数据包源自的（源）主机 IP 地址或域名，或触发事件的流量的目标主机。

Source Port/ICMP Type

触发事件数据包的源端口。对 ICMP 流量，当没有端口号时，系统显示 ICMP 类型。

Destination Port/ICMP Code

接收流量的主机的端口号。对 ICMP 流量，当没有端口号时，系统显示 ICMP 代码。

Email Headers

提取自邮件报头的数据。请注意，邮件报头不显示在入侵事件表视图中，但可以将邮件报头数据作为搜索条件。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器 **Log Headers** 选项。对基于规则的事件，提取邮件数据时会显示此行。

HTTP Hostname

提取自 HTTP 请求主机报头的主机名（如果有）。此行显示完整的主机名（最多包含 256 个字节）。如果完整主机名不再是单行，则可以将其展开。

要显示主机名，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。

请注意，HTTP 请求数据包并非总是包含主机名。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI（如果有）。此行显示完整 URI（最多包含 2048 个字节）。如果完整 URL 不再是单行，则可以将其展开。

要显示 URI，必须启用 HTTP 检查预处理器 **Log URI** 选项。

请注意，HTTP 请求数据包并非总是包含 URI。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。

入侵策略

启用了生成入侵事件的入侵规则、预处理器规则或解码器规则的入侵策略（如果有）。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则相关联。

访问控制策略

包含启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略的访问控制策略。

Access Control Rule

与生成事件的入侵规则关联的访问控制规则。默认操作指示启用了规则的入侵策略未与访问控制规则关联，而是配置为访问控制策略的默认操作。

规则

对于标准文本规则事件，是指生成事件的规则。

请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

由于规则数据可能包含有关网络的敏感信息，管理员可以使用用户角色编辑器中的 View Local Rules 权限来设置用户查看数据包视图中的规则信息的权限。

操作

对于标准文本规则事件，展开**操作 (Actions)** 以对触发事件的规则执行以下任何操作：

- 编辑规则
- 查看有关规则修订的文档
- 向规则添加注释
- 更改规则的状态
- 设置规则的阈值
- 抑制规则

请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

在数据包视图中配置入侵规则

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在入侵事件的数据包视图中，可以对触发事件的规则执行几项操作。请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 有以下选项可供选择：

- 注释 - 对于标准文本规则事件，点击**规则注释 (Rule Comment)** 可以向生成事件的规则添加文本注释。这样做可以提供有关规则以及其识别出的漏洞或策略违规的额外上下文和信息。还可以在入侵规则编辑器中添加和查看规则注释。
- 禁用 - 点击**禁用此规则...(Disable this rule...)** 可禁用规则。
  如果此事件由标准文本规则生成，必要时可以禁用此规则。可以在能够在本地编辑的所有策略中设置此规则。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

注释　**不能**从数据包视图禁用共享对象规则，也不能禁用默认策略中的规则。

- 丢弃数据包 - 点击**将此规则设置为丢弃触发数据包...(Set this rule to drop the triggering packet...)**可将规则设置为丢弃触发该事件的数据包。
  如果受管设备在网络中以内联方式部署，可以在能够在本地编辑的所有策略中将触发事件的规则设置为丢弃触发该规则的数据包。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。请注意，仅在当前策略中启用了 **Drop when Inline** 的情况下，才会显示此选项。

- 编辑 - 对于标准文本规则事件，点击**编辑 (Edit)** 可修改生成事件的规则。如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

  注释　如果编辑由系统提供的规则（而不是自定义的标准文本规则），则实际上会创建新的本地规则。请确保将本地规则设置为生成事件，并禁用当前入侵策略中的原始规则。但请注意，**不能**启用默认策略中的本地规则。

- 生成事件 - 点击**将此规则设置为生成事件...(Set this rule to generate events...)** 可将规则设置为生成事件。
  如果此事件由标准文本规则生成，则可以将规则设置为在可本地编辑的所有策略中生成事件。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

  注释　**不能**将共享对象规则设置为从数据包视图生成事件，也不能禁用默认策略中的规则。

- 设置抑制选项 - 展开**设置抑制选项 (Set Suppression Options)**，然后如在数据包视图中设置抑制选项，第 1565 页中所述继续操作。
  可以使用此选项以在能够在本地编辑的所有策略中抑制触发此事件的规则。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中抑制此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

- 设置阈值选项 - 展开**设置抑制选项 (Set Thresholding Options)**，然后如在数据包视图中设置阈值选项，第 1564 页中所述继续操作。
  可以使用此选项在能够在本地编辑的所有策略中为触发此事件的规则创建阈值。或者，如果能够在本地编辑当前策略，可以仅为当前策略（即，生成事件的策略）创建阈值。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认入侵策略。

- 查看文档 - 对于标准文本规则事件，点击**查看文档 (View Documentation)** 可了解有关生成事件的规则修订版的详细信息。

在数据包视图中设置阈值选项

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

通过在入侵事件的数据包视图中设置阈值选项，可以控制每个规则随时间推移生成的事件数。可以在能够在本地编辑的所有策略中设置阈值选项；或者，如果能够在本地编辑策略，可以仅在当前策略（即，导致事件生成的策略）中设置阈值选项。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 展开**设置阈值选项 (Set Thresholding Options)**，并在两个选项中选择一个：

- **in the current policy**
- **in all locally created policies**

  注释 仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

步骤 3 选择要设置的阈值的类型：

- 点击**限制 (limit)** 以将通知限制为每个时间段内仅为指定数目的事件实例提供通知。
- 点击**阈值 (threshold)** 为每个时间段内每发生指定数目的事件实例提供通知。
- 点击**两者 (both)** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 4 点击相应的单选按钮，以指明是要按**源 (Source)** 还是**目标 (Destination)** IP 地址跟踪事件实例。

步骤 5 在**计数 (Count)** 字段中，输入要用作阈值的事件实例数。

步骤 6 在**秒 (Seconds)** 字段中，输入一个 1 和 86400 之间的数字来指定跟踪事件实例的时间段。

步骤 7 如果要覆盖现有入侵策略中的规则的所有当前阈值，请选中**覆盖此规则的任何现有设置 (Override any existing settings for this rule)** 复选框。

步骤 8 点击 **Save Thresholding**。

在数据包视图中设置抑制选项

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以使用抑制选项抑制全部入侵事件或者基于源或目标IP地址抑制入侵事件。可在在能够在本地编辑的所有策略中设置抑制选项。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置抑制选项。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 展开**设置抑制选项 (Set Suppression Options)**，并在两个可能的选项中选择一个：

- **in the current policy**
- **in all locally created policies**

注释 仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

步骤 3 选择以下其中一个**跟踪方式 (Track By)** 选项：

- 点击**源 (Source)** 可抑制由指定源 IP 地址发出的数据包生成的事件。
- 点击**目标 (Destination)** 可抑制由发往指定目标 IP 地址的数据包生成的事件。
- 点击**规则 (Rule)** 可完全抑制触发此事件的规则的事件。

步骤 4 在 **IP address or CIDR block** 字段中，输入要指定为源或目标 IP 地址的 IP 地址或 CIDR 块/前缀长度。

步骤 5 点击 **Save Suppression**。

帧信息字段

在数据包视图中，点击 **Frame** 旁边的箭头可查看捕获的帧的信息。数据包视图可以显示单个帧或多个帧。每个帧提供有关单个网络数据包的信息。您会看到多个帧，例如，对于已标记的数据包或重组的 TCP 数据流中的数据包。

Frame n

捕获的帧，其中，*n*为1（对于单帧数据包）或递增帧编号（对于多帧数据包）。帧中捕获的字节数将附加到帧编号后面。

Arrival Time

捕获帧的日期和时间。

Time delta from previous captured frame

对于多帧数据包，表示自捕获上一个帧以来经过的时间。

Time delta from previous displayed frame

对于多帧数据包，表示自显示上一个帧以来经过的时间。

Time since reference or first frame

对于多帧数据包，表示自捕获第一个帧以来经过的时间。

Frame Number

递增的帧编号。

Frame Length

帧的长度，以字节为单位。

Capture Length

捕获的帧的长度，以字节为单位。

Frame is marked

帧是否被标记（true 或 false）。

Protocols in frame

帧中包括的协议。

数据链路层信息字段

在数据包视图中，点击数据链路层协议（例如，**Ethernet II**）旁边的箭头可查看有关数据包的数据链路层信息，这些信息包括源主机和目标主机的 48 位介质访问控制 (MAC) 地址。它还可能显示有关数据包的其它信息，取决于硬件协议。

注释 请注意，本示例讨论以太网链路层信息；也可能出现其他协议。

数据包视图反映数据链路层使用的协议。以下列表说明在数据包视图中可能会看到的以太网 II 或 IEEE 802.3 以太网数据包的信息。

目标

目标主机的 MAC 地址。

注释 以太网还可以使用组播地址和广播地址作为目标地址。

来源

源主机的 MAC 地址。

Type

对于以太网 II 数据包，代表在以太网帧中封装的数据包的类型；例如，IPv6 或 ARP 数据报。请注意，此项目仅对以太网 II 数据包显示。

长度

对于 IEEE 802.3 以太网数据包，代表数据包的长度（以字节为单位，不包括校验和）。请注意，此项目仅对 IEEE 802.3 以太网数据包显示。

查看网络层信息

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

在数据包视图中，点击网络层协议（例如，**Internet Protocol**）旁边的箭头可查看有关与数据包相关的网络层的更多详细信息。

注释 请注意，本示例讨论 IP 数据包；也可能出现其他协议。

IPv4 网络层信息字段

以下列表介绍在 IPv4 数据包中可能显示的协议特定信息。

版本

互联网协议的版本号。

Header Length

报头（包括任何 IP 选项）中的字节数。不带选项的 IP 报头的长度为 20 字节。

Differentiated Services Field

差分服务的值，用以指明发送主机如何支持显式堵塞通知 (ECN)：

- `0x0` - 不支持具有 ECN 功能的传输 (ECT)

- `0x1` 和 `0x2` - 支持 ECT
- `0x3` - 堵塞情况 (CE)

总长度

IP 数据包的长度（以字节为单位，不包括 IP 报头在内）。

标识

唯一标识源主机发送的 IP 数据报的值。此值用于跟踪同一数据报的数据分片。

标志

控制 IP 分片的值，其中：

Last Fragment 标志的值指明是否有更多与数据报相关的分片。

- `0` - 没有更多与数据报相关的分片
- `1` - 有更多与数据报相关的分片

Don’t Fragment 标志的值控制数据报是否可以分片：

- `0` - 数据报可以分片
- `1` - 数据报**不**可分片

分段偏移量

自数据报开始以来分片偏移量的值。

Time to Live (ttl)

数据包在过期之前可以在路由器之间跳转的剩余跳数。

协议

封装在 IP 数据报中的传输协议；例如，ICMP、IGMP、TCP 或 UDP。

报头校验和

指明 IP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

Source/Destination

源（或目标）主机的 IP 地址或域名。

请注意，要显示域名，必须启用 IP 地址解析。

点击地址或域名查看上下文菜单，然后选择 **Whois** 可在主机上执行 whois 搜索，选择 **View Host Profile** 可查看主机信息，选择 **Blacklist Now** 或 **Whitelist Now** 可将地址添加到全局黑名单或白名单。

IPv6 网络层信息字段

以下列表介绍在 IPv6 数据包中可能显示的协议特定信息。

流量类别

IPv6 报头中的试验性 8 位字段，用于识别 IPv6 数据包类别或优先级，类似于 IPv4 提供的差分服务功能。未使用时，此字段设为零。

流标签

可选的 20 位 IPv6 十六进制值（从 1 到 FFFFF），用于识别特殊流（例如，非默认服务质量和实时服务）。未使用时，此字段设为零。

负载长度

表示 IPv6 负载中八位组数的 16 位字段，负载由 IPv6 报头后面的所有数据包组成，包括任何扩展报头。

下一报头

表示紧随 IPv6 报头之后的报头类型的 8 位字段，使用与 IPv4 协议字段相同的值。

跳数限制

一个 8 位十进制整数，其中用于转发数据包的每个节点每次减 1。如果递减的值达到零，则丢弃数据包。

来源

源主机的 128 位 IPv6 地址。

目标

目标主机的 128 位 IPv6 地址。

查看传输层信息

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

步骤 1 在数据包视图中，点击传输层协议（例如，**TCP**、**UDP** 或 **ICMP**）旁边的箭头。

步骤 2 或者，点击**数据 (Data)**（如果显示）可在紧接其上方的数据包视图的“数据包信息”(Packet Information) 部分中查看协议负载的前二十四个字节。

步骤 3 查看 TCP、UDP 和 ICMP 协议的传输层内容，如TCP 数据包视图字段，第 1570 页、UDP 数据包视图字段，第 1571 页或ICMP 数据包视图字段，第 1571 页中所述。

注释 请注意，这些示例讨论 TCP、UDP 和 ICMP 数据包；也可能出现其他协议。

TCP 数据包视图字段

本节介绍 TCP 数据包的特定于协议的信息。

源端口

用于识别发起应用协议的编号。

目的端口

用于识别接收应用协议的编号。

序列号

当前 TCP 分段中第一个字节的值，包含在 TCP 数据流中的初始序列号中。

Next sequence number

在响应数据包中，要发送的下一个数据包的序列号。

确认号

TCP 确认，包含在之前接受的数据的序列号中。

Header Length

报头中的字节数。

标志

六位，表示 TCP 分段的传输状态：

- `U` - 紧急指针有效
- `A` - 确认号有效
- `P` - 接收方应推送数据
- `R` - 重置连接

- S - 同步序列号以开始新连接
- F - 发送方完成发送数据

窗口大小

接收主机将接受的未确认数据数量（以字节为单位）。

校验和

指明 TCP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

Urgent Pointer

TCP 分段中发送紧急数据的位置（如果存在）。与 U 标记一起使用。

Options

TCP 选项的值（如果有）。

UDP 数据包视图字段

本节介绍 UDP 数据包的特定于协议的信息。

源端口

用于识别发起应用协议的编号。

目的端口

用于识别接收应用协议的编号。

长度

UDP 报头和数据的总长度。

校验和

指明 UDP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

ICMP 数据包视图字段

本节介绍 ICMP 数据包的特定于协议的信息。

Type

ICMP 消息的类型：

- 0 - 回应应答
- 3 - 目标不可达
- 4 - 源抑制
- 5 - 重定向

- 8 - 回应请求
- 9 - 路由器通告
- 10 - 路由器请求
- 11 - 超时
- 12 - 参数问题
- 13 - 时间戳请求
- 14 - 时间戳应答
- 15 - 信息请求（过时）
- 16 - 信息应答（过时）
- 17 - 地址掩码请求
- 18 - 地址掩码应答

代码

ICMP 消息类型随附的代码。ICMP 消息类型 3、5、11 和 12 都有一个相应的代码，如 RFC 792 中所述。

校验和

指名 ICMP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

查看数据包字节信息

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

过程

在数据包视图中，点击 **Packet Bytes** 旁边的箭头可查看构成数据包的字节的十六进制和 ASCII 版本。如果系统已解密流量，可以查看解密的数据包字节。

入侵事件剪贴板

剪贴板是一个保留区域，可从任何入侵事件视图复制入侵事件到其中。

剪贴板的内容按生成事件的日期和时间排序。在将入侵事件添加到剪贴板之后，可以将它们从剪贴板删除以及根据剪贴板内容生成报告。

还可以将剪贴板中的入侵事件添加到事故（怀疑涉及到对安全策略的可能违反的事件的集合）。

生成剪贴板报告

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

可以为剪贴板中的事件生成报告，就像从任何事件视图中执行此操作一样。

开始之前

- 如使用入侵事件工作流程，第 1555 页或使用入侵事件数据包视图，第 1558 页中所述，将一个或多个事件添加到剪贴板。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **剪贴板 (Clipboard)**。

步骤 2 您有以下选择：

- 要包括剪贴板上某个页面中的特定事件，请导航到该页面，选中该事件旁边的复选框，然后点击**生成报告 (Generate Report)**。
- 要包括剪贴板中的所有事件，点击 **Generate Report All**。

步骤 3 指定报告布局，然后点击 **Generate**。

步骤 4 选择一种或多种输出格式，或者也可以修改任何其他设置。

步骤 5 点击 **Generate**，然后点击 **Yes**。

步骤 6 有以下选项可供选择：

- 点击报告链接以在新窗口中显示该报告。
- 点击**确定 (OK)** 返回到“报告模板”(Report Templates) 页面，可在其中修改报告设计。

从剪贴板删除事件

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

如果在剪贴板上有不想添加到事故的入侵事件，可以删除事件。

注释 从剪贴板删除事件**不会**从事件数据库删除该事件。但是，从事件数据库删除事件会从剪贴板删除该事件。

过程

步骤 1 选择**分析 (Analysis)** > **入侵 (Intrusions)** > **剪贴板 (Clipboard)**。

步骤 2 您有以下选择：

- 删除特定事件 - 要删除剪贴板上某个页面中的特定入侵事件，请导航至该页面，选中事件旁边的复选框，然后点击**删除 (Delete)**。
- 删除所有事件 - 要删除剪贴板中的所有入侵事件，请点击**全部删除 (Delete All)**。请注意，如果选择“事件首选项”(Event Preferences) 中的**确认“所有”操作 (Confirm “All” Actions)** 选项，系统首先会提示您确认是否要删除所有事件。

查看入侵事件统计信息

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

Intrusion Event Statistics 页面提供设备当前状态和网络生成的所有入侵事件的简要摘要。

页面上显示的每个 IP 地址、端口、协议和事件消息等均为链接。点击任意链接可查看相关的事件信息。例如，如果前 10 大目标端口之一是 `80 (http)/tcp`，点击该链接会显示默认入侵事件工作流程的第一个页面，并列出以该端口为目标的事件。请注意，只会显示当前时间范围内的事件（以及生成事件的受管设备）。此外，标记为“已审核”的入侵事件会继续显示在统计信息中。例如，如果当前时间范围是过去一小时，但第一个事件是在五小时前生成的，当点击 **First Event** 链接时，打开的事件页面将不会显示事件，直至时间范围被更改。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述 (Overview)** > **摘要 (Summary)** > **入侵事件统计信息 (Intrusion Event Statistics)**。

步骤 2 从页面顶部的两个选择框选择要查看其统计信息的区域和设备，或者选择**所有安全区域 (All Security Zones)** 和**所有设备 (All Devices)** 以查看收集入侵事件的所有设备的统计信息。

步骤 3 点击 **Get Statistics**。

提示 要查看自定义时间范围内的数据，请点击页面右上角区域的链接并按照更改时间窗口，第 1461 页中的指示操作。

主机统计信息

“入侵事件统计信息”(Intrusion Event Statistics) 页面的“主机统计信息”(Host Statistics) 部分提供有关设备本身的信息。在Firepower 管理中心上，此节还提供有关所有受管设备的信息。

这些信息包括以下内容：

Time

设备的当前时间。

正常运行时间

设备本身重新启动以来的天数、小时数和分钟数。在Firepower 管理中心上，Uptime 还显示每个受管设备上一次重新启动的时间、已登录用户数和平均负载。

磁盘使用情况

正使用的磁盘空间的百分比。

内存使用率

正使用的系统内存的百分比。

Load Average

过去 1 分钟、5 分钟和 15 分钟内 CPU 队列的平均进程数。

事件概述

Intrusion Event Statistics 页面的 Event Overview 章节提供入侵事件数据库中信息的概述。

这些统计信息包括以下内容：

活动

入侵事件数据库中的事件数。

时间范围内的事件 (Events in Time Range)

当前选定的时间范围以及数据库中属于该时间范围的事件数量和所占百分比。

第一个事件 (First Event)

事件数据库中第一个事件的事件消息。

上一事件

事件数据库中最后一个事件的事件消息。

注释 如果在 Firepower 管理中心上查看入侵事件数据时选择受管设备，将会转而显示该设备的“事件概述”(Event Overview) 部分。

事件统计信息

Intrusion Event Statistics 页面的 Event Statistics 部分提供有关入侵事件数据库中信息的更具体信息。这些信息包括以下方面的详细信息：

- 前 10 大事件类型
- 前 10 大源 IP 地址
- 前 10 大目标 IP 地址
- 前 10 大目标端口
- 具有最大数量事件的协议、入口安全区域、出口安全区域和设备

注释 在多域部署中，系统会为每个枝叶域构建单独的网络映射。因此，枝叶域可以包含这样一个 IP 地址，该地址在它的网络内是唯一的，但与另一枝叶域中的 IP 地址完全相同。在祖先域中查看事件统计信息时，系统可以展示该重复IP地址的多个实例。初看上去，似乎是重复条目。但是，如果向下展开到每个 IP 地址的主机配置数据，则系统会显示它们属于不同的枝叶域。

查看入侵事件性能图表

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

在入侵事件性能页面上，可生成用于说明Firepower管理中心或受管设备的入侵事件在特定时间段内的性能统计信息的图表。可以生成图表来反映每秒入侵事件数、每秒兆位数、每个数据包的平均字节数、Snort 未检查的数据包百分比以及因 TCP 标准化而被阻止的数据包数量。这些图表可以显示过去一小时、前一天、上一周或上个月的运行统计信息。

注释 新数据将进行累计，统计信息图表每五分钟更新一次。因此，如果快速重新加载图表，直到下一次五分钟更新间隔之前数据可能不会更改。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述 (Overview)** > **摘要 (Summary)** > **入侵事件性能 (Intrusion Event Performance)**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择要查看其数据的设备。

步骤 3 从**选择图表 (Select Graph[s])** 列表中，选择要创建的图表类型，如入侵事件性能统计信息图表类型，第 1577 页中所述。

步骤 4 从**选择时间范围 (Select Time Range)** 列表中，选择要用于图表的时间范围。

步骤 5 点击 **Graph**。

步骤 6 要保存图表，请右键单击它并按照浏览器的指示保存图像。

入侵事件性能统计信息图表类型

下表列出了可用的图表类型。请注意，如果图表类型填充的数据受网络分析策略的**内联模式 (Inline Mode)** 设置影响，则图表类型显示会有所不同。如果禁用**内联模式 (Inline Mode)**，Web 界面上标有星号 (*) 的图表类型（在下方列中列出 `yes`）会使用有关流量的数据进行填充；如果禁用**内联模式 (Inline Mode)**，则系统会修改或丢弃数据。

表 *279*：入侵事件性能图表类型

要为以下项生成数据：	您必须.....	代表含义.....	是否受 **Inline Mode** 影响？
平均字节/数据包	n/a	每个数据包中包含的平均字节数。	否
在 TCP 流量/数据包中规范化的 ECN 标志	启用 **Explicit Congestion Notification** 并选择 **Packet**	无论是否协商，以数据包为单位，已为其清除 ECN 标记的数据包的数量。	yes
在 TCP 流量/会话中规范化的 ECN 标记	启用 **Explicit Congestion Notification** 并选择 **Stream**	未协商使用 ECN 使用时，以数据流为单位，ECN 标记被清除的次数。	yes
Events/Sec	n/a	设备上每秒生成的事件数。	否
ICMPv4 回显规范化	启用 **Normalize ICMPv4**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv4 数据包的数量。	yes
ICMPv6 回显规范化	启用 **Normalize ICMPv6**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv6 数据包的数量。	yes
IPv4 DF 标记规范化	启用**规范化 IPv4 (Normalize IPv4)** 和**规范化不分片位 (Normalize Don’t Fragment Bit)**	IPv4 Flags 报头字段的一位 Don’t Fragment 子字段被清除的 IPv4 数据包的数量。	yes

要为以下项生成数据：	您必须.....	代表含义.....	是否受 **Inline Mode** 影响？
IPv4 选项规范化	启用 **Normalize IPv4**	选项八位字节被设置为 1 (No Operation) 的 IPv4 数据包的数量。	yes
IPv4 保留标记规范化	启用**规范化 IPv4 (Normalize IPv4)** 和**规范化保留位 (Normalize Reserved Bit)**	IPv4 Flags 报头字段的一位 Reserved 子字段被清除的 IPv4 数据包的数量。	yes
IPv4 调整大小规范化	启用 **Normalize IPv4**	已按照 IP 报头中指定数据报长度截断多余长度负载的 IPv4 数据包的数量。	yes
IPv4 TOS 规范化	启用**规范化 IPv4 (Normalize IPv4)** 和**规范化 TOS 位 (Normalize TOS Bit)**	单字节 Differentiated Services (DS) 字段（之前叫做 Type of Service (TOS) 字段）被清除的 IPv4 数据包的数量。	yes
IPv4 TTL 规范化	启用 **Normalize IPv4**、**Maximum TTL** 和 **Reset TTL**	IPv4 生存时间规范化的数量。	yes
IPv6 选项规范化	启用 **Normalize IPv6**	Hop-by-Hop Options 或 Destination Options 扩展报头中 Option Type 字段设置为 `00`（跳过并继续处理）的 IPv6 数据包的数量。	yes
IPv6 TTL 规范化	启用 **Normalize IPv6**、**Minimum TTL** 和 **Reset TTL**	IPv6 跳数限制 (TTL) 规范化的数量。	yes
兆位/秒	n/a	每秒通过设备的流量兆位数。	否
调整大小以适应 MSS 的数据包规范化	启用 **Trim Data to MSS**	负载长于 TCP Data 字段，因而被调整至 Maximum Segment Size 的数据包的数量。	yes
调整大小以适应 TCP 窗口的数据包规范化	启用 **Trim Data to Window**	TCP Data 字段被调整以适应接收主机的 TCP 窗口的数据包的数量。	yes
丢包率	n/a	所有选定设备上未经检查的数据包的平均百分比。例如，如果选择两个设备，那么平均百分比 50% 可能表示一个设备的丢包率为 90%，另一个的丢包率为 10%。也可能表示这两个设备的丢包率均为 50%。当选择一个设备时，此图表仅表示总丢包率。	否
数据条带化的 RST 数据包规范化	启用 **Remove Data on RST**	数据被从 TCP 重置 (RST) 数据包移除的数据包的数量。	yes

要为以下项生成数据：	您必须.....	代表含义.....	是否受 **Inline Mode** 影响？
数据条带化的 SYN 数据包规范化	启用 **Remove Data on SYN**	当 TCP 操作系统不是 Mac OS 时数据被从 SYN 数据包移除的数据包的数量。	yes
TCP 报头填充规范化	启用 **Normalize/Clear Option Padding Bytes**	选项填充字节设置为 0 的 TCP 数据包的数量。	yes
无选项 TCP 规范化	启用 **Allow These TCP Options** 并设置为 `any` 之外的任意选项	Time Stamp 选项条带化的数据包的数量。	yes
TCP NS 标记规范化	启用 **Explicit Congestion Notification** 并选择 **Packet**	ECN Nonce Sum (NS) 选项规范化的数量。	yes
TCP 选项规范化	启用 **Allow These TCP Options** 并设置为 `any` 之外的任意选项	选项字段设置为 No Operation (TCP Option 1) 的选项的数量（MSS、Window Scale、Time Stamp 以及明确允许的选项除外）。	yes
TCP 数据包阻止条件规范化	启用 **Normalize TCP Payload**（分段重组必须失败）	因为 TCP 分段无法正确重组而被丢弃的数据包的数量。	yes
TCP 保留标记规范化	启用 **Normalize/Clear Reserved Bits**	Reserved 位被清除的 TCP 数据包的数量。	yes
TCP 分段重组规范化	启用 **Normalize TCP Payload**（分段重组必须成功）	TCP Data 字段已规范化以确保重传传输的数据的一致性的数据包数量（无法正确重组的所有片段都被丢失）。	yes
TCP SYN 选项规范化	启用 **Allow These TCP Options** 并设置为 `any` 之外的任意选项	由于未设置 SYN 控制位，Maximum Segment Size 或 Window Scale 选项被设置为 No Operation (TCP Option 1) 的选项的数量。	yes
TCP 时间戳 ECR 规范化	启用 **Allow These TCP Options** 并设置为 `any` 之外的任意选项	Time Stamp Echo Reply (TSecr) 选项字段由于未设置 Acknowledgment (ACK) 控制位而被清除的数据包的数量。	yes
TCP 紧急指针规范化	启用 **Normalize Urgent Pointer**	双字节 TCP 报头 Urgent Pointer 字段大于负载长度，因而被设置成负载长度的数据包的数量。	yes
被阻止的地址块总数	配置 **Inline Mode** 或 **Drop when Inline**	丢弃的数据包总数，包括规则、解码器和预处理器丢弃。	否
总计注入的数据包	配置 **Inline Mode**	在重新传输前调整大小的数据包的数量。	否

要为以下项生成数据：	您必须.....	代表含义.....	是否受 **Inline Mode** 影响？
总 TCP 过滤的数据包	配置 TCP Stream Preprocessing	由于TCP端口过滤而被数据流跳过的数据包的数量。	否
总 UDP 过滤的数据包	配置 UDP Stream Preprocessing	由于 UDP 端口过滤而被数据流跳过的数据包的数量。	否
紧急标记清除规范化	启用 **Clear URG if Urgent Pointer is Not Set**	因为未设置紧急指针，TCP 报头 URG 控制位被清除的数据包的数量。	yes
紧急指针和紧急标记清除规范化	启用 **Clear Urgent Pointer/URG on Empty Payload**	TCP 报头 Urgent Pointer 字段和 URG 控制位由于没有负载而被清除的数据包的数量。	yes
紧急指针清除规范化	启用 **Clear Urgent Pointer if URG=0**	16 位 TCP 报头 Urgent Pointer 字段由于未设置紧急 (URG) 控制位而被清除的数据包的数量。	yes

查看入侵事件图表

智能许可证	经典许可证	支持的设备	支持的域	Access
威胁	保护	任何环境	任何环境	管理员/入侵管理员

Firepower 系统提供显示入侵事件随时间推移变化趋势的图表。可为一个或所有受管设备生成时间变化范围为过去一小时至上个月的入侵事件图表。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述 (Overview)** > **摘要 (Summary)** > **入侵事件图表 (Intrusion Event Graphs)**。

步骤 2 在**选择设备 (Select Device)** 下，选择**全部 (all)** 以包括所有设备，或选择要包括在图表中的特定设备。

步骤 3 在**选择图表 (Select Graph[s])** 下，选择要生成的图表类型：

- 前 10 个目标端口
- 前 10 个源 IP 地址
- 前 10 个事件消息

步骤 4 在**选择时间范围 (Select Time Range)** 下，选择图表的时间范围：

- 过去一小时
- 最近一天
- 上周
- 上个月

步骤 5 点击 **Graph**。

第 86 章

文件/恶意软件事件和网络文件轨迹

以下主题提供文件和恶意软件事件的概述、本地恶意软件分析、动态分析、捕获文件和网络文件轨迹。

文件/恶意软件事件和网络文件轨迹概述

为了帮助您识别和减轻恶意软件的影响，Firepower 系统的文件控制、网络文件轨迹和面向 *Firepower* 的 *AMP* 组件可以检测、跟踪、捕获、分析记录和阻止（可选）文件传输（包括恶意软件文件和档案文件中的嵌套文件）。

您还可以将系统与您的组织的面向终端的 *AMP* 部署集成，以导入扫描记录、恶意软件检测和隔离以及危害表现 (IOC)。

情景管理器、控制面板和报告功能也有助于更深入地了解检测、捕获和阻止的文件及恶意软件。您也可以使用事件触发关联策略违规或者通过邮件、SMTP 或系统日志向您发出警报。

注释 Firepower 系统支持显示和输入使用 Unicode (UTF-8) 字符的文件名。但是，Unicode 文件名在 PDF 报告中以转译形式显示。此外，SMB 协议将文件名中不可打印的字符替换为英文句号。

文件和恶意软件事件

Firepower管理中心可以记录各种类型的文件和恶意软件事件。可用于任何单个事件的信息可能会根据该事件的生成方式和原因而异：

- 文件事件表示文件，包括面向 Firepower 的 AMP 检测到的恶意软件。文件事件不包含面向终端的 AMP 相关字段。
- 恶意软件事件表示面向 Firepower 的 AMP 或面向终端的 AMP 检测到的恶意软件；恶意软件事件还可以记录除来自面向终端的 AMP 部署的威胁以外的数据，例如扫描和隔离。
- 追溯性恶意软件事件表示面向 Firepower 的 AMP 检测到的其处置情况（文件是否为恶意软件）已更改的文件。

注释 由面向 Firepower 的 AMP 识别为恶意软件的字段同时生成文件事件和恶意软件事件。基于终端的恶意软件事件并不具备对应文件事件。

文件和恶意软件事件类型

File Events

系统将按照当前部署的文件策略记录当受管设备在网络流量中检测或阻止文件时生成的文件事件。

无论调用访问控制规则采用何种日志记录配置，系统生成文件事件时，都会将相关连接的终止记录到 Firepower 管理中心数据库中。

基于网络的恶意软件事件（面向 Firepower 的 AMP）

系统可以在整体访问控制配置过程中检测网络流量中的恶意软件。面向 Firepower 的 AMP 可以生成恶意软件事件，其中包含所生成事件的处置情况以及有关检测到恶意软件的方式、位置和时间的情景数据。

表 *280*：面向 *Firepower* 的 *AMP* 恶意软件事件生成场景

当面向 Firepower 的 AMP 检测到文件和.....	处理结果
成功查询 AMP 云（执行恶意软件云查找）以了解文件的处置情况	恶意软件、干净或未知
查询 AMP 云，但无法建立连接或云因其他原因而不可用	不可用 您可以查看很少一部分事件发生此情况；这是预期行为。
与文件关联的威胁评分超过检测到该文件的文件策略中定义的恶意软件威胁评分阈值，或者本地恶意软件分析识别恶意软件	恶意软件

当面向 **Firepower** 的 **AMP** 检测到文件和.....	处理结果
它包含在自定义检测列表中（手动标记为恶意软件）	自定义检测
它包含在干净的列表中（手动标记为干净）	清洁

追溯性恶意软件事件（面向 **Firepower** 的 **AMP**）

对于在网络流量中检测到的恶意软件文件，处置情况可以更改。例如，AMP 云可以确定先前被视为干净的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是干净的。当上周查询的文件的处置情况发生更改时，AMP 云会通知系统。然后将发生两件事情：

- Firepower 管理中心产生新追溯性恶意软件事件。

  新追溯性恶意软件事件代表上一周检测到的具备相同 SHA-256 哈希值的所有文件的性质发生变更。因此，这些事件包含限定信息：Firepower 管理中心接到性质变更通知的日期和时间、新性质、文件 SHA-256 哈希值以及威胁名称。它们不包含 IP 地址或其他上下文信息。

- Firepower 管理中心变更此前检测到的具有追溯事件相关 SHA-256 哈希值的文件的文件性质。

  如果文件性质变更为 Malware，Firepower 管理中心在其数据库内记录新恶意软件事件。除了新性质，新恶意软件事件信息与最初检测到文件时生成的文件事件中的信息都相同。

  如果文件处置情况更改为“干净”(Clean)，则 Firepower 管理中心不会删除恶意软件事件。相反，该事件反映处置情况更改。这表示文件性质为安全的文件能够出现在恶意软件表中，前提是它们最初被视为恶意软件。从未识别为恶意软件的文件只会出现在文件表中。

基于终端的恶意软件事件（面向 **Firepower** 的 **AMP**）

如果您的组织使用面向终端 AMP，则个人用户可以在终端（计算机和移动设备）上安装轻量级连接器。连接器可在进行上传、下载、执行、打开、复制、移动等操作后检查文件。这些连接器与 AMP 云进行通信，以确定检查的文件是否包含恶意软件。

文件被确定为恶意软件后，AMP 云会向 Firepower 管理中心发送威胁识别。AMP 云还可以向 Firepower 管理中心发送其他类型的信息，包括有关扫描、隔离、受阻执行和云召回的数据。Firepower 管理中心将这些信息记录为恶意软件事件。

注释 基于终端的恶意软件事件所报告的 IP 地址可能不在网络映射上 - 甚至可能完全不在监控的网络上。根据部署、合规性级别以及其他因素，您的组织中由面向终端的 AMP 监控的终端可能与面向 Firepower 的 AMP 监控的终端不是相同的主机。

使用文件和恶意软件事件工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

事件查看器允许您在表格中查看文件和恶意软件事件。您可以根据与您的分析相关的信息操作事件视图。在访问事件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以从广泛视图移动到更加突出重点的视图，使用这些页面评估事件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

选择以下其中一个选项：

- **分析 (Analysis)** > **文件 (Files)** > **文件事件 (File Events)**
- **分析 (Analysis)** > **文件 (Files)** > **恶意软件事件 (Malware Events)**

提示 事件表视图中的一些字段在默认情况下处于隐藏状态。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

提示 要快速查看检测到特定文件的连接，使用事件查看器中的复选框选择文件，然后从**跳转至 (Jump to)** 下拉列表中选择**连接事件 (Connections Events)**。

文件和恶意软件事件字段

文件和恶意软件事件（您可以通过工作流程查看和搜索文件和恶意软件事件）包含此部分中列出的字段。请记住，可用于任何单个事件的信息可能会根据该事件的生成方式和原因而异。

注释 由面向 Firepower 的 AMP 识别为恶意软件的字段同时生成文件事件和恶意软件事件。基于终端的恶意软件事件没有对应的文件事件，并且文件事件没有与面向终端的 AMP 相关的字段。

操作

检测文件的文件策略规则相关操作以及任何相关文件规则操作选项。

AMP 云 (AMP Cloud)

产生面向终端的 AMP 事件的 AMP 云名称。

Application File Name

检测面向终端的 AMP 期间访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制无关联。

Application File SHA256

检测面向终端的 AMP 期间访问被检测或隔离文件的父文件的 SHA-256 散列值。

应用协议

受管设备检测到文件的流量所用应用协议。

应用协议类别或标记 (Application Protocol Category or Tag)

展示应用特征的条件，协助您了解应用功能。

Application Risk

与连接中检测到的应用流量关联的风险：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

Archive Depth

文件嵌入存档文件的层级（如有）。

Archive Name

恶意软件文件相关的存档文件（如有）的名称。要查看存档文件内容，请右键单击该存档文件的事件查看器行，打开上下文菜单，然后点击 **View Archive Contents**。

Archive SHA256

恶意软件文件相关的存档文件（如有）的 SHA-256 哈希值。要查看存档文件的内容，请右键单击该存档文件的事件查看器行，打开上下文菜单，然后点击 **View Archive Contents**。

业务相关性

与连接中检测到的应用流量关联的业务关联性：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

类别/文件类型类别 (Category / File Type Category)

文件类型的一般类别，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。

Client

在主机上运行并依靠服务器发送文件的客户端应用。

客户端类别或标记 (Client Category or Tag)

展示应用特征的条件，协助您了解应用功能。

计数

应用创建两个或多个相同行的限制条件后，与每行中的信息匹配的事件数。

检测名称 (Detection Name)

被测恶意软件名称。

检测器

识别恶意软件的面向终端的 AMP 检测器，例如 ClamAV、Spero 或 SHA。

设备

对于文件事件和基于网络的恶意软件事件，显示检测到文件的设备的名称。

对于基于终端的恶意软件事件和 AMP 云生成的追溯性恶意软件事件，显示 Firepower 管理中心的名称。

处置情况/文件处置情况 (Disposition / File Disposition)

文件的处置情况：

恶意软件

表示 AMP 云将文件归类为恶意软件，本地恶意软件分析识别的恶意软件或文件威胁评分超过文件策略中定义的恶意软件阈值。

清洁

表示 AMP 云将文件分类为干净，或用户将文件添加到干净的列表。干净的文件仅在变更为干净后才会显示在恶意软件表中。

未知

表示系统已查询 AMP 云，但文件尚未被分配处置情况；换句话说，AMP 云尚未对文件进行分类。

自定义检测

表示用户将文件添加到自定义检测列表。

不可用

表示系统无法查询 AMP 云。您可以查看很少一部分事件发生此情况；这是预期行为。

不适用

表示“检测文件”(Detect Files) 或“阻止文件”(Block Files) 规则处理了文件，Firepower 管理中心未查询 AMP 云。

只有系统已查询 AMP 云的文件才会显示文件处置情况。

域

对于文件事件和基于网络的恶意软件事件，显示检测到文件的设备的域。对于基于终端的恶意软件事件和 AMP 云生成的追溯性恶意软件事件，显示与报告事件的 AMP 云连接关联的域。

仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

Event Subtype

导致恶意软件检测的面向终端的 AMP 操作，例如，“创建”(Create)、“执行”(Execute)、“移动”(Move) 或“扫描”(Scan)。

事件类型

恶意软件事件的子类型。

文件名

恶意软件文件名。

File Path

面向终端的 AMP 检测到的恶意软件文件的文件路径，不包括文件名。

File Policy

检测文件的文件策略。

文件存储/已存储 (File Storage / Stored)（仅限搜索）

与事件关联的文件的存储状态：

已存储 (Stored)

返回当前存储相关文件的所有事件。

已在连接中存储 (Stored in connection)

返回系统捕获并存储相关文件的所有事件，无论当前是否已存储相关文件。

失败

返回系统无法存储相关文件的所有事件。

File Timestamp

面向终端的 AMP 检测到恶意软件文件创建的时间和日期。

HTTP 响应代码 (HTTP Response Code)

传输文件时，系统响应客户端的 HTTP 请求发送的 HTTP 状态代码。

IOC

对于连接涉及的主机，恶意软件事件是否触发危险表现 (IOC)。当面向终端的 AMP 数据触发 IOC 规则时，将生成 AMP IOC 类型的完整恶意软件事件。

消息

恶意软件事件相关的其他信息。对于文件事件和基于网络的恶意软件事件，系统仅对文件处置情况发生变更的文件填充此字段，即具有相关追溯性事件。

Receiving Continent

接收文件的主机所在大洲。

Receiving Country

接收文件的主机所在国家/地区。

正在接收 IP

对于文件事件和基于网络的恶意软件事件，显示接收文件的主机的 IP 地址。对于基于终端的恶意软件事件，显示连接器报告事件的终端的 IP 地址。

Receiving Port

检测到文件的流量所用目标端口。

安全情景

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 填充此字段。

Sending Continent

发送文件的主机所在大洲。

Sending Country

发送文件的主机所在国家/地区。

正在发送 IP

发送文件的主机的 IP 地址。

Sending Port

检测到文件的流量所用源端口。

SHA256/文件 SHA256 (SHA256 / File SHA256)

文件的 SHA-256 散列值，以及代表最近检测到的文件事件和文件处置情况且链接到网络文件轨迹的网络文件轨迹图标。要具有 SHA256 值，文件必须已经过以下任一文件规则处理：

- 启用了 **Store Files** 的 Detect Files 文件规则
- 启用了 **Store Files** 的 Block Files 文件规则
- Malware Cloud Lookup 文件规则
- Block Malware 文件规则
- 面向终端的 AMP

大小 (KB)/文件大小 (KB) (Size [KB] / File Size [KB])

文件大小（千字节）。请注意，如果系统在完全接收文件前确定一个文件的文件类型，则可能不会计算文件大小，该字段为空。

SSL 实际操作 (SSL Actual Action)（仅限搜索）

系统应用于已加密流量的操作：

阻止/阻止并重置 (Block/Block with reset)

表示阻止的加密连接。

Decrypt (Resign)

表示使用重新签名的服务器证书解密的传出连接。

Decrypt (Replace Key)

表示使用具有替代公钥的自签名服务器证书解密的传出连接。

Decrypt (Known Key)

表示使用已知私钥解密的传入连接。

默认操作

表示连接采用默认操作处理。

不解密 (Do not Decrypt)

表示系统未解密的连接。

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 证书信息 (SSL Certificate Information)（仅限搜索）

用于加密流量的公钥证书上存储的信息，包括：

- Subject/Issuer Common Name
- Subject/Issuer Organization
- Subject/Issuer Organization Unit
- Not Valid Before/After

- 序列号、证书指纹
- Public Key Fingerprint

SSL 失败原因 (SSL Failure Reason)（仅限搜索）

系统无法解密已加密流量的原因：

- 未知
- No Match
- 成功
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- 内部错误
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure

- Invalid Action

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL Status

与记录加密连接的 **SSL 实际操作 (SSL Actual Action)**（SSL 规则、默认操作或无法解密的流量操作）关联的操作。指向 SSL 证书详细信息的锁定图标 () 链接。如果证书不可用（例如，对于因 SSL 握手错误而受阻的连接），锁定图标会灰显。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

当搜索该字段时，请键入一个或多个 **SSL 实际操作 (SSL Actual Action)** 和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区 (SSL Subject/Issuer Country)（仅限搜索）

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

Threat Name

被测恶意软件名称。

威胁评分

与此文件相关的最新威胁评分。威胁评分图标可连接到“动态分析摘要”(Dynamic Analysis Summary) 报告。

Time

事件生成的日期和时间。此字段不可搜索。

类型/文件类型 (Type / File Type)

文件类型，例如 HTML 或 MSEXE。

URI/文件 URI (URI / File URI)

文件原始 URI，例如用户下载文件的 URL。

User

发生事件的主机 (**Receiving IP**) 的用户。

对于文件事件和基于网络的恶意软件事件，通过网络发现确定该用户。由于用户与目标主机关联，因此用户与其上传恶意软件文件的恶意软件事件无关联。

对于基于终端的恶意软件事件，面向终端的 AMP 确定用户名。这些用户**不受**用户发现或控制束缚。他们不会出现在用户表中，您也无法查看这些用户详细信息。

Web 应用

代表连接内被检测 HTTP 流量内容或所请求 URL 的应用。

Web 应用类别或标记 (Web Application Category or Tag)

展示了应用特征的标准，协助您了解应用功能。

恶意软件事件子类型

下表列出了恶意软件事件子类型、是基于网络还是基于终端的恶意软件事件可拥有该子类型，以及系统是否使用该子类型来建立网络文件轨迹。

表 *281*：恶意软件事件类型

恶意软件事件子类型/搜索值	面向 Firepower 的 AMP	面向终端的 AMP	文件轨迹
网络文件传送中检出威胁	是	否	yes
网络文件传送（回溯）中检出威胁	是	否	yes
Threat Detected	否	是	是
排除部分检出威胁	否	是	是
隔离威胁	否	是	是
AMP IOC（危害表现）	否	是	否
执行受阻	否	是	否
云召回隔离	否	是	否
云召回隔离尝试失败	否	是	否
开始云召回隔离	否	是	否
从隔离中恢复云召回	否	是	否
从隔离中恢复云召回失败	否	是	否
从隔离中恢复云召回启动	否	是	否
隔离失败	否	是	否
恢复隔离项目	否	是	否
恢复隔离失败	否	是	否

恶意软件事件子类型/搜索值	面向 Firepower 的 AMP	面向终端的 AMP	文件轨迹
开始恢复隔离	否	是	否
扫描完成，未检出	否	是	否
扫描完成，检出	否	是	否
扫描失败	否	是	否
开始扫描	否	是	否

文件和恶意软件事件字段中的可用信息

下表列出系统是否显示每个文件和恶意软件事件字段的信息。请记住，并不是每个事件的每个字段都填写。例如：

- 由于面向 Firepower 的 AMP 会检测网络流量中的恶意软件文件，因此文件事件和基于网络的恶意软件事件包含有关用于传输文件的连接的端口、应用协议和源 IP 地址信息。
- 从面向终端的 AMP 部署导入的恶意软件事件和危害表现 (IOC) 不包含情景连接信息，但其确实包含在下载或执行时获取的信息，例如文件路径、调用客户端应用等等。
- 文件事件表视图不显示与面向终端的 AMP 相关的字段。

表 *282*：文件和恶意软件事件字段中的可用信息

字段	文件事件	面向 Firepower 的 AMP 恶意软件事件	面向 Firepower 的 AMP 追溯性事件	面向终端的 AMP 恶意软件事件
操作	是	是	是	否
AMP 云 (AMP Cloud)	否	否	否	yes
Application File Name	否	否	否	yes
Application File SHA256	否	否	否	yes
应用协议	是	是	否	否
应用协议类别或标记 (Application Protocol Category or Tag)	是	是	是	否
Application Risk	是	是	是	否
Archive Depth	是	是	否	yes

字段	文件事件	面向 **Firepower** 的 **AMP** 恶意软件事件	面向 **Firepower** 的 **AMP** 追溯性事件	面向终端的 **AMP** 恶意软件事件
Archive Name	是	是	否	yes
Archive SHA256	是	是	否	yes
业务相关性	是	是	是	否
类别/文件类型类别 (Category / File Type Category)	是	是	否	yes
Client	是	是	是	否
客户端类别或标记 (Client Category or Tag)	是	是	是	否
计数	是	是	是	是
检测名称 (Detection Name)	否	是	否	否
检测器	否	否	否	yes
设备	是	是	是	是
处置情况/文件处置情况 (Disposition / File Disposition)	是	是	是	否
域	是	是	是	是
Event Subtype	否	否	否	yes
事件类型	否	是	是	是
文件名	是	是	否	yes
File Path	否	否	否	yes
File Policy	是	否	否	否
File Timestamp	否	否	否	yes
HTTP 响应代码 (HTTP Response Code)	是	是	否	否
IOC（危害表现）	否	是	是	是
消息	是	是	否	yes

字段	文件事件	面向 **Firepower** 的 **AMP**恶意软件事件	面向 **Firepower** 的 **AMP** 追溯性事件	面向终端的 **AMP** 恶意软件事件
Receiving Continent	是	是	是	否
Receiving Country	是	是	否	否
正在接收 IP	是	是	否	yes
Receiving Port	是	是	否	否
安全情景	是	是	是	是
Sending Continent	是	是	是	否
Sending Country	是	是	否	否
正在发送 IP	是	是	否	否
Sending Port	是	是	否	否
SHA256/文件 SHA256 (SHA256 / File SHA256)	是	是	是	是
大小 (KB)/文件大小 (KB) (Size [KB] / File Size [KB])	是	是	否	yes
SSL 实际操作 (SSL Actual Action)（仅限搜索）	是	是	否	否
SSL 证书信息 (SSL Certificate Information)（仅限搜索）	是	是	否	否
SSL 失败原因 (SSL Failure Reason)（仅限搜索）	是	是	否	否
SSL Status	是	是	否	否
SSL 使用者/颁发者所在国家/地区 (SSL Subject/Issuer Country)（仅限搜索）	是	是	否	否
文件存储/已存储 (File Storage / Stored)（仅限搜索）	是	是	否	否
Threat Name	否	是	是	是
威胁评分	是	是	否	否

字段	文件事件	面向 Firepower 的 AMP 恶意软件事件	面向 Firepower 的 AMP 追溯性事件	面向终端的 AMP 恶意软件事件
Time	是	是	是	是
类型/文件类型 (Type / File Type)	是	是	否	yes
URI/文件 URI (URI / File URI)	是	是	否	否
User	是	是	否	yes
Web 应用	是	是	是	否
Web 应用类别或标记 (Web Application Category or Tag)	是	是	是	否

本地恶意软件分析

本地恶意软件分析允许托管设备使用由 Cisco Talos 安全情报和研究小组 (Talos) 提供的检测规则集，在本地检查可执行文件、PDF、办公文档以及其他类型的文件是否存在最常见的恶意软件类型。由于本地恶意软件分析不需要向 AMP 云提交文件，也不运行该文件，因此节约了时间和系统资源。

如果系统通过本地恶意软件分析识别恶意软件，则它会将现有文件处置情况从“未知”(Unknown) 更改为“恶意软件”(Malware)。然后，系统会生成一个新恶意软件事件。如果系统未识别恶意软件，则它不会将文件处置情况从“未知”(Unknown) 更改为“干净”(Clean)。系统运行本地恶意软件分析后，会缓存 SHA-256 散列值、时间戳以及处置情况等文件信息，以便在特定时间段内再次检测时，系统可以在不进行其他分析的情况下识别恶意软件。

从事件查看器，您可以通过情景菜单手动提交文件进行本地恶意软件分析，文件可以一次提交一个，也可以一次提交多达二十五个捕获文件。系统运行本地分析，然后将这些文件提交到云进行动态分析。

本地恶意软件分析不需要与 AMP Threat Grid 云建立通信。但是，您必须配置与云的通信，以提交预分类为恶意软件的文件以进行动态分析，并将更新下载到本地恶意软件分析规则集。

文件构成

如果配置本地恶意软件分析或动态分析，则系统会在分析文件后会生成文件构成报告。您可以通过此报告进一步分析文件，并确定它们是否可能携带嵌入式恶意软件。

文件构成报告列出文件属性、文件中嵌入的任何对象以及任何检测到的病毒。文件构成报告还可能列出特定于该文件类型的其他信息。当系统删除存储的文件时，也会删除相关联的文件构成报告。

动态分析

如果要提高 AMP 云的准确性并提供额外的恶意软件分析和威胁识别，您可以向 AMP Threat Grid 云或内部 AMP Threat Grid 设备提交合格的捕获文件，以用于动态分析。AMP 云在沙盒环境下运行文件，以确定文件是否包含恶意软件。

您是否可以提交文件用于动态分析取决于：

- 文件类型
- 文件大小
- 文件规则的操作
- 系统将文件预分类为恶意软件，以进行自动提交

如果将一条规则配置为阻止恶意软件或执行恶意软件云查找，则系统只会提交具有“未知”(Unknown) 或“不可用”(Unavailable) 处置情况的匹配文件。

AMP Threat Grid 云会查询文件以用于动态分析，并在沙盒环境下运行每个文件。云返回威胁评分，详细展示文件中包含恶意软件的可能性。您可以自动阻止威胁评分超过定义阈值的文件。

通过事件查看器、捕获文件视图或网络文件轨迹，您可以确定一个文件是否已提交用于动态分析，手动提交文件用于本地恶意软件和动态分析，或查看为何云分配这一威胁评分的摘要。您还可以检索动态分析摘要报告，该摘要报告介绍组成整体威胁评分的各种评级，以及当云尝试运行该文件时启动的其他进程。

自动动态和 Spero 分析

可以将文件策略配置为自动提交预分类为恶意软件的文件进行动态分析。

要补充动态分析，可以自动提交已查询的文件进行 Spero 分析。Spero 分析对 SHA-256 散列值的分析进行补充，从而可更完整地识别可执行文件中的恶意软件。

Spero 分析涉及检查文件结构特征，例如元数据和报头信息。根据此信息生成 Spero 签名后，设备会将其提交到 AMP 云中的 Spero 启发式引擎。基于 Spero 签名，Spero 引擎返回文件是否为恶意软件的结果。如果文件当前还具有“未知”(Unknown) 文件处置情况，则系统会分配“恶意软件”(Malware) 文件处置情况。

请注意，您只能在检测时提交可执行文件进行 Spero 分析；此后将无法人工提交文件。您还可以提交文件进行 Spero 分析，而不另外提交这些文件进行动态分析。

手动动态分析

可以从事件查看器、情景菜单或网络文件轨迹手动提交存储的文件以进行动态分析。从捕获的文件视图，一次可以手动提交最多 25 个存储的文件。

除了可执行文件，您也可以提交不适合自动提交的文件类型，例如 .swf、.jar 和其他类型。这样，您可以更快速地分析多种文件（而不管处置情况为何），并准确确定事故具体成因。

注释 系统会检查 AMP 云，确定动态分析合格文件类型列表是否更新（不超过一日一次）以及可提交的最小和最大文件大小。

动态分析和容量处理

通过容量处理，您可以在当前无法将文件提交到云进行动态分析时，将其暂时存储在设备上。设备将文件存储在其硬盘或恶意软件存储包中。

系统可以暂时存储为其执行恶意软件云查找的已启用动态分析的任何文件。如果文件预分类为恶意软件，且设备已达到最大云提交数或无法与云进行通信，则系统会存储该文件。

在以下任一情况下，设备会将存储的文件重新提交到云：

- 设备无法与云进行通信，并重新建立云通信。
- 设备已达到最大云提交数，并且经过了足够的时间。

威胁评分和动态分析摘要报告

威胁评分

表 *283*：威胁评分等级

威胁评分	图标
Low	
Medium	
High	
Very High	

Firepower管理中心对文件威胁评分进行缓存的时间与对文件处置情况进行缓存的时间相同。如果系统之后检测到这些文件，则会显示缓存威胁评分而不是重新查询 AMP Threat Grid 云或 AMP Threat Grid 内部设备。您可以自动向威胁评分超过已定义的恶意软件阈值威胁评分的文件分配恶意软件文件处置情况。

动态分析总结

如有动态分析总结，您可以点击威胁评分图标进行查看。如果存在多份报告，该总结应当基于与精确威胁评分匹配的最新报告。如果没有报告与精确威胁评分匹配，则会显示威胁评分最高的报告。如果存在多份报告，您可以选择一个威胁评分查看各份报告。

总结将列明构成威胁评分的各部分威胁。每个组件威胁都可以扩展至列出AMP云查找结果，以及与此组件威胁相关的任何进程。

进程树显示AMP Threat Grid云尝试运行该文件时启动的进程。这有助于识别包含恶意软件的文件是否在尝试访问超出预期的进程和系统资源（例如，运行 Word 文档打开 Microsoft Word，接着启动 Internet Explorer，然后运行 Java 运行时环境）。

列出的每个进程都包含可用于验证实际进程的进程标识符。进程树中的子节点表示由于父进程而启动的进程。

从动态分析摘要中，您可以点击**查看完整报告 (View Full Report)** 以查看完整分析报告，其中详述AMP云的完整分析，包括常规文件信息、对检测到的所有进程的更深入审核、文件分析明细以及其他相关信息。

文件分析评估

根据Spero分析、本地恶意软件分析、动态分析或综合分析结果，系统可能会更新文件的处置情况。

系统先在文件上运行 Spero 分析，然后运行本地恶意软件分析，再进行动态分析。如果系统将该文件预分类为恶意软件，即使其识别了恶意软件，也会将该文件提交到 AMP Threat Grid云。

如果您在文件规则中配置本地恶意软件分析或动态分析，则系统会对与规则匹配的文件进行预分类并生成文件处置情况报告。它不会将文件的处置情况更改为预分类结果。

下表详细介绍每种类型文件分析的优点和缺点，以及系统如何根据分析更改文件处置情况。

表 *284*：文件分析类型比较

分析类型	优点	限制	恶意软件识别
斯佩罗分析	可执行文件的结构分析，将 Spero 签名提交到AMP云进行分析	没有本地恶意软件分析或动态分析彻底，仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
本地恶意软件分析	比动态分析消耗的资源少，返回结果更快，尤其当检测到的恶意软件较常见时	分析结果没有动态分析的结果彻底	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。

分析类型	优点	限制	恶意软件识别
动态分析	分析结果更彻底，用 AMP Threat Grid 云在沙盒环境中运行文件	比单独的本地恶意软件分析消耗的资源多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况根据文件策略中配置的威胁评分阈值更改。
Spero 分析结合本地恶意软件分析	比配置本地恶意软件分析和动态分析消耗的资源少，仍使用 AMP 云资源识别恶意软件	没有动态分析彻底，Spero 分析仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
Spero 分析结合动态分析	在提交文件和 Spero 签名时使用完整的 AMP 云功能	获取结果的速度没有使用本地恶意软件分析获取结果的速度快	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况根据文件策略中配置的威胁评分阈值更改，并在 Spero 分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)。
本地恶意软件分析结合动态分析	使用两种类型的文件分析使评分析结果更彻底	比单独使用任一种分析消耗的资源多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
Spero 分析、本地恶意软件分析结合动态分析	分析结果最彻底	运行所有三种类型的文件分析消耗的资源最多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在 Spero 分析或本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。

捕获的文件和文件存储

根据文件策略配置，您可以使用文件控制功能检测和阻止文件。但是，来自可疑主机或网络的文件或者发送至您网络上受监控主机的多余文件可能需要进一步分析。通过文件存储功能，您可以捕获在流量中检测到的选定文件，并自动将其存储至设备硬盘驱动器或（如果已安装）恶意软件存储包内。

当设备在流量中检测到文件时，可以捕获该文件。这将创建一个副本，系统可以存储或者提交该副本以进行动态分析。在设备捕获文件后，您有若干选择：

- 将捕获文件存储至设备硬盘驱动器中供后期分析使用。
- 将存储的文件下载至本地计算机，以便进一步实施人工分析或存档。
- 将捕获文件提交给 AMP 云进行动态分析。

请注意，文件存储在设备中之后，如果未来检测到该文件且设备仍存有该文件，则不会再捕获该文件。

注释 在网络上第一次检测到某个文件时，您可以生成代表文件检测情况的文件事件。但如果您的文件规则执行恶意软件云查找，则系统需要额外的时间来查询 AMP 云并返回处置情况。由于这种延迟，在网络上第二次出现此文件之前，系统无法存储此文件，并且系统可以立即确定此文件的处置情况。

无论系统捕获还是存储文件，您都可以：

- 从事件查看器中审查捕获文件的信息，包括文件是否存储或提交用于动态分析、文件性质和威胁评分，以便迅速查看网络中检测到的恶意软件潜在威胁。
- 查看文件轨迹，确定其如何穿过网络以及哪些主机有副本。
- 向清空列表或自定义检测列表添加文件，以便在未来检测过程中始终将该文件作为清空或恶意软件性质。

您可以在文件策略中配置文件规则，以便捕获并存储特定类型或者具有特定文件性质的文件（如有）。如果将该文件策略与访问控制策略相关联，并将其部署到设备上，则系统将捕获并存储流量中的匹配文件。还可以限制要存储的最小和最大文件大小。不能将存储的文件放入系统备份文件。

恶意软件存储包

基于文件策略配置，设备可以将大量文件数据存储在硬盘驱动器中。您可以在设备上安装恶意软件存储包。系统将文件存储在恶意软件存储包内，允许主硬盘驱动器留出更多空间存储事件和配置文件。系统定期删除早期文件。如果设备的主硬盘驱动器没有足够的可用空间，也未安装恶意软件存储包，则无法存储文件。

注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买，而且**仅**限用于 8000 系列设备。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。有关详细信息，请参阅 《*Firepower* 系统恶意软件存储包指南》。

如果未安装恶意软件存储包，则在配置设备以存储文件时，该设备会将主硬盘驱动器空间的设定部分分配用于存储捕获文件。如果将容量处理配置为暂时存储文件以进行动态分析，则系统会使用相同的硬盘驱动器分配来存储这些文件，直至可以将这些文件重新提交到云。

在设备中安装恶意软件存储包并配置文件存储或容量处理时，该设备会分配整个恶意软件存储包来用于存储这些文件。设备不会在恶意软件存储包中存储其他任何信息。

当分配的用于存储捕获文件的空间用尽时，系统删除最早的存储文件，直至分配空间达到系统定义的阈值。依据存储文件数量，在系统删除文件后，磁盘用量将大幅下降。

如果在安装恶意软件存储包时，设备已经存储文件，则下次重新启动设备时，存储在主硬盘驱动器上的任何捕获文件或容量处理文件都会移至恶意软件存储包。设备未来存储的文件都将存储至恶意软件存储包。

存储的文件下载

设备存储文件后，只要Firepower管理中心可以与该设备保持通信并且未删除文件，就可以将文件下载本地主机以供长期存储和分析，并手动分析文件。您可以从相关文件事件、恶意软件事件、捕获文件视图或文件轨迹中下载文件。

由于恶意软件有害，默认情况下，您必须在每次下载文件时进行确认。但是，可以在“用户首选项”(User Preferences) 中禁用确认。

因为性质为Unknown的文件可能包含恶意软件，当您下载文件时，系统会首先将该文件存档至 `.zip` 压缩包。`.zip` 文件名包含文件处置情况和文件类型（如有）以及 SHA-256 散列值。您可以对 `.zip` 文件采用密码保护以防意外解压缩。可以在“用户首选项”(User Preferences) 中编辑或删除默认 `.zip` 文件密码。

注意 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

使用已捕获文件工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
因功能而异	因功能而异	任何环境	任何环境	管理员/任何安全分析师

当受管设备捕获在网络流量中检测到的文件时，它会记录一个事件。

注释 如果设备捕获包含恶意软件的文件，设备会生成两个事件：其检测文件时的文件事件，以及其识别恶意软件时的恶意软件事件。

事件查看器允许您在表格中查看捕获的文件。您也可以根据与您的分析相关的信息操作事件视图。在访问捕获的文件时看到的页面因工作流程有所不同。工作流程只是一系列页面，您可以使用这些页面从较宽泛的视图移动至更精细化的视图来评估事件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

如果系统在配置更改后重新捕获文件（如更新的文件策略），则会更新该文件的现有信息。

例如，如果您将文件策略配制为通过**恶意软件云查找 (Malware Cloud Lookup)** 操作捕获文件，则系统会连同文件一起存储文件处置情况和威胁评分。然后，如果您更新文件策略，且系统因新的**检测文件 (Detect Files)** 操作重新捕获同一文件，则系统会更新该文件的**上次更改时间 (Last Changed)** 值。但系统不会删除现有处置情况和威胁评分，即使您没有再次执行恶意软件云查找。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

选择**分析 (Analysis)** > **文件 (Files)** > **捕获的文件 (Captured Files)**。

提示 事件表视图中的一些字段在默认情况下处于隐藏状态。要显示事件视图的隐藏字段，请展开搜索限制，然后点击 **Disabled Columns** 下的字段名称。

捕获文件字段

捕获文件表视图是预定义捕获文件工作流程的最终页面，也可以添加到自定义工作流程中，且该视图为捕获文件表中的每个字段都准备了对应的列。

搜索此表时，请记住搜索结果取决于所搜索事件的可用数据；根据可用数据，搜索限制可能并不适用。例如，如果文件从未被提交用于动态分析，可能没有与其关联的威胁评分。

表 *285*：捕获文件字段

字段	说明
Archive Inspection Status	对于存档文件，存档检查状态： • “待定”(Pending) 表示系统仍在检查存档文件及其内容。如果文件再次通过您的系统，就可以提供完整的信息。 • “已提取”(Extracted) 表示系统能够提取和检查存档内容。 • 在极少数情况下，如果系统无法处理提取内容，会出现“失败”(Failed) 状态。 • “超出深度”(Depth Exceeded) 表示存档包含超出最大允许深度的进一步嵌套存档文件。 • “已加密”(Encrypted) 表示存档文件内容已加密，无法进行检查。 • “不可检查”(Not Inspectable) 表示系统未提取和检查存档内容。策略规则操作、策略配置和损坏文件是出现此状态的三个主要原因。 要查看存档文件内容，请右键点击文件事件查看器行，打开情景菜单，然后选择**查看存档内容 (View Archive Contents)**。
类别	文件类型的一般类别，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。
检测名称 (Detection Name)	被测恶意软件名称。
处理结果	文件的面向 Firepower 的 AMP 处置情况： • “恶意软件”(Malware) 表示本地恶意软件分析识别出恶意软件，AMP 云将文件归类为恶意软件，或文件威胁评分超过文件策略中定义的恶意软件阈值。 • “干净”(Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。 • “未知”(Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。 • “自定义检测”(Custom Detection) 表示用户将文件添加到自定义检测列表。 • “不可用”(Unavailable) 表示系统无法查询 AMP 云。您可以查看很少一部分事件发生此情况；这是预期行为。 • “不适用”(N/A) 表示“检测文件”(Detect Files) 或“阻止文件”(Block Files) 规则处理了文件，Firepower 管理中心未查询 AMP 云。
域	检测到捕获文件的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

字段	说明
Dynamic Analysis Status	以下一个或多个值表示是否已提交文件以供由面向 Firepower 的 AMP 执行动态分析： • “分析完成”(Analysis Complete) - 已提交文件以供动态分析且收到威胁评分和动态分析摘要报告 • “容量已处理”(Capacity Handled) - 已存储文件，因为当前无法提交文件 • “容量已处理（网络问题）”(Capacity Handled [Network Issue]) - 已存储文件，因为由于网络连接问题而无法提交文件 • “容量已处理（速率限制）”(Capacity Handled [Rate Limit]) - 已存储文件，因为已达到最大提交数量而无法提交文件 • “设备未激活”(Device Not Activated) - 未提交文件，因为未在内部 AMP Threat Grid 设备上激活设备。如果看到此状态，请联系支持部门。 • “失败（分析超时）”(Failure [Analysis Timeout]) - 文件已提交，但 AMP 云尚未为其返回结果 • “失败（无法运行文件）”(Failure [Cannot Run File]) - 文件已提交，但 AMP 无法在测试环境中运行文件 • “失败（网络问题）”(Failure [Network Issue]) - 文件由于网络连接失败而未提交 • “未发送以供分析”(Not Sent for Analysis) - 文件未提交 • “不可疑（未发送以供分析）”(Not Suspicious [Not Sent For Analysis]) - 文件预先分类为非恶意软件 • “之前已分析”(Previously Analyzed) - 文件含有缓存的威胁评分，用户尝试再次提交 • “已发送以供分析”(Sent for Analysis) - 文件被预先分类为恶意软件，并排队等待动态分析
动态分析状态已更改 (Dynamic Analysis Status Changed)	上一次文件分析状态发生变化的时间。
文件名	最近检测到的与文件 SHA-256 哈希值相关的文件名。
Last Changed	上一次更新与该文件有关信息的时间。
Last Sent	最近一次向 AMP 云提交文件以供面向 Firepower 的 AMP 执行动态分析的时间。

字段	说明
本地恶意软件分析状态 (Local Malware Analysis Status)	下列值之一表示系统是否对文件执行本地恶意软件分析： • “分析完成”(Analysis Complete) - 系统使用本地恶意软件分析检查文件，并对文件预先分类。 • “分析失败”(Analysis Failed) - 系统尝试使用本地恶意软件分析检查文件但已失败。 • “手动请求已提交”(Manual Request Submitted) - 用户提交文件以供本地恶意软件分析 • “未分析”(Not Analyzed) - 系统未使用本地恶意软件分析检查文件
SHA256	文件的 SHA-256 哈希值以及显示最近检测文件事件和文件性质的网络文件轨迹图标。要查看网络文件轨迹，请点击轨迹图标。
Storage Status	表示文件是否存储于受管设备： • File Stored • 未存储（处置情况待定）(Not Stored [Disposition Was Pending])
威胁评分	与此文件相关的最新威胁评分。 要查看动态分析总结报告，请点击威胁评分图标。
Type	文件类型；例如 HTML 或 MSEXE。

网络文件轨迹

网络文件轨迹功能映射出主机怎样在网络中传送文件，包括恶意软件文件。轨迹以图表形式展示文件传输数据、文件处置情况以及是否阻止文件传送或是否隔离文件。您可以确定哪些主机可能已传送恶意软件、哪些主机存在风险，并观察文件传送趋势。

您可以跟踪具有 AMP 云分配处置情况的所有文件。系统可以使用与检测和阻止来自面向 Fireower 的 AMP 和面向终端的 AMP 的恶意软件相关的信息来建立轨迹。

最近检测到的恶意软件和分析的轨迹

“网络文件轨迹列表”(Network File Trajectory List) 页面显示网络上最近检测到的恶意软件，以及最近查看过轨迹映射的文件。从这些列表中，可以查看最近在网络上查看每个文件的时间，该文件的 SHA-256 散列值、名称、类型、当前文件处置情况、内容（对于存档文件），以及与该文件相关联的事件的数量。

该页面还包含一个可让您定位文件的搜索框，可基于 SHA-256 哈希值、文件名或传送或接收文件主机的 IP 地址进行查找。定位一个文件后，您可以点击 **File SHA256** 值，查看详细轨迹映射。

网络文件轨迹详细视图

您可以通过查看网络文件详细轨迹在网络中跟踪文件。搜索文件的 SHA 256 值或点击网络文件轨迹列表中的**文件 SHA 256 (File SHA 256)** 链接可查看该文件的详细信息。

“网络文件轨迹详细信息”(Network File Trajectory Details) 页面包含三个部分：

- 摘要信息 - 文件的轨迹页面显示文件的相关摘要信息，包括文件识别信息、首次及最近一次在网络上查看该文件的时间、与该文件相关的事件和主机数量以及该文件的当前处置情况。从本节开始，如果受管设备已存储文件，您可以进行本地下载、提交文件进行动态分析或将文件添加至文件列表。
- 轨迹映射 - 文件的轨迹映射直观地跟踪从网络上第一次检测到文件至最近一次检测到该文件的情况。该映射显示出主机传送或接收文件的时间、传送文件频率和阻止或隔断文件的时间。数据点之间的垂直线代表文件在主机之间传送。连接数据点的水平线表示随时间推移的主机文件活动。

  该映射同时显示该文件生成文件事件的频率，以及系统为文件分配性质或回溯性质的时间。您可以在映射中选择数据点，并突出显示追溯至主机第一次传输该文件的实例的路径；此路径还将贯穿每次主机作为该文件接收方或发送方的事例，。
- 相关事件 -“事件”(Events) 表列出映射中各数据点的事件信息。使用该表和映射，您可以准确定位特定文件事件、网络上传送或接收该文件的主机、映射中的相关事件以及表中受选定值限制的其他关联事件。

网络文件轨迹摘要信息

对于“网络文件轨迹”(Network File Trajectory) 列表中显示的文件，“详细信息”(Details) 页面顶部会显示以下摘要信息。

提示 要查看相关文件事件，请点击字段值链接。在新窗口中打开文件事件默认工作流程首页，显示包含选定值的所有文件事件。

表 *286*：网络文件轨迹摘要信息字段

名称	描述
Archive Contents	对已检查存档文件，指存档文件包含的文件数量。

名称	描述
Current Disposition	以下面向 Firepower 的 AMP 文件处置情况之一： • 恶意软件 (Malware) 表示 AMP 云将文件分类为恶意软件，本地恶意软件分析识别恶意软件，或者文件的威胁评分超过文件策略中定义的恶意软件阈值。 • 干净 (Clean) 表示 AMP 云将文件归类为干净，或者用户将该文件添加到干净列表。 • 未知 (Unknown) 表示系统查询了 AMP 云，但是尚未为文件分配处置情况；换句话说，AMP 云尚未将文件分类。 • 自定义检测 (Custom Detection) 表示用户将文件添加到自定义检测列表。 • 不可用 (Unavailable) 表示系统无法查询 AMP 云。您可以查看很少一部分事件发生此情况；这是预期行为。 • 不适用 (N/A) 表示“检测文件”(Detect Files) 或“阻止文件”(Block Files) 规则处理了文件，Firepower 管理中心未查询 AMP 云。
检测名称 (Detection Name)	本地恶意软件分析检测到的恶意软件的名称。
Event Count	网络上看到的与该文件相关事件的数量，以及如检测到超过 250 个事件时映射中显示的事件数量。
File Category	文件类型的一般类别，例如 Office Documents 或 System Files。
文件名	事件关联文件的名称，如网络上所示。 如果一个 SHA-256 哈希值与多个文件名关联，列出最近检测到的文件名。您还可通过点击 more 将其展开以查看其余文件名。
File SHA256	文件的 SHA-256 哈希值。 默认情况下以压缩格式显示哈希值。要查看完整哈希值，请将指针悬停在上方。如果一个文件名与多个 SHA-256 哈希值关联，将指针悬停在链接上方查看全部哈希值。
File Size (KB)	文件大小（千字节）。
文件类型	文件类型，例如 HTML 或 MSEXE。
首次查看时间	面向 Firepower 的 AMP 或面向终端的 AMP 首次检测到文件以及主机（第一个上传该文件的主机）的 IP 地址的时间。
上次查看时间	面向 Firepower 的 AMP 或面向终端的 AMP 最近一次检测到文件以及主机（最后一个下载该文件的主机）的 IP 地址的时间。

名称	描述
Parent Application	在面向终端的 AMP 执行检测时访问恶意软件文件的客户端应用。这些应用与网络发现或应用控制无关联。
Seen On	发送或接收文件的主机数量。因为一台主机可以在不同时间上传和下载文件，在 `Seen On Breakdown` 字段中的主机总数可能与发送方总数加上接收方总数之和并不匹配。
Seen On Breakdown	发送文件的主机数量，然后紧接接收文件的主机数量。
Threat Name	通过面向终端的 AMP 与检测到的恶意软件相关联的威胁的名称。
威胁评分	文件的威胁评分。

网络文件轨迹映射和相关事件列表

文件轨迹映射的 y 轴包含与该文件交互的所有主机 IP 地址的列表。IP 地址按照系统在主机上首次检测到该文件的时间降序排列。每行都包含与该 IP 地址相关的所有事件，无论是单一文件事件、文件传送还是回溯事件。x 轴包含系统检测到各个事件的日期和时间。时间戳按时间顺序排列。如果一分钟内发生多个事件，在同一栏中列出所有事件。您可以水平或垂直滚动映射，以查看其他事件和 IP 地址。

映射中显示多达 250 个与文件 SHA-256 哈希值有关的事件。如有超过 250 个事件，则映射上只显示前十个，并用箭头图标 () 截略其他事件。然后映射显示剩下 240 个事件。

将在新窗口中显示文件事件默认工作流程的首页，同时显示所有基于文件类型受限的其他事件。如果未显示基于终端的恶意软件事件，您必须切换到 Malware Events 表进行查看。

每个数据点都表示一个事件及其文件处置情况，如映射下方图例中所述。例如，Malware Block 事件图标结合了 Malicious Disposition 图标和 Block Event 图标。

基于终端的恶意软件事件包含一个图标。回溯事件在栏中为各检测到文件的主机显示一个图标。文件传送事件始终包括两个图标，一个文件发送图标和一个文件接收图标，两者之间用垂直线连接。箭头表示从发送方到接收方的文件传送方向。

要跟踪文件在网络中的历程，可以点击任意数据点突出显示一个轨迹，其中包括与选定数据点相关的所有数据点。这包括与下列类型的事件相关的数据点：

- 无论关联 IP 地址作为发送方还是接收方的任何文件传送
- 涉及关联 IP 地址的任何基于终端的恶意软件事件
- 如果涉及另一个 IP 地址，无论该关联 IP 地址作为发送方还是接收方的所有文件传送
- 如果涉及另一个 IP 地址，涉及该 IP 地址的基于终端的任何恶意软件事件

同时突出显示与任何突出显示数据点相关的所有 IP 地址和时间戳。同时突出显示事件表中相应事件。如果一条轨迹中包含截略事件，则用虚线突出显示轨迹本身。可能有截略事件与轨迹相交，但并不在映射中进行显示。

使用网络文件轨迹

智能许可证	经典许可证	支持的设备	支持的域	Access
恶意软件（面向 Firepower 的 AMP） 任意（面向终端的 AMP）	恶意软件（面向 Firepower 的 AMP） 任意（面向终端的 AMP）	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **文件 (Files)** > **网络文件轨迹 (Network File Trajectory)**。

提示 您还可以从情景管理器、控制面板或具有文件信息的事件视图来访问文件轨迹。

步骤 2 点击列表中的**文件 SHA 256 (File SHA 256)** 链接。

步骤 3 或者，在搜索字段输入完整的 SHA-256 散列值、主机 IP 地址或要跟踪的文件的名称，然后按 Enter 键。

提示 如果只有一个结果匹配，系统将显示该文件的 Network File Trajectory 页面。

步骤 4 在“摘要信息”(Summary Information) 部分中，可以执行以下操作：

- 将文件添加到文件列表 - 要在干净的列表或自定义检测列表中添加或删除文件，请点击编辑图标 ( )。
- 下载文件 - 要下载文件，请点击下载文件图标 ( )，并在出现提示时，确认要下载该文件。如果该文件无法下载，则此图标呈灰色显示。
- 报告 - 点击威胁评分图标，查看“动态分析摘要”(Dynamic Analysis Summary) 报告。
- 提交动态分析 - 点击 AMP 云图标 ( ) 以提交文件进行动态分析。如果该文件无法提交或您无法连接到 AMP 云，则此图标呈灰色显示。
- 查看存档内容 - 要查看有关存档文件内容的信息，请点击查看图标 ( )。
- 查看文件组成 - 要查看文件的组成，请点击文件列表图标 ( )。如果系统未生成文件组成报告，则此图标呈灰色显示。
- 查看威胁评分相同的捕获文件 - 点击威胁评分链接，查看具有该威胁评分的所有捕获文件。

注释 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

步骤 5 在轨迹映射上，可以执行以下操作：

- 确定第一个实例 - 点击一个 IP 地址，确定第一次发生涉及 IP 地址的文件事件的位置。突出显示连至该数据点的轨迹，以及与第一个文件事件相关的任何介于其间的文件事件和IP地址。同时突出显示事件表中相应事件。如当前不可见，映射会滚动至该数据点。
- 跟踪 - 点击任意数据点，突出显示包含与所选数据点相关的所有数据点的轨迹，从而通过网络跟踪文件的进度。
- 查看隐藏事件 - 点击箭头图标，查看“文件摘要”(File Summary) 事件视图中未显示的所有事件。
- 查看匹配文件事件 - 将指针悬停在事件图标 () 上方，查看事件的摘要信息。如果点击任何事件摘要信息链接，则会在新窗口中显示“文件事件”(File Events) 默认工作流程的首页，其中包含基于文件类型限制的所有其他事件。“文件摘要”(File Summary) 事件视图在新窗口中打开，显示与所点击的条件值相匹配的所有文件事件。

步骤 6 在“事件”(Events) 表中，可以执行以下操作：

- 突出显示 - 选择表行，突出显示映射中的数据点。如当前不可见，映射会滚动至选定文件事件并显示该事件。
- 排序 - 点击列标题以按升序或降序对事件进行排序。

第 87 章

使用主机配置文件

以下主题介绍如何使用主机配置文件：

主机简档

主机配置文件可完整展现系统搜集到的有关单台主机的全部信息。要访问主机配置文件，请执行以下操作：

- 从任何网络映射视图进行导航。
- 从包含受监控网络上主机的 IP 地址的任何事件视图进行导航。

主机配置文件提供有关检测到的主机或设备的基本信息，例如主机名或 MAC 地址。根据许可证和系统配置，主机配置文件还可提供以下信息：

- 在主机上运行的操作系统
- 在主机上运行的服务器
- 在主机上运行的客户端和 Web 应用
- 在主机上运行的协议
- 主机上的危害表现 (IOC) 标记
- 主机上的 VLAN 标记
- 过去 24 小时网络上的用户活动
- 与主机关联的白名单违规
- 主机的最新恶意软件事件
- 与主机关联的漏洞
- 主机的 Nmap 扫描结果

配置文件中还会列出主机属性。您可以对您的网络环境而言重要的方式使用主机属性对主机进行分类例如，您可以：

- 分配表示主机所在建筑物的主机属性
- 使用主机重要性属性指定特定主机的业务重要性，并根据主机重要性定制关联策略和警报

从主机配置文件中，您可以查看应用于该主机的现有主机属性，并修改主机属性值。

如果将自适应配置文件用作被动入侵防御部署的一部分，则可以定制系统处理流量的方式，以使其最适合于主机上的操作系统的类型，以及主机正在运行的服务器和客户端。

或者，可以从主机配置文件执行Nmap扫描，以扩充主机配置文件中的服务器和操作系统信息。Nmap扫描仪主动扫描主机以获得在主机上运行的操作系统和服务器的有关信息。扫描结果会添加到主机操作系统和服务器标识列表。

主机配置文件限制包括：

不可用主机

主机配置文件可能并不适用于网络上的每台主机。可能的原因包括：

- 主机由于超时而从网络映射中删除。
- 已达到主机许可证限制。
- 主机所在的网段不受网络发现策略的监控。

不可用信息

主机配置文件中显示的信息可能根据主机类型和有关主机的可用信息而异。

例如：

- 例如，如果系统检测到使用非基于 IP 的协议（例如 STP、SNAP 或 IPX）的主机，则会将该主机作为 MAC 主机添加到网络映射中，并且该主机的可用信息远远少于 IP 主机。
- 系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

查看主机配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

您有两种选择：

- 在任何网络映射上，钻取至想要浏览的配置文件的主机的 IP 地址。
- 在任何事件视图上，点击想要浏览的配置文件的主机 IP 地址旁边的主机配置文件图标 () 或受攻击的主机图标 ()。

主机配置文件中的基本主机信息

主机配置文件包含有关检测到的主机或其他设备的基本信息。

主机配置文件中的每个基本字段的描述如下。

域

与主机关联的域。

IP 地址

所有与主机相关的 IP 地址（IPv4 和 IPv6）。系统检测与主机相关的 IP 地址，并且，如果支持的话，把同一主机使用的多个 IP 地址进行分组。IPv6 主机通常至少有两个 IPv6 地址（仅本地和全局路由），也可能拥有 IPv4 地址。纯 IPv4 主机可拥有多个 IPv4 地址。

主机配置文件列出所有检测到的与主机相关的 IP 地址。如可用，路由主机 IP 地址还包含一个表明与地址相关的地理位置数据的旗帜图标和国家代码。

请注意，默认情况下，仅显示前三个地址。点击 **show all** 显示主机的所有地址。

Hostname

如果已知，为主机的完全限定域名。

NetBIOS Name

如可用，为主机的 NetBIOS 名称。为使用 NetBIOS 而配置的 Microsoft Windows 主机、以及 Macintosh、Linux 或其他平台都可以拥有一个 NetBIOS 名称。例如，配置为 Samba 服务器的 Linux 主机可拥有多个 NetBIOS 名称。

设备（跳数）(Device [Hops])

可以为以下任意一项：

- 根据网络发现策略中的定义，主机所在网络的报告设备，或者
- 处理把主机添加至网络映射的 NetFlow 数据的设备

检测到主机的设备与设备名称后面的主机之间的网络跳数（使用括号括起）。如果多台设备可看见主机，报告设备以粗体显示。

如果该字段为空，可能出现以下情况：

- 按照网络发现策略中的规定，由未明确监控主机所在网络的设备将该主机添加到网络映射中，或
- 已使用主机输入功能成功添加该主机，但 Firepower 系统尚未检测到。

MAC 地址 (TTL) (MAC Addresses [TTL])

主机被检测到的 MAC 地址或多个地址和相关 NIC 供应商，括号中为 NIC 硬件供应商和当前生存时间 (TTL) 值。如果 MAC 地址以粗体显示，则 MAC 地址是系统通过 ARP 和 DHCP 流量检测到的主机的实际 MAC 地址。如果有多台设备检测到主机，不管是哪台设备报告的地址，Firepower 管理中心都会显示与主机相关的所有 MAC 地址和 TTL 值。

通常，路由器主机配置文件在该列表中显示路经的网络分段中的主机（IP 地址），以及频繁出现的监控路由器的 IP 地址（针对监控工作站和服务器）。MAC 地址的真实 IP 地址以粗体显示。

Host Type

系统检测到的设备类型：主机、移动设备、越狱的移动设备、路由器、网桥、NAT 设备或负载均衡器。

系统可用下列方法区分网络设备：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型（仅限思科设备）
- 检测生成树协议 (STP)，可识别作为交换机或网桥的设备

- 检测使用同一 MAC 地址的多台主机，可用于识别 MAC 地址为属于路由器
- 检测客户端 TTL 值变化，或检测比典型启动时间变化更频繁的 TTL 值，可识别 NAT 设备和负载均衡器
- 系统可用下列方法区分移动设备：
- 分析来自移动设备的移动浏览器的 HTTP 流量中的用户代理字符串
- 监控特定移动应用的 HTTP 流量

如果一种设备未被确定为网络设备或移动设备，该设备将归类为主机。

上次查看时间

最后一次检测主机的 IP 地址的日期和时间。

Current User

最近一次登录该主机的用户。

请注意，只有当现有当前用户不是授权用户时，登录主机的非授权用户才注册为当前用户。

查看

连接、发现、恶意软件和入侵事件数据视图链接，使用该事件类型的默认工作流程并仅限于显示与主机相关的事件；如果可能，这些事件包括与主机相关的所有 IP 地址。

主机配置文件中的操作系统

通过分析流量中主机生成的网络和应用堆栈或分析用户代理报告的主机数据，系统被动检测运行在主机上的操作系统的标识。此外，系统还将核对其他来源的操作系统信息，比如通过主机输入功能导入的 Nmap 扫描仪或应用数据。当确定将要使用的标识时，系统会考虑分配给每个标识源的优先级。默认情况下，用户输入具有最高优先级，其次是应用或扫描工具源，最后是所发现的身份。

有时候，系统会提供通用操作系统定义而非具体的定义，因为流量和其他标识源无法提供足够信息以确定更具针对性的标识。系统核对其他来源的信息，以尽可能利用最详细的定义。

由于操作系统会影响主机的漏洞列表以及针对主机的事件的事件影响关联，因此可能要手动提供更多具体的操作系统信息。此外，可标明已经应用到操作系统的修复，比如补丁包和更新，以及使修复已经解决的漏洞失效。

例如，如果系统确定主机的操作系统为 Microsoft Windows 2003，但主机实际上运行的是 Microsoft Windows XP Professional SP2，可相应地设置操作系统的标识。设置更具体的操作系统标识可以完善主机漏洞列表，以便该主机的影响相关性更具针对性、更准确。

如果系统检测到的主机操作系统信息与由活动源提供的现有操作系统标识相冲突，会发生标识冲突。当确实存在标识冲突时，系统同时使用漏洞标识和影响相关性。

可以配置网络发现策略以将发现数据添加到受 NetFlow 导出器监控的主机的网络映射中。但是，除非设置主机输入功能来设置操作系统身份，否则没有可用于这些主机的操作系统数据。

如果主机运行的操作系统违反已激活的网络发现策略中的合规白名单，则Firepower管理中心会使用白名单违规图标 (!) 来标记操作系统信息。此外，如果越狱的移动设备违反有效的白名单，该图标会出现在该设备的操作系统旁边。

可以为主机的操作系统标识设置自定义显示字符串。上述自定义显示字符随后用于主机配置文件中。

注释 更改主机的操作系统信息可能会更改其与合规白名单的合规情况。

在网络设备的主机配置文件中，“操作系统”(Operating Systems) 部分的标签更改为“系统”(Systems)，并会另外显示“硬件”(Hardware) 列。如果 Systems 下列出硬件平台值，该系统是网络设备后检测出的一个或多个移动设备。请注意，移动设备可能有，也可能没有硬件平台信息，但不会检测到非移动设备系统的硬件平台信息。

主机配置文件中显示的操作系统信息字段说明如下。

硬件

移动设备的硬件平台。

OS Vendor/Vendor

操作系统供应商。

OS Product/Product

选择以下值之一：

- 根据从所有来源收集的身份数据确定为最可能在主机上运行的操作系统
- `Pending`，如果系统尚未识别操作系统，并且没有其他身份数据可用
- `unknown`，如果系统无法识别操作系统，并且没有其他身份数据可用于操作系统

注释 如果主机的操作系统不是系统可以检测得到的系统，要使用下列任何一种策略：

- 创建主机的自定义指纹。
- 对主机运行 Nmap 扫描。
- 使用主机输入功能将数据导入到网络映射中。
- 手动输入操作系统信息。

操作系统版本/版本

操作系统版本。如果主机是破解的移动设备，则版本后面的括号里会指示 `Jailbroken`。

来源

可为下列任何一种值：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（Nmap 或其他扫描工具）
- Firepower

系统可能会从多个源协调数据，以确定操作系统的身份。

查看操作系统身份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可查看发现的或添加的主机特定操作系统的标识。系统利用来源优先分级来确定主机当前的标识。在标识列表中，当前标识以粗体突出显示。

请注意，仅当主机存在多个操作系统身份时，**查看 (View)** 按钮才可用。

过程

步骤 1 点击主机配置文件的**操作系统 (Operating System)** 或**操作系统冲突 (Operating System Conflicts)** 部分中的**查看 (View)**。

步骤 2 查看主机配置文件中的操作系统，第 1619 页中所述的信息。

步骤 3 或者，点击任何操作系统身份旁边的删除图标 ( )。

注释 不能删除思科检测到的操作系统身份。

此系统从“操作系统身份信息”(Operating System Identity Information) 弹出窗口中删除身份，并在适用情况下更新主机配置文件中的操作系统的当前身份。

设置当前操作系统身份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以使用 Firepower 系统 Web 界面设置主机的当前操作系统身份。在网络界面设置标识来覆盖所有其他标识源，以便把标识用于漏洞评估和影响相关性。但是，如果在编辑操作系统后，系统检测到主机存在冲突的操作系统身份，则会发生操作系统冲突。在解决冲突前，这两种操作系统都被视为当前操作系统。

过程

步骤 1 点击主机配置文件的**操作系统 (Operating System)** 部分中的**编辑 (Edit)**。

步骤 2 此时有多个选择：

- 从**操作系统定义 (OS Definition)** 下拉列表中选择**当前定义 (Current Definition)**，通过主机输入确认当前的操作系统身份，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择当前操作系统身份的变体，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择**用户定义 (User-Defined)**，然后继续执行步骤 3。

步骤 3 或者，选择**使用自定义显示字符串 (Use Custom Display String)**，然后修改要在**供应商字符串 (Vendor String)**、**产品字符串 (Product String)** 和 **版本字符串 (Version String)** 字段中显示的自定义字符串。

步骤 4 或者，要更改为不同供应商提供的操作系统，请从**供应商 (Vendor)** 和**产品 (Product)** 下拉列表中选择。

步骤 5 或者，要配置操作系统的产品版本级别，请从**主要版本 (Major)**、**次要版本 (Minor)**、**修订版本 (Revision)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中选择。

步骤 6 或者，如果要表示已经应用操作系统的修复，请点击**配置修复 (Configure Fixes)**。

步骤 7 在下拉列表中选择适用的修复，然后点击**添加 (Add)**。

步骤 8 或者，使用 **Patch** 和 **Extension** 下拉列表添加相关补丁和扩展。

步骤 9 点击 **Finish**。

操作系统身份冲突

如果当前标识是由诸如扫描仪、应用或用户之类的活动源提供，当系统检测到的新标识与当前标识冲突时，会发生操作系统标识冲突。

冲突的操作系统标识列表在主机配置文件中以粗体显示。

可在系统网络界面解决标识冲突并设置主机当前的操作系统标识。在网络界面设置标识来覆盖所有其他标识源，以便把标识用于漏洞评估和影响相关性。

使冲突的操作系统身份成为当前身份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 导航至主机配置文件的**操作系统 (Operating System)** 部分。

步骤 2 您有两种选择：

- 点击要设置为主机操作系统的操作系统标识旁边的 **Make Current**。
- 如果不希望作为当前标识的标识来自活动源，请删除不必要的标识。

解决操作系统身份冲突

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 在主机配置文件的**操作系统冲突 (Operating System Conflicts)** 部分点击**解决 (Resolve)**。

步骤 2 有以下选项可供选择：

- 从**操作系统定义 (OS Definition)** 下拉列表中选择**当前定义 (Current Definition)**，通过主机输入确认当前的操作系统身份，然后跳转至步骤 6。
- 从**操作系统定义 (OS Definition)** 下拉列表中选择相互冲突的操作系统身份上的一个变体，然后跳转至步骤 6。

- 从**操作系统定义 (OS Definition)** 下拉列表中选择**用户定义 (User-Defined)**，然后继续执行步骤 3。

步骤 3 或者，选择**使用自定义显示字符串 (Use Custom Display String)**，然后输入要在**供应商字符串 (Vendor String)**、**产品字符串 (Product String)** 和**版本字符串 (Version String)** 字段中显示的自定义字符串。

步骤 4 或者，要更改为不同供应商提供的操作系统，请从**供应商 (Vendor)** 和**产品 (Product)** 下拉列表中选择。

步骤 5 或者，要配置操作系统的产品版本级别，请从**主要版本 (Major)**、**次要版本 (Minor)**、**修订版本 (Revision)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中选择。

步骤 6 或者，如果要表示已经应用操作系统的修复，请点击**配置修复 (Configure Fixes)**。

步骤 7 把已经应用的修复添加至修复列表。

步骤 8 点击 **Finish**。

主机配置文件中的服务器

主机配置文件的“服务器”(Servers) 部分列出在受监控网络中的主机上检测到的服务器、从导出的 NetFlow 记录添加的服务器、或者通过主动源（如扫描工具）或主机输入功能添加的服务器。

列表中每台主机最多可包含 100 台服务器。达到限制后，不管是源自活动源或被动源的新服务器信息都会被删除，直到您从主机上删除服务器或服务器超时。

如果使用 Nmap 扫描主机，Nmap 会把此前未检测到的在开放 TCP 端口运行的服务器的结果添加至服务器列表。如果进行 Nmap 扫描或导入 Nmap 结果，可展开的“扫描结果”(Scan Results) 部分内容也会出现在主机配置文件中，列出 Nmap 扫描工具在主机上检测到的服务器信息。此外，如果从网络映射中删掉主机，主机服务器的 Nmap 扫描结果会被丢弃。

注释 系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

使用主机配置文件中的服务器的流程取决于访问文件的方式：

- 如果通过网络映射访问主机配置文件，会出现该服务器的详细信息，粗体高亮该服务器的名称。如果要查看主机上的任何其他服务器的详细信息，请点击服务器名称旁边的查看图标()。
- 如果以任何其他方式访问主机配置文件，展开服务器部分并点击要查看详细信息的服务器旁边的查看图标 ()。

注释 如果主机正在运行的是违反经激活的关联策略中的合规白名单的服务器，则 Firepower 管理中心利用白名单违规图标 () 来标记不合规的服务器。

服务器列表中的列说明如下。

协议

服务器所用协议名称。

端口

运行服务器的端口。

应用协议

以下任一项：

- 应用协议的名称
- 如果系统由于多个原因之一无法肯定或否定地识别应用协议，则为 `pending`
- 如果系统无法根据已知应用协议指纹识别应用协议或如果在没有添加相应服务器的情况下，通过主机输入功能添加具有端口信息的漏洞来添加服务器，则为 `unknown`

将鼠标悬停在应用协议名称上，会显示标记。

供应商和版本 (Vendor and Version)

由 Firepower 系统、Nmap 或其他主动源识别的或通过主机输入功能获得的供应商和版本。如果没有可用源提供任何识别信息，字段为空。

主机配置文件中的服务器详细信息

Firepower 管理中心列出的每个服务器的被动检测到的身份最多可达 16 个。被动检测源包括网络发现数据和NetFlow记录。如果系统检测到多个供应商或服务器版本，该服务器可拥有多个被动标识。例如，如果网络服务器运行不同版本的服务器软件，受管设备和网络服务器场之间的负载均衡器会让系统识别多种 HTTP 被动标识。请注意，Firepower 管理中心对源自活动源的服务器标识数量没有限制，例如，用户输入、扫描仪或其他应用。

Firepower管理中心以粗体显示当前的标识。系统可把服务器当前的标识用于各种用途，包括把漏洞分配给主机、影响评估、根据主机配置文件限制性条件和合规性白名单编写评估相关性规则等。

服务器详细信息可显示与所选服务器相关的更新后的子服务器信息。

查看主机配置文件中的服务器时，服务器详细信息也可在服务器详细信息下方显示服务器横幅。服务器横幅提供服务器的额外信息，以帮助您识别服务器。当攻击者有意修改服务器横幅字符串时，系统无法识别或检测被错误识别的服务器。服务器横幅显示检测到的服务器的第一个数据包中的前 256 个字节。这类信息仅在系统第一次检测到服务器的时候收集，而且仅收集一次。横幅内容分两列列出，左侧以十六进制表示，右侧以相应的 ASCII 表示。

注释 要查看服务器横幅，您必须启用网络发现策略中的 **Capture Banners** 复选框。默认情况下该选项处于禁用状态。

主机配置文件的服务器详细信息部分显示以下信息：

协议

服务器所用协议名称。

端口

运行服务器的端口。

Hits

由 Firepower 系统受管设备或 Nmap 扫描工具检测到的服务器的次数。除非系统检测到该服务器的流量，否则通过主机输入导入的服务器的命中次数为 0。

Last Used

最后一次检测到服务器的时间和日期。除非系统检测到该服务器有新的流量，否则主机输入数据的上次使用时间反映了初始数据导入时间。根据 Firepower 管理中心配置中的设置，通过主机输入功能导入的扫描工具和应用数据会超时，但通过管理中心 Web 界面的用户输入不会超时。

应用协议

如果已知，服务器所用的应用协议的名称。

Vendor

服务器供应商。如果供应商未知，不显示该字段。

版本

服务器版本。如果版本未知，不显示该字段。

来源

可为下列任何一种值：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（Nmap 或其他扫描工具）
- 对于 Firepower 系统检测到的应用，为 `Firepower`、`Firepower Port Match` 或 `Firepower Pattern Match`
- 对于从 NetFlow 记录添加到网络映射的服务器，为 `NetFlow`

系统可能会从多个源协调数据，以确定服务器的身份。

查看服务器详细信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

在主机配置文件中，点击**服务器 (Servers)** 部分的服务器旁边的查看图标 ()。

编辑服务器身份

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可手动更新主机上服务器的标识设置和配置已经应用到主机的任何修复，以删除经修复解决的漏洞。此外，还可以删除服务器标识。

删除身份不会删除服务器，即使删除唯一身份也如此。删除标识会将标识从 Server Detail 弹出窗口移除，而且如果适用，更新主机配置文件中的服务器当前的标识。

不能编辑或删除由思科管理的设备添加的服务器身份。

过程

步骤 1 导航至主机配置文件的**服务器 (Servers)** 部分。

步骤 2 点击**查看 (View)** 以打开“服务器详细信息”(Server Detail) 弹出窗口。

步骤 3 要删除服务器标识，请点击要移除的服务器标识旁边的删除图标 ()。

步骤 4 要修改服务器标识，请点击服务器列表中的服务器旁边的编辑图标 ()。

步骤 5 您有两种选择：

- 从**选择服务器类型 (Select Server Type)** 下拉列表中选择当前定义。
- 从**选择服务器类型 (Select Server Type)** 下拉列表中选择服务器类型。

步骤 6 或者，要仅列出该服务器类型的供应商和产品，请选中**按服务器类型限制 (Restrict by Server Type)** 复选框。

步骤 7 或者，要自定义服务器的名称和版本，请选择**使用自定义显示字符串 (Use Custom Display String)**，然后输入**供应商字符串 (Vendor String)** 和**版本字符串 (Version String)**。

步骤 8 在**产品映射 (Product Mappings)** 部分中，选择要使用的操作系统、产品和版本。

示例：
例如，如果希望服务器映射到 Red Hat Linux 9，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 9 如果要指示已应用服务器的修复，请点击**配置修复 (Configure Fixes)**，并将要为该服务器应用的补丁添加到修复列表。

步骤 10 点击 **Finish**。

解决服务器身份冲突

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

当应用或扫描仪等活动源将服务器身份数据添加到主机上时，如果系统随后检测到该端口上出现表明冲突服务器身份的流量，则会出现服务器身份冲突。

过程

步骤 1 在主机配置文件中，导航至**服务器 (Servers)** 部分。

步骤 2 点击服务器旁边的解决图标。

步骤 3 从**选择服务器类型 (Select Server Type)** 下拉列表中选择服务器类型。

步骤 4 或者，要仅列出该服务器类型的供应商和产品，请选中**按服务器类型限制 (Restrict by Server Type)** 复选框。

步骤 5 或者，要自定义服务器的名称和版本，请选择**用户自定义显示字符串 (Use Custom Display String)**，然后输入**供应商字符串 (Vendor String)** 和**版本字符串 (Version String)**。

步骤 6 在**产品映射 (Product Mappings)** 部分中，选择要使用的操作系统、产品和版本。

示例：

例如，如果希望服务器映射到 Red Hat Linux 9，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 7 如果要指示已应用服务器的修复，请点击**配置修复 (Configure Fixes)**，并将要为该服务器应用的补丁添加到修复列表。

步骤 8 点击 **Finish**。

主机配置文件中的 Web 应用

主机配置文件的“Web 应用”(Web Application) 部分显示系统识别为在您的网络主机上运行的客户端和 Web 应用。系统可同时从被动和主动检测源识别客户端和 Web 应用信息，但是从 NetFlow 记录添加的主机信息有限。

此部分的详细信息包含在主机上检测到的应用的产品和版本、任何可用客户端或 Web 应用信息，以及上一次检测到使用应用的时间。

此部分最多列出16个在主机上运行的客户端。在达到限制后，会丢弃来自主动或被动来源的新客户端信息，直到您从主机上删除客户端应用，或系统由于客户端闲置把客户端从主机配置文件中删除（客户端超时）。

此外，对于每个检测到的网络浏览器，系统会显示浏览器访问的前 100 个 Web 应用。在达到限制后，来自主动或被动源的与该浏览器相关的新的网络应用均会丢弃，直到出现下列任何一种情况：

- 网络浏览器客户端应用超时，或
- 从主机配置文件删除与网络应用相关的应用信息

如果主机正在运行的是违反经激活的关联策略中的合规白名单的应用，则Firepower管理中心利用白名单违规图标 () 来标记不合规的应用。

提示

要分析与主机上特定应用相关的连接事件，请点击该应用旁边的事件图标()。系统将显示连接事件首选工作流程的首页，该页面显示受应用的类型、产品和版本，以及主机的 IP 地址限制的连接事件。如果连接事件没有首选工作流程，必须选择一个首选工作流程。

在主机配置文件中显示的应用信息说明如下。

应用协议

显示应用（HTTP 浏览器、DNS 客户端等等）所使用的应用协议。

Client

来源于负载的客户端信息，由Firepower系统识别、由Nmap捕获、或通过主机输入功能获得。如果没有可用源提供任何识别信息，字段为空。

版本

显示客户端版本。

Web 应用

对于网络浏览器，系统在 HTTP 流量中检测到的内容。Web 应用信息表示由 Firepower 系统识别、由 Nmap 捕获、或通过主机输入功能获得的特定类型的内容（例如，WMV 或 QuickTime）。如果没有可用源提供任何识别信息，字段为空。

从主机配置文件中删除 Web 应用

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

要移除已知的未在主机上运行的应用，您可从主机配置文件删除该应用。请注意，删除主机上的应用可让主机符合白名单。

注释 如果系统再次检测到应用，系统会将该应用重新添加至网络映射和主机配置文件。

过程

步骤 1 在主机配置文件中，导航至**应用 (Applications)** 部分。

步骤 2 点击要删除的应用旁边的删除图标 ( )。

主机配置文件中的主机协议

每个主机配置文件都包含在网络流量中检测到的与主机关联的协议有关的信息。此信息包括：

协议

指主机使用的协议的名称。

层

指协议运行的网络层（`Network` 或 `Transport`）。

如果主机配置文件中显示的协议违反经激活的关联策略中的合规白名单，则Firepower管理中心会利用白名单违规图标 ( ) 来标记不符合规定的协议。

如果主机配置文件列出您已知不在该主机上运行的协议，则可以删除那些协议。从主机上删除协议可让主机符合合规白名单。

注释 如果系统再次检测到协议，系统会将该协议重新添加至网络映射和主机配置文件。

从主机配置文件中删除协议

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 导航至主机配置文件的**协议 (Protocols)** 部分。

步骤 2 点击要删除的协议旁边的删除图标 ( )。

主机配置文件中的危害表现

Firepower 系统将各种类型的数据（入侵事件、安全情报、连接事件及文件或恶意软件事件）进行关联，以确定受监控网络上的主机是否可能受到恶意手段的危害。事件数据的某些组合和频率触发了受影响主机上的危害表现 (IOC) 标记。

主机配置文件中 Indications of Compromise 部分显示了所有主机的 IOC 标记。

要配置系统以标记危害表现，请参阅启用危害表现规则，第 1223 页。

有关使用危害表现的详细信息，请参阅危害表现数据，第 1664 页和相应主题下的子主题。

主机配置文件中的 VLAN 标记

如果主机构成虚拟局域网 (VLAN) 的一部分，系统会显示主机配置文件的 VLAN Tag 部分。

物理网络设备通常使用 VLAN 从各种网络块创建逻辑网段。系统检测到 802.1q VLAN 标记并显示每个标记的下列信息：

- **VLAN ID** 标识主机所属的 VLAN。对于 802.1q VLAN，它可以是 0 至 4095 之间的任何一个整数。
- **Type** 标识包含 VLAN 标记的封装包，可以是以太网或令牌环。
- **Priority** 标识在 VLAN 标记中的优先级，可以是 0 至 7 之间的任何一个整数，其中 7 表示最高优先级。

如果 VLAN 标记嵌套在数据包中，系统进行处理，且Firepower管理中心显示最里面的 VLAN 标记。系统仅收集并显示其通过 ARP 和 DHCP 流量识别的 MAC 地址的 VLAN 标记信息。

例如，在一个全部由打印机构成的 VLAN 中，并且系统在该 VLAN 中检测到 Microsoft Windows 2000 操作系统，VLAN 标记信息是有用的。此外，VLAN 信息帮助系统生成更准确的网络映射。

主机配置文件中的用户历史记录

主机配置文件中的用户历史部分图示了过去二十四个小时的用户活动。用户通常会在晚上注销，而且可能与其他用户分享主机资源。用正常的短条形表示定期登录请求，例如要查看邮件的登录请求。用户标识列表附带有条形图，表明检测到用户登录的时间。请注意，对于未授权的登录，条形图将灰显。

请注意，系统的确会将主机上未授权的用户登录与该主机的 IP 地址关联，因此，用户会显示在该主机的用户历史中。然而，如果检测到同一台主机的授权用户登录，则与授权用户登录相关的用户将沿用与主机 IP 地址的关联，而新的未授权用户登录不会破坏用户与主机 IP 地址的关联。如果在网络发现策略中配置捕获失败的登录，列表包括登录主机失败的用户。

主机配置文件中的主机属性

可利用主机属性按照对网络环境而言重要的方式来对主机进行分门别类。Firepower 系统中有三种类型的属性：

- 预定义主机属性
- 白名单主机属性
- 用户定义的主机属性

在设置预定义主机属性或创建用户定义的主机属性后，必须分配主机属性值。

注释 主机属性可在任意域级别定义。可以分配在当前和祖先域中创建的主机属性。

预定义主机属性

Firepower 管理中心提供两项个定义的主机属性：

主机重要性

此属性用于指定特定主机的业务重要性，并根据主机重要性定制关联响应。例如，如果您认为公司的邮件服务器比一般用户工作站对业务更重要，可把 High 值分配给邮件服务器和其他业务关键设备，把 Medium 或 Low 值分配给其他主机。然后，根据受影响的主机重要性创建可发出不同警报的关联策略。

说明

此特定主机属性用于记录需要其他分析师查看的主机的信息。例如，如果网络上有使用测试用旧版未打补丁操作系统的计算机，可使用注释功能注明此系统特意未打补丁。

白名单主机属性

所创建的每个合规性白名单会创建与白名单具有相同名称的主机属性。白名单主机属性的可能值包括：

- 合规 (Compliant) - 识别符合白名单的主机。
- 不合规 (Non-Compliant) - 识别违反白名单的主机。
- 未评估 (Not Evaluated) - 识别不是白名单的有效目标或因任何原因尚未评估的主机。

不能编辑白名单主机属性值或删除白名单主机属性。

用户定义的主机属性

如果要使用与那些预定义主机属性或白名单主机属性中所用的不同的条件识别主机，您可以创建用户定义的主机属性。例如，您可以：

- 向主机分配物理位置标识符，比如设施代码、城市或房间号码。
- 分配表明特定主机的系统管理员的责任方标识符。然后，制定相关性规则和策略，当检测到与主机相关的问题时，把警报发送给适当的系统管理员。
- 根据主机的IP地址自动将预先定义的列表值分配给主机。当新主机第一次出现在网络上时，可使用此功能将值分配给新主机。

用户定义的主机属性显示在主机配置文件页面中，可在此页面为每台主机分配值。您还可以：

- 在关联策略和搜索中使用这些属性。
- 在事件的主机属性表视图中查看属性并据此生成报告。

用户定义的主机属性可以是以下类型之一：

文本

允许您手动将文本字符串分配给主机。

整数

允许用户指定一系列正整数中的第一个和最后一个数字，然后手动把这些数字中的一个数字分配给主机。

清单

允许用户创建字符串值列表，然后手动将这些值中的其中一个分配给主机。此外，还可根据主机的 IP 地址自动把值分配给主机。

如果根据具有多个 IP 地址的主机的一个 IP 地址自动分配值，那些值将应用到与该主机相关的所有地址。当查看 Host Attributes 表时，请记住此点。

自动分配列表值时，请考虑使用网络对象而不是文字 IP 地址。此方法可提高可维护性，尤其是在多域部署中。在这种部署中，通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义祖先配置。在多域部署中，在祖先域级别定义自动分配的列表时务必要小心谨慎，以避免在后代域使用重叠 IP 地址时与非预定主机匹配。

URL

允许用户手动把 URL 值分配给主机。

删除用户定义的主机属性可将用户定义的主机属性从所有使用该主机属性的主机配置文件中删除。

创建基于文本或 URL 的主机属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

步骤 1 选择**分析 (Analysis)** > **主机 (Hosts)** > **主机属性 (Host Attributes)**。

步骤 2 点击 **Host Attribute Management**。

步骤 3 点击 **Create Attribute**。

步骤 4 输入 **Name**。

步骤 5 在**类型 (Type)** 中选择要创建的属性的类型，如 中所述 用户定义的主机属性，第 1633 页

步骤 6 点击**保存 (Save)**。

创建基于整数的主机属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

当定义基于整数的主机属性时，必须指定属性接受的数字范围。

过程

步骤 1 选择**分析 (Analysis)** > **主机 (Hosts)** > **主机属性 (Host Attributes)**。

步骤 2 点击 **Host Attribute Management**。

步骤 3 点击 **Create Attribute**。

步骤 4 输入 **Name**。

步骤 5 在**类型 (Type)** 中选择要创建的属性的类型，如用户定义的主机属性，第 1633 页中所述。

步骤 6 在 **Min** 字段，输入可分配给主机的最小整数值。

步骤 7 在 **Max** 字段，输入可分配给主机的最大整数值。

步骤 8 点击**保存 (Save)**。

创建基于列表的主机属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

当定义基于列表的主机属性时，必须为列表提供所有的值。这些值可包含字母数字字符、空格和符号。

过程

步骤 1 选择**分析 (Analysis)** > **主机 (Hosts)** > **主机属性 (Host Attributes)**。

步骤 2 点击 **Host Attribute Management**。

步骤 3 点击 **Create Attribute**。

步骤 4 输入 **Name**。

步骤 5 在**类型 (Type)** 中选择要创建的属性的类型，如用户定义的主机属性，第 1633 页中所述。

步骤 6 要将值添加到列表，请点击**添加值 (Add Value)**。

步骤 7 在**名称 (Name)** 字段中，输入要添加的第一个值。

步骤 8 或者，要自动分配刚刚添加到主机属性值，请点击**添加网络 (Add Networks)**。

步骤 9 从**值 (Value)** 下拉列表中选择已添加的值。

步骤 10 在 **IP 地址 (IP Address)** 和 **网络掩码 (Netmask)** 字段中，输入代表要自动分配该值的 IP 地址块的 IP 地址和网络掩码 (IPv4)。

步骤 11 重复第 6 步至第 10 步，在列表中添加更多值，并自动将其分配给 IP 地址块中的新主机。

步骤 12 点击**保存 (Save)**。

设置主机属性值

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以设置预定义和自定义主机属性的值。不过，无法为系统生成的白名单主机属性设置值。

过程

步骤 1 打开要修改的主机配置文件。

步骤 2 在**属性 (Attributes)** 部分中，点击 **编辑属性 (Edit Attributes)**。

步骤 3 根据需要更新属性。

步骤 4 点击**保存 (Save)**。

主机配置文件中的白名单违规事件

合规性白名单（或白名单）指允许用户指定可在特定子网上运行的操作系统、应用协议、客户端、网络应用和协议的一系列标准。

如果在活动关联策略中添加白名单，系统检测到主机违反白名单时，Firepower管理中心会将白名单事件（一种特殊类型的关联活动）记入数据库。这些白名单事件中的任何一个事件都对应一种白名单违规，表明特定主机违反白名单的原因和方式。如果主机违反一个或多个白名单，可以两种方式查看其主机配置文件中的这些违规情况。

首先，主机配置文件列出与主机相关的单个白名单违规事项。

主机配置文件中的白名单违规信息的说明如下。

Type

违规类型，即违规是由于操作系统、应用、服务器还是协议不符合规定造成的。

Reason

出现违规的具体原因。例如，如果白名单仅容许 Microsoft Windows 主机，主机配置文件会显示当前运行在主机上的操作系统（比如，`Linux Linux 2.4、2.6`）

White List

与违规关联的白名单的名称。

其次，在与操作系统、应用、协议和服务器有关的部分中，Firepower管理中心将为不合规元素标记白名单违规图标 ( )。例如，对于仅容许 Microsoft Windows 主机的白名单，主机配置文件会在该主机操作系统信息旁边显示白名单违规图标。

注释 您可以利用主机的配置文件为合规白名单创建共享主机配置文件。

创建共享白名单主机配置文件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

合规性白名单共享主机配置文件明确规定操作系统、应用协议、客户端、网络应用和允许在多个白名单的目标主机上运行的协议。也就是说，如果创建多个白名单，但要使用相同的主机配置文件来评估运行白名单中规定的特定操作系统的主机，要使用共享主机配置文件。

可使用任何 IP 地址已知的主机的主机配置文件创建可供合规性白名单使用的共享主机配置文件。但请注意，如果系统尚未识别主机的操作系统，则无法根据单个主机的主机配置文件创建共享主机配置文件。

过程

步骤 1 在主机配置文件中，点击**生成白名单配置文件 (Generate White List Profile)**。

步骤 2 根据特定需要修改并保存共享主机配置文件。

主机配置文件中的恶意软件检测

Most Recent Malware Detections 部分列出主机发送或接收恶意软件文件的最新恶意软件事件，最多 100 个。主机配置文件列出基于网络（面向 Firepower 的 AMP）和基于终端（面向终端的 AMP）的恶意软件事件。

如果主机涉及文件事件，且文件在回溯时被确定为恶意软件，在识别恶意软件开始后，恶意软件检测列表会显示传输文件的原始事件。当确定为恶意软件的文件在回溯时被确定为非恶意软件时，该列表不会再显示与该文件相关的恶意软件事件。例如，如果文件性质为 `Malware`，并且该性质更改为 `Clean`，则从主机配置文件中的恶意软件检测列表中移除针对该文件的事件。

在主机配置文件中查看恶意软件检测情况时，可在事件查看器中查看该主机的恶意软件事件。要查看事件，请点击恶意软件图标 ()。

对主机配置文件中 Most Recent Malware Detection 部分中各列的描述如下。

Time

事件的生成日期和时间。

对于文件在回溯时被确定为恶意软件的事件，请注意，这是指原始事件的时间而非确定恶意软件的时间。

Host Role

主机在传输检测到的恶意软件中的角色，发送方或接收方。请注意，对于基于终端的恶意软件事件，主机扮演的角色始终是接收者。

Threat Name

检测到的恶意软件的名称。

文件名

恶意软件文件的名称。

文件类型

文件类型；例如，`PDF` 或 `MSEXE`。

主机配置文件中的漏洞

主机配置文件 Vulnerabilities 部分显示影响该主机的漏洞。这些漏洞基于系统在主机上检测到的操作系统、服务器和应用。

如果主机操作系统标识或主机上的一种应用协议存在标识冲突，系统会在冲突解决前显示这两种标识的漏洞。

对于从 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”(Vulnerable)（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。

流量通常不包括有关服务器供应商和版本的信息。默认情况下，系统并不映射此类流量的发送和接收主机的关联漏洞。但可配置系统以映射没有供应商或版本信息的特定应用协议的漏洞。

如果使用主机输入功能添加网络中主机的第三方漏洞信息，系统会额外显示 Vulnerabilities 部分。例如，如果导入从 QualysGuard 扫描仪获得的漏洞，系统上的主机配置文件将包含 QualysGuard Vulnerabilities 部分。对于第三方漏洞，主机配置文件中相应的“漏洞”(Vulnerabilities) 部分包含的信息仅限于用户使用主机输入功能导入漏洞数据时提供的信息。

您可把第三方漏洞与操作系统和应用协议关联起来，但不得关联客户端。有关导入第三方漏洞的信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

主机配置文件中“漏洞”(Vulnerabilities) 部分中各列的说明如下。

Name

漏洞名称。

远程

表明漏洞是否可以远程利用。如果该列为空，漏洞定义不包含此信息。

组件

与漏洞有关的操作系统、应用协议或客户端的名称。

端口

端口号，如果漏洞与在特定端口运行的应用协议相关。

下载漏洞补丁

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以下载补丁以减少在网络中主机上发现的漏洞。

过程

步骤 1 访问要下载补丁的主机的主机配置文件。

步骤 2 展开 **Vulnerabilities** 部分。

步骤 3 点击要修补漏洞的名称。

步骤 4 展开**修复 (Fixes)** 部分以显示漏洞的补丁列表。

步骤 5 点击要下载的补丁旁边的 **Download**。

步骤 6 下载补丁并应用到受影响的系统上。

停用单个主机的漏洞

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以使用主机漏洞编辑器逐台主机停用漏洞。当停用主机漏洞时，该主机的影响相关性依然在使用该漏洞，但其影响级别自动降低一个级别。

过程

步骤 1 导航至主机配置文件的**漏洞 (Vulnerabilities)** 部分。

步骤 2 点击**编辑漏洞 (Edit Vulnerabilities)**。

步骤 3 从**有效漏洞 (Valid Vulnerabilities)** 列表中选择漏洞，然后点击向下箭头将其移至**无效漏洞 (Invalid Vulnerabilities)** 列表。

提示 可以点击并拖动以选择多个相邻漏洞；也可以双击任何漏洞以在列表间将其移动。

步骤 4 点击**保存 (Save)**。

接下来的操作

- 或者，通过将主机的漏洞从**无效漏洞 (Invalid Vulnerabilities)** 列表移至**有效漏洞 (Valid Vulnerabilities)** 列表来停用该漏洞。

停用单个漏洞

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

如果停用主机配置文件中的漏洞，则网络中的所有主机都会停用该漏洞。但是，可随时重新激活。

在多域部署中，停用祖先域中的某个漏洞将会使其在所有后代域中都停用。如果在祖先域中激活漏洞，则枝叶域可以为其设备激活或停用该漏洞。

过程

步骤 1 访问漏洞详细信息：

- 在受影响的主机配置文件，展开**漏洞 (Vulnerabilities)** 部分，点击要启用或禁用的漏洞的名称。
- 在预定义工作流程中，选择**分析 (Analysis)** > **漏洞 (Vulnerabilities)** > **漏洞 (Vulnerabilities)**，然后点击要启用或禁用的漏洞旁边的查看图标 ( )。

步骤 2 从**影响限定条件 (Impact Qualification)** 下拉列表中选择**已禁用 (Disabled)**。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 确认要更改网络映射上所有主机的**影响限定条件 (Impact Qualification)** 值。

步骤 4 点击 **Done**。

接下来的操作

- 或者，通过在执行上述步骤时从**影响限定条件 (Impact Qualification)**下拉列表中选择**已启用 (Enabled)** 激活漏洞。

主机配置文件中的扫描结果

当您使用 Nmap 扫描主机时，或者导入 Nmap 的扫描结果时，这些结果出现在所有被扫描的主机的主机配置文件中。

直接把 Nmap 搜集到的有关主机操作系统和运行在开放式未经过滤的端口的服务器的信息分别添加到主机配置文件的 Operating System 和 Servers 部分。此外，Nmap 在 Scan Results 部分添加该主机的扫描结果列表。请注意，扫描必须找到主机上的开放端口，以便“扫描结果”(Scan Results) 部分出现在配置文件中。

结果代表的是信息源、扫描的端口的数量和类型、运行在端口的服务器的名称和任何 Nmap 检测到的其他信息，比如端口状态或服务器的供应商名称。如果扫描UDP端口，在这些端口上检测到的服务器仅出现在 Scan Results 部分。

请注意，可从主机配置文件运行 Nmap 扫描。

扫描主机配置文件中的主机

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

可对主机配置文件中的主机进行 Nmap 扫描。在扫描完后，更新主机配置文件中的该主机的服务器和操作系统信息。所有其他扫描结果可添加至主机配置文件中的 Scan Results 部分。

注意 在再一次运行 Nmap 扫描或用更高优先级的主机输入覆盖之前，Nmap 提供的服务器和操作系统数据保持不变。如果计划使用 Nmap 来扫描主机，请定期安排扫描。

开始之前

- 添加 Nmap 扫描实例；请参阅添加 Nmap 扫描实例 ， 第 1165 页。

过程

步骤 1 在主机配置文件中，点击 **Scan Host**。

步骤 2 点击要用来扫描主机的扫描更正旁边的 **Scan**。
系统扫描主机并将结果添加到主机配置文件中。

第 88 章

处理发现事件

以下主题介绍如何处理发现事件：

发现事件中的发现和身份数据

系统会生成代表受监控网络上检测到的更改的事件表。您可以使用这些表查看网络上的用户活动，并确定如何做出响应。网络发现和身份策略指定要收集的数据类型、要监控的网段以及要使用的特定硬件接口。

您可以使用发现和身份事件表识别与网络上的主机、应用和用户相关联的威胁。系统会提供一系列可用于分析系统生成的事件的预定义工作流程。也可创建仅显示与特定需求匹配的自定义工作流程。

要收集和存储网络发现和身份数据以用于分析，您必须配置网络发现和身份策略。配置身份策略后，您必须将其调用到访问控制策略中，并将其部署到要用于监控流量的设备中。

网络发现策略提供主机、应用和非授权用户数据。身份策略提供授权用户数据。

以下发现事件表位于“分析”(Analysis) > “主机”(Hosts)、“分析”(Analysis) > “用户”(Users) 和“分析”(Analysis) > “漏洞”(Vulnerabilities) 菜单下。

发现事件表	已填充发现数据？	已填充身份数据？
主机数	是	否
危害表现	是	否
应用	是	否
应用详情	是	否

发现事件表	已填充发现数据？	已填充身份数据？
服务器	是	否
Host Attributes	是	否
Discovery Events	是	是
用户活动	是	是
用户	是	是
漏洞	是	否
Third-Party Vulnerabilities	是	否

查看发现事件统计信息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

“发现统计信息”(Discovery Statistics) 页面显示系统检测到的主机、事件、协议、应用协议和操作系统的摘要。

此页面列出了最近一小时的统计数据和全部的累积统计数据。可选择查看特定设备或所有设备的统计信息。也可通过点击摘要内列出的事件、服务器、操作系统或操作系统供应商查看与此页面上条目匹配的事件。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述 (Overview)** > **摘要 (Summary)** > **发现统计信息 (Discovery Statistics)**。

步骤 2 从**选择设备 (Select Device)** 列表中选择要查看其统计信息的设备。或者，选择**全部 (All)** 查看由 Firepower 管理中心管理的所有设备的统计信息。

步骤 3 您有以下选择：

- 在“统计信息摘要”中，查看一般统计信息，如统计信息摘要部分，第 1645 页中所述。
- 在“事件明细”(Event Breakdown) 中，点击要查看的事件类型。如果未显示事件，可能需要调整时间范围，如更改时间窗口，第 1461 页中所述。

- 在“协议明细”(Protocol Breakdown) 中，查看检测到的主机当前所使用的协议。
- 在“应用协议明细”(Application Protocol Breakdown) 中，点击要查看的应用协议的名称。
- 在“操作系统明细”(OS Breakdown) 中，点击**操作系统名称 (OS Name)** 或**操作系统供应商 (OS Vendor)**。

统计信息摘要部分

以下对统计摘要部分的各行进行了说明。

Total Events

Firepower 管理中心上存储的发现事件的总数。

Total Events Last Hour

最近一小时生成的发现事件的总数。

Total Events Last Day

最后一天生成的发现事件的总数。

Total Application Protocols

检测到的主机上运行的服务器所使用的应用协议总数。

Total IP Hosts

通过唯一 IP 地址识别的检测到的主机总数。

Total MAC Hosts

不是通过 IP 地址识别的检测到的主机总数。

注意无论用户是否查看所有设备或特定设备的发现统计数据，Total MAC Hosts 统计数据都保持不变。这是因为受管设备是根据其 IP 地址发现主机的。此统计数据提供通过其他方式识别的独立于给定受管设备的所有主机的总数。

Total Routers

检测到的识别为路由的节点总数。

Total Bridges

检测到的识别为网桥的节点总数。

Host Limit Usage

当前所使用主机上限的总百分比。主机限制根据 Firepower 管理中心的型号来定义。注意只有在查看所有受管设备的统计数据时才会显示主机上限的使用情况。

注释 如果达到主机上限且已删除一台主机，则此主机不会再出现在您清除了发现数据的网络映射上。

Last Event Received

最新发现事件发生的日期和时间。

Last Connection Received

最新连接完成的日期和时间。

事件明细部分

“事件明细”(Event Breakdown) 部分列出了最近一小时内发生的各种发现事件和主机输入事件的计数，以及数据库中存储的每种事件类型的总数的计数。

也可通过事件明细部分查看发现和主机输入事件的详细信息。

协议明细部分

协议明细部分列出了检测到的主机当前所使用的协议。显示每个检测到的协议的名称、其在协议栈中的“协议层”和使用此协议进行通信的主机的总数。

应用协议明细部分

应用协议明细部分列了检测到的主机当前所使用的应用协议。列出了协议名称、最近一个小时内运行应用协议的主机的总数和检测到的随时运行协议的主机的总数。

也可通过应用协议明细部分查看使用所检测到协议的服务器的详细信息。

操作系统明细部分

OS 明细列部分出了当前在受监控网络中运行的操作系统，及其供应商和运行每个操作系统的主机的总数。

操作系统名称或版本的 `unknown` 值是指操作系统或其版本与系统的任何指纹都不匹配。`pending` 值表明系统尚未采集到足够的信息用于识别操作系统或其版本。

可通过 OS 明细部分查看检测到的操作系统的详细信息。

查看发现性能图表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/维护人员

可利用发现事件生成显示受管设备性能统计数据的图表。

每五分钟累积一次统计图表新数据。因此，如果快速重新加载图表，直到下一次五分钟更新间隔之前数据可能不会更改。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**概述 (Overview)** > **摘要 (Summary)** > **发现性能 (Discovery Performance)**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择 Firepower 管理中心或要包括的受管设备。

步骤 3 从**选择图表 (Select Graph[s])** 列表中，选择要创建的图表类型，如发现性能图表类型，第 1647 页中所述。

步骤 4 从**选择时间范围 (Select Time Range)** 列表中，选择要用于图表的时间范围。

步骤 5 点击 **Graph** 生成所选统计数据的图表。

发现性能图表类型

可用图表类型的说明如下。

Processed Events/Sec

显示表示数据相关器每秒钟所处理事件数量的图表

Processed Connections/Sec

显示表示数据相关器每秒钟所处理连接数量的图表

Generated Events/Sec

显示表示系统每秒钟所生成的事件数量的图表

Mbits/Sec

显示表示发现进程每秒钟所分析流量兆比数的图表

Avg Bytes/Packet

显示表示发现进程所分析的每个数据包中所含平均兆比数的图表

K Packets/Sec

显示表示发现进程每秒钟所分析的数千个数据包数量的图表

使用发现和身份工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	任务相关

Firepower管理中心提供一组可用于分析为您的网络生成的发现和身份数据的事件工作流程。工作流程与网络映射是关于网络资产的关键信息来源。

Firepower管理中心为发现和身份数据、受检测主机及其主机属性、服务器、应用、应用详细信息、漏洞、用户活动和用户提供预定义工作流程。也可创建自定义工作流程。

过程

步骤 1 要访问预定义工作流程，请执行以下操作：

- 发现和主机输入数据 - 请参阅查看发现和主机输入事件， 第 1655 页。
- 主机数据 - 请参阅查看主机数据， 第 1657 页。
- 主机属性数据 - 请参阅查看主机属性， 第 1662 页。
- 危害表现数据 - 请参阅查看危害表现数据， 第 1665 页。
- 服务器数据 - 请参阅查看服务器数据， 第 1669 页。
- 应用数据 - 请参阅查看应用数据， 第 1672 页。
- 应用详细信息数据 - 请参阅查看应用详细信息数据， 第 1674 页。
- 用户数据 - 请参阅查看用户数据， 第 1685 页。
- 用户活动数据 - 请参阅查看用户活动数据， 第 1691 页。
- 网络映射 - 请参阅查看网络映射， 第 1417 页。

步骤 2 要访问自定义工作流程，请选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义工作流程 (Custom Workflows)**。

步骤 3 要根据自定义表访问工作流程，请选择**分析 (Analysis)** > **自定义 (Custom)** > **自定义表 (Custom Tables)**。

步骤 4 执行以下任何操作，这些操作对于网络发现工作流程中访问的所有页面通用：

- 限制列 - 要限制显示的列，请点击要隐藏的列标题中的关闭图标 ( )。在显示的弹出窗口中，点击 **Apply**。

提示 要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击 Disabled Columns 下的列名称。

- 删除 - 要删除当前受限制视图中的部分或所有项目，请选中要删除的项目旁边的复选框，然后点击**删除 (Delete)**，或者点击**全部删除 (Delete All)**。这些项目保持删除状态，直到系统的发现功能重新启用时才可再次检测到这些项目。

  注释 **不能**删除思科（与第三方相对）漏洞；但是，可以将其标记为已审核。

- 向下展开 - 要向下展开到工作流程中的下一个页面，请参阅使用向下钻取页面，第 1450 页。
- 导航当前页面 - 要在当前工作流程页面中导航，请参阅工作流程页面导航工具，第 1447 页。
- 在工作流程中导航 - 要在当前工作流程中的页面之间进行导航，从而保留当前限制，请点击工作流程页面左上方的相应页面链接。
- 导航到其他工作流程 - 要导航到其他事件视图以检查关联事件，请参阅工作流程间导航，第 1466 页。
- 对数据进行排序 - 要在工作流程中对数据进行排序，请点击列标题。再次点击列标题以反转排列顺序。
- 查看主机配置文件 - 要查看 IP 地址的主机配置文件，请点击主机配置文件图标 ()，或者对于具有活动危害表现 (IOC) 标记的主机，点击该 IP 地址旁边显示的受损主机图标 ()。
- 查看用户配置文件 - 要查看用户身份信息，请点击显示在用户身份旁边的用户图标（  ）。

发现和主机输入事件

系统生成变化详情在受监控网段中通信的发现事件。为新发现的网络功能生成新的事件，并为先前识别的网络资产的任何变化生成更改事件。

在初始网络发现阶段，系统为每台主机以及已发现在每台主机上运行的每个 TCP 或 UDP 服务器生成新的事件。或者，可配置系统，以使用导出的 NetFlow 记录生成这些新主机和服务器事件。

此外，系统为每个网络、传送和在每台已发现主机上运行的应用协议生成新的事件。您可以在配置用于监控 NetFlow 导出器的发现规则中禁用应用协议的删除，但不可以在配置用于监控 Firepower 系统管理的设备的发现规则中禁用应用协议的删除。如果在非 NetFlow 发现规则中启用的主机或用户发现，系统自动发现应用。

初次网络映射完成后，系统通过生成更改事件持续记录网络变化。无论先前发现的资产配置何时发生改变，系统都会生成更改事件。

如果生成发现事件，表明已登录到数据库。您可使用 Firepower 管理中心 Web 界面查看、搜索和删除发现事件，也可以在关联规则中使用发现事件。根据生成的发现事件类型以及其他指定条件，用于关联策略时可生成关联规则，网络流量符合条件时可启动修复和系统记录、SNMP和邮件警报响应。

可使用主机输入功能向网络映射中添加数据。可添加、修改或删除操作系统信息，这些操作会导致系统停止更新此主机的此信息。也可手动添加，修改或删除应用协议、客户端、服务器和主机属性或修改漏洞信息。执行此操作时，系统生成主机输入事件。

发现事件类型

可以配置系统在网络发现策略中记录的发现事件的类型。查看发现事件表时，**事件 (Event)** 列中列出事件类型。以下是发现事件类型的说明。

Additional MAC Detected for Host

系统检测到先前所发现主机的新 MAC 地址时，生成此事件。

系统检测到主机经流量通过路由器时，经常生成此事件。虽然每台主机都有不同的 IP 地址，但它们似乎有与路由器关联的 MAC 地址。系统检测到与 IP 地址关联的实际 MAC 地址时，主机配置文件中 MAC 地址显示为粗体文本且在事件视图的事件说明中 MAC 地址显示为“检测到 ARP/DHCP”消息。

Client Timeout

系统从数据库中删除一个不活跃的客户端时，生成此事件。

Client Update

系统在 HTTP 流量中检测到负载（即特定类型的内容，例如音频、视频或网页邮件）时，生成此事件。

DHCP: IP Address Changed

系统检测到主机 IP 地址因 DHCP 地址分配改变时，生成此事件。

DHCP: IP Address Reassigned

主机重新使用 IP 地址时，生成此事件；即主机因 DHCP IP 地址分配获得另一物理主机以前使用的 IP 地址时。

Hops Change

系统检测到主机与检测此主机的设备之间的网络跳数发生变化时，生成此事件。如果出现以下情况，则会发生跳数更改：

- 设备通过不同路由器看到主机流量，并能更好地确定主机的位置。
- 如果设备检测到来自该主机的 ARP 传输，这表明主机在本地网段。

Host Deleted: Host Limit Reached

在超过 Firepower 管理中心上的主机限制并从网络映射删除一台受监控主机时，发生此事件。

Host Dropped: Host Limit Reached

在Firepower管理中心中达到主机上限时发生此事件且并丢弃一台新主机。对比此事件与达到主机上限时旧主机从网络映射中被删除的先前事件

要在达到主机限制时丢弃新主机，请转至**策略 (Policies)** > **网络发现 (Network Discovery)** > **高级 (Advanced)** 并将**达到主机限制时 (When Host Limit Reached)** 设为**丢弃主机 (Drop hosts)**。

Host IOC Set

为主机设置 IOC（危害表现）时生成此事件并并生成警报。

Host Timeout

主机由于未在网络发现策略规定的区间内发生流量而从网络映射中丢失时生成此事件。注意个别主机 IP 地址和 MAC 地址会单独超时；主机不会从网络映射中消失除非其所有关联地址均已超时。

如果更改了网络发现策略需监控的网络，可能需要从网络映射中手动删除旧主机，以免主机限制受到影响。

Host Type Changed to Network Device

系统检测到的主机实际上是网络设备时生成此事件。

Identity Conflict

系统检测到新服务器或操作系统标识与服务器或操作系统的当前活跃标识相冲突时生成此事件。

如果要通过重新扫描主机获取更新的有效标识数据来解决标识冲突，可使用标识冲突事件触发Nmap修复。

Identity Timeout

来自主动源的服务器或操作系统身份数据超时时，生成此事件。

如果要通过重新扫描主机获取更新的有效标识数据来刷新标识冲突，可使用标识冲突事件触发Nmap修复。

MAC Information Change

系统检测到与特定 MAC 地址或 TTL 值关联的信息发生变化时，生成此事件。

系统检测到主机流量通过路由器时，经常生成此事件。虽然每台主机都有不同的IP地址，但它们似将都有与路由器关联的 MAC 地址。系统检测到与 IP 地址关联的实际 MAC 地址时，主机配置文件中MAC地址显示为粗体文本且在事件视图的事件说明中MAC地址显示为“检测到ARP/DHCP”消息。TTL可能会因为流量可能通过不同的路由器或者系统检测到主机的实际MAC地址而发生改变。

NETBIOS Name Change

系统检测到主机的NetBIOS名称改变时，生成此事件。只有有主机使用NetBIOS协议时才会生成此事件。

New Client

系统检测到新的客户端时，生成此事件。

注释 要采集和存储客户数据用于分析，请确保网络发现策略的发现规则中启用应用检测。

New Host

系统检测到新主机在网络中运行时，生成此事件。

设备处理涉及新主机的NetFlow数据时，也可生成此事件。要在此情况下生成事件，请将管理NetFlow数据的网络发现规则配置为发现主机。

New Network Protocol

系统检测到主机使用新的网络协议（IP、ARP 等）通信时，生成此事件。

New OS

系统检测到主机适用新的操作系统或者主机操作系统发生变化时，生成此事件。

New TCP Port

系统检测到主机上有活跃的新 TCP 服务器端口（例如，SMTP 或网络服务使用的端口）时，生成此事件。此事件不用于识别应用协议或与其关联的服务器；此信息在 TCP 服务器信息更新事件中传输。

设备在处理涉及网络映射中已不存在的受监控网络中服务器的 NetFlow 数据时，也会生成此事件。要在此情况下生成事件，请将管理 NetFlow 数据的网络发现规则配置为发现应用。

New Transport Protocol

系统检测到主机使用新的传输协议，例如 TCP 或 UDP，通信时，生成此事件。

New UDP Port

系统检测到主机上有新的 UDP 服务器端口时，生成此事件。

设备在处理涉及网络映射中已不存在的受监控网络中服务器的 NetFlow 数据时，也会生成此事件。要在此情况下生成事件，请将管理 NetFlow 数据的网络发现规则配置为发现应用。

TCP Port Closed

系统检测到主机上的 TCP 端口关闭时，生成此事件。

TCP Port Timeout

系统在系统网络发现策略规定的区域内未检测到来自 TCP 端口的活动时，生成此事件。

TCP Server Information Update

系统检测到主机上运行的已发现 TCP 服务器发生变化时，生成此事件。

如果 TCP 服务器已升级，则生成此事件。

UDP Port Closed

系统检测到主机上 UDP 端口关闭时，生成此事件。

UDP Port Timeout

系统在网络发现策略规定的区域内未检测到来自 UDP 端口的活动时，生成此事件。

UDP Server Information Update

系统检测到主机上运行的已发现 UDP 服务器发生变化时，生成此事件。

如果 UDP 服务器已升级，则生成此事件。

VLAN Tag Information Update

系统检测到主机的 VLAN 标签发生改变时，生成此事件。

主机输入事件类型

查看发现事件表时，**Event** 列中列出事件类型。

对比用户执行特定操作（例如手动添加主机）时生成的主机输入事件与系统自身检测到受监控网络发生变化（例如来自之前未检测到主机的流量）时生成的发现事件。

可通过修改网络发现策略配置主机输入事件的类型。

如果了解了不同类型主机输入事件事件所提供的信息，可以更有效地确定需记录和警报的事件以及如何在关联策略中使用这些警报。此外，了解事件类型的名称有助于更有效地进行事件搜索。不同类型的主机输入事件的说明如下。

Add Client

用户添加客户端时，生成此事件。

Add Host

用户添加主机时，生成此事件。

Add Protocol

用户添加协议时，生成此事件。

Add Scan Result

系统成功将 Nmap 扫描的结果添加到主机时，生成此事件。

Add Port

用户添加服务器端口时，生成此事件。

Delete Client

用户从系统中删除客户端时，生成此事件。

Delete Host/Network

用户从系统中删除 IP 地址或子网时，生成此事件。

Delete Protocol

用户从系统中删除协议时，生成此事件。

Delete Port

用户从系统中删除服务器端口或服务器端口组时，生成此事件。

Host Attribute Add

用户创建新的主机属性时，生成此事件。

Host Attribute Delete

用户删除自定义主机属性时，生成此事件。

Host Attribute Delete Value

用户删除主机属性赋值值时，生成此事件。

Host Attribute Set Value

用户设置为主机设置主机属性值时，生成此事件。

Host Attribute Update

用户改变自定义主机属性的定义时，生成此事件。

Set Host Criticality

用户设置或修改主机的主机重要性时，生成此事件。

Set Operating System Definition

用户设置主机的操作系统时，生成此事件。

Set Server Definition

用户设置服务器的供应商和版本定义时，生成此事件。

Set Vulnerability Impact Qualification

设置漏洞影响限制时，生成此事件。

在全球层面上禁止漏洞用于影响限制，或者在全球层面上禁用漏洞时，生成此事件。

Vulnerability Set Invalid

用户作废（或审查）一个漏洞或多个漏洞时，生成此事件。

Vulnerability Set Valid

用户作废之前标记为无效的漏洞时，生成此事件。

查看发现和主机输入事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

通过发现事件工作流程，从发现事件和主机输入事件均可查看数据。可以根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问事件时所看到的页面因所使用的工作流程而异。可使用预定义工作流程，包括发现事件的表视图和终止主机视图页面。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 选择**分析 (Analysis)** > **主机 (Hosts)** > **发现事件 (Discovery Events)**。

步骤 2 您有以下选择：

- 调整时间范围，如更改时间窗口，第 1461 页中所述。

  注释 如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间窗口（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅发现事件字段，第 1655 页。

发现事件字段

可在以下发现事件表中查看和搜索的字段的说明。

Time

系统生成事件的时间。

Event

发现事件的类型或主机输入事件的类型。

IP 地址

与事件所涉及主机关联的 IP 地址。

User

事件生成前登录到事件所涉及的主机的最后一名用户。如果授权用户登录后只有未授权用户登录，除非其他授权用户登录，否则此授权用户仍是主机的当前用户。

MAC Address

触发发现事件的网络流量所使用NIC的MAC地址。MAC地址可以是事件所涉及的主机的实际MAC地址或者是有流量通过的网络设备的 MAC 地址。

MAC Vendor

触发发现事件的网络流量所使用 NIC 的 MAC 硬件供应商。

搜索此字段时，请输入 virtual_mac_vendor 以匹配涉及虚拟主机的事件。

端口

如适用，是指触发此事件的流量所使用的端口。

说明

事件的文字说明。

域

发现主机的设备的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

设备

生成事件的受管设备的名称。对于基于 NetFlow 数据的新主机和新服务器事件，此设备是处理数据的受管设备。

主机数据

系统检测到主机并采集其有关信息用于生成主机配置文件时，生成此事件。可使用Firepower管理中心网络界面查看，搜索和删除主机。

查看主机时，可根据所选主机创建流量量变曲线和合规性白名单。也可赋予主机属性，包括主机对于主机重要性。然后可使用这些关键性值、白名单和关联规则和策略中的流量量变曲线。

系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

查看主机数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower 管理中心查看列出了系统检测到的主机的表。然后，可根据要查找的信息操作视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问主机时所看到的页面因所使用工作流程的不同而不同。两个预定义工作流程结束于主机视图中，该视图包含符合限制条件的每台主机的配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问主机数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **主机 (Hosts)**。
- 如果使用的是不包含主机表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**主机 (Hosts)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅主机数据字段，第 1657 页。
- 为特定主机分配主机属性；请参阅为所选主机设置主机属性，第 1664 页。
- 为特定主机创建流量量变曲线，请参阅为所选主机创建流量量变曲线，第 1661 页。
- 根据特定主机创建合规白名单，请参阅根据所选主机创建合规白名单，第 1662 页。

主机数据字段

系统发现主机时，会采集有关此主机的数据。该数据可能包括主机的IP 地址、其运行的操作系统等等。可在主机表视图中查看部分该信息。

可以在下面的主机表中查看和搜索的字段说明。

上次查看时间

系统最后检测到的任何主机 IP 地址的日期和时间。至少应按网络发现策略中配置的更新间隔更新 Last Seen 值，另外当系统为任何主机 IP 地址生成新的主机事件时，也要执行该更新。

对于使用主机输入功能更新操作系统数据的主机，Last Seen 值表示最初添加数据的日期和时间。

IP 地址

与主机关联的 IP 地址。

MAC Address

检测到的主机 NIC 的 MAC 地址。

MAC Address 字段显示在主机表视图中，该视图可在主机工作流程中找到。也可将 MAC Address 字段添加至：

- 包括来自主机表的字段的自定义表
- 基于主机表的自定义工作流程中的向下钻取页面

MAC Vendor

检测到的主机 NIC 的 MAC 硬件供应商。

MAC Vendor 字段显示在主机表视图中，该视图可在主机工作流程中找到。也可将 MAC Vendor 字段添加至：

- 包括来自主机表的字段的自定义表
- 基于主机表的自定义工作流程中的向下钻取页面

搜索此字段时，请输入 `virtual_mac_vendor` 以匹配涉及虚拟主机的事件。

Current User

主机当前登录用户的用户标识（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

主机重要性

分配给主机的用户指定的关键性值。

NetBIOS Name

主机的 NetBIOS 名称。只有运行 NetBIOS 协议的主机才有 NetBIOS 名称。

VLAN ID

主机使用的 VLAN ID。

跳数

逐一检测主机的设备的网络跳数。

Host Type

主机的类型。可以为以下任意一种：主机、移动设备、破解移动设备、路由器、网桥、NAT 设备和负载均衡器。

系统用于区分网络设备的方法包括：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型（仅限思科设备）
- 检测生成树协议 (STP)，可识别作为交换机或网桥的设备
- 检测使用同一 MAC 地址的多台主机，可用于识别 MAC 地址为属于路由器
- 检测客户端 TTL 值的变化或变化频率高于典型启动时间的 TTL 值，可用于识别 NAT 设备和负载均衡器

如果设备未被识别为网络设备，则归类为主机。

搜索此字段中，请输入 `!host` 以搜索所有网络设备。

硬件

移动设备的硬件平台。

操作系统

以下项之一：

- 在主机上检测到的或使用 Nmap 或主机输入功能更新的操作系统（名称、供应商和版本）。
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个身份，这些身份将显示在逗号分隔列表中。

从控制面板上 Custom Analysis 构件中调用主机事件视图时，此字段显示。它也是基于主机表的自定义表中的一个字段选项。

搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

OS Conflict

此字段仅供搜索。

操作系统供应商

以下项之一：

- 主机上检测到的或使用 Nmap 或主机输入功能升级的操作系统的供应商。
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个供应商，这些供应商将显示在逗号分隔列表中。
搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

OS Name

以下项之一：

- 在主机上检测到的或使用 Nmap 或主机输入功能更新的操作系统。
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个名称，这些名称将显示在逗号分隔列表中。
搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

OS Version

以下项之一：

- 在主机上检测到的或使用 Nmap 或主机输入功能升级的操作系统的版本
- 如果操作系统不匹配任何已知指纹，则为 `unknown`
- 如果系统尚未采集到足够的信息用于识别操作系统，则为 `pending`

如果系统检测到多个版本，这些版本将显示在逗号分隔列表中。
搜索此字段时，请输入 `n/a` 以包含操作系统尚未识别的主机。

Source Type

用于建立主机操作系统身份的源类型：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（通过网络发现配置添加的 Nmap 或扫描工具）
- 对于系统检测到的操作系统，则为 `Firepower`

系统可能会从多个源协调数据，以确定操作系统的身份。

信心

以下项之一：

- 对于系统检测到的主机，指系统对在主机上运行的操作系统的标识的置信百分比
- 对于通过活跃源识别的操作系统，则为 100%，例如主机输入功能或 Nmap 扫描仪
- 对于系统不能确定操作系统标识的主机和根据 NetFlow 数据已添加到网络映射的主机，则为 `unknown`。

搜索此字段时，请输入 `n/a` 以包含根据 NetFlow 数据添加到网络映射的主机。

说明

注释主机属性的自定义内容。

域

与主机关联的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

设备

检测到流量的受管设备或者处理 NetFlow 或主机输入数据的设备。

如果此字段为空，则以下任一条件成立：

- 按照网络发现策略中的规定，由未明确监控主机所在网络的设备将该主机添加到网络映射中。
- 已使用主机输入功能成功添加该主机，但系统尚未检测到。

计数

与每行中所显示的信息匹配的事件数。仅在应用创建两个或多个相同行的限制后，才会显示此字段。

为所选主机创建流量量变曲线

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

流量量变曲线是以指定的时间跨度内采集的连接数据为基础的网络流量的配置文件。创建流量量变曲线后，可通过对照配置文件评估新流量的方式检测异常网络流量，新流量应代表正常网络流量。

可使用主机页面创建指定主机组的流量量变曲线。流量量变曲线以检测到的连接为基础，其中所指定主机之一是启动连接的主机。使用排序和搜索功能隔离要为其创建配置文件的主机。

过程

步骤 1 在主机工作流程中的表视图上，选中要为其创建白名单的主机旁边的复选框。

步骤 2 在页面底部，点击 **Create Traffic Profile**。

步骤 3 根据特定需要修改并保存流量量变曲线。

根据所选主机创建合规白名单

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

使用合规性白名单可以指定网络允许的操作系统、客户端和网络、传送或应用协议。

可在主机页面上根据指定的主机组的主机配置文件创建合规性白名单。使用排序和搜索功能隔离要用于创建白名单的主机。

过程

步骤 1 在主机工作流程中的表视图上，选中要为其创建白名单的主机旁边的复选框。

步骤 2 在页面底部，点击 **Create White List**。

步骤 3 根据特定需要修改并保存白名单。

主机属性数据

Firepower 系统采集有关其检测到的主机的信息，并使用该信息生成主机配置文件。但是，可能会有要提供给分析师的有关网络上主机的附加信息。可在主机配置文件中添加注释，设置主机的业务关键性或提供您所选择的任何其他信息。每个信息都称为主机属性。

可在主机配置文件限制中使用主机属性，用于生成流量量变曲线时限制所采集的数据，也可限制用于触发关联规则的条件。也对应关联规则设置属性值。

查看主机属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower管理中心查看系统检测到的主机表，与他们的主机属性。然后，可根据要查找的信息操作视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问主机属性时所看到的页面因所使用工作流程的不同而不同。可使用预定义工作流程，此流程包括列出了所有检测到的主机及其属性的主机属性表视图，并在主机视图页面结束，此页面包含符合限制条件的每台主机的主机配置文件。

还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问主机属性数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **主机属性 (Host Attributes)**。
- 如果使用的是不包含主机属性表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**属性 (Attributes)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅主机属性数据字段，第 1663 页。
- 为特定主机分配主机属性；请参阅为所选主机设置主机属性，第 1664 页。

主机属性数据字段

注意主机属性表不显示仅通过 MAC 地址识别的主机。

以下对主机属性表中可以查看和搜索的字段进行了说明。

IP 地址

与主机关联的 IP 地址。

Current User

主机当前登录用户的用户标识（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

主机重要性

用户赋予主机对于您所在企业的重要性。可在关联规则和策略中使用主机重要性用于修改策略违规和对事件中所涉及主机重要性的响应。可封皮低级、中级、高级或零级主机重要性。

说明

有关希望其他分析师查看的主机的信息。

所有自定义主机属性，包括适用于合规性白名单的属性。

自定义主机属性值。主机属性表包括每个自定义主机属性的字段。

域

与主机关联的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

计数

与每行中所显示的信息匹配的事件数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。

为所选主机设置主机属性

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以从主机工作流程配置预定义和用户定义的主机属性。

过程

步骤 1 在主机工作流程中，选中要向其添加主机属性的主机旁边的复选框。

提示 使用排序和搜索功能隔离要为其分配特定属性的主机。

步骤 2 在页面底部，点击 **Set Attributes**。

步骤 3 或者，为所选主机设置主机重要性。可以选择**无 (None)**、**低 (Low)**、**中 (Medium)** 或**高 (High)**。

步骤 4 或者，在文本框中选择的主机的主机配置文件中添加注释。

步骤 5 或者，设置已配置的任何用户定义的主机属性。

步骤 6 点击**保存 (Save)**。

危害表现数据

Firepower 系统将各种类型的数据（入侵事件、安全情报、连接事件及文件或恶意软件事件）进行关联，以确定受监控网络上的主机是否可能受到恶意手段的危害。事件数据的某些组合和频率触发了受影响主机上的危害表现 (IOC) 标记。 这些主机的 IP 地址在事件视图中以红色的受危害主机图标 () 显示。

您可以通过 Firepower 系统 Web 界面的多个部分查看并使用 IOC 数据：

- 事件查看器 - 连接、安全情报、入侵、恶意软件和 IOC 发现事件的视图指示事件是否触发了 IOC。请注意，触发 IOC 规则的基于终端的恶意软件事件的事件类型为 AMP IOC，并同时显示指明危害的事件子类型。事件视图可在“分析”(Analysis) 选项卡下的各个选项卡中找到。
- 控制面板 - 在控制面板中，“摘要控制面板”(Summary Dashboard) 的“威胁”(Threats) 选项卡默认情况下会按主机、和一段时间内触发的新 IOC 规则显示 IOC 标记。Custom Analysis 构件根据 IOC 数据提供预设。
- 情景管理器 - 情景管理器的“危害表现”(Indications of Compromise) 部分按 IOC 类别显示主机图，按主机显示 IOC 类别。
- “网络映射”(Network Map) 页面 -“分析”(Analysis) >“主机”(Hosts) >“网络映射”(Network Map) 下的“危害表现”(Indications of Compromise) 选项卡会按危害类型和 IP 地址对您网络上可能受到危害的主机进行分组。
- “网络文件轨迹详细信息”(Network File Trajectory Detailss) 页面 -“分析”(Analysis) >“文件”(Files) >“网络文件轨迹”(Network File Trajectory) 下列出的文件的详细信息页面允许您跟踪您网络中的危害表现。
- “危害表现”(Host Indications of Compromise) 页面 -“分析”(Analysis) >“主机”(Hosts) 菜单下的“危害表现”(Indications of Compromise) 页面列出按 IOC 标记分组的受监控主机。使用本页面上的工作流程深入了解您的数据。
- “主机配置文件”(Host Profile) 页面 - 可能受到危害的主机的主机配置文件会显示与该主机相关联的所有 IOC 标记，并允许您解决 IOC 标记及配置 IOC 规则状态。

要配置系统以将事件标记为危害表现，请参阅启用危害表现规则，第 1223 页。

查看危害表现数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可以使用Firepower 管理中心查看显示危害表现 (IOC) 的表。可以根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

所看到的页面因所使用的工作流程而异。预定义 IOC 工作流程会在配置文件视图中终止，此视图包含符合限制条件的每台主机的主机配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

开始之前

- 为使系统能够检测和标记危害表现 (IOC)，必须激活网络发现策略中的 IOC 功能并至少启用一个 IOC 规则。请参阅启用危害表现规则，第 1223 页。

过程

步骤 1 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **危害表现 (Indications of Compromise)**。
如果使用的是不包含主机 IOC 表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**危害表现 (Indications of Compromise)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅危害表现数据字段，第 1666 页。
- 通过点击 **IP 地址 (IP Address)** 列中的受危害主机图标 () 来查看受危害主机的主机配置文件。
- 将 IOC 事件标记为“已解决”，这样它们就不会再显示在此列表中。为此，请选中要修改的 IOC 事件旁边的复选框，然后点击**标记为已解决 (Mark Resolved)**。
- 通过点击**首次查看时间 (First Seen)** 或**上次查看时间 (Last Seen)** 列中的查看图标 () 来查看触发 IOC 的事件的详细信息。

危害表现数据字段

以下是 IOC（危害表现）表中的字段。并非每个与 IOC 相关的表都包含所有字段。

IP 地址

与触发 IOC 的主机关联的 IP 地址。

类别

所指示危害类型的简要说明，例如 `Malware Executed` 或 `Impact 1 Attack`。

事件类型

与特定 IOC 关联的标识符，指触发该 IOC 的事件。

说明

对可能受到危害的主机的影响的说明，例如此主机可能受到远程控制 (`This host may be under remote control`) 或已针对此主机执行了恶意软件 (`Malware has been executed on this host`)。

首次查看时间/上次查看时间

触发 IOC 的事件首次/最近出现的日期与时间。

域

触发 IOC 的主机的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

编辑单台主机的危害表现规则状态

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师（只读除外）

如果在网络发现策略中启用，危害表现规则适用于监控网络中的所有主机。您可以禁用单台主机的规则，以避免无用的 IOC 标记（例如，您可能不希望看到 DNS 服务器的 IOC 标记）。如果在适用的网络发现策略中禁用规则，则无法针对特定的主机启用该规则。

过程

步骤 1 导航至主机配置文件的**危害表现 (Indications of Compromise)** 部分。

步骤 2 点击**编辑规则状态 (Edit Rule States)**。

步骤 3 在规则的 **Enabled** 列中，点击滑块启用或禁用规则。

步骤 4 点击**保存 (Save)**。

查看危害表现标记的源事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

您可利用主机配置文件的“危害表现”(Indications of Compromise) 部分快速导航至触发了 IOC 标记的事件。通过分析这些事件，可获得所需信息，以确定是否需要采取措施处理危害威胁以及采取什么措施。

点击 IOC 标记时间戳旁边的查看图标 ( ) 可导航至相关事件类型的事件表视图，仅显示触发 IOC 标记的事件。

过程

步骤 1 在主机配置文件中，导航至**危害表现 (Indications of Compromise)** 部分。

步骤 2 点击要调查的 IOC 标记的**首次发现 (First Seen)** 或**最后发现(Last Seen)** 列中的查看图标 ( )。

解决危害表现标记

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在分析和处理完危害表现 (IOC) 标记指示的威胁后，或者如果确定 IOC 标记代表误报，可将事件标记为已解决。将事件标记为已解决会将其从主机配置文件中删除；如果配置文件上的所有活动 IOC 标记均已解决，则受到危害的主机图标 ( ) 将不再显示。对于已经解决的 IOC，仍然可查看 IOC 触发事件。

如果触发 IOC 标记的事件再次出现，系统会重新设置此标记，除非您已为主机禁用 IOC 规则。

过程

步骤 1 在主机配置文件中，导航至**危害表现 (Indications of Compromise)** 部分。

步骤 2 您有两种选择：

- 要将单个 IOC 标记标记为已解决，请点击要解决的标记右侧的删除图标 ( )。
- 要将配置文件上所有的 IOC 标记标记为已解决，请点击**将所有标记为已解决 (Mark All Resolved)**。

服务器数据

Firepower 系统收集有关在受监控网段中的主机上运行的所有服务器的信息。此信息包括：

- 服务器的名称
- 服务器使用的应用和网络协议
- 服务器的供应商和版本
- 与运行服务器的主机关联的 IP 地址
- 服务器进行通信的端口

系统检测到服务器时，生成发现事件，除非关联的主机已达到其最大服务器数量。可使用Firepower管理中心网络界面查看、搜索和删除服务器事件。

关联规则也可基于服务器事件。例如，可在系统检测到其中一台主机上有聊天服务器运行时触发关联规则，例如 ircd。

系统可以将主机从导出的 NetFlow 记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow 和受管设备数据之间的差异，第 1128 页。

查看服务器数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower 管理中心查看检测到的服务器表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问服务器时所看到的页面因所使用的工作流程的而异。所有预定义的工作流程均在主机视图中终止，该主机视图包含符合限制条件的每台主机的主机配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问数据库数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **服务器 (Servers)**。
- 如果使用的是不包含服务器表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**服务器 (Servers)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅服务器数据字段，第 1669 页。
- 通过选中要编辑的服务器事件旁边的复选框，然后点击**设置服务器身份 (Set Server Identity)** 来编辑服务器身份。

服务器数据字段

可以在下面的服务器表中查看和搜索的字段的说明。

Last Used

上次在网络上使用服务器的日期和时间或原先使用主机输入功能更新服务器的日期和时间。至少按网络发现策略中配置的更新间隔更新 Last Used 值，当系统检测到服务器信息更新时也更新该值。

IP 地址

与运行服务器的主机关联的 IP 地址。

端口

服务器运行所在端口。

协议

服务器使用的网络或传输协议。

应用协议

以下项之一：

- 服务器应用协议的名称。
- 如果系统由于多个原因之一无法肯定或否定地识别服务器，则为 `pending`。
- 如果系统无法根据已知服务器指纹识别服务器或者服务器通过主机输入进行添加但不包含应用协议，则为 `unknown`。

Category、Tags、Risk 或 Business Relevance for Application Protocols

已分配给应用协议的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。

Vendor

以下项之一：

- 系统、Nmap 或其他活跃源识别的服务器供应商或者使用主机输入功能指定的服务器供应商
- 如果系统无法根据已知服务器指纹识别其供应商或者服务器是使用 NetFlow 数据添加至网络映射的，则为 blank。

版本

以下项之一：

- 系统、Nmap 或其他活跃源识别的服务器版本或者使用主机输入功能指定的服务器版本
- 如果系统无法根据已知服务器指纹识别其版本或者服务器是使用 NetFlow 数据添加至网络映射的，则为 blank。

Web 应用

基于系统在 HTTP 流量中检测到的负载内容的 Web 应用。注意，如果系统检测到 `HTTP` 应用协议，但无法检测到特定网络应用，则系统提供通用网络浏览名称。

Category、Tags、Risk 或者 Business Relevance for Web Applications

分配给网络应用的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。

Hits

服务器被访问的次数。对于使用主机输入功能添加的服务器，此值始终为 0。

Source Type

选择以下值之一：

- 用户：user_name
- 应用：app_name
- 扫描工具：scanner_type（通过网络发现配置添加的 Nmap 或扫描工具）
- 对于 Firepower 系统检测到的服务器，为 `Firepower`、`Firepower Port Match` 或 `Firepower Pattern Match`
- 对于使用 NetFlow 数据添加的服务器，为 `NetFlow`

域

运行服务器的主机的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

设备

检测到流量的受管设备或者处理 NetFlow 或主机输入数据的设备。

Current User

主机当前登录用户的用户标识（用户名）。

当非授权用户登录主机中时，该登录会记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

计数

与每行中所显示的信息匹配的事件数。仅在应用创建两个或多个相同行的限制后，才会显示此字段。

应用和应用详细信息数据

当受监控主机连接到另一台主机时，在许多情况下，系统可以确定所使用的应用。Firepower 系统检测许多邮件、即时消息、对等设备、Web 应用以及其他类型应用的使用情况。

对于每个检测到的应用，系统均将记录使用该应用的 IP 地址、产品、版本和检测到的使用次数。可使用网络界面查看、搜索和删除应用事件。也可在主机上使用主机输入功能更新应用数据。

如果知道哪些应用在哪些主机上运行，则可使用此信息创建主机配置文件限制，以便在构建流量量变曲线时限制所采集的数据，也可限制用于触发关联规则的条件。关联规则也可基于应用检测。例如，如果希望员工使用特定邮件客户端，可在系统检测到一台主机上有不同的邮件客户端运行时触发关联规则。

您可以通过仔细阅读每个 Firepower 系统更新的版本说明和每个 VDB 更新的公告来获取有关 Firepower 的应用检测器的最新信息。

要采集和存储应用数据用于分析，请确保在网络发现策略中启用应用检测。

查看应用数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower 管理中心查看检测到的应用表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问应用时所看到的页面因所使用的工作流程而异。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问应用数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **应用详细信息 (Application Details)**。
- 如果使用的是不包含应用详细信息的表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择 **客户端 (Clients)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅应用数据字段，第 1673 页。
- 通过点击客户端、应用协议或 Web 应用旁边的应用详细信息视图图标 ()，打开特定应用的“应用详细信息视图”(Application Detail View)。

应用数据字段

系统检测已知客户端流量、应用协议或网络应用时，会记录有关该应用及运行该应用的主机的信息。可在以下应用表中查看和搜索的字段说明。

应用

检测到的应用的名称。

IP 地址

与使用应用的主机关联的 IP 地址。

Type

应用类型：

应用协议

代表主机之间的通信。

客户端应用

代表主机上运行的软件。

Web Applications

代表 HTTP 流量的内容或所请求的 URL。

类别

说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。

标签

有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。

风险

应用被用于可能违反组织安全策略之目的的可能性。应用风险的取值范围为“极低”(Very Low) 到“极高”(Very High)。

在应用协议风险、客户端风险和网络应用风险中，如适用，则是触发入侵事件的流量中检测到的三个风险中级别最高的风险。

业务相关性

应用被用于组织的企业运营中（而不是被用于娱乐目的）的可能性。应用的业务关联性的取值范围为“极低”(Very Low) 到“极高”(Very High)。

在应用协议业务相关性、客户端业务相关性和网络应用业务相关性中，如适用，则是触发入侵事件的流量中检测到的三个业务关联性中关联性最低的一个。

Current User

主机当前登录用户的用户标识（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

域

使用应用的主机的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

计数

与每行中所显示的信息匹配的事件数。注意，Count字段仅在应用了创建两个或多个相同行的约束后才显示。

查看应用详细信息数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower 管理中心查看检测到的应用详情表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问应用详情时看到的页面因使用的工作流程而异。有两个预定义工作流程。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问应用详细信息数据

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **主机 (Hosts)** > **应用详细信息 (Application Details)**。
- 如在使用的自定义工作流程不包括应用详情表视图，请点击 **(switch workflow)**，然后选择 **Clients**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅应用详细信息数据字段，第 1675 页。

- 通过点击客户端旁边的应用详细信息视图图标 ()，打开特定应用的“应用详细信息视图”(Application Detail View)。

应用详细信息数据字段

系统检测已知客户端流量、应用协议或网络应用时，会记录有关该应用及运行该应用的主机的信息。

可在以下应用详细信息表中查看和搜索的字段的说明。

Last Used

最后一次检测到该应用的时间或使用主机输入功能更新该应用的数据的时间。至少按网络发现策略中配置的更新间隔更新 Last Used 值，当系统检测到应用信息更新时也更新该值。

IP 地址

与使用应用的主机关联的 IP 地址。

Client

应用的名称。注意：如果系统检测到应用协议但无法检测到特定客户端，则 `client` 会附加至应用协议名称以提供通用名。

版本

应用的版本。

客户端、应用协议以及 Web 应用的类别、标记、风险或业务关联性

分配给应用的分类、标记、风险级别和业务相关性。这些过滤器可用于集中过滤特定数据集。

应用协议

应用所使用的应用协议。注意：如果系统检测到应用协议但无法检测到特定客户端，则 `client` 会附加至应用协议名称以提供通用名。

Web 应用

基于系统在 HTTP 流量中检测到的负载内容或 URL 的 Web 应用。请注意，如果系统检测到 HTTP 应用协议，但无法检测到特定网络应用，系统会在此处提供通用的 网络浏览应用。

Hits

系统检测到在使用的应用的次数。对于使用主机输入功能添加的应用，此值始终为 `0`。

域

使用应用的主机的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

设备

生成发现事件的设备，包括应用详情。

Current User

主机当前登录用户的用户标识（用户名）。

注意：当未授权用户登录主机时，该登录操作将记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。此外，未授权用户是主机当前用户时，该用户仍不能进行用户管理。

计数

与每行中所显示的信息匹配的事件数。注意，Count字段仅在应用了创建两个或多个相同行的约束后才显示。

漏洞数据

Firepower系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，用于识别与网络中主机关联的漏洞。主机上运行的操作系统、服务器和客户端有不同组关联漏洞。

您可以使用 Firepower 管理中心执行以下操作：

- 跟踪和审查每个主机的漏洞。
- 在修复主机或者以其他方式将其判断为对漏洞免疫后，停用该主机的漏洞。

除非在Firepower管理中心配置中映射服务器所使用的应用协议，否则不会映射无供应商和无版本服务器的漏洞。无法映射无供应商和无版本客户端的漏洞。

漏洞数据字段

可以在漏洞的表视图和在漏洞详细信息显示中查看下述漏洞数据字段，如下所示：

表 *287*：按显示位置划分的漏洞数据字段

字段	表格视图	详细信息显示
更多信息	否	yes
Available Exploits	是	是
Bugtraq ID	是	是
CVE ID	否	yes
计数	是	否
Date Published	是	是

字段	表格视图	详细信息显示
说明	是	是
Fixes	否	yes
Impact Qualification	否	yes
远程	是	是
Snort ID	是	是
解决方案	是	是
SVID	是	是
Technical Description	是	是
职位	是	是
Vulnerability Impact	是	是

更多信息

点击箭头查看其他有关漏洞的信息（如果可用），例如已知使用和其可用性、使用情景和缓解策略。

Available Exploits

指示是否有对漏洞的已知利用 (`TRUE`/`FALSE`)。

Bugtraq ID

与 Bugtraq 数据库中漏洞关联的标别号。(http://www.securityfocus.com/bid/)

计数

与每行中所显示的信息匹配的事件数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。

CVE ID

与 MITRE 的通用漏洞与披露 (CVE) 数据库 (http://www.cve.mitre.org/) 中的漏洞相关联的识别号。

Date Published

发布漏洞的日期。

说明

漏洞的简要说明。

Fixes

提供所选漏洞可用的可下载的补丁的链接。

提示 如果出现修复程序或补丁下载的直接链路，右击该链接并保存至本地计算机。

Impact Qualification

使用下拉列表启用或禁用漏洞。Firepower 管理中心忽略其影响相关性中的禁用漏洞。

此处指定的设置确定如何在整个系统范围内处理漏洞，而且该设置不限于选择该值的主机配置文件。

远程

指示漏洞是否可以远程利用 (TRUE/FALSE)。

Snort ID

与 Snort ID (SID) 数据库中的漏洞相关联的识别号。也就是说，如果入侵规则能检测到利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

注意，一个漏洞可能与多个 SID（或根本不与 SID）关联。如果一个漏洞与多个 SID 关联，则每个 SID 在漏洞表中各占一行。

解决方案

有关修补漏洞的信息。

SVID

系统用于跟踪漏洞的思科漏洞标识号。

点击视图图标 ( ) 访问 SVID 的漏洞详情。

Technical Description

漏洞的详细技术说明。

职位

漏洞的标题。

Vulnerability Impact

显示分配给 Bugtraq 数据库中漏洞的严重性，等级从 0 级至 10 级，10 级最严重。漏洞影响是由 Bugtraq 条目编者根据其最佳判断并按照 SANS 重要漏洞分析 (CVA) 标准确定的。

漏洞停用

停用漏洞可防止系统使用该漏洞评估入侵影响关联。您可以在修复网络上的主机或者以其他方式将其判断为免疫后停用漏洞。注意，如果系统发现一台新主机受该漏洞影响，可视为该漏洞对此主机有效（不会自动停用）。

停用**不**受IP地址限制的漏洞工作流程中的漏洞会停用网络上所有受检测主机的漏洞。您只能在以下位置停用漏洞工作流程中的漏洞：

- 默认漏洞工作流程的第二页，**网络上的漏洞 (Vulnerabilities on the Network)**，该页面仅显示适用于网络上的主机的漏洞
- 使用搜索根据 IP 地址限制的自定义或预定义漏洞工作流程中的页面。

您可以使用网络映射，使用主机的主机配置文件，或通过根据要停用漏洞的一个或多个主机的IP地址限制漏洞工作流程来停用单个主机的漏洞。对有多个关联IP地址的主机，此功能仅适用于该主机的单一选定 IP 地址。

在多域部署中，停用祖先域中的某个漏洞将会使其在所有后代域中都停用。如果在祖先域中激活漏洞，则枝叶域可以为其设备激活或停用该漏洞。

查看漏洞数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可使用Firepower 管理中心查看漏洞表。然后，可根据要查找的信息操纵事件视图。

访问漏洞时所看到的页面因所使用的工作流程而异。可使用包含漏洞表视图的预定义工作流程。数据库中的每个漏洞在表视图中都各占一行，无论任何检测到的主机是否显示这些漏洞。适用于网络中所检测到主机的每个漏洞（未停用）在预定义工作流程的第二页都各占一行。预定义工作流程在漏洞详情视图中终止，该视图包含符合限制条件的每个漏洞的详细说明。

提示 如要查看适用于单台主机或一组主机的漏洞，应通过指定主机 IP 地址或 IP 地址范围的方式执行漏洞搜索。

还可创建自定义工作流程，仅显示匹配特定需求的信息。

漏洞表不受多域部署中的域限制。

过程

步骤 1 访问漏洞表：

- 如果使用的是预定义漏洞工作流程，请选择**分析 (Analysis)** > **漏洞 (Vulnerabilities)** > **漏洞 (Vulnerabilities)**。
- 如果使用的是不包含漏洞表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**漏洞 (Vulnerabilities)**。

步骤 2 您有以下选择：

- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 停用漏洞，以使这些漏洞不再用于当前易受攻击主机的入侵影响关联；请参阅停用多个漏洞，第 1680 页。
- 通过点击 SVID 列中的查看图标 () 来查看漏洞的详细信息。或者，限制漏洞 ID 并向下钻取至漏洞详情页面。
- 通过右键点击标题并选择**显示全文 (Show Full Text)** 来查看漏洞标题的全文。

查看漏洞详细信息

过程

可以通过下列任意方法查看漏洞详细信息：

- 选择**分析 (Analysis)** > **漏洞 (Vulnerabilities)** > **漏洞 (Vulnerabilities)**，然后点击 SVID 旁边的查看图标 ()。
- 选择**分析 (Analysis)** > **漏洞 (Vulnerabilities)** > **第三方漏洞 (Third-Party Vulnerabilities)**，然后点击 SVID 旁边的查看图标 ()。
- 选择**分析 (Analysis)** > **主机 (Hosts)** > **网络映射 (Network Map)**，然后点击**漏洞 (Vulnerabilities)** 选项卡。
- 查看受漏洞影响的主机配置文件，并展开配置文件的**漏洞 (Vulnerabilities)** 部分。

停用多个漏洞

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

停用不受 IP 地址限制的漏洞工作流程中的漏洞会停用网络上所有受检测主机的漏洞。

在多域部署中，停用祖先域中的某个漏洞将会使其在所有后代域中都停用。只要在祖先域中激活了漏洞，枝叶域即可激活或停用其设备的该漏洞。

过程

步骤 1 访问漏洞表：

- 如果使用的是预定义漏洞工作流程，请选择**分析 (Analysis)** > **漏洞 (Vulnerabilities)** > **漏洞 (Vulnerabilities)**。
- 如果使用的是不包含漏洞表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**漏洞 (Vulnerabilities)**。

步骤 2 点击**网络上的漏洞 (Vulnerabilities on the Network)**。

步骤 3 选中要停用的漏洞旁边的复选框。

步骤 4 点击页面底部的**审核 (Review)**。

第三方漏洞数据

Firepower 系统有自己的漏洞跟踪数据库，该数据库与系统的指纹识别功能相结合，用于识别与网络中主机关联的漏洞。

可以使用从第三方应用导入的网络映射数据来扩充系统的漏洞数据。为此，组织必须能够编写脚本或创建命令行导入文件来导入该数据。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

要将已导入数据纳入影响关联，必须将第三方漏洞信息映射至数据库中的操作系统和应用定义。不能将第三方漏洞信息映射至客户端定义。

查看第三方漏洞数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

使用主机输入功能导入第三方漏洞数据后，可使用Firepower管理中心查看第三方漏洞表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问第三方漏洞时所看到的页面因所使用的工作流程而异。有两个预定义工作流程。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问第三方漏洞数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **漏洞 (Vulnerabilities)** > **第三方漏洞 (Third-Party Vulnerabilities)**。
- 如果使用的是不包含第三方漏洞的表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**按源划分的漏洞 (Vulnerabilities by Source)** 或**按 IP 地址划分的漏洞 (Vulnerabilities by IP Address)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅第三方漏洞数据字段，第 1682 页。
- 通过点击 SVID 列中的查看图标 () 来查看第三方漏洞的漏洞详细信息。或者，限制漏洞 ID 并向下钻取至漏洞详情页面。

第三方漏洞数据字段

可以在第三方漏洞表中查看和搜索的字段说明如下。

Vulnerability Source

第三方漏洞的来源，例如， QualysGuard 或 NeXpose。

Vulnerability ID

与其源漏洞关联的 ID 编码。

IP 地址

与受漏洞影响主机关联的 IP 地址。

端口

如果漏洞与特定端口上运行的服务器关联，则为端口号。

Bugtraq ID

与 Bugtraq 数据库中漏洞关联的标别号。(http://www.securityfocus.com/bid/)

CVE ID

与 MITRE 的通用漏洞与披露 (CVE) 数据库 (http://www.cve.mitre.org/) 中的漏洞相关联的识别号。

SVID

系统用于跟踪漏洞的旧版漏洞标识号

点击视图图标 () 访问 SVID 的漏洞详情。

Snort ID

与 Snort ID (SID) 数据库中的漏洞相关联的识别号。也就是说，如果入侵规则能检测到利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。

注意，一个漏洞可能与多个 SID（或根本不与 SID）关联。如果一个漏洞与多个 SID 关联，则每个 SID 在漏洞表中各占一行。

职位

漏洞的标题。

说明

漏洞的简要说明。

域

具有漏洞的主机的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

计数

与每行中所显示的信息匹配的事件数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。

用户数据

当身份源报告尚未包含在数据库中的用户的用户登录时，除非专门限制该登录类型，否则会将该用户添加到数据库中。用户数据始终保留在用户数据库中，直至出现以下其中一种情形：

- 某个 Firepower 管理中心用户从“用户”(Users) 表中手动删除用户。
- 某个身份源报告该用户已注销。
- 某个领域根据其**用户会话超时：通过身份验证的用户 (User Session Timeout: Authenticated Users)**、**用户会话超时：身份验证失败的用户 (User Session Timeout: Failed Authentication Users)** 或**用户会话超时：访客用户 (User Session Timeout: Guest Users)** 设置结束用户会话。

注释 如果已配置 ISE，则您可能会在用户表中看到主机数据。由于不完全支持由 ISE 检测主机，因此无法使用 ISE 报告的主机数据执行访问控制。

系统检测到的用户登录类型确定存储的有关新用户的信息内容。

Identity Source	登录类型	存储的用户数据
ISE	Active Directory LDAP RADIUS RSA	• username • 当前 IP 地址 • 安全组标记 (SGT) • 终端配置文件 • 终端位置 • 类型 (LDAP)
用户代理	Active Directory	• username • 当前 IP 地址 • 类型 (LDAP)
强制网络门户	Active Directory LDAP	• username • 当前 IP 地址 • 类型 (LDAP)
基于流量的检测	LDAP AIM Oracle SIP HTTP FTP MDNS	• username • 当前 IP 地址 • 类型 (AD)
	POP3 IMAP	• username • 当前 IP 地址 • 邮件地址 • 类型（`pop3` 或 `imap`）

如果将领域配置为自动下载用户，则Firepower管理中心会根据指定的间隔查询服务器。系统检测到新用户登录后，Firepower 管理中心数据库可能需要五到十分钟的时间来使用用户元数据更新。Firepower 管理中心获取关于每个用户的以下信息和元数据：

- username
- 名和姓
- 邮件地址
- department
- 电话号码
- 当前 IP 地址
- 安全组标记 (SGT)（如果可用）
- 终端配置文件（如果可用）
- 终端位置（如果可用）

Firepower 管理中心可在其数据库中存储的用户数取决于 Firepower 管理中心型号。当检测到未授权用户登录主机时，会在用户和主机历史记录中记录该登录。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，检测至一个授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。

请注意，对 AIM、Oracle 和 SIP 登录进行基于流量的检测会创建重复用户记录，因为它们不与系统从 LDAP 服务器获取的任何用户元数据关联。要防止由于这些协议中的用户记录重复而过度使用用户计数，请配置基于流量的检测以忽略这些协议。

可从数据库中搜索、查看和删除用户；也可从数据库中清除所有用户。

查看用户数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

可查看用户表，然后根据所查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问用户时所看到的页面因所使用的工作流程而异。可使用预定义工作流程并在用户详情页面终止，此工作流程包括列出了所有已检测到用户的用户表视图。用户详情页面提供有关符合限制条件的所有用户的信息。

过程

步骤 1 访问用户数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **用户 (Users)** > **用户 (Users)**。
- 如果使用的是不包含用户表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**用户 (Users)**。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅用户数据字段，第 1686 页。

用户数据字段

如果系统发现用户，会收集有关该用户的数据并将其存储在数据库中，直至出现以下其中一种情形：

- 某个 Firepower 管理中心用户从“用户”(Users) 表中手动删除用户。
- 某个身份源报告该用户已注销。
- 某个领域根据其**用户会话超时：通过身份验证的用户 (User Session Timeout: Authenticated Users)**、**用户会话超时：身份验证失败的用户 (User Session Timeout: Failed Authentication Users)** 或**用户会话超时：访客用户 (User Session Timeout: Guest Users)** 设置结束用户会话。

以下字段可在用户视图表中查看和搜索。

User

至少，此字段会显示用户的领域和用户名。例如，`Lobby\jsmith`，其中 Lobby 为领域，jsmith 为用户名。

如果领域从 LDAP 服务器下载其他用户数据，且系统将其与一名用户相关联，则此字段也会显示用户的姓氏、名字和类型。例如，`John Smith (Lobby\jsmith, LDAP)`，其中 John Smith 为用户的姓名，LDAP 为类型。

注释 由于基于流量的检测可记录失败的 AIM 登录尝试，因此 Firepower 管理中心可存储无效 AIM 用户（例如，用户名拼写错误的用户）。

领域 (Realm)

与用户关联的身份领域。

用户名

与用户关联的用户名。

Current IP

与用户登录的主机关联的 IP 地址。如果该用户登录后另一授权用户登录具有相同 IP 地址的主机，则此字段为空，除非该用户为授权用户且新用户为未授权用户。（系统将 IP 地址与登录该主机的最后一名授权用户关联。）

名字

由领域获取的用户名字。如果符合以下条件，则此字段为空：

- 您尚未配置领域。
- Firepower 管理中心无法将管理中心数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）
- 没有与 LDAP 服务器上的用户关联的名字。

姓氏

由领域获取的用户姓氏。如果符合以下条件，则此字段为空：

- 您尚未配置领域。
- Firepower 管理中心无法将管理中心数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）
- 没有与 LDAP 服务器上的用户关联的姓氏。

邮件

用户的邮件地址。如果符合以下条件，则此字段为空：

- 用户已通过 AIM 登录添加到数据库。
- 用户已通过 LDAP 登录添加到数据库且没有与 LDAP 服务器用户关联的邮箱地址。

部门

由领域获取的用户所在部门。如果没有明确地与您的服务器上用户关联的部门，则该部门列为服务器分配的任何默认组。例如，在 Active Directory 中，这是 `Users (ad)`。如果符合以下条件，则此字段为空：

- 您尚未配置领域。
- Firepower 管理中心无法将管理中心数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）

电话

由领域获取的用户电话号码。如果符合以下条件，则此字段为空：

- 您尚未配置领域。
- Firepower 管理中心无法将管理中心数据库中的用户与 LDAP 记录关联（例如，对于通过 AIM、Oracle 或 SIP 登录添加到数据库的用户）
- 没有与您的服务器上用户关联的电话号码。

Type

用于检测用户的协议。以下类型之一：ldap、pop3、imap、oracle、sip、http、ftp、mdns 和 aim。用户未基于 SMTP 登录而添加到数据库，因此 smtp 未显示在此字段中。

域

与用户的领域关联的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

计数

与每行中所显示的信息匹配的用户数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。

用户详细信息和主机历史记录

您可以通过查看“用户”(User) 弹出窗口了解有关特定用户的详细信息。出现的页面在本文档中称为“用户简档”，在 Web 界面中的标题为“用户身份”。

可以通过以下方式显示该窗口：

- 将用户数据与其他类型的事件相关联的任何事件视图
- 用户的表视图

用户信息也可在用户工作流程终止页面上显示。

所看到的用户数据与将在用户的表视图中看到的数据相同。

“危害表现”部分

有关此部分的信息，请参阅：

- 危害表现，第 1222 页
- 危害表现数据字段，第 1666 页
- 编辑单台主机的危害表现规则状态，第 1667 页
- 解决危害表现标记，第 1668 页
- 查看危害表现标记的源事件，第 1667 页

“主机历史记录”部分

主机历史记录以图表再现了最后二十四个小时的用户活动。用户所登录和所注销主机的IP地址的列表以条形图大约显示登录和注销次数。典型用户在一天中可能登录和注销多台主机。例如，如果定期自动登录邮件服务器，则将显示多个短期会话，而如果长时间登录（例如在工作时间），则将显示长时间会话。

如果使用基于流量的检测或强制网络门户捕获失败的登录，则主机历史记录还包含用户无法登录的主机。

用于生成主机历史记录的数据存储在用户历史记录数据库中，默认情况下可存储10百万次用户登录事件。如果在主机历史记录中未看到特殊用户的任何数据，则该用户为非活动用户，或者可能需要增加数据库限制。

查看用户详细信息和主机历史记录

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

过程

此时您有两种选择：

- 在列出用户的任何事件视图中，点击用户身份旁边显示的用户图标（  ）。
- 在任何用户工作流程中，点击 Users terminating 页面。

用户活动事件类型

Firepower系统生成在网络上传达用户活动详细信息的事件。当系统检测到用户活动时，会将用户活动数据记录到数据库中。可查看、搜索和删除用户活动；也可从数据库中清除所有用户活动。

当某用户首次出现在您的网络上时，系统会记录该用户的活动事件。当该用户再次出现时，不会记录新的用户活动事件。但是，如果该用户的 IP 地址发生更改，则系统会记录新的用户活动事件。

Firepower系统也会将用户活动与其他类型的事件相关联。例如，入侵事件可以指出在事件发生时登录源主机和目标主机的用户。这种关联可让您了解哪个用户已登录作为攻击目标的主机，或者了解内部攻击或端口扫描的发起者。

也可在关联规则中使用用户活动。根据用户活动的类型和指定的其他条件，用于关联策略时可构建关联规则，网络流量符合条件时可启动补救和警报响应。

注释 如果已配置 ISE，则您可能会在用户活动表中看到主机数据。由于不完全支持由 ISE 检测主机，因此无法使用 ISE 报告的主机数据执行访问控制。

以下对四种类型的用户活动数据进行了说明。

New User Identity

当系统检测到数据库中不存在的未知用户登录时，将生成此类事件。

当某用户首次出现在您的网络上时，系统会记录该用户的活动事件。当该用户再次出现时，不会记录新的用户活动事件。但是，如果该用户的 IP 地址发生更改，则系统会记录新的用户活动事件。

用户登录

出现以下任一情况时，将生成此类型事件：

- 用户代理或 ISE 报告成功的用户登录。
- 强制网络门户执行成功或失败的用户身份验证。
- 基于流量的检测检测到成功或失败的用户登录。

注释 系统将不记录由基于流量的检测发现的 SMTP 登录，除非数据库中已有匹配邮件地址的用户。

当非授权用户登录主机中时，该登录会记录在用户和主机历史记录中。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。

如果使用的是强制网络门户或基于流量的检测，请注意以下有关失败用户登录和失败用户身份验证数据的内容：

- 基于流量的检测（LDAP、IMAP、FTP 和 POP3 流量）报告的失败登录显示在用户活动表视图中，但不显示在用户表视图中。如果已知用户登录失败，则系统将通过其用户名来识别用户。如果未知用户登录失败，则系统将使用 **Failed Authentication** 作为其用户名。
- 强制网络门户报告的失败身份验证既显示在用户事件表视图中，又显示在用户表视图中。如果已知用户身份验证失败，则系统将通过其用户名来识别用户。如果未知用户身份验证失败，则系统将通过其输入的用户名来识别用户。

Delete User Identity

手动删除数据库中用户时，将生成此类型事件。

User Identity Dropped: User Limit Reached

当系统检测到数据库中不存在的用户但是无法添加该用户（因为数据库中用户数已经达到Firepower管理中心型号规定的最大数量）时，将生成此类型事件。

在达到用户限制后，系统在多数情况下会停止向数据库添加新用户。要添加新用户，必须手动从数据库中删除旧的或非活动用户，或者清除数据库中的所有用户。

但是，系统支持授权用户。如果已达到极限且系统检测到先前未检测到的授权用户登录，则系统会删除保持非活动状态时间最长的未授权用户，并用新授权用户替换该用户。

查看用户活动数据

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

可查看用户活动表，然后根据所需查找的信息操纵事件视图。访问用户活动时看到的页面因所使用的工作流程而异。可使用预定义工作流程（该工作流程包括用户活动表视图）并在用户详细信息页面（该页面包括符合限制条件的每个用户的详细信息）中终止。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 访问用户活动数据：

- 如果使用的是预定义工作流程，请选择**分析 (Analysis)** > **用户 (Users)** > **用户活动 (User Activity)**。
- 如果使用的是不包含用户活动的表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**用户活动 (User Activity)**。

提示 如未显示事件，可能需要调整时间范围；请参阅更改时间窗口，第 1461 页。

步骤 2 您有以下选择：

- 通过点击（**切换工作流程**）**([switch workflow])** 来使用不同的工作流程，包括自定义工作流程。
- 执行基本工作流程操作；请参阅使用发现和身份工作流程，第 1648 页。
- 了解有关表中各列内容的详细信息；请参阅用户活动数据字段，第 1691 页。

用户活动数据字段

可在以下用户活动表中查看和搜索的字段的说明。

Time

系统检测到用户活动的时间。

Event

用户活动事件类型。

领域 (Realm)

与用户关联的身份领域。

用户名

与用户关联的用户名。

Type

用于检测用户的协议。例如，当系统检测到**类型 (Type)** 为 `pop3` 的 POP3 登录时，用户将被添加到数据库中。

IP 地址

对于用户登录活动、登录中所涉的 IP 地址，可能是用户主机（对于 LDAP、POP3、IMAP、FTP、HTTP、MDNS 和 AIM 登录）、服务器（对于 SMTP 和 Oracle 登录）或会话发起者（对于 SIP 登录）的 IP 地址。

注意，关联的 IP 地址并不意味着用户是该 IP 地址的当前用户；未授权用户登录一台主机时，用户历史记录和主机历史记录中会记录此次登录。如果没有授权用户与该主机相关联，则未授权用户可能是该主机的当前用户。但是，授权用户登录该主机后，只有另一授权用户登录才能改变当前用户。

对于其他类型的用户活动，此字段留空。

说明

对于“删除用户身份”(Delete User Identity) 和“用户身份已丢弃”(User Identity Dropped activity) 活动，是指从数据库中删除的或未能添加到数据库的用户的领域和用户名。对于网络资源的登录，显示 `network login`。对于其他类型的用户活动，此字段留空。

安全组标签

当数据包进入受信任的 TrustSec 网络时思科 TrustSec 应用的安全组标记 (SGT) 属性。如果未配置 ISE，此字段留空。

Endpoint Profile

用户终端设备类型，如思科 ISE 所识别。如果未配置 ISE，此字段留空。

终端位置 (Endpoint Location)

使用 ISE 对用户进行身份验证的网络设备的 IP 地址，如 ISE 所识别。如果未配置 ISE，此字段留空。

域

检测到用户活动的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

设备

对于通过基于流量的检测操作检测到的用户活动，是指检测到用户的设备的名称。对于其他用户活动类型，是管理Firepower 管理中心。

计数

与每行中所显示的信息匹配的事件数。注意，Count字段仅在应用了创建两个或多个相同行的约束后才显示。

第 89 章

关联事件和合规性事件

以下主题介绍如何查看关联事件和合规性事件。

查看关联事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师

当活动的关联策略中的关联规则触发时，系统生成关联事件并将其记录至数据库。

注释 当活动的关联策略中的合规白名单触发时，系统生成白名单事件。

您可以查看关联事件表，然后根据查找的信息操作事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问关联事件时看到的页面随使用的工作流程而变化。可以使用预定义的工作流程，其中包括关联事件表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 选择**分析 (Analysis)** > **关联 (Correlation)** > **关联事件 (Correlation Events)**。

或者，要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**。

提示　如果使用的是不包含关联事件表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**关联事件 (Correlation Events)**。

步骤 2　或者，调整时间范围，如更改时间窗口，第 1461 页中所述。

步骤 3　执行下列操作之一：

- 要了解有关显示的列的详细信息，请参阅关联事件字段，第 1696 页。
- 要查看 IP 地址的主机配置文件，请点击显示在 IP 地址旁边的主机配置文件图标。
- 要查看用户身份信息，请点击显示在用户身份旁边的用户图标（  ）。
- 要对事件进行排序和限制，或者要在当前工作流程页面中导航，请参阅使用工作流程，第 1442 页。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- 要向下展开到工作流程中的下一个页面，限制具体值，请参阅使用向下钻取页面，第 1450 页。
- 要删除部分或全部关联事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**，并确认要删除当前限制视图中的所有事件。
- 要导航至其他事件视图以查看关联事件，请参阅工作流程间导航，第 1466 页。

关联事件字段

当关联规则触发时，系统会生成关联事件。下表介绍关联事件表中可以查看和搜索的字段。

表 *288*：关联事件字段

字段	说明
说明	关联事件的说明。说明中的信息取决于规则触发方式。 例如，如果操作系统的信息更新事件触发规则，则系统显示新的操作系统名称和可信度。
设备	生成触发策略违规的事件的设备的名称。
域	其受监控流量触发了策略违规的设备的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

字段	说明
影响	基于入侵数据、发现数据和漏洞信息之间的关联分配给关联事件的影响级别。 搜索此字段时，有效值（不区分大小写）包括 `Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4` 和 `Impact Level 4`。请勿使用影响图标颜色或部分字符串（例如，请勿使用 `blue`、`level 1` 或 `0`）。
“入口接口”(Ingress Interface) 或“出口接口”(Egress Interface)	触发策略违规的入侵或连接事件的入口或出口界面。
“入口安全区域”(Ingress Security Zone) 或“出口安全区域”(Egress Security Zone)	触发策略违规的入侵或连接事件的入口或出口安全区域。
Inline Result	以下任一项： • 一个黑色向下箭头，表示系统丢弃触发入侵规则的数据包 • 一个灰色向下箭头，表示如果启用 **Drop when Inline** 入侵策略选项，则系统已经丢弃内联中的数据包、交换或路由部署 • 空白，表示触发的入侵规则未设置为 Drop and Generate Events 使用此字段搜索入侵事件触发的策略违规时，请输入： • `dropped`，用来指定是否已经在内联、交换的或路由的部署中丢弃数据包 • `would have dropped`，用来指定如果已经设置入侵策略以在内联、交换的或路由的部署中丢弃数据包，则是否将丢弃该数据包 请注意，不管规则状态或入侵策略的丢弃行为如何（包括当内联集处于分路模式下），系统都无法在被动部署情况下丢失数据包。
策略	违反的策略的名称。
优先级	关联事件的优先级，由触发的规则或违规的关联策略的优先级确定。搜索此字段时，请输入 `none` 表示无优先级。
规则	触发策略违规的规则的名称。
Security Intelligence Category	代表或包含触发策略违规的事件中的列入黑名单的 IP 地址的被列入黑名单的对象的名称。 搜索此字段时，请指定与触发策略违规的关联事件相关联的安全情报类别。安全情报类别可能是安全情报对象的名称、全局黑名单、自定义安全情报列表或源，或者情报源中的其中一个类别。

字段	说明
“源大洲”(Source Continent) 或“目标大洲”(Destination Continent)	与触发策略违规的事件中的源或目标主机 IP 地址相关联的大洲。
Source Country 或 Destination Country	与触发策略违规的事件中的 源 IP 地址或目标 IP 地址相关的国家/地区。
Source Host Criticality 或 Destination Host Criticality	涉及关联事件的源主机或目标主机的用户分配的主机重要性：`None`、`Low`、`Medium` 或 `High`。 请注意，只有基于发现事件、主机输入事件或连接事件按规则生成的关联事件才包含源主机重要性。
“源 IP”(Source IP) 或“目标 IP”(Destination IP)	触发策略违规的事件中的源主机或目标主机的 IP 地址。
Source Port/ICMP Type 或 Destination Port/ICMP Code	与触发策略违规的事件有关的源流量的源端口或 ICMP 类型或者目标流量的目标端口或 ICMP 代码。
“源用户”(Source User) 或“目标用户”(Destination User)	登录触发策略违规的事件中的源主机或目标主机的用户的姓名。
Time	生成关联事件的日期和时间。此字段不可搜索。
计数	与每行中所显示的信息匹配的事件数。注意，**Count** 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索

使用合规白名单工作流程

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/发现管理员

Firepower管理中心提供了一组工作流程，可用于分析为您的网络生成的白名单事件和违规。工作流程与网络映射和控制面板一起构成关于网络资产合规性的关键信息的来源。

系统为白名单事件和违规提供预定义工作流程。也可创建自定义工作流程。在使用合规性白名单工作流程时，可以执行许多常见操作。

过程

步骤 1 使用**分析 (Analysis)** > **关联 (Correlation)** 菜单访问白名单工作流程。

步骤 2 您有以下选择：

- “切换工作流程”(Switch Workflow) - 要使用不同的工作流程（包括自定义工作流程），请点击（**切换工作流程**）**([switch workflow])**。
- “时间范围”(Time Range) - 要调整时间范围（如果未显示事件，则非常有用），请参阅更改时间窗口，第 1461 页。
- “主机配置文件”(Host Profile) - 要查看 IP 地址的主机配置文件，请点击主机配置文件图标 ()，或者对于带有效危害表现 (IOC) 标记的主机，请点击显示在 IP 地址旁边的危害主机图标 ()。
- “用户配置文件”(User Profile)（仅事件）- 要查看用户身份信息，请点击显示在用户身份旁边的用户图标（  ）。
- “限制”(Constrain) - 要限制显示的列，请在要隐藏的列标题中点击关闭图标 ()。在显示的弹出窗口中，点击 **Apply**。

  提示 要隐藏或显示其他列，请选择或清除相应的复选框，然后点击 **Apply**。要将已禁用列添加回视图中，请展开搜索限制条件，然后点击“已禁用列”(Disabled Columns) 下的列名称。

- 向下展开 - 请参阅使用向下钻取页面，第 1450 页。
- “排序”(Sort) - 要对工作流程中的数据排序，请点击列标题。再次点击列标题以反转排列顺序。
- “导航此页面”(Navigate This Page) - 请参阅工作流程页面遍历工具，第 1447 页。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “删除事件”(Delete Events)（仅事件）- 要删除当前限制视图中的部分或全部项目，请选中要删除的项目旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。

查看白名单事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/发现管理员

完成初始评估后，每当受监控的主机违反有效的白名单，系统会生成白名单事件。白名单事件是特殊类型的关联事件，会被记录到管理中心关联事件数据库中。

您可以使用Firepower管理中心查看合规白名单事件表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问白名单事件时系统显示的页面取决于您使用的工作流程。可以使用预定义的工作流程，最终会产生事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

过程

步骤 1 选择**分析 (Analysis)** > **关联 (Correlation)** > **白名单事件 (White List Events)**。

步骤 2 您有以下选择：

- 要执行基本工作流程操作，请参阅使用合规白名单工作流程，第 1698 页。
- 要了解有关表中各列内容的详细信息，请参阅白名单事件字段，第 1700 页。

白名单事件字段

白名单事件（您可以通过工作流程查看和搜索白名单事件）包含以下字段。

设备

检测到白名单违规行为的受管设备的名称。

说明

说明白名单是如何被违反的。例如：

```
Client “AOL Instant Messenger” is not allowed.
```

涉及应用协议的违规指明应用协议的名称和版本，以及所使用的端口和协议（TCP 或 UDP）。如果限制禁止某个特定的操作系统，描述中会包含操作系统的名称。例如：

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating System
“Linux Linux 2.4 or 2.6”.
```

域

已变为不符合白名单的主机的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

主机重要性

用户向不符合白名单的源主机所分配的主机重要性：“无”(None)、“低”(Low)、“中”(Medium)或“高”(High)。

IP 地址

已变为不符合白名单的主机的 IP 地址。

策略

被违反的关联策略的名称，即包含该白名单的关联策略。

端口

与触发应用协议白名单违规（违规应用协议造成的违规）的发现事件关联的端口（如有）。对于其他类型的白名单违规活动，该字段为空白。

优先级

策略或触发策略违规的白名单所指定的优先级。根据关联策略中白名单的优先级或关联策略自身的优先级来确定。请注意，白名单的优先级优先于策略的优先级。搜索此字段时，请输入 `none` 表示无优先级。

Time

白名单事件生成时的日期和时间。此字段不可搜索。

User

登录已变为不符合白名单的主机的任何已知用户的身份。

White List

白名单的名称。

计数

与每行中所显示的信息匹配的事件数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

查看白名单违规事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理员/任何安全分析师/发现管理员

系统会记录您的网络上的当前白名单违规事件。每个违规事件代表一个禁止在您的其中一台主机上运行的事件。如果主机变为合规，则系统将从数据库移除现已纠正的违规。

您可以使用Firepower管理中心查看所有活动白名单的白名单违规事件表。然后，可根据要查找的信息操纵事件视图。

访问白名单违规事件时显示的页面取决于您使用的工作流程。预定义工作流程会产生主机视图，该视图包含符合限制条件的每台主机的配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **关联 (Correlation)** > **白名单违规事件 (White List Violations)**。

步骤 2 您有以下选择：

- 要执行基本工作流程操作，请参阅使用合规白名单工作流程，第 1698 页。
- 要了解有关表中各列内容的详细信息，请参阅白名单违规事件字段，第 1702 页。

白名单违规事件字段

可使用工作流程查看和搜索的白名单违规事件包含以下字段。

域

违规主机所在的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。

信息

与该白名单违规事件相关的任何可用的供应商、产品或版本信息。对于违反白名单的协议，此字段还指出违规是由网络协议还是传输协议造成的。

IP 地址

违规主机的 IP 地址。

端口

与触发应用协议白名单违规（违规应用协议造成的违规）的事件关联的端口（如有）。对于其他类型的白名单违规活动，该字段为空白。

协议

与触发应用协议白名单违规（违规应用协议造成的违规）的事件关联的通信协议（如有）。对于其他类型的白名单违规活动，该字段为空白。

Time

该白名单违规事件被检测到的日期和时间。

Type

白名单违规事件的类型，即，该违规事件是否由于下列内容不合规而导致的：

- 操作系统 (os)（搜索此字段时，请输入 os 或 operating system。）
- 应用协议 (server)
- 客户端
- protocol
- Web 应用 (web)（搜索此字段时，请输入 web application。）

White List

被违反的白名单的名称。

计数

与每行中所显示的信息匹配的事件数。注意，Count字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

补救状态事件

当补救触发时，系统会将补救状态事件记录到数据库。可在“补救状态”(Remediation Status) 页面中查看这些事件。可搜索、查看和删除补救状态事件。

查看补救状态事件

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

视乎在使用的工作流程，访问补救状态事件时看到的页面有所不同。可使用预定义工作流程，包括补救的表视图。在表视图中，每个补救状态事件占一行。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **关联 (Correlation)** > **状态 (Status)**。

步骤 2 或者，调整时间范围，如更改时间窗口，第 1461 页中所述。

步骤 3 或者，要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**。

提示 如果使用的是不包含补救表视图的自定义工作流程，则按工作流程标题点击（**切换工作流程**）**([switch workflow])** 菜单，然后选择**补救状态 (Remediation Status)**。

步骤 4 您有以下选择：

- 要了解有关显示的列的详细信息，请参阅补救状态表字段，第 1704 页。
- 要对事件进行排序和限制，请参阅使用工作流程，第 1442 页。
- 要导航至关联事件视图查看相关事件，请点击**关联事件 (Correlation Events)**。
- 要为当前页面添加书签以便快速返回该页面，请点击**将此页面加入书签 (Bookmark This Page)**。要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。
- 要根据表视图中的数据生成报告，请点击**报告设计器 (Report Designer)**，如从事件视图创建报告模板，第 1345 页中所述。
- 要向下展开到工作流程中的下一个页面，请参阅使用向下钻取页面，第 1450 页。
- 要从系统删除补救状态事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**，并确认要删除当前限制视图中的所有事件。
- 要搜索补救状态事件，请点击**搜索 (Search)**。

补救状态表字段

下表介绍补救状态表中可以查看和搜索的字段。

表 *289*： 补救状态字段

字段	说明
域	其受监控流量触发了策略违规（反过来又触发了补救）的设备的域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
策略	已违反并触发补救的关联策略的名称。
Remediation Name	已发起的补救的名称。

字段	说明
Result Message	描述在发起补救后所发生情况的消息。状态消息包括： • 成功完成补救 • 提供给补救模块的输入出错 • 补救模块配置出错 • 登录远程设备或服务器出错 • 无法在远程设备或服务器上获得所需权限 • 登录远程设备或服务器超时 • 执行远程命令或服务器超时 • 远程设备或服务器不可达 • 尝试补救失败 • 未能执行补救程序 • 未知/意外错误 如已安装自定义补救模块，则可能出现自定义模块实现的其他状态消息。
规则	触发了补救的关联规则的名称。
Time	Firepower 管理中心发起补救的日期和时间。
计数	与每行中所显示的信息匹配的事件数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

使用补救状态事件表

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

您可以更改事件视图的布局或按字段值限制视图中的事件。

当禁用列时，除非稍后重新添加该列，否则该列在会话持续时间内处于禁用状态。如果禁用第一列，则会添加“计数”(Count) 列。

点击表视图行中的值可限制表视图，且不会向下钻取到下一页。

提示 表视图的页面名称中始终包括“Table View”。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析 (Analysis)** > **关联 (Correlation)** > **状态 (Status)**。

提示 如果使用的是不包含补救表视图的自定义工作流程，则按工作流程标题点击（**切换工作流程**）**([switch workflow])** 菜单，然后选择**补救状态 (Remediation Status)**。

步骤 2 您有以下选择：

- 要了解有关显示的列的详细信息，请参阅补救状态表字段，第 1704 页。
- 要对事件进行排序和限制，请参阅使用工作流程，第 1442 页。

第 90 章

审核系统

以下主题介绍如何审核系统上的活动：

系统审核简介

您可以用两种方式审计系统中的活动。隶属 Firepower 系统的设备会为用户每次与 Web 界面的交互生成审核记录，同时也在系统日志中记录系统状态消息。

审核记录

Firepower 管理中心和 7000 和 8000 系列设备记录用户活动的只读审核信息。审计日志显示在标准事件视图中，您可以依据审计视图中的任何项目查看、排序和过滤审计日志消息。您可以轻松删除和报告审计信息，也可以查看用户所作更改的详细报告。

审核日志中最多可以存储 100,000 个条目。当审核日志中条目的数量超过 100,000 时，设备会从数据库中删除最旧的记录，保持数据库中条目的数量为 100,000。

注释 如果重新启动 7000 或 8000 系列设备，请尽快登录辅助 CLI，在本地 Web 界面可用之前，您执行的任何命令都不会记录在审核日志中。

查看审核记录

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

在 Firepower 管理中心或 7000 和 8000 系列设备上，您可以查看审核记录表。预定义的审计工作流程包括一个事件表视图。可以根据要查找的信息操纵表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 使用**系统 (System)** > **监控 (Monitoring)** > **审核 (Audit)**访问审核日志工作流程。

步骤 2 如果未显示事件，您可能需要调整时间范围。有关详细信息，请参阅事件时间限制，第 1458 页。

注释 如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间窗口（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。

步骤 3 有以下选项可供选择：

- 要了解有关表中各列内容的详细信息，请参阅系统日志，第 1714 页。
- 要对当前工作流程页面上的事件进行排序和限制，请参阅使用表视图页面，第 1450 页。
- 要在当前工作流程页面中导航，请参阅时间窗口进度，第 1463 页。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。有关详细信息，请参阅使用工作流程，第 1442 页。
- 要向下展开到工作流程中的下一个页面，请参阅使用向下钻取页面，第 1450 页。
- 要限制特定值，请点击行中的值。如果在详细浏览页面中点击一个值，您将进入下一个页面并限制该值。请注意，点击表视图行中的值可限制表视图，且**不**会向下钻取到下一页。有关详细信息，请参阅事件视图限制，第 1464 页。

  提示 表视图的页面名称中始终包含“Table View”。
- 要删除审核记录，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)**，或者点击**全部删除 (Delete All)** 以删除当前受限制视图中的所有事件。
- 要将当前页面加入书签，以便您可以快速返回到该页面，请点击**将此页面加入书签 (Bookmark This Page)**。有关详细信息，请参阅书签，第 1467 页。
- 要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。有关详细信息，请参阅书签，第 1467 页。
- 要根据当前视图中的数据生成报告，请点击**报告设计器 (Report Designer)**。有关详细信息，请参阅从事件视图创建报告模板，第 1345 页。
- 要查看审核日志中记录的更改摘要，请点击**消息 (Message)** 列中的适用事件旁边的比较图标 ()。有关详细信息，请参阅使用审核日志检查更改，第 1710 页。

审核日志工作流程字段

下表介绍了可以查看和搜索的审核日志字段。

表 *290*：审核日志字段

字段	说明
Time	设备生成审计记录的时间和日期。
User	触发审计事件的用户的用户名。
Subsystem	用户生成审核记录所遵循的完整菜单路径。例如，**系统 (System)** > **监控 (Monitoring)** > **审核 (Audit)**是查看审核日志的菜单路径。 对于菜单路径不相关的少数情况，Subsystem 字段仅显示事件类型。例如，**Login** 分类用户登录尝试。
消息	用户执行的操作或用户在页面上点击的按钮。 例如，`Page View` 表示用户简单查看了子系统中显示的页面，而 `Save` 意味着用户点击了页面上的 **Save** 按钮。 对 Firepower 系统的更改会以一个比较图标 () 显示，您可以点击以查看更改摘要。
源 IP	与用户使用的主机相关联的 IP 地址。 注意：搜索此字段时，必须输入特定的 IP 地址；搜索审核日志时不可以使用 IP 范围。
域	触发审核事件时用户的当前域。仅当曾为多租户配置 Firepower 管理中心时，此字段才存在。
Configuration Change （仅限搜索）	指定是否查看搜索结果中配置更改的审核记录。（`yes` 或 `no`）
计数	与每行中所显示的信息匹配的事件数。注意，Count 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

审核事件表视图

您可以更改事件视图的布局或按字段值限制视图中的事件。当禁用某列时，在点击想要隐藏的列标题中的关闭图标 () 后，系统会显示弹出窗口，在窗口中点击 **Apply**。禁用列时，该列在会话持续时间内处于禁用状态（除非稍后重新添加该列）。请注意，禁用第一列时，会添加 Count 列。

要隐藏或显示其他列，或将已禁用列添加回视图中，选择或清除相应的复选框，然后点击 **Apply**。

请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且不会向下展开到工作流程中的下一个页面。

提示 表视图的页面名称中始终包含“Table View”。

使用审核日志检查更改

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

您可以使用审计日志查看系统更改的详细报告。这些报告会比较系统的当前配置和特定更改之前的最近配置。

Compare Configurations 页面显示更改前的系统配置和采用并行格式的运行配置之间的差异。审计事件类型、最后修改时间、作出更改的用户名称会在每个配置上的标题栏中显示。

两种配置之间的差异会突出显示：

- 蓝色表示突出显示设置的设置在两个配置中有所不同，差异会以红色文本标记。
- 绿色表示突出显示的设置在一个配置中显示，但在另一个配置中不显示。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**系统 (System)** > **监控 (Monitoring)** > **审核 (Audit)**。

步骤 2 点击比较图标 ()，其位于 **Message** 列的适用审计日志事件旁边。

提示 可以点击标题栏上方的**上一个 (Previous)** 或**下一个 (Next)** 在不同更改间切换。如果更改摘要长度超过一个页面，您也可以使用右侧的滚动条查看其他的更改。

抑制审核记录

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	任何环境	管理

如果审核策略不要求您审核特定类型的用户与 Firepower 系统之间的交互，则可以防止这些交互在 Firepower 管理中心或 7000 和 8000 系列设备上生成审核记录。例如，默认情况下，每次用户查看联

机帮助时，Firepower 系统都会生成一个审核记录。如果您不需要保留这些交互记录，可以自动屏蔽它们。

要配置审计事件屏蔽，您必须具备设备的管理员用户帐户权限，且必须能够访问设备的控制台或打开一个安全外壳。

注意 确保仅授权人员可以访问设备及其管理员帐户。

过程

在 `/etc/sf` 目录中，创建以下形式的一个或多个 `AuditBlock` 文件，其中 type 是审核块类型，第 1711 页中所述的类型之一：

`AuditBlock.type`

注释 如果为特定类型的审核消息创建 `AuditBlock.type` 文件，但之后确定不想再抑制它们，则必须删除 `AuditBlock.type` 文件的内容，但在 Firepower 系统上保留该文件本身。

审核块类型

每种审计块类型的内容都必须为特定格式，如下表所述。确保您使用的是正确的文件名大写字母。另请注意，文件的内容区分大小写。

请注意，当您添加 `AuditBlock` 文件时，带 `Audit` 子系统和 `Audit Filtertype Changed` 消息的审核记录会被添加到审核事件中。出于安全原因，该审计记录**不能**被屏蔽。

表 *291*：审核块类型

类型	说明
Address	创建一个以 `AuditBlock.address` 命名的文件，并包括您想要从审计日志中屏蔽的各 IP 地址，每行一个。您可以使用部分 IP 地址，前提是它们从地址开始处映射。例如，部分地址 `10.1.1` 匹配从 `10.1.1.0` 到 `10.1.1.255` 的地址。
消息	创建一个命名为 `AuditBlock.message` 的文件，并包括您想要屏蔽的消息子字符串，每行一个。 请注意，子字符串匹配，这样，如果您的文件中包括 `backup`，则包括文字 `backup` 的所有消息都将被屏蔽。
Subsystem	创建一个命名为 `AuditBlock.subsystem` 的文件，并包括您想要屏蔽的各子系统，每行一个。 请注意，子字符串**不**匹配。您必须使用准确的字符串。有关所审核的子系统列表，请参阅已审核的子系统，第 1712 页。

类型	说明
User	创建一个命名为 `AuditBlock.user` 的文件，并包括您想要屏蔽的各用户帐号，每行一个。您可以使用部分字符串匹配，前提是它们从用户名开始处映射。例如，部分用户名 `IPSAnalyst` 匹配用户名 `IPSAnalyst1` 和 `IPSAnalyst2`。

已审核的子系统

下表列出了经审计的子系统。

表 *292*：子系统名称

Name	包括与下列各项的用户交互...
管理	管理功能，例如系统和访问配置、时间同步、备份和恢复、设备管理、用户帐户管理和调度
警报	警报功能，例如邮件、SNMP 和系统警报
审核日志	审计事件视图
Audit Log Search	审计事件搜索
命令行	命令行界面
配置	邮件警报
COOP	操作功能连续性
日期	事件视图的日期和时间范围
Default Subsystem	没有已分配子系统的选项
Detection & Prevention Policy	入侵策略的菜单选项
Error	系统级错误
eStreamer	eStreamer 配置
EULA	审核最终用户许可协议
活动	入侵和发现事件视图
Events Clipboard	入侵事件剪贴板
Events Reviewed	经审核的入侵事件

Name	包括与下列各项的用户交互...
Events Search	任何事件搜索
未能安装规则更新 (Failed to install rule update) `rule_update_id`	安装规则更新
标头	用户登录后用户界面的初次展示
健康状况	运行状况监控
Health Events	运行状况监控事件视图
帮助	联机帮助
IDS Impact Flag	影响标记配置
IDS Policy	入侵策略
IDSRule sid:`sig_id` rev:`rev_num`	按 SID 划分的入侵规则
突发事件	入侵事故
安装	安装更新
入侵事件	入侵事件
登录	网络界面登录和注销功能
菜单	任何菜单选项
Configuration export > `config_type` > `config_name`	导入特定类型和名称的配置
Permission Escalation	用户角色升级
偏好设置	用户首选项，例如，用户帐户和单个事件首选项的时区
策略	任何策略，包括入侵策略
注册	在管理中心上注册设备
RemoteStorageDevice	配置远程存储设备
报告	报告列表和报告设计者功能

Name	包括与下列各项的用户交互...
Rules	入侵规则，包括入侵规则编辑器和规则导入进程
Rule Update Import Log	查看规则更新导入日志
Rule Update Install	安装规则更新
状态	系统日志以及主机和性能统计数据
System	各种系统范围设置
Task Queue	查看后台进程状态
用户	创建和修改用户帐户和角色

系统日志

System Log (syslog) 页面上提供了设备的系统日志信息。系统日志显示系统生成的每条消息。以下项目会按顺序列出：

- 生成消息的日期
- 生成消息的时间
- 生成消息的主机
- 消息本身

查看系统日志

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

系统日志信息是本地消息。例如，您**不能**使用Firepower管理中心查看受管设备上系统日志中的系统状态消息。

在 Firepower 管理中心或 7000 和 8000 系列设备上，可以通过对特定组件进行过滤来修改系统日志消息的视图。

过程

步骤 1 选择**系统 (System)** > **监控 (Monitoring)** > **系统日志 (Syslog)**。

步骤 2 如果要搜索系统日志中的特定消息内容，请参阅过滤系统日志消息，第 1715 页。

过滤系统日志消息

智能许可证	经典许可证	支持的设备	支持的域	Access
任何环境	任何环境	任何环境	仅全局	管理员/维护人员

在 Firepower 管理中心或 7000 和 8000 系列设备上，可以通过对特定组件进行过滤来修改系统日志消息的视图。过滤功能使您可以根据内容搜索特定的消息。

过滤功能使用 UNIX 文件搜索实用程序 Grep，正因如此，您可以使用 Grep 接受的大部分语法。这包括使用与 Grep 兼容的正则表达式实现模式匹配。您可以使用一个单词作为过滤器，也可以使用 Grep 支持的正则表达式搜索内容。

过程

步骤 1 选择**系统 (System)** > **监控 (Monitoring)** > **系统日志 (Syslog)**。

步骤 2 在过滤器字段中输入单词或查询，如系统日志过滤器的语法，第 1716 页中所述。

注释 支持仅与 Grep 兼容的搜索语法。例如，您可使用 `ntp` 作为过滤器搜索所有 NTP 相关的系统日志消息，或将 `Nov` 用作过滤器搜索在 11 月生成的所有消息。可以通过使用 `Nov[[:space:]]*27` 或 `Nov.*27` 查看从 11 月 27 日起的消息，但是无法使用 `Nov 27` 或 `Nov*27` 查看这些消息。

步骤 3 如果要使搜索区分大小写，请选中**区分大小写 (Case-sensitive)**。（默认情况下，过滤器不区分大小写。）

步骤 4 或者，勾选 **Exclusion** 搜索不符合所输入标准的所有系统日志消息。

步骤 5 点击 **Go**（前往）。

示例

要搜索在 11 月 5 日生成的所有日志条目，请使用 `Nov[[:space:]]*5`。

要搜索包含用户名“Admin”的所有日志条目，请使用 `Admin`。

要搜索包含 11 月 5 日的授权调试信息的所有日志条目，请使用 `Nov[[:space:]]*5.*AUTH.*DEBUG`。

系统日志过滤器的语法

下表显示了在系统日志过滤器中可以使用的正则表达式语法：

表 *293*：系统日志过滤器语法

语法构成	描述	示例
.	匹配任意字符或空格	`Admi.` 匹配 `Admin`、`AdmiN`、`Admi1` 和 `Admi&`
`[[:alpha:]]`	匹配任意字母字符	`[[:alpha:]]dmin` 匹配 `Admin`、`bdmin` 和 `Cdmin`
`[[:upper:]]`	匹配任意大写字母字符	`[[:upper:]]dmin` 匹配 `Admin`、`Bdmin` 和 `Cdmin`
`[[:lower:]]`	匹配任意小写字母字符	`[[:lower:]]dmin` 匹配 `admin`、`bdmin` 和 `cdmin`
`[[:digit:]]`	匹配任意数字字符	`[[:digit:]]dmin` 匹配 `0dmin`、`1dmin` 和 `2dmin`
`[[:alnum:]]`	匹配任意字母数字字符	`[[:alnum:]]dmin` 匹配 `1dmin`、`admin`、`2dmin` 和 `bdmin`
`[[:space:]]`	匹配任意空格，包括选项卡	`Feb[[:space:]]29` 匹配从 2 月 29 日起的日志
*	匹配其符合的字符或表达式的零个或更多实例	`ab*` 匹配 `a`、`ab`、`abb`、`ca`、`cab` 和 `cabb` `[ab]*` 匹配所有字符
?	匹配零个或一个实例	`ab?` 匹配 `a` 或 `ab`
\	您可以搜索一般会被解释为正则表达式语法的字符	`alert\?` 匹配 `alert?`

附 录 A

安全、互联网接入和通信端口

以下主题提供有关系统安全、互联网接入和通信端口的信息：

概述：安全、互联网接入和通信端口

为了保护 Firepower 管理中心，应将其安装在受保护的内部网络中。虽然Firepower 管理中心已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它（或任何受管设备）。

如果Firepower管理中心及其受管设备位于同一个网络，则可将这些设备上管理接口连接至与Firepower管理中心相同的受保护内部网络。这样您就可以安全地通过Firepower管理中心控制设备。您还可以配置多个管理接口，使Firepower 管理中心能够管理和隔离来自其他网络上设备的流量。

无论设备如何部署，设备内部通信都会被加密。但是，您仍需采取措施，确保系统设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

另请注意，Firepower 系统的特定功能需要连接互联网。默认情况下，系统设备配置为直接连接到互联网。此外，系统还要求某些端口对基本内部设备通信保持开放以实现安全的设备访问，以便特定系统功能访问其正常运行所需的本地或互联网资源。

互联网接入要求

默认情况下，系统设备会配置为直接连接到互联网的 443/tcp (HTTPS) 和 80/tcp (HTTP) 端口，这些端口在所有 Firepower 系统设备上均默认打开。请注意，大多数系统设备支持使用代理服务器。另外还请注意，代理服务器不能用于 whois 访问。

Firepower 系统功能互联网接入要求

下表介绍 Firepower 系统特定功能的互联网接入要求。

表 *294*: *Firepower* 系统功能互联网接入要求

特性	需要互联网接入以便...	设备
面向 Firepower 的 AMP	执行恶意软件云查找。	管理中心
思科高级恶意软件防护（思科 AMP）集成	接收来自思科AMP云的基于终端的（面向终端的 AMP）恶意软件事件。	管理中心
动态分析：查询	查询 AMP Threat Grid 以了解之前提交以供动态分析的文件的威胁评分。	管理中心
动态分析：提交	将文件提交到 AMP Threat Grid 以供动态分析。	任何设备
入侵规则、VDB 和 GeoDB 更新	将入侵规则、GeoDB 或 VDB 更新直接下接至设备，或安排该等下载。	管理中心
本地恶意软件分析和文件预分类签名更新	将签名更新下载到本地恶意软件分析和预分类引擎。	管理中心
RSS 源控制面板构件	从外部源（包括思科）下载 RSS 源数据。	管理中心 7000 和 8000 系列
安全情报过滤	从外部来源下载安全情报源数据，包括思科提供的情报源。	管理中心
系统软件更新	将系统更新下载至设备或安排该等下载。	任何设备，除了 NGIPSv
URL 过滤	下载 URL 类别和信誉数据以进行访问控制，并查询未分类的 URL。	管理中心
whois	请求外部主机的 whois 信息。	管理中心

通信端口要求

Firepower 管理中心及其受管设备使用双向、SSL 加密通信通道进行通信，该通道默认使用端口 8305/tcp。系统**需要**此端口保持开放以进行基本平台内通信。其他开放端口允许：

- 访问 Web 界面
- 保护与设备或 Firepower 管理中心的远程连接
- 系统的某些功能访问其正常运行所需的本地或互联网资源

一般来说，功能相关端口会保持关闭，直至启用或配置关联的功能。例如，在将Firepower管理中心连接至 User Agent 之前，代理通信端口 (3306/tcp) 会一直保持关闭。又例如，在启用 LOM 之前，7000 和 8000 系列设备上的端口 623/udp 保持关闭。

注意 在了解此操作对部署的影响之前，请**勿**关闭打开的端口。

例如，在受管设备上关闭出站端口 25/tcp (SMTP) 会阻止设备为单个入侵事件发送邮件通知。又例如，可通过关闭端口 443/tcp (HTTPS) 禁用对物理受管设备的 Web 界面的访问，但是，这也会阻止设备将可疑恶意软件文件提交到 AMP Threat Grid 云进行动态分析。

请注意，系统允许更改其某些通信端口：

- 在配置系统与身份验证服务器之间的连接时，您可以指定用于 LDAP 和 RADIUS 身份验证的自定义端口。
- 您可以更改管理端口 (8305/tcp)。但是，思科强烈建议保留默认设置。如果更改管理端口，则必须为部署中需要相互通信的所有 Firepower 管理中心及其受管设备都进行此更改。
- 您可以使用端口 32137/tcp 来允许已升级的管理中心与思科 AMP 云进行通信。但是，思科建议切换至端口 443，该端口是版本 5.3 和更高版本全新安装的默认端口。

用于 Firepower 系统功能和操作的默认通信端口

下表列出了各种设备类型所需的开放端口，以便充分利用 Firepower 系统功能。

表 *295*：用于 *Firepower* 系统功能和操作的默认通信端口

端口	说明	Direction	开放对象...	所需的操作…
22/tcp	SSH/SSL	双向	任意	允许与设备进行安全远程连接。
25/tcp	SMTP	发送	任意	从设备发送邮件通知和警报。
53/tcp	DNS	发送	任意	使用 DNS。
67/udp 68/udp	DHCP	发送	任意	使用 DHCP。请注意，这些端口默认为**关闭**。
80/tcp	HTTP	发送	管理中心、7000 和 8000 系列	允许 RSS 源控制面板构件连接到远程 Web 服务器。

端口	说明	Direction	开放对象...	所需的操作…
		双向	管理中心	通过 HTTP 更新自定义和第三方安全情报源。 下载 URL 类别和信誉数据（还需要 443 端口）。
161/udp	SNMP	双向	任意	允许通过 SNMP 轮询接入设备的 MIB。
162/udp	SNMP	发送	任意	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP	发送	任何设备，除了 NGIPSv	与一个 LDAP 服务器通信，以进行外部身份验证。
389/tcp 636/tcp	LDAP	发送	管理中心	获取检测到的 LDAP 用户元数据。
443/tcp	HTTPS	接收	任何设备，除了 NGIPSv	接入设备的网络接口
443/tcp	HTTPS AMQP AMP 云、AMP Threat Grid 云和威胁情报通信首选项	双向	管理中心	获取： • 软件、入侵规则、VDB 和 GeoDB 更新 • URL 类别和信誉数据（还需要 80 端口） • 情报源和其他安全的安全情报源 • 基于终端（面向终端的 AMP）的恶意软件事件 • 网络流量中检测到的文件的恶意软件性质 • 已提交文件的动态分析信息
		双向	管理中心，7000 和 8000 系列	使用设备的本地网络界面下载软件更新。
		双向	任何受管设备	提交文件以供动态分析。
514/udp	系统日志	发送	任意	发送警报至远程系统日志服务器。
623/udp	SOL/LOM	双向	7000 和 8000 系列	允许使用局域网串行 (SOL) 连接执行无人值守管理
1500/TCP 2000/TCP	数据库访问	接收	管理中心	允许第三方客户端对数据库进行只读访问。
1812/UDP 1813/UDP	RADIUS	双向	任何设备，除了 NGIPSv	与 RADIUS 服务器通信以进行外部身份验证和记帐。
3306/tcp	用户代理	接收	管理中心	与 User Agent 进行通信。

端口	说明	Direction	开放对象...	所需的操作…
8302/tcp	eStreamer	双向	管理中心 、 7000 和 8000 系列	与 eStreamer 客户端通信。
8305/tcp	设备通信	双向	任意	在同一部署中的设备之间安全地进行通信。**Required.**
8307/tcp	主机输入客户端	双向	管理中心	与主机输入客户端通信。
32137/tcp	AMP 云和威胁情报通信首选项	双向	管理中心	允许升级的 管理中心与思科 AMP 云进行通信。

附 录 B

Firepower 命令行参考

CLI 命令

本参考介绍以下设备的命令行界面 (CLI)：

- 7000 和 8000 系列
- ASA FirePOWER
- NGIPSv

通过 CLI 登录设备后，即可使用下述命令查看、配置 Firepower 系统和进行故障排除。

注释 在 Firepower 管理中心上不支持命令行界面。

有许多 CLI 模式（例如 `show` 和 `configure`）包含以模式名称开头的命令集。可进入一个模式，然后在该模式中输入有效命令；也可从任何模式输入完整的命令。例如，要显示有关一个名为 Analyst1 的用户帐户的信息，可在 CLI 提示符处输入以下信息：

```
show user Analyst1
```

如果之前已进入 `show` 模式，请在 CLI 提示符处输入以下信息：

```
user Analyst1
```

在每个模式中，可用于某个用户的命令取决于该用户的 CLI 访问权限。创建用户帐户时，可为其分配以下 CLI 访问级别之一：

- 基本 - 用户具有只读访问权限，不能运行会影响系统性能的命令。
- 配置 - 用户具有读写访问权限，可以运行会影响系统性能的命令。
- 无 - 用户无法登录到外壳。

在 7000 和 8000 系列设备上，可以在 Web 界面中的“用户管理”(User Management) 页面上分配命令行权限。在 NGIPSv 和 ASA FirePOWER 上，通过 CLI 本身分配命令行权限。

注释 如果重新启动 7000 或 8000 系列 设备后尽快登录 CLI，则所执行的任何命令均不记录在审核日志中，直至网络界面可用。

请注意，CLI 命令不区分大小写，但其文本不是 CLI 框架一部分的参数除外，例如用户名和搜索过滤器。

基本 CLI 命令

基本 CLI 命令可用于与 CLI 交互。这些命令不影响设备的运行。基本命令可供所有 CLI 用户使用。

configure password

允许当前用户更改其密码。发出命令后，CLI 会提示用户其当前（或旧）密码，然后提示用户输入新密码两次。

Access

基本

语法

```
configure password
```

示例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

end

使用户返回到默认模式。（将用户从任何较低级别的 CLI 上下文向上移至默认模式。）

Access

基本

语法

```
end
```

示例

```
configure network ipv4> end
>
```

exit

将 CLI 上下文上移至下一个最高级别的 CLI 上下文。从默认模式发出此命令会使用户注销当前 CLI 会话，这相当于发出 `logout` CLI 命令。

Access

基本

语法

```
exit
```

示例

```
configure network ipv4> exit
configure network>
```

help

显示 CLI 语法的概述。

Access

基本

语法

```
help
```

示例

```
> help
```

history

显示当前会话的命令行历史记录。

Access

基本

语法

```
history limit
```

其中，`limit` 设置历史记录列表的大小。要将大小设置为无限，请输入零。

示例

```
history 25
```

logout

使当前用户注销当前 CLI 控制台会话。

Access

基本

语法

```
logout
```

示例

```
> logout
```

?（问号）

为 CLI 命令和参数显示上下文相关帮助。按照以下说明使用问号 (?)：

- 要为当前 CLI 上下文中可用的命令显示帮助，请在命令提示符处输入问号 (?)。
- 要显示以特定字符集开头的可用命令的列表，请输入缩写命令，再紧接着输入问号 (?)。
- 要为命令的合法变元显示帮助，请在命令提示符处输入问号 (?) 代替变元。

请注意，问号 (?) 不会回送到控制台。

Access

基本

语法

```
?
```

```
abbreviated_command ?
command [arguments] ?
```

示例

```
> ?
```

?? (double question marks)

为 CLI 命令和参数显示详细的上下文相关帮助。

Access

基本

语法

```
??
abbreviated_command end??
command [arguments] ??
```

示例

```
> configure manager add ??
```

显示命令

显示命令提供有关设备状态的信息。这些命令不会改变设备的操作模式，运行这些命令对系统运行的影响极小。大多数显示命令可供所有 CLI 用户使用；但是，只有拥有配置 CLI 权限的用户才能发出 `show user` 命令。

access-control-config

显示当前部署的访问控制配置，包括：

- 安全情报设置
- 访问控制策略调用的任何子策略的名称
- 入侵变量集数据
- 日志记录设置
- 其他高级设置，包括策略级性能、预处理以及常规设置

还显示策略相关的连接信息，例如源端口和目标端口数据（包括 ICMP 条目的类型和代码）以及与每条访问控制规则匹配的连接数（命中次数）。

Access

基本

语法

```
show access-control-config
```

示例

```
> show access-control-config
```

alarms

显示设备上当前活动的（故障/停机）硬件报警。此命令在 NGIPSv 和 ASA FirePOWER 设备上不可用。

Access

基本

语法

```
show alarms
```

示例

```
> show alarms
```

arp-tables

显示适用于您网络的地址解析协议表。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show arp-tables
```

示例

```
> show arp-tables
```

audit-log

按时间倒序显示审核日志；首先列出最近的审核日志事件。

Access

基本

语法

```
show audit-log
```

示例

```
> show audit-log
```

bypass

列出使用中的内联集并显示这些内联集的旁路模式状态（常规或旁路）。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show bypass
```

示例

```
> show bypass
```

high-availability 命令

显示有关高可用性配置、状态和成员设备或堆栈的信息。此命令在 NGIPSv 和 ASA FirePOWER 设备上不可用。

Access

基本

config

显示设备的高可用性配置。

语法

```
show high-availability config
```

示例

```
> show high-availability config
```

high-availability ha-statistics

显示高可用性对中设备的状态共享统计信息。

语法

```
show high-availability ha-statistics
```

示例

```
> show high-availability ha-statistics
```

cpu

显示适合用于设备上所有 CPU 的平台的当前 CPU 使用情况统计信息。对于 7000 和 8000 系列设备，会显示以下值：

- CPU - 处理器数。
- 负载 - CPU 利用率，用 0 到 100 之间的任意数字表示。0 表示空负载，100 表示满负载。

对于 NGIPSv 和 ASA FirePOWER，会显示以下值：

- CPU - 处理器数。
- %user - 在用户级别（应用）执行时发生的 CPU 利用率百分比。
- %nice - 在具有 nice 优先级的用户级别执行时发生的 CPU 利用率百分比。
- %sys - 在系统级别（内核）执行时发生的 CPU 利用率百分比。这不包括中断或软件中断修复时间。softirq（软件中断）是可以同时在多个 CPU 上运行的 32 个枚举软件中断之一。
- %iowait - 当系统有未处理的磁盘 I/O 请求时 CPU 空闲时间的百分比。
- %irq - CPU 修复中断所用时间的百分比。
- %soft - CPU 修复软件中断所用时间的百分比。
- %steal - 当虚拟机监控程序为其他虚拟处理器提供服务时，虚拟 CPU 被强制等待时间的百分比。
- %guest - CPU 运行虚拟处理器所用时间的百分比。
- %idle - 当系统没有未处理的磁盘 I/O 请求时 CPU 空闲时间的百分比。

Access

基本

语法

```
show cpu [procnum]
```

其中，`procnum` 是要显示其利用率信息的处理器数。有效值为 0 到比系统的处理器总数小 1 的数值。如果 `procnum` 用于 7000 或 8000 系列设备，它将被忽略，因为对于该平台，只能为所有处理器显示利用率信息。

示例

```
> show cpu
```

database 命令

`show database` 命令配置设备的管理接口。

Access

基本

processes

显示运行中数据库查询的列表。

Access

基本

语法

```
show database processes
```

示例

```
> show database processes
```

slow-query-log

显示数据库的慢查询日志。

Access

基本

语法

```
show database slow-query-log
```

示例

```
> show database slow-query-log
```

device-settings

显示有关当前设备专用应用旁路设置的信息。

Access

基本

语法

```
show device-settings
```

示例

```
> show device-settings
```

disk

显示当前磁盘使用情况。

Access

基本

语法

```
show disk
```

示例

```
> show disk
```

disk-manager

显示系统每个部分（包括竖井、低水位线和高水位线）的磁盘使用情况详细信息。

Access

基本

语法

```
show disk-manager
```

示例

```
> show disk-manager
```

dns

显示当前 DNS 服务器地址和搜索域。

Access

基本

语法

```
show dns
```

示例

```
> show dns
```

expert

调用 SHELL。

Access

基本

语法

```
expert
```

示例

```
> expert
```

fan-status

显示硬件风扇的当前状态。此命令在 NGIPSv 和 ASA FirePOWER 设备上不可用。

Access

基本

语法

```
show fan-status
```

示例

```
> show fan-status
```

fastpath-rules

显示当前配置的 8000 系列快速路径规则。此命令仅在 8000 系列设备上可用。

Access

基本

语法

```
show fastpath-rules
```

示例

```
> show fastpath-rules
```

gui

显示网络界面的当前状态。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show gui
```

示例

```
> show gui
```

主机名

显示设备的主机名和设备 UUID。如果使用 CLI 编辑设备的主机名，请确认在管理Firepower 管理中心上反映更改。在某些情况下，您可能需要手动编辑设备管理设置。

Access

基本

语法

```
show hostname
```

示例

```
> show hostname
```

主机

显示 ASA FirePOWER 模块的 /etc/hosts 文件的内容。

Access

基本

语法

```
show hosts
```

示例

```
> show hosts
```

hyperthreading

显示超线程是处于启用状态还是禁用状态。此命令在 ASA FirePOWER上不可用。

Access

基本

语法

```
show hyperthreading
```

示例

```
> show hyperthreading
```

inline-sets

显示所有内联安全区域和关联接口的配置数据。此命令在 ASA FirePOWER上不可用。

Access

基本

语法

```
show inline-sets
```

示例

```
> show inline-sets
```

接口

如未指定参数，将显示所有已配置接口的列表。如已指定参数，将显示有关指定接口的详细信息。

Access

基本

语法

```
show interfaces interface
```
其中，*interface* 是想要获得其详细信息的特定接口。

示例

```
> show interfaces
```

ifconfig

显示适用于 ASA FirePOWER 模块的接口配置。

Access

基本

语法

```
show ifconfig
```

示例

```
> show ifconfig
```

lcd

显示 LCD 硬件显示器是处于启用状态还是禁用状态。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show lcd
```

示例

```
> show lcd
```

link-aggregation 命令

`show link-aggregation` 命令显示链路聚合组 (LAG) 的配置和统计信息。此命令在 NGIPSv 和 ASA FirePOWER 设备上不可用。

Access

基本

配置

为所配置的每个 LAG 显示配置详情，包括 LAG ID、接口数量，配置模式、负载平衡模式、LACP 信息和物理接口类型。

Access

基本

语法

```
show link-aggregation configuration
```

示例

```
> show link-aggregation configuration
```

statistics

按照接口为所配置的每个LAG显示统计信息，包括状态、链路状态和速度、配置模式、已接收和已传输数据包的计数器以及已接收和已传输字节的计数器。

Access

基本

语法

```
show link-aggregation statistics
```

示例

```
> show link-aggregation statistics
```

link-state

显示设备端口的类型、链路、速度、双工状态和旁路模式。此命令不适用于ASA FirePOWER设备。

Access

基本

语法

```
show link-state
```

示例

```
> show link-state
```

log-ips-connection

显示与记录的入侵事件相关联的连接事件日志记录是处于启用状态还是禁用状态。

Access

基本

语法

```
show log-ips-connection
```

示例

```
> show log-ips-connection
```

managers

显示Firepower管理中心 的配置和通信状态。仅在注册处于待处理状态时，才会显示注册密钥和NAT ID。

如果设备被配置为堆叠配置中的次要设备，将会同时显示有关管理 管理中心 和主设备的信息。

Access

基本

语法

```
show managers
```

示例

```
> show managers
```

memory

显示设备的总内存、使用中内存和可用内存。

Access

基本

语法

```
show memory
```

示例

```
> show memory
```

model

显示设备的型号信息。

Access

基本

语法

```
show model
```

示例

```
> show model
```

mpls-depth

显示在管理接口上配置的 MPLS 层的数量，有效值为 0 至 6。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show mpls-depth
```

示例

```
> show mpls-depth
```

NAT 命令

`show nat` 命令可显示管理接口的 NAT 数据和配置信息。此命令在 NGIPSv 和 ASA FirePOWER 设备上不可用。

Access

基本

active-dynamic

显示根据动态规则转换的NAT流量。当有流量与规则匹配时，这些条目会显示，直至相匹配的规则超时。因此，该列表可能不准确。超时取决于协议：ICMP 为 5 秒，UDP 为 120 秒，TCP 为 3600 秒，所有其他协议均为 60 秒。

语法

```
show nat active-dynamic
```

示例

```
> show nat active-dynamic
```

active-static

显示根据静态规则转换的NAT流量。对设备部署规则后，这些条目就会显示；该列表不会指出与静态 NAT 规则匹配的活动流量。

语法

```
show nat active-static
```

示例

```
> show nat active-static
```

allocators

为所有 NAT 分配器（动态规则使用的转换后地址池）显示信息。

语法

```
show nat allocators
```

示例

```
> show nat allocators
```

config

显示管理接口的当前 NAT 策略配置。

语法

```
show nat config
```

示例

```
> show nat config
```

dynamic-rules

显示使用指定的分配器 ID 的动态 NAT 规则。

语法

```
show nat dynamic-rules allocator_id
```
其中，`allocator_id` 是有效的分配器 ID 号。

示例

```
> show nat dynamic-rules 9
```

flows

显示使用指定的分配器 ID 的规则的流数量。

语法

```
show nat flows allocator-id
```
其中，*allocator_id* 是有效的分配器 ID 号。

示例

```
> show nat flows 81
```

static-rules

显示所有静态 NAT 规则。

语法

```
show nat static-rules
```

示例

```
> show nat static-rules
```

netstat

显示 ASA FirePOWER 模块的活动网络连接。

Access

基本

语法

```
show netstat
```

示例

```
> show netstat
```

网络

显示管理接口、管理接口的MAC地址、HTTP代理地址、端口和用户名（如已配置）的IPv4和IPv6配置。

Access

基本

语法

```
show network
```

示例

```
> show network
```

network-modules

显示所有已安装的模块及其信息（包括序列号）。此命令在NGIPSv和ASA FirePOWER上不可用。

Access

基本

语法

```
show network-modules
```

示例

```
> show network-modules
```

network-static-routes

显示所有已配置的网络静态路由及其相关信息，包括接口、目标地址、网络掩码和网关地址。

Access

基本

语法

```
show network-static-routes
```

示例

```
> show network-static-routes
```

ntp

显示 ntp 配置。

Access

基本

语法

```
show ntp
```

示例

```
> show ntp
```

perfstats

显示设备的性能统计信息。

Access

基本

语法

```
show perfstats
```

示例

```
> show perfstats
```

portstats

显示安装在设备上的所有端口的统计信息。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show portstats [copper | fiber | internal | external | all]
```

其中，copper 表示所有铜端口，fiber 表示所有光纤端口，internal 表示所有内部端口，external 表示所有外部端口（铜端口和光纤端口），all 表示所有端口（外部端口和内部端口）。

示例

```
> show portstats fiber
```

power-supply-status

显示硬件电源的当前状态。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show power-supply-status
```

示例

```
> show power-supply-status
```

process-tree

显示当前正在设备上运行的进程，按类型以树格式排序。

Access

基本

语法

```
show process-tree
```

示例

```
> show process-tree
```

processes

显示当前正在设备上运行的进程，按 CPU 使用情况降序排序。

Access

基本

语法

```
show processes sort-flag filter
```

其中，*sort-flag* 可以是 `-m`，表示按内存（降序）排序；可以是 `-u`，表示按用户名而非进程名称进行排序；也可以是 `verbose`，表示将会显示命令的全名和路径。*filter* 参数指定命令或用户名中作为过滤依据的搜索条件。标题行仍然显示。

示例

```
> show processes -u user1
```

route

显示 ASA FirePOWER 模块的路由信息。

Access

基本

语法

```
show route
```

示例

```
> show route
```

routing-table

如未指定参数，将会显示所有虚拟路由器的路由信息。如已指定参数，将会显示指定路由器的路由信息以及该路由器的指定路由协议类型（如适用）。所有参数均为可选。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show routing-table name [ ospf | rip | static ]
```

其中，*name* 是要获得其信息的特定路由器的名称，`ospf`、`rip` 和 `static` 指定路由协议类型。

示例

```
> show routing-table Vrouter1 static
```

serial-number

显示机箱序列号。此命令在 NGIPSv 上不可用。

Access

基本

语法

```
show serial-number
```

示例

```
> show serial-number
```

ssl-policy-config

显示当前部署的 SSL 策略配置，包括策略说明、默认日志记录设置、所有已启用的 SSL 规则和规则配置、受信任 CA 证书以及无法解密的流量操作。

Access

基本

语法

```
show ssl-policy-config
```

示例

```
> show ssl-policy-config
```

堆叠

显示受管设备上的堆叠配置和位置；在配置为主设备的设备上，也列出所有次要设备的数据。对于高可用性对中的堆栈，此命令还指明堆栈是高可用性对的成员。用户必须使用网络界面来启用或（在大多数情况下）禁用堆叠；如未启用堆叠，此命令将返回 `Stacking not currently configured`。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

```
show stacking
```

示例

```
> show stacking
```

summary

显示有关设备的最常用信息（版本、类型、UUID 等）的摘要。有关详细信息，请参阅以下 `show` 命令：`version`、`interfaces`、`device-settings` 和 `access-control-config`。

Access

基本

语法

```
show summary
```

示例

```
> show summary
```

time

以协调世界时 (UTC) 以及为当前用户配置的本地时区显示当前日期和时间。

Access

基本

语法

```
show time
```

示例

```
> show time
```

traffic-statistics

如未指定参数，将显示有关通过所有端口传输和接收的字节的详细信息。如已指定端口，则仅为指定端口显示该信息。不能为 ASA FirePOWER 模块指定端口，系统仅显示数据平面接口。

Access

基本

语法

```
show traffic-statistics port
```
其中，*port* 是想要获得其信息的特定端口。

示例

```
> show traffic-statistics s1p1
```

user

仅适用于 NGIPSv。显示指定用户的详细配置信息。会显示以下值：

- 登录 - 登录名
- UID - 数字用户 ID
- 身份验证（`Local` 或 `Remote`）- 如何对用户进行身份验证
- 访问权限（`Basic` 或 `Config`）- 用户的权限级别
- 已启用（`Enabled` 或 `Disabled`）- 用户是否处于活动状态
- 重置（`Yes` 或 `No`）- 用户下次登录时是否必须更改密码
- 到期（`Never` 或一个数字）- 还剩下多少天必须更改用户密码
- 警告（`N/A` 或一个数字）- 在密码到期前允许用户更改密码的天数
- 强度（`Yes` 或 `No`）- 用户密码是否符合强度检查标准
- 锁定（`Yes` 或 `No`）- 用户帐户是否因登录失败太多次而被锁定
- 最大（`N/A` 或一个数字）- 用户帐户被锁定前允许的最多登录失败次数

Access

配置

语法

```
show user username username username ...
```
其中，*username* 指定用户的名称；用户名以空格分隔。

示例

```
> show user jdoe
```

用户

仅适用于 NGIPSv。显示所有本地用户的详细配置信息。会显示以下值：

- 登录 - 登录名
- UID - 数字用户 ID
- 身份验证（`Local` 或 `Remote`）- 如何对用户进行身份验证
- 访问权限（`Basic` 或 `Config`）- 用户的权限级别
- 已启用（`Enabled` 或 `Disabled`）- 用户是否处于活动状态
- 重置（`Yes` 或 `No`）- 用户下次登录时是否必须更改密码
- 到期（`Never` 或一个数字）- 还剩下多少天必须更改用户密码
- 警告（`N/A` 或一个数字）- 在密码到期前允许用户更改密码的天数
- 强度（`Yes` 或 `No`）- 用户密码是否符合强度检查标准
- 锁定（`Yes` 或 `No`）- 用户帐户是否因登录失败太多次而被锁定
- 最大（`N/A` 或一个数字）- 用户帐户被锁定前允许的最多登录失败次数

Access

配置

语法

```
show users
```

示例

```
> show users
```

版本

显示产品的版本和内部版本。如已指定详细参数，将会显示附加组件的版本。

Access

基本

语法

```
show version [detail]
```

示例

```
> show version
```

virtual-routers

如未指定参数，将会显示当前已配置的所有带有 DHCP 中继、OSPF 和 RIP 信息的虚拟路由器的列表。如已指定参数，将会显示指定路由器（受指定路由类型的限制）的信息。所有参数均为可选。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

`show virtual-routers [ dhcprelay | ospf | rip ] name`
其中，`dhcprelay`、`ospf` 和 `rip` 指定路由类型，*name* 是想要获得其信息的特定路由器的名称。如果指定 `ospf`，则可进一步在路由类型与路由器名称（如存在）之间指定 `neighbors`、`topology` 或 `lsadb`。

示例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

如未指定参数，将显示当前已配置的所有交换机的列表。如已指定参数，将显示指定交换机的信息。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

基本

语法

`show virtual-switches name`

示例

```
> show virtual-switches Vswitch1
```

vmware-tools

指示当前是否在虚拟设备上启用了 VMware 工具。此命令仅在 NGIPSv 上可用。

VMware工具是专用于提高虚拟机性能的一套实用工具。通过这些实用工具，您可以充分利用VMware产品方便的功能。该系统在所有虚拟设备上均支持以下插件：

- guestInfo
- powerOps
- timeSync
- vmbackup

有关 VMware 工具以及受支持插件的详细信息，请访问 VMware 网站 (http://www.vmware.com)。

Access

基本

语法

```
show vmware-tools
```

示例

```
> show vmware-tools
```

VPN 命令

`show VPN` 命令显示 VPN 连接的 VPN 状态和配置信息。此命令在 NGIPSv 和 ASA FirePOWER 设备上不可用。

Access

基本

config

显示所有 VPN 连接的配置。

语法

```
show vpn config
```

示例

```
> show vpn config
```

config by virtual router

显示适用于虚拟路由器的所有 VPN 连接的配置。

语法

```
show vpn config virtual router
```

示例

```
> show vpn config VRouter1
```

status

显示所有 VPN 连接的状态。

语法

```
show vpn status
```

示例

```
> show vpn status
```

status by virtual router

显示适用于虚拟路由器的所有 VPN 连接的状态。

语法

```
show vpn status virtual router
```

示例

```
> show vpn status VRouter1
```

counters

显示所有 VPN 连接的计数器。

语法

```
show vpn counters
```

示例

```
> show vpn counters
```

counters by virtual router

显示适用于虚拟路由器的所有 VPN 连接的计数器。

语法

```
show vpn counters virtual router
```

示例

```
> show vpn counters VRouter1
```

配置命令

配置命令可供用户配置和管理系统。这些命令会影响系统运行；因此，除了基本级别的 `configure password` 外，只有拥有配置 CLI 访问权限的用户才能发出这些命令。

bypass

打开或关闭内联对的旁路模式。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

配置

语法

```
configure bypass {open | close} {interface}
```
其中，`interface` 是内联对中任一硬件端口的名称。

示例

```
> configure bypass open s1p1
```

high-availability

禁用或配置绕行以在设备上实现高可用性。此命令在 NGIPSv、ASA FirePOWER 或配置为辅助堆栈成员的设备上不可用。

Access

配置

语法

```
configure high-availability {disable | bypass}
```

示例

```
> configure high-availability disable
```

gui

启用或禁用设备网络界面，包括在系统主要更新期间出现的简化升级网络界面。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

配置

语法

```
configure gui [enable | disable]
```

示例

```
> configure gui disable
```

lcd

启用或禁用设备正面的 LCD 显示器。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

配置

语法

```
configure lcd {enable | disable}
```

示例

```
> configure lcd disable
```

log-ips-connections

启用或禁用与记录的入侵事件关联的连接事件日志记录。

Access

配置

语法

```
configure log-ips-connections {enable | disable}
```

示例

```
> configure log-ips-connections disable
```

manager 命令

configure manager 命令配置设备与其管理 Firepower 管理中心 之间的连接。

Access

配置

add

将设备配置为接受来自管理 Firepower 管理中心 的连接。此命令仅在设备并非处于主动托管状态时才起作用。

向 Firepower 管理中心 注册设备时，始终需要唯一字母数字注册密钥。在大多数情况下，必须随注册密钥一起提供主机名或 IP 地址。但是，如有 NAT 设备将设备与 Firepower 管理中心 分开，则必须随注册密钥一起输入唯一 NAT ID，并指定 DONTRESOLVE 而非主机名。

语法

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

其中，{hostname | IPv4_address | IPv6_address | DONTRESOLVE} 指定管理此设备的 Firepower 管理中心的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 Firepower 管理中心不是直接可寻址的，请使用 DONTRESOLVE。如果使用 DONTRESOLVE，则需要 nat_id。regkey 是将设备注册到 Firepower 管理中心所需的唯一字母数字注册密钥。nat_id 是在 Firepower 管理中心和设备之间的注册过程中使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，此项为必填项。

示例

```
> configure manager add DONTRESOLVE abc123 efg456
```

delete

从设备移除 Firepower 管理中心 的连接信息。此命令仅在设备并非处于主动托管状态时才起作用。

语法

```
configure manager delete
```

示例

```
> configure manager delete
```

mpls-depth

在管理接口上配置 MPLS 层的数量。此命令在 NGIPSv 和 ASA FirePOWER 上不可用。

Access

配置

语法

```
configure mpls-depth depth
```
其中，*depth* 是 0 至 6 之间的任意数字。

示例

```
> configure mpls-depth 3
```

network 命令

`configure network` 命令配置设备的管理接口。

Access

配置

dns searchdomains

用在命令中指定的列表替换当前的 DNS 搜索域列表。

语法

```
configure network dns searchdomains {searchlist}
```
其中，`searchlist` 是以逗号分隔的域列表。

示例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

用在命令中指定的列表替换当前的 DNS 服务器列表。

语法

```
configure nework dns servers {dnslist}
```
其中，dnslist 是以逗号分隔的 DNS 服务器列表。

示例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

主机名

设置设备的主机名。

语法

```
configure network hostname {name}
```
其中，name 是新主机名。

示例

```
> configure network hostname sfrocks
```

http-proxy

在 7000 和 8000 系列和 NGIPSv 设备上，配置 HTTP 代理。发出命令后，CLI 会提示用户 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

可在 NGIPSv 上使用此命令配置 HTTP 代理服务器，以便虚拟设备将文件提交给 AMP 云进行动态分析。

语法

```
configure network http-proxy
```

示例

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

在 7000 系列、8000 系列或 NGIPSv 设备上，删除任何 HTTP 代理配置。

语法

```
configure network http-proxy-disable
```

示例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

ipv4 delete

禁用设备管理接口的 IPv4 配置。

语法

```
configure network ipv4 delete
```

示例

```
> configure network ipv4 delete
```

ipv4 dhcp

将设备管理接口的 IPv4 配置设置为 DHCP。管理接口与 DHCP 服务器通信以获取其配置信息。

语法

```
configure network ipv4 dhcp
```

示例

```
> configure network ipv4 dhcp
```

ipv4 manual

手动配置设备管理接口的 IPv4 配置。

语法

```
configure network ipv4 manual ipaddr netmask gw
```
其中，*ipaddr* 是 IP 地址，*netmask* 是子网掩码，*gw* 是默认网关的 IPv4 地址。

示例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

禁用设备管理接口的 IPv6 配置。

语法

```
configure network ipv6 delete
```

示例

```
> configure network ipv6 delete
```

ipv6 dhcp

将设备管理接口的 IPv6 配置设置为 DHCP。管理接口与 DHCP 服务器通信以获取其配置信息。

语法

```
configure network ipv6 dhcp
```

示例

```
> configure network ipv6 dhcp
```

ipv6 manual

手动配置设的管理接口的 IPv6 配置。

语法

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw]
```
其中，ip6addr/ip6prefix 是 IP 地址和前缀长度，ip6gw 是默认网关的 IPv6 地址。

示例

```
> configure network ipv6 manual
2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

ipv6 router

将设备管理接口的 IPv6 配置设置为“路由器”。管理接口与 IPv6 路由器通信以获取其配置信息。

语法

```
configure network ipv6 router
```

示例

```
> configure network ipv6 router
```

management-interface disable

删除与管理接口关联的 IP 地址和静态路由。

语法

```
configure network management-interface disable ethn
```
其中 *n* 表示您要删除其 IP 地址分配的管理接口的数量。

示例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

禁用通过指定的管理接口进行的事件传输。

语法

```
configure network management-interface disable-event-channel ethn
```
其中 *n* 是要禁用的管理接口的数量。

示例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

禁用通过指定的管理接口进行的管理传输。

语法

```
configure network management-interface disable-management-channel ethn
```
其中 *n* 是要禁用的管理接口的数量。

示例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

启用指定的管理接口。

语法

```
configure network management-interface enable ethn
```
其中 *n* 是要启用的管理接口的数量。

示例

```
> configure network management-interface enable eth1
```

management-interface enable-event-channel

启用通过指定的管理接口进行的事件传输。

语法

```
configure network management-interface enable-event-channel ethn
```
其中 *n* 是要启用的管理接口的数量。

示例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

启用通过指定的管理接口进行的管理传输。

语法

```
configure network management-interface enable-management-channel ethn
```
其中 *n* 是要启用的管理接口的数量。

示例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

更改用于管理的 TCP 端口的值。

语法

```
configure network management-interface tcpport port
```
其中，*port* 是您想要配置的管理端口值。

示例

```
> configure network management-interface tcpport 8500
```

management-port

设置设备 TCP 管理端口的值。

语法

```
configure network management-port number
```

其中，*number* 是要配置的管理端口值。

示例

```
> configure network management-port 8500
```

static-routes ipv4 add

为指定的管理接口添加 IPv4 静态路由。

语法

```
configure network static-routes ipv4
add interface destination netmask gateway
```

其中 interface 是管理接口，destination 是目标 IP 地址，netmask 是网络掩码地址，gateway 是要添加的网关地址。

示例

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

为指定的管理接口删除 IPv4 静态路由。

语法

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

其中 interface 是管理接口，destination 是目标 IP 地址，netmask 是网络掩码地址，gateway 是要删除的网关地址。

示例

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv6 add

为指定的管理接口添加 IPv6 静态路由。

语法

```
configure network static-routes ipv6
add interface destination prefix gateway
```

其中 interface 是管理接口，destination 是目标 IP 地址，prefix 是 IPv6 前缀长度，gateway 是要添加的网关地址。

示例

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

static-routes ipv6 delete

为指定的管理接口删除 IPv6 静态路由。

语法

```
configure network static-routes ipv6
delete interface destination prefix gateway
```

其中 interface 是管理接口，destination 是目标 IP 地址，prefix 是 IPv6 前缀长度，gateway 是您想要删除的网关地址。

示例

```
> configure network static-routes ipv6
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

password

允许当前用户更改其密码。发出命令后，CLI 会提示用户其当前（或旧）密码，然后提示用户输入新密码两次。

Access

基本

语法

```
configure password
```

示例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

在 7000 和 8000 系列设备上，移除该设备上存在的任何堆叠配置：

- 在配置为主设备的设备上，完全移除堆栈。
- 在配置为辅助设备的设备上，从堆栈中移除该设备。

此命令不适用于 NGIPSv 或 ASA FirePOWER 模块，不能用于断开设备高可用性对。

无法与堆叠层次结构中较高级别的设备建立通信时，可使用此命令。如果 Firepower 管理中心 可用于通信，会显示一条消息，提示您换用 Firepower 管理中心 网络界面；同样，如在主设备可用时在配置为次要设备的设备上输入 `stacking disable`，将会显示一条消息，提示您从主设备输入该命令。

Access

配置

语法

```
configure stacking disable
```

示例

```
> configure stacking disable
```

user 命令

仅适用于 NGIPSv，`configure user` 命令管理设备的本地用户数据库。

Access

配置

接入层

修改指定用户的访问级别。此命令在指定用户下次登录时生效。

语法

```
configure user access username [basic | config]
```

其中，*username* 指定您想要为其修改访问权限的用户的名称，`basic` 指明基本访问权限，`config` 指明配置访问权限。

示例

```
> configure user access jdoe basic
```

add

创建具有指定名称和访问级别的新用户。此命令提示输入用户密码。

语法

```
configure user add username [basic | config]
```

其中，username 指定新用户的名称，basic 表示基本访问权限，config 表示配置访问权限。

示例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

强制用户密码到期。

语法

```
configure user aging username max_days warn_days
```
其中，username 指定用户的名称，max_days 表示密码有效的最大天数，warn_days 表示密码到期前允许用户更改密码的天数。

示例

```
> configure user aging jdoe 100 3
```

delete

删除用户及其主目录。

语法

```
configure user delete username
```
其中，username 指定用户的名称。

示例

```
> configure user delete jdoe
```

disable

禁用用户。被禁用的用户将无法登录。

语法

```
configure user disable username
```
其中，username 指定用户的名称。

示例

```
> configure user disable jdoe
```

enable

启用用户。

语法

```
configure user enable username
```
其中，username 指定用户的名称。

示例

```
> configure user enable jdoe
```

forcereset

强制用户在下次登录时更改密码。当用户登录并更改密码时，会自动启用强度检查。

语法

```
configure user forcereset username
```
其中，*username* 指定用户的名称。

示例

```
> configure user forcereset jdoe
```

maxfailedlogins

为指定用户设置最多登录失败次数。

语法

```
configure user maxfailedlogins username number
```
其中，*username* 指定用户的名称，*number* 指定最多登录失败次数。

示例

```
> configure user maxfailedlogins jdoe 3
```

password

设置用户密码。此命令提示输入用户密码。

语法

```
configure user password username
```

其中，*username* 指定用户的名称。

示例

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

启用或禁用针对用户密码的强度要求。当用户密码到期时，或者使用了 configure user forcereset 命令，此要求会在用户下次登录时自动启用。

语法

`configure user strengthcheck` *`username`* `{enable | disable}`
其中，*username* 指定用户的名称，`enable` 设置针对指定用户密码的要求，`disable` 移除针对指定用户密码的要求。

示例

```
> configure user strengthcheck jdoe enable
```

解锁

解锁超过最多登录失败次数的用户。

语法

`configure user unlock` *`username`*
其中，*username* 指定用户的名称。

示例

```
> configure user unlock jdoe
```

vmware-tools

启用或禁用 NGIPSv上的 VMware 工具功能。此命令仅在 NGIPSv上可用。

VMware工具是专用于提高虚拟机性能的一套实用工具。通过这些实用工具，您可以充分利用VMware产品方便的功能。该系统在所有虚拟设备上均支持以下插件：

- guestInfo
- powerOps
- timeSync

- vmbackup

有关 VMware 工具以及受支持插件的详细信息，请访问 VMware 网站 (http://www.vmware.com)。

Access

基本

语法

```
configure vmware-tools [enable | disable]
```

示例

```
> configure vmware-tools enable
```

系统命令

系统命令可供用户管理整个系统的文件以及访问控制设置。只有拥有配置 CLI 访问权限的用户才能在系统模式中发出命令。

access-control 命令

`system access-control` 命令可供用户管理设备上的访问控制配置。

Access

配置

存档

将当前部署的访问控制策略作为文本文件另存在 `/var/common`。

语法

```
system access-control archive
```

示例

```
> system access-control archive
```

clear-rule-counts

将访问控制规则命中次数重置为 0。

语法

```
system access-control clear-rule-counts
```

示例

```
> system access-control clear-rule-counts
```

rollback

将系统恢复为之前部署的访问控制配置。不能对堆栈或高可用性对中的设备使用此命令。

语法

```
system access-control rollback
```

示例

```
> system access-control rollback
```

disable-http-user-cert

移除系统中存在的所有 HTTP 用户认证。

Access

配置

语法

```
system disable-http-user-cert
```

示例

```
> system disable-http-user-cert
```

file 命令

`system file` 命令可供用户管理设备上公共目录中的文件。

Access

配置

copy

使用 FTP 将文件传输至使用登录用户名的主机上的某个远程位置。本地文件必须位于公共目录中。

语法

```
system file copy hostname username path filenames filenames ...
```
其中 `hostname` 指定目标远程 主机的名称或 IP 地址，`username` 指定远程主机上用户的名称， `path` 指定远程主机上的目标路径， `filenames` 指定要传输的本地文件；文件名 以空格分隔。

示例

```
> system file copy sfrocks jdoe /pub *
```

delete

从公共目录中移除指定文件。

语法

```
system file delete filenames filenames ...
```
其中，`filenames` 指定要删除的文件；文件名以空格分隔。

示例

```
> system file delete *
```

列表

如未指定文件名，将显示公共目录中所有文件的修改时间、大小和文件名。如已指定文件名，将显示与指定文件名匹配的文件的修改时间、大小和文件名。

语法

```
system file list filenames
```
其中，*filenames* 指定要显示的文件；文件名以空格分隔。

示例

```
> system file list
```

secure-copy

使用 SCP 将文件传输至使用登录用户名的主机上的某个远程位置。本地文件必须位于 `/var/common` 目录中。

语法

```
system file secure-copy hostname username path filenames filenames ...
```
其中，*hostname* 指定目标远程主机的名称或 IP 地址，*username* 指定远程主机上用户的名称，*path* 指定远程主机上的目标路径， *filenames* 指定要传输的本地文件；文件名以空格分隔。

示例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

生成供思科进行分析的故障排除数据。

Access

配置

语法

```
system generate-troubleshoot
```

此语法显示可选参数列表以指定应显示哪些故障排除数据。

示例

```
> system generate-troubleshoot
```

ldapsearch

使用户对指定 LDAP 服务器执行查询。请注意，所有参数均为必需。

Access

配置

语法

```
system ldapsearch host port baseDN userDN basefilter
```

其中，host 指定 LDAP 服务器域，port 指定 LDAP 服务器端口，baseDN 指定要在其之下进行搜索的 DN（可分辨名称），userDN 指定绑定到 LDAP 目录的用户的 DN，basefilter 指定要搜索的一个或多个记录。

示例

```
> system ldapsearch ldap.example.com 389 cn=users,

dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

移除 `expert` 命令并访问设备上的 bash SHELL。

注意 没有支持部门提供的修复程序，就无法撤销此命令。请谨慎使用。

Access

配置

语法

```
system lockdown-sensor
```

示例

```
> system lockdown-sensor
```

nat rollback

将系统恢复为之前应用的 NAT 配置。此命令在 NGIPSv 或 ASA FirePOWER 上不可用。不能对堆栈或高可用性对中的设备使用此命令。

Access

配置

语法

```
system nat rollback
```

示例

```
> system nat rollback
```

reboot

重新启动设备。

Access

配置

语法

```
system reboot
```

示例

```
> system reboot
```

restart

重新启动设备应用程序。

Access

配置

语法

```
system restart
```

示例

```
> system restart
```

shutdown

关闭设备。此命令不适用于 ASA FirePOWER 模块。

Access

配置

语法

```
system shutdown
```

示例

```
> system shutdown
```