Common Criteria Supplemental User Guide for Cisco NGIPSv 7.0 with FMC/FMCv 7.0

Version 1.0

May 16, 2023

© 2023 Cisco Systems, Inc. All rights reserved.

Prepared by:

Cisco Systems, Inc.,

170 West Tasman Drive, San Jose,

CA 95134-1706 USA

© 2023 Cisco Systems, Inc. All rights reserved.

Table of Contents

© 2023 Cisco Systems, Inc. All rights reserved.

© 2023 Cisco Systems, Inc. All rights reserved.

1 Introduction

The Cisco Firepower Next-Generation Intrusion Prevention System virtual (NGIPSv) combines both SNORT® open source and proprietary technology. The system is used to filter and monitor all incoming and outgoing network traffic for security events and violations. All packets on the monitored network are scanned, decoded, preprocessed and compared against a set of access control and intrusion rules to determine whether inappropriate traffic, such as system attacks, is being passed over the network. The system then notifies a designated administrator of these attempts and/or blocks the malicious traffic. The system generates these alerts when deviations of the expected network behavior are detected and when there is a match to a known attack pattern.

In addition, the system also provides real-time contextual awareness, advanced malware protection, and security intelligence for blocking malicious URLs and IP addresses. The Cisco NGIPSv System is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. In a typical deployment, multiple traffic-sensing managed devices (i.e., sensors) installed on network segments monitor traffic for analysis and report to a managing Firepower Management Center (FMC). Deployed inline, devices can affect the flow of traffic.

The Firepower Management Center provides a centralized management console with web interface that you can use to perform administrative, management, analysis, and reporting tasks. The CLI on the devices are used to perform setup, basic analysis, and configuration tasks.

This document is a supplement to the Cisco administrative guidance, which is comprised of the installation and administration documents identified in section 1.3. This document supplements those manuals by specifying how to install, configure and operate this product in the Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Network Device collaborative Protection Profile (NDcPP) and meets all the required guidance assurance activities from the NDcPP.

© 2023 Cisco Systems, Inc. All rights reserved.

1.1 Common Criteria (CC) Evaluated Configuration

The following sections describe the scope of evaluation, required configuration, assumptions, and operational environment that the system must be in to ensure a secure deployment. To ensure the system is in the CC evaluated configuration, the users must do the following:

- Configure all the required system settings and default policy as documented in this guide.
- Disable all the features that would violate the NDcPP and MOD_IPS_V1.0 requirements or would make the system vulnerable to attacks as documented in this guide.
- Ensure all the environmental assumptions in section 2 are met.
- Ensure that your operational environment is consistent with section 2.
- Follow the guidance in this document.

Accessing the shell should be limited to authorized administrators for pre-operational setup (for example, Security Technical Implementation Guide (STIG) compliance testing), for troubleshooting, or regular maintenance.

In addition, the PROTECTION license must be purchased and activated to use all the IPS features to meet the IPS Extended Package requirements. Optionally, to use the malware protection feature MALWARE license is required and to use URL filtering capability URL FILTERING license is required.

© 2023 Cisco Systems, Inc. All rights reserved.

Scope of Evaluation

The list below identifies features or protocols that are not evaluated and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration. It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion.

The following features and protocols are not evaluated:

- VPN Gateway with IPsec – This feature is not evaluated as part of the evaluation. The VPN Gateway Extended Package is not claimed in this evaluation.
- External Authentication Servers – The NDcPP and MOD_IPS_V1.0 does not require external authentication servers. However, if they are used, the connection between the TOE and server must be protected by the approved security protocol.
- Shell Access – The shell access is only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting.
- Timeout Exemption Option – The use of the "Exempt from Browser Session Timeout" setting is not permitted. This allows a user to be exempted from the inactivity timeout feature.
- REST API – This feature is not evaluated as part of the evaluation. REST API relies on HTTPS as the underlying communication protocol and can be used to build a management interface. This feature is not tested and is out of scope.
- Modbus and DNP3 SCADA preprocessors – These features are not evaluated as part of the evaluation. These features are related to detection of traffic anomalies, but they are beyond the scope of testing defined in MOD_IPS_V1.0.
- HTTP and Telnet for management purposes – HTTP and Telnet pass credentials in clear text and are disabled in the evaluated system.
- SNMPv3 for management purposes – SNMPv3 is supported but is not permitted for management—only for sending SNMP traps for alerting.
- Any features not associated with SFRs in claimed NDcPP and MOD_IPS_V1.0 – NDcPP and MOD_IPS_V1.0 forbids adding additional requirements to the Security Target (ST). If additional functionalities are mentioned in the ST, it is for completeness only.

© 2023 Cisco Systems, Inc. All rights reserved.

1.2 References

TOE (Target of Evaluation) References

Cisco NGIPSv System[1] running Version 7.0 with FMC 7.0

Table 1: TOE Series and Models

Firepower Management Center (FMC) • FMC1000-K9 • FMC2500-K9 • FMC4500-K9 • FMC1600-K9 • FMC2600-K9 • FMC4600-K9; and • FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3
NGIPSv • NGIPSv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3.

[1] In the evaluated configuration, the TOE must comprise of at least one FMC and one or more devices all running version 7.0

© 2023 Cisco Systems, Inc. All rights reserved.

Documentation References

The Cisco Firepower System documentation set includes online help and PDF files.

The following product guidance documents are provided online or by request:

Cisco Firepower Release Notes, Version 7.0, updated August 10, 2022 *https://www.cisco.com/c/en/us/td/docs/security/firepower/70/relnotes/firepower-release-notes-700.html*
Firepower Management Center Configuration Guide, Version 7.0, updated September 20, 2022 [FMC-CG] *https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html*
Cisco Firepower NGIPSv Quick Start Guide for VMware, updated August 16, 2016 *https://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick.html*
Cisco Common Criteria Supplemental User Guide [This Document]

Online help can be accessed in two ways:

- By selecting Product Support > Select a Product
- Search for the Product

The most up-to-date versions of the documentation can be accessed on the Cisco Support web site (http://www.cisco.com/c/en/us/support/index.html).

© 2023 Cisco Systems, Inc. All rights reserved.

2 Operational Environment

This section describes the components in the environment and assumptions made about the environment.

2.1 Operational Environment Components

The system can be configured to rely on and utilize a number of other components in its operational environment.

- Management Workstation (**Required**) – The system supports Command Line Interface (CLI) and web access and as such an administrator would need a terminal emulator or SSH client (supporting SSHv2) or web browser (supporting HTTPS) to utilize those administrative interfaces.

  NOTE! The management network should be physically or logically separated (e.g., VLANs) from the monitored network.

- Audit server (**Required**) – The system can be configured to deliver audit records to an external log server.

  NOTE! It is recommended that the audit server is physically or logically separated (e.g., VLANs) from the monitored network. It can be on the same trusted internal network as the management network.

- Authentication servers – The system can be configured to utilize external authentication servers.

  WARNING! This use of external authentication server is not allowed in the evaluated configuration unless the channel is securely protected either logically (e.g., VLAN) or physically (e.g., dedicated connection).

- Certificate Authority (CA) server – The system can be configured to import X.509v3 certificates from a CA, e.g., for TLS connection to syslog server.
- NTP server – The system can be configured to obtain time from a trusted time source. The use of an NTP server is outside the scope of this evaluation.
- DNS server – The system supports domain name service in the network.

© 2023 Cisco Systems, Inc. All rights reserved.

2.2 Environmental Assumptions

The assumptions state the specific conditions that are expected to be met by the operational environment and administrators.

Table 2: Operational Environment Security Measures

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Administrators must ensure the system is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Administrators must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the system.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	Administrators must configure the security devices in the Operation environment of the TOE to secure the network.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Administrators must be properly trained in the usage and proper operation of the system and all the enabled functionality. These administrators must follow the provided guidance.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must regularly update the system to address any known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must protect their access credentials where ever they may be.

© 2023 Cisco Systems, Inc. All rights reserved.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.COMPONENTS_RUNNING	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

© 2023 Cisco Systems, Inc. All rights reserved.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.	The Administrator ensures that the attack surface of the VMs is reduced to its minimum. All the virtual networking, management channels and audit reporting that are not essential to the ND functionality are eliminated.
OE.CONNECTIONS	TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Note: The TOE contains SSD storage media in all hardware appliances and could also contain SSD storage on an NGIPSv and FMCv (the underlying Cisco UCS server hardware supports SSD storage options). SSD storage devices use wear-leveling that could result in blocks of residual data remaining when the SSD marks worn blocks as inactive. When these TOE components are being decommissioned, TOE administrators should follow their own organizational security policies and guidelines for destruction of sensitive data on wear-leveling SSD storage media.

© 2023 Cisco Systems, Inc. All rights reserved.

3 Before Installation

Before you install your appliance, Cisco highly recommends that the users must consider the following:

- Locate the Cisco Firepower System appliance in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the Cisco appliance.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access. This management interface is separate from the data interface described in the section “Passive vs Inline”.
- Identify the specific management workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using the Access Lists feature.
- To safeguard the FMC, user must deploy the FMC on a protected internal network. Although the FMC is configured to have only the necessary services and ports available, user must make sure that attacks cannot reach it from outside the access control.
- Connect the management interface of managed devices to the same protect internal network as the FMC. This allows the administrators to securely control the device from the FMC and aggregate the event data generated on the managed device’s network segment.
- By default, several ports are open to allow the system to take advantage of additional features and functionality. The following table lists these ports. Note that DHCP on ports 67 and 68 is disabled by default.

Ports	Description	Protocol	Direction	Open the port to …
22	SSH	TCP	Bidirectional	Allow a secure remote connection to the appliance.
25	SMTP	TCP	Outbound	Send email notices and alerts from the appliance.
53	DNS	TCP	Outbound	Use DNS.
67, 68	DHCP	UDP	Outbound	Use DHCP. Disabled by default.
161, 162	SNMP	UDP	Bidirectional (161); Outbound (162)	Provide access if you enabled SNMP polling (inbound) and SNMP traps (outbound).
443	HTTPS	TCP	Bidirectional	Allow a secure remote connection to the appliance. **Required** Download software updates.
514	SYSLOG	UDP	Outbound	Send alerts to a remote syslog server. The remote syslog server must allow port 6514 to be opened.
8305	TLS	TCP	Bidirectional	Allow for device management. **Required**

© 2023 Cisco Systems, Inc. All rights reserved.

Audience

This document is written for administrators configuring the Cisco Firepower system running software version 7.0. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you are trained to use the Internet and its associated terms and applications.

© 2023 Cisco Systems, Inc. All rights reserved.

4 Assurance Activity Configuration

This section has the required guidance and settings as specified in the NDcPP and MOD_IPS_V1.0.

4.1 Logging into the Appliance

4.1.1 Login to Web Interface

The FMC has a web interface that administrators can use to perform administrative, management, and analysis tasks. The WebUI (GUI) is only available on FMC, NGIPSv does not have its own GUI and is managed via FMC. Administrators can access the web interface by logging into the appliance using a web browser. The following table lists web browser compatibility.

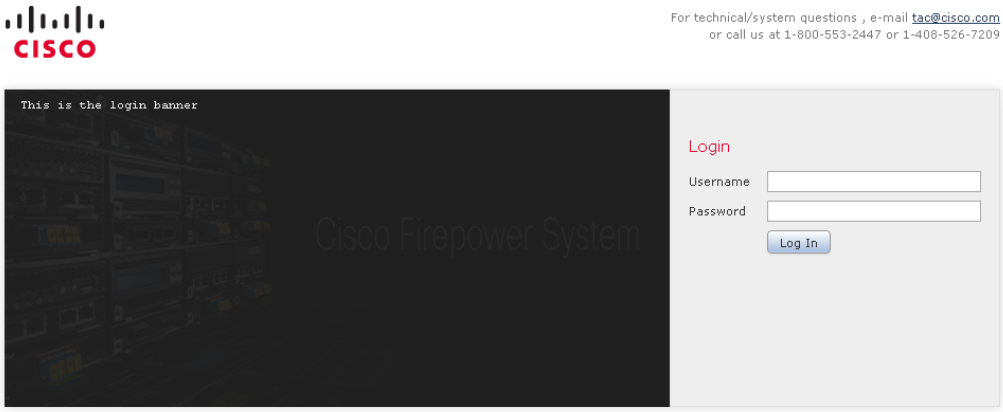
Browser	Required Enabled Options and Settings
Firefox 52.0 and later	JavaScript, cookies, Transport Layer Security (TLS) v1.1 and 1.2
Google Chrome 57 and later	JavaScript, cookies Note: The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add a self-signed certificate to the trust store of the browser/OS or use another web browser.

In addition, for managed devices only, a CLI is provided to manage the devices. This interface provides only a subset of the operations provided by the web interface. It is highly recommended that the users use the web interface over the CLI. All appliances, regardless of series or models, can access the shell bash (different from CLI) but this will remove the appliances from the evaluated configuration.

If you are the first administrator to log into a Firepower appliance (physical or virtual) after it is installed, you must log in using the factory-default administrative (**admin**) account to complete the initial setup process, including changing the default password. The default password for Firepower Services and FMC is Admin123. By default, Firepower administrative sessions will automatically timeout after 60 minutes of inactivity.

1. Direct your web browser to https://hostname/, where hostname corresponds to the host name of the appliance. You can also use the IP address of the appliance.

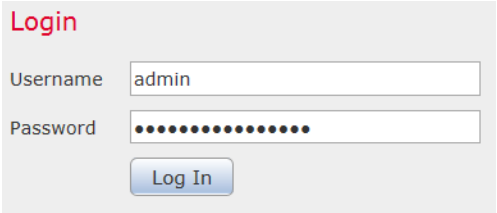
   The Login page appears.



© 2023 Cisco Systems, Inc. All rights reserved.

NOTE! Observe the login banner under the Cisco Firepower logo.

2. In the **Username** and **Password** fields, type your username and password.

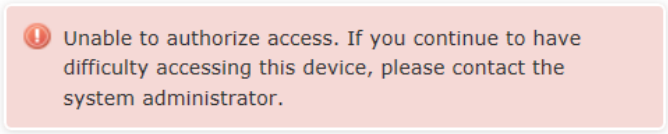


NOTE! Observe the password is not displayed.

3. Click **Log In**.

   The default start page appears if the authentication is successful.

   If authentication fails, the following error message is displayed:



Audit Record:

2013-02-26 17:52:01	admin	Login	Login Success	10.4.10.227
2013-02-26 17:51:55	admin	Login	Login Failed	10.4.10.227

4.1.2 Login to CLI Remotely

1. Direct an SSHv2 connection to the appliance at ***hostname***, where hostname corresponds to the host name of the appliance. You can also use the IP address of the appliance.

   The **login in:** command prompt appears.

2. Type your username and press **Enter**.

   The login banner and **Password:** prompt appear.

© 2023 Cisco Systems, Inc. All rights reserved.

3. Type your password and press **Enter**.

NOTE! Observe the password is not displayed.

The standard command prompt appears if the authentication is successful.

If authentication fails, the following error message is displayed:

Access denied

Audit Record:

Jun 11 2013 15:41:15 Quince sshd[4501]: pam_unix(sshd:session): session closed for user admin

Jun 11 2013 15:40:38 Quince sshd[4501]: pam_unix(sshd:session): session opened for user admin by (uid=0)

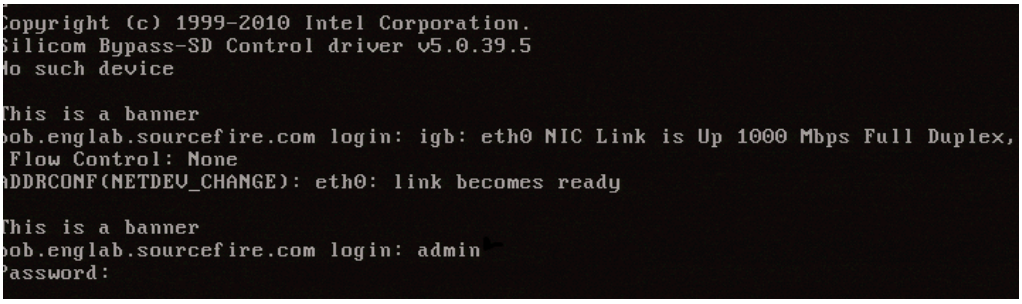
Jun 11 2013 15:40:38 Quince sshd[4501]: Accepted keyboard-interactive/pam for admin from 10.4.11.111 port 56817 ssh2

Note: Search for “sshd:session”

4.1.3 Login to CLI Locally

1. Use the serial or console connection to the appliance.

   The login banner and **<hostname> login:** prompt appear.



2. Type your username and press **Enter**.

   The **Password:** prompt appears.

3. Type your password and press **Enter**.

© 2023 Cisco Systems, Inc. All rights reserved.

NOTE! Observe the password is not displayed.

The standard command prompt appears if the authentication is successful.

If authentication fails, the following error message is displayed:

Login incorrect

Audit Record:

```
Jun 11 2013 15:54:27 Quince login[5194]: pam_unix(login:session): session opened for user admin by LOGIN(uid=0)
Jun 11 2013 15:54:22 Quince login[2329]: pam_unix(login:session): session closed for user admin
```

Note: Search for “login:session”

4.1.4 Logout

1. For web session, from the drop-down list under your username, select **Log Out**.
2. Close the web browser.
3. For CLI, type the command ***exit***.

IMPORTANT! For security purpose, always logout as instructed above when you are finished using the management interface. Do NOT rely solely on the inactivity timeout feature.

Audit Record:

2013-02-26 18:26:30	admin	Logout	Logout Success	10.4.10.227

© 2023 Cisco Systems, Inc. All rights reserved.

4.2 Auditable Events

Each appliance generates an audit event for each user interaction with the web interface and CLI command executed. Each event includes at least a timestamp, the user name of the user whose action generated the event, a source IP, and text describing the event. The common fields are described in the table below. The appliance includes an internal log database implementation that can be used to store and review audit records locally. However, the internal log only stores a default of 100,000 entries in the local database (to configure the size, go to System > Configuration > Database, and click on "Audit Event Database"). When the audit log is full, the oldest audit records are overwritten by the newest audit records. In addition, the appliance also includes a local syslog storage in /var/log/messages. Similar to the audit log, when the syslog is full, the oldest syslogs messages are overwritten by the newest one.

For audit log, the events are stored in partitioned event tables. The TOE will prune (i.e., delete) the oldest partition whenever the oldest partition can be pruned without dropping the number of events count below the configured event limit. Note this limit defaults to 10,000 if you set it any lower. For example, if you set the limit to 10,000 events, the events count may need to exceed 15,000 events before the oldest partition can be deleted. For syslog, the logs are stored in /var/log/messages and are rotated daily or when the log file size exceeds 25 MB. After the maximum number of backlog files is reached, the oldest is deleted and the numbers on the other backlogs file are incremented.

Web UI

Field	Description
Time	Time and date that the appliance generated the audit record.
User	User name of the user that triggered the audit event.
Subsystem	Menu path the user followed to generate the audit record. For example, **System > Monitoring > Audit** is the menu path to view the audit log. In a few cases where a menu path is not relevant, the Subsystem field displays only the event type. For example, **Login** classifies user login attempts or **Command Line** classifies a command executed.
Message	Action the user performed. For example, **Page View** signifies that the user simply viewed the page indicated in the Subsystem, while **Save** means that the user clicked the Save button on the page. If the Subsystem field is **Command Line**, the Message field will show the command executed. Changes made to the Cisco 3D System appear with a compare icon ( ) that you can click to see a summary of the changes.
Source IP	IP address of the host used by the user.

CLI

© 2023 Cisco Systems, Inc. All rights reserved.

Field	Description
Time	Time and date that the appliance generated the audit record.
Event Type	The type of action.
Subsystem	Command Line
Actor	User name of the user that executed the command.
Message	The command that was executed.
Result	Success or Failure
Source IP	IP address of the host used by the user.
Destination IP	IP address of the appliance.

Syslog

© 2023 Cisco Systems, Inc. All rights reserved.

Field	Description
Date	Date that the appliance generated the audit record.
Time	Time that the appliance generated the audit record.
Subsystem	This identifies the subsystem, process, or daemon that generates the audit record. This information is sometime included as part of the Message field.
Message	Identify the event type, user name (if applicable), outcome (if applicable), and IP address (if applicable). For example, **[SSH session establishment and termination]** *Mar 12 2013 13:49:30 FMCv sshd[20605]: pam_unix(sshd:session): session opened for user admin by (uid=0)* *Mar 12 2013 11:10:04 FMCv sshd[7456]: Accepted keyboard-interactive/pam for admin from 172.16.16.248 port 49662 ssh2* *Mar 12 2013 13:49:42 FMCv sshd[20605]: pam_unix(sshd:session): session closed for user admin* **[Trying to connect with SSHv1 only (SSH failure)]** *Mar 12 2013 11:26:19 FMCv sshd[15102]: Did not receive identification string from 172.16.16.248* [Trying to connect with diffie-hellman-group1-sha1 only (SSH failure)] *May 25 2016 18:15:49 FMCv sshd[2775]: fatal: Unable to negotiate with 172.16.16.126: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1 [preauth]* **[SSH rekey event audit]** *Jul 28 17:34:55 NGIPSv sshd[31989]: Outbound-ReKey for172.16.16.105:50244* NOTE: Filter “system” in the syslog. **[TLS session establishment and termination]** *Jul 26 00:20:20 FMC syslog-ng[18245]: Syslog connection established; fd='15', server='AF_INET(172.18.152.193:6514)', local='AF_INET(0.0.0.0:0)'* NOTE: Filter “syslog-ng” in the syslog. **[Trying to connect with mismatched ciphersuites (TLS failure)]** *Jul 25 23:13:20 NGIPS syslog-ng[22691]: SSL error while reading stream; tls_error='SSL routines:ssl3_get_client_hello:no shared cipher'* **[Unable to determine revocation status (X509 failure)]** *Feb 22 18:42:00 amp7150 syslog-ng[21468]: X509 Certificate Validation; depth='0', ok='0', errnum='3', error='unable to get certificate CRL'* **[System shutdown]** *Jul 26 2016 16:49:10 FMCv shutdown[18868]: shutting down for system reboot* **[System startup]** *Jul 26 2016 16:49:10 FMCv pmmon Crypto Self Tests Succeed (0)* *Jul 26 2016 16:49:11 FMCv pmmon Starting the Process Manager...*

© 2023 Cisco Systems, Inc. All rights reserved.

Message	**[Handshake failure]** *Jul 3 15:22:50 fs750 syslog-ng[9535]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure'* **[Decryption filed or bad record MAC]** *Jul 3 15:32:50 fs750 syslog-ng[12688]: SSL error while writing stream; tls_error='SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac'* [**Digest check failed]** *Jul 3 15:32:03 fs750 syslog-ng[12439]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_finished:digest check failed'* **[Wrong SSL version]** *Jul 3 15:29:16 fs750 syslog-ng[11102]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_hello:wrong ssl version'* **[Unknown cipher returned]** *Jul 3 15:28:38 fs750 syslog-ng[10210]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_hello:unknown cipher returned'* **[bad signature]** *Jul 3 15:29:53 fs750 syslog-ng[11362]: SSL error while writing stream; tls_error='rsa routines:RSA_private_encrypt:bad signature'* **[decrypt error]** *Jul 3 15:34:51 fs750 syslog-ng[13251]: SSL error while writing stream; tls_error='SSL routines:ssl3_read_bytes:tlsv1 alert decrypt error'* **[Certificate Subject mismatch]** Jan 06 2017 10:25:38 firepower syslog-ng[17493]: Certificate subject does not match configured hostname; ,hostname='192.168.144.243', certificate='testlab1v.ctn.gss.com' [**Certificate Expired]** *Jul 3 16:42:38 fs750 syslog-ng[29762]: Certificate validation failed; subject='emailAddress=server-rsa-rsa-expired@example.com, CN=test.example.com, O=Cisco, L=RTP, ST=NC, C=US', issuer='emailAddress=subsubca-rsa-rsa@example.com, CN=Example RSA Sub Sub CA, O=Cisco, L=RTP, ST=NC, C=US', error='certificate has expired', depth='0'* **[Certificate Revoked]** *Jun 29 21:45:03 fs750 syslog-ng[23414]: Certificate validation failed; subject='emailAddress=subca-rsa-rsa@example.com, CN=Example RSA Sub CA, O=Cisco, L=RTP, ST=NC, C=US', issuer='CN=Example RSA Root CA, emailAddress=rootca-rsa@example.com, O=Cisco, L=RTP, ST=NC, C=US', error='certificate revoked', depth='2'* **[CRL is not yet valid]** *Jun 29 21:44:03 fs750 syslog-ng[23414]: Certificate validation failed; subject='emailAddress=server-rsa-rsa@example.com, CN=test.example.com, O=Cisco, L=RTP, ST=NC, C=US', issuer='emailAddress=subsubca-rsa-rsa@example.com, CN=Example RSA Sub Sub CA, O=Cisco, L=RTP, ST=NC, C=US', error='CRL is not yet valid', depth='0'*

© 2023 Cisco Systems, Inc. All rights reserved.

Message	**[Establishing a Syslog Connection]** *Jan 26 00:21:41 fs750 syslog-ng[31597]: Syslog connection established; fd='15', server='AF_INET(192.168.144.243:6514)', local='AF_INET(0.0.0.0:0)'* **[Terminating a Syslog Connection]** *Jan 26 00:20:41 fs750 syslog-ng[31597]: Syslog connection broken; fd='15', server='AF_INET(192.168.144.243:6514)', time_reopen='60'* **[Failures of a Syslog Connection]** *Jan 26 00:20:41 fs750 syslog-ng[31597]: Syslog connection broken; fd='15', server='AF_INET(192.168.144.243:6514)', time_reopen='60'*

Examples of audit log events for web interface and CLI:

Time	User	Subsystem	Message	Source IP
2013-02-27 12:03:29	admin	Overview > Dashboards > Summary Dashboard	Page View	10.2.100.243
2013-02-27 12:03:24	admin	Audit Log Events	Delete	10.2.100.243
2013-02-27 12:03:24	admin	System > Monitoring > Audit	Page View	10.2.100.243
2013-02-27 12:02:15	admin	System > Monitoring > Audit	Page View	10.2.100.243
2013-02-27 12:01:30	admin	Login	Login Success	10.2.100.243
2013-02-27 12:01:16	admin	System > Local > Configuration > Time	Page View	10.2.100.243
2013-02-27 12:01:10	admin	Logout	Logout Success	10.2.100.243
2013-02-27 12:01:01	admin	Operations > System Settings	Save	10.2.100.243
2013-02-27 12:00:53	admin	System > Local > User Management > Users	Page View	10.2.100.243
2013-02-27 12:00:52	admin	System > Local > User Management > Users	Edited user - tester:221	10.2.100.243
2013-02-27 12:00:39	admin	System > Local > User Management > Users > Edit User	Page View	10.2.100.243

© 2023 Cisco Systems, Inc. All rights reserved.

```
Audit Log Output:
 time                  :  1361985099 (Wed Feb 27 17:11:39 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- show audit-log
 result                :  Success
 action_source_ip      :  10.2.100.243
 action_destination_ip :  Default Target IP
-----------------------------------------------------------
 time                  :  1361985092 (Wed Feb 27 17:11:32 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- configure gui Enable
 result                :  Success
 action_source_ip      :  10.2.100.243
 action_destination_ip :  Default Target IP
-----------------------------------------------------------
 time                  :  1361985072 (Wed Feb 27 17:11:12 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- show time
 result                :  Success
 action_source_ip      :  10.2.100.243
 action_destination_ip :  Default Target IP
-----------------------------------------------------------
 time                  :  1361985045 (Wed Feb 27 17:10:45 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- configure password
 result                :  Success
 action_source_ip      :  10.2.100.243
 action_destination_ip :  Default Target IP
```

Samples of audit messages viewable via the FMC WebUI are shown in screenshots throughout this document in sections describing configuration actions relevant to the auditable actions. Samples text-based audit messages, as would be seen on a syslog server, are listed in a table at the end of this section. The FMC WebUI audit log screenshots are presented in this document in the format shown here:

Audit Record:

Actual audit record screenshot

Audit Record Syntax:

<date><time><user><message/action><result of action><source IP>

CLI Audit Log Syntax:

<date><time><type><subsystem><user><message><result><source IP><destination IP>

The connection and intrusion events (hereafter, referred to as events) are generated by the “log” operation in the rule. The events are default to 100,000 entries size each (200,000 total). However, the

© 2023 Cisco Systems, Inc. All rights reserved.

internal database stores a maximum of 10,000,000 entries (depending on FMC models) and a minimum of 10,000 entries in the local database (to configure the size, go to System > Configuration > Database, and click on “Intrusion Event Database” or “Connection Database”). When the events log is full, the oldest events are overwritten by the newest events.

The following information is associated with each event in Table View mode:

Events

Field	Description
Date	Time and date that the appliance generated the event record.
Access Control Rule	The access control rule that triggered the event.
Action	The configured action of the rule.
Initiator IP	The source IP address of the packet that triggered the event.
Responder IP	The destination IP address of the packet that triggered the event.
Source Port/ ICMP Type	The source port (for TCP and UDP) or ICMP type for IP of the packet that triggered the event.
Destination Port/ ICMP Code	The destination port (for TCP and UDP) or ICMP code for IP of the packet that triggered the event.
Protocol	The protocol of the packet that triggered the event.
Ingress Interface	The incoming interface of the packet.
Egress Interface	The outgoing interface of the packet.

Examples of events for access control rules:

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2013-04-08 14:51:33		Block	IP Block	10.22.35.100		176.65.80.2	ITA	External	Internal	30845 / udp	58117 / udp
2013-04-08 14:51:31		Block	IP Block	10.22.240.17		65.49.70.243	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:51:18		Block	IP Block	10.5.32.68		64.6.144.6	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:51:18		Block	IP Block	10.5.32.177		65.49.70.243	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:51:04		Block	IP Block	10.5.56.143		64.6.144.6	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:50:59		Block	IP Block	10.5.59.62		65.49.70.244	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:50:58		Block	IP Block	10.5.32.112		4.28.136.39	CAN	External	Internal	62906 / tcp	80 (http) / tcp
2013-04-08 14:50:58		Block	IP Block	10.5.60.86		64.6.144.6	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:50:53		Block	IP Block	10.5.11.104		38.101.77.21	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:50:50		Block	IP Block	10.5.59.102		64.6.144.6	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
2013-04-08 14:50:39		Block	IP Block	10.5.31.73		38.101.77.21	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp

Examples of connection events:

Examples of intrusion events:

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Servers | Host Attributes | More

Message	Priority	Classification	Count
FRAG3_TINY_FRAGMENT (123:13)	medium	Attempted Denial of Service	2
FRAG3_ANOMALY_OVLP (123:8)	low	Generic Protocol Command Decode	1

Page 1 of 1 | Displaying rows 1–2 of 2 rows

© 2023 Cisco Systems, Inc. All rights reserved.

4.2.1 Audit Messages Generated by Firepower Services

SFR	Auditable Event	Audit Messages Generated by Firepower Services
FAU_GEN.1	Start up and shutdown of audit functions	**Start Up** *{date-time} {hostname}* SF-IMS[9917]: [9917] init script:system [INFO] pmmon Starting the Process Manager... **Shutdown** *{date-time} {hostname}* shutdown[20717]: shutting down for system reboot
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	**Enabling** *{date-time} {hostname}* SF-IMS[10512]: [7308] sftunnelId:sf_ssl [INFO] Peer *{ip-address}* registration is complete remotely **Disabling** *{date-time} {hostname}* SF-IMS[10470]: [10511] sftunnelId:sf_connections [INFO] <<<<<<<<<<<<<<<<<<<< ShutDownPeer fmcv >>>>>>>>>>>>>>>>>>>>
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	*Not Applicable.*
FCS_SSHS_EXT.1	Failure to establish an SSH session	*{date-time} {hostname} sshd[27611]:* Unable to negotiate with *{ip-address}* port 58748: no matching key exchange method found. Their offer: *{key-exchange-method}*,ext-info-c [preauth]
	Successful SSH rekey	*{date-time} {hostname}* sshd[27736]: Outbound-ReKey for *{ip-address}:37100*
FCS_TLSC_EXT.2	Failure to establish an TLS Session	*Syslog* *General Failure:* *{date-time} NGIPSv syslog-ng[24047]: SSL error while writing stream; tls_error='SSL routines:ssl3_read_bytes:sslv3 alert handshake failure', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Invalid Purpose:* *{date-time} NGIPSv syslog-ng[8949]: X509 Certificate Validation; depth='0', ok='0', errnum='26', error='unsupported certificate purpose'* *Uknown Cipher:* *{date-time} ngipsv syslog-ng[8519]: SSL error while writing stream; tls_error='SSL routines:set_client_ciphersuite:unknown cipher returned', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Invalid TLS Version:*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
		{date-time} ngipsv syslog-ng[8519]: SSL error while writing stream; tls_error='SSL routines:ssl_choose_client_version:unsupported protocol', location='/etc/syslog-ng.d/syslog-tls.conf:17:9' *Wrong Curve:* *{date-time} ngipsv syslog-ng[8519]: SSL error while writing stream; tls_error='SSL routines:tls_process_ske_ecdhe:wrong curve', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Bad Signature:* *{date-time} NGIPSv syslog-ng[8949]: SSL error while writing stream; tls_error='rsa routines::bad signature', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Certificate Validation Failure:* *{date-time} NGIPSv syslog-ng[19424]: SSL error while writing stream; tls_error='SSL routines:tls_process_server_certificate:certificate verify failed', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Identifier Match Failed:* *{date-time} ngipsv syslog-ng[29394]: Certificate subject does not match configured hostname; hostname='tl2116x.example.com'* *Bad Signature:* *{date-time} ngipsv syslog-ng[8519]: SSL error while writing stream; tls_error='rsa routines::bad signature', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Bad Finished Message:* *{date-time} ngipsv syslog-ng[8519]: SSL error while writing stream; tls_error='SSL routines:tls_process_finished:digest check failed', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Invalid CA Certificate:* *{date-time} NGIPSv syslog-ng[8949]: X509 Certificate Validation; depth='1', ok='0', errnum='24', error='invalid CA certificate'* *Corrupt ASN.1:*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
		{date-time} NGIPSv syslog-ng[8949]: SSL error while writing stream; tls_error='asn1 encoding routines:asn1_check_tlen:wrong tag', location='/etc/syslog-ng.d/syslog-tls.conf:17:9' *Expired Certificate:* *{date-time} ngipsv syslog-ng[8519]: Certificate validation failed; subject='emailAddress=server-expired-rsa@gossamersec.com, CN=tl2116x.example.com, O=GSS, L=Catonsville, ST=MD, C=US', issuer='emailAddress=subsubca-rsa@gossamersec.com, CN=subsubca-rsa, O=GSS, L=Catonsville, ST=MD, C=US', error='certificate has expired', depth='0'* *Revoked Certificate (CRL):* *{date-time} ngipsv syslog-ng[8519]: X509 Certificate Validation; depth='0', ok='0', errnum='23', error='certificate revoked'* *No CRLSign Purpose:* *{date-time} ngipsv syslog-ng[8519]: X509 Certificate Validation; depth='0', ok='0', errnum='35', error='key usage does not include CRL signing'* *Invalid Chain:* *{date-time} ngipsv syslog-ng[8519]: X509 Certificate Validation; depth='1', ok='0', errnum='20', error='unable to get local issuer certificate'* *Distributed TOE Communication (ITT):* *General Failure:* *{date-time} ngipsv SF-IMS[18299]: [18815] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed* *Invalid EKU:* *{date-time} NGIPSv SF-IMS[18299]: [18722] sftunneld:sf_ssl [WARN] Base Peer Certificate from 172.16.16.82 does not meet Cisco Common Criteria, Upgrade it to 6.1.0.* *Invalid Identifier:*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
		*{date-time} NGIPSv SF-IMS[29134]: [29380] sftunneld:sf_ssl [ERROR] CERT subject_title(*ea826d54-75a3-11ed-be21-8cb4c4033eb7) did not match connected peer uuid(ea826d54-75a3-11ed-be21-8cb4c4033eb7)* *Expired Certificate:* *{date-time} NGIPSv SF-IMS[18299]: [21295] sftunneld:sf_ssl [ERROR] err 10:certificate has expired* *Corrupt ASN.1:* *{date-time} NGIPSv SF-IMS[3637]: [3637] IDSEventProcessor:TunnelHandler [WARN] Error processing received message: General read error* *Invalid Signature:* *{date-time} NGIPSv SF-IMS[18299]: [22168] sftunneld:sf_ssl [ERROR] err 7:certificate signature failure* *Invalid CA:* *{date-time} NGIPSv SF-IMS[18299]: [22744] sftunneld:sf_ssl [ERROR] err 24:invalid CA certificate* *Invalid Chain:* *{date-time} NGIPSv SF-IMS[18299]: [21125] sftunneld:sf_ssl [ERROR] err 20:unable to get local issuer certificate*
FCS_TLSS_EXT.1	Failure to establish an TLS Session	**Distributed TOE Communication** *{date-time} {hostname}* SF-IMS[6423]: [11592] sftunneld:sf_ssl [ERROR] Accept:SSL handshake failed
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	*{date-time} {hostname}* sshd[28533]: pam_tally(sshd:auth): user *{username}* (1000) tally 4, deny 3 *{date-time} {hostname}* sshd[28533]: Failed password for *{username}* from *{ip-address}* port 50140 ssh2
FIA_PMG_EXT.1	Resetting Password	*{date-time} ngipsv sudo: admin : TTY=pts/1 ; PWD=/Volume/home/admin ; USER=root ; COMMAND=/usr/local/sf/bin/cli_usrmgr passwd testuser2*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	**SSH** *{date-time} {hostname}* sshd[27641]: Accepted keyboard-interactive/pam for *{username}* from *{ip-address}* port 58790 ssh2 *{date-time} {hostname}* sshd[16626]: error: PAM: Authentication failure for *{username}* from *{hostname}* **Console** *{date-time} {hostname}* login[1501]: pam_unix(login:session): session opened for user *{username}* by LOGIN(uid=0) *{date-time} ngipsv login[20224]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=admin*
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	See FIA_UIA_EXT.1
FIA_X509_EXT.1/ITT FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Failure: *See Failure Audits for TLSC_EXT.2.* *Trust Anchor Addition:* *<date> <time> <host> % SF-IMS [111008]: User 'enable_1' executed the 'crypto ca trustpoint rootca-rsa-no-revocation' command.* *<date> <time> <host> % SF-IMS [111010]: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'crypto ca trustpoint rootca-rsa-no-revocation'* *<date> <time> <host> % SF-IMS [111008]: User 'enable_1' executed the 'crypto ca authenticate rootca-rsa-no-revocation nointeractive' command.* *<date> <time> <host> % SF-IMS [111010]: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'crypto ca authenticate rootca-rsa-no-revocation nointeractive'* *<date> <time> <host> % SF-IMS [111008]: User 'enable_1' executed the 'crypto ca enroll rootca-rsa-no-revocation noconfirm' command.* *Trust Anchor Deletion:* *<date> <time> <host> % SF-IMS [111008]: User 'enable_1' executed the 'no crypto ca trustpoint rootca-rsa-no-revocation noconfirm' command.* *<date> <time> <host> % SF-IMS [111010]: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'no crypto ca trustpoint rootca-rsa-no-revocation noconfirm'*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	*{date-time} {hostname}* SF-IMS[31925]: [31925] *Sourcefire_3D_Device_S3_Patch-6.2.2.5-57:*000_start/100_start_messages.sh [INFO] Upgrade starting *{date-time} ngipsv SF-IMS[2650]: [2650] sftunneld:control_services [INFO] FSTREAM_STATUS: Sending back task status 'Completed'*
FMT_SMF.1	All management activities of TSF data.	Note that some audits for management functions come from either the FMC1600 or FMC Virtual since they manage the NGIPS Virtual device. Ability to administer the TOE locally and remotely: Refer to FIA_UIA_EXT.1 Ability to configure the access banner: *{date-time} 172.16.16.223 mojo_server.pl: FMCv: admin@127.0.0.1, Devices > Platform Settings > Login Banner > Modified: Custom Login Banner This is the TESTING Banner defined by Gossamer during CC evaluation testing for Sensors.#015#012#015#012History:#015#0121) originally defined 12/21/2016#015#0122) updated on 02/25/2021 > This is the TESTING Banner defined by Gossamer during CC evaluation testing for Sensors.#015#012#015#012History:#015#0121) originally defined 12/21/2016#015#0122) updated on 02/25/2023#012, Save#000x0a#000x00* *{date-time} 172.16.16.223 mojo_server.pl: FMCv: admin@127.0.0.1, Devices > Platform Settings > Platform Edit, Save#000x0a#000x00"* Ability to configure the session inactivity time before session termination or locking: *{date-time} 172.16.16.223 mojo_server.pl: FMCv: admin@127.0.0.1, Devices > Platform Settings > User Interface > Modified: cli_setting_session_timeout 10 > 101#012, Save#000x0a#000x00* *{date-time} 172.16.16.223 mojo_server.pl: FMCv: admin@127.0.0.1, Devices > Platform Settings > User Interface > Modified: CLI Timeout (Minutes) 10 > 101#012, Save#000x0a#000x00"*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
		Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates: Ability to update the TOE: *Refer to update audits found in the FPT_TUD_EXT.1 section of the audit table.* Ability to Verify Updates: *{date-time} FMCv sudo: www : TTY=unknown ; PWD=/usr/local/sf/htdocs/admin ; USER=root ; COMMAND=/usr/local/sf/bin/verify_signed_image.sh -m -s /var/tmp/sigstatus_Y5JV0wsd -i /var/sf/updates/Cisco_Firepower_NGIPS_Virtual_Upgrade-7.0.5-72.sh.REL.tar"* Ability to configure the authentication failure parameters for FIA_AFL.1 *{date-time} ngipsv sudo: admin : TTY=pts/1 ; PWD=/Volume/home/admin ; USER=root ; COMMAND=/usr/local/sf/bin/cli_usrmgr maxf testuser2 3* Ability to configure the cryptographic functionality *Ciphers are configured by CC compliance mode. Instructions for enabling CC mode are found in the AGD.* Ability to importX.509v3 certificates to the TOE's trust store *{date-time} ngipsv sudo: admin : TTY=pts/0 ; PWD=/Volume/home/admin ; USER=root ; COMMAND=/usr/local/sf/bin/sfcli.pl import audit_cert* Ability to configure the interaction between TOE components; *See audits for FCO_CPC_EXT.1* Ability to manage the trusted public keys database; *{date-time} ngipsv cmd_log.pl: 'firepower': admin@172.16.16.82, Command Line, Executed expert- command* Ability to re-enable an Administrator account;

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
		{date-time} ngipsv sudo: admin : TTY=pts/1 ; PWD=/Volume/home/admin ; USER=root ; COMMAND=/usr/local/sf/bin/cli_usrmgr unlock testuser2 Ability to set the time which is used for time-stamps; See audits for FPT_STM_EXT.1 Ability to configure the reference identifier for the peer; *See audits for FMT_SMF.1: Ability to configure the cryptographic functionality.* Ability to modify the behavior of the transmission of audit data to an external IT entity; See audits for "Ability to modify the behavior of the transmission of audit data to an external IT entity" and "Ability to configure the interaction between TOE components"
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	*{date-time} {hostname}* SF-IMS[31925]: [31925] Sourcefire_3D_Device_S3_Patch-6.2.2.5-57:000_start/100_start_messages.sh [INFO] Upgrade starting *{date-time} ngipsv SF-IMS[2650]: [2650] sftunneld:control_services [INFO] FSTREAM_STATUS: Sending back task status 'Completed'*
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	*{date-time} {hostname}* SF-IMS[18755]: ntpd:cmos [INFO] *Updated system clock by offset of 0 seconds* *{date-time} {hostname}* ntpd[19557]: ntpd 4.2.8p11*@1.3728-o {date-time} (1):* Starting *{date-time} {hostname}* ntpd[19557]: Command line: /usr/bin/ntpd -n -p /var/run/ntpd.pid -c /etc/ntp.conf -I lo -I eth0 eth0 *{date-time} {hostname}* ntpd[19557]: proto: precision = 0.069 usec (-24) *{date-time} {hostname}* ntpd[19557]: switching logging to file /var/log/ntp.log
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	**Console** *{date-time}ngipsv login[10120]: pam_unix(login:session): session closed for user admin*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	**SSH** *{date-time} {hostname} expire-session.pl: 'firepower': admin@172.16.16.82, Session Expiration, Session terminated on pts/1 due to inactivity (admin)#000x0a#000x00*
FTA_SSL.4	The termination of an interactive session.	**SSH** *{date-time} {hostname}* sshd[27641]: pam_unix(sshd:session): session closed for user *{username}* **Console** *{date-time} {hostname}* login[9903]: pam_unix(login:session): session closed for user *{username}*
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**Established** *{date-time} {hostname}* syslog-ng[20192]: Syslog connection established; fd='52', server='AF_INET*({ip-address}:6514)',* local='AF_INET(0.0.0.0:0)' **Terminated** *{date-time} {hostname}* syslog-ng[20192]: Syslog connection broken; fd='16', server='AF_INET*({ip-address}:6514)',* time_reopen='60' **Failure** *{date-time} ngipsv syslog-ng[24047]: SSL error while writing stream; tls_error='SSL routines:ssl3_read_bytes:sslv3 alert handshake failure', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'*
FTP_TRP.1/Admin	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	**Initiation** See FIA_UIA_EXT.1 **Termination** See FTA_SSL.4 **Failure** See FCS_HTTPS_EXT.1 and FCS_SSHS_EXT.1.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**Initiation** *{date-time} {hostname}* SF-IMS[6425]: [6432] sfmbservice:sfmb_service [INFO] Established connection to peer *{ip-address}* **Termination**

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by Firepower Services
		{date-time} {hostname} SF-IMS[6425]: [11606] sfmbservice:sfmb_service [INFO] Connection closed to host *{ip-address}* **Failure** *{date-time} {hostname}* SF-IMS[6423]: [10802] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed

4.2.2 Audit Messages Generated by Firepower Management Center

SFR	Auditable Event	Audit Messages Generated by FMC
FAU_GEN.1	Start up and shutdown of audit functions	Syslog Startup: <date> <time> <host> syslog-ng[25980]: syslog-ng starting up; version='3.7.3' Syslog Stop: <date> <time> <host> syslog-ng[13011]: syslog-ng shutting down; version='3.7.3'
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Enable: <date> <time> <host>: mojo_server.pl: <host>: <user>@172.16.16.47, Devices > Device Management, Add Device - 172.16.16.221 Disable: <date> <time> <host>: mojo_server.pl: <host>: <user>@172.16.16.47, Devices > Device Management, Delete Device - fp4140ftd
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	<date> <time> <host> syslog-ng[23928]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure'
FCS_SSHS_EXT.1	Failure to establish an SSH session	*Bad Cipher:* *<date> <time> <host> sshd[30273]: Unable to negotiate with 10.6.16.46 port 46850: no matching cipher found. Their offer: aes256-ctr [preauth]* *Bad Auth Alg:* *<date> <time> <host> sshd[30885]: Unable to negotiate with 10.6.16.46 port 47588: no matching host key type found. Their offer: ecdsa-sha2-nistp521-cert-v01@openssh.com [preauth]* *Bad MAC Alg:* *<date> <time> <host> sshd[11527]: Unable to negotiate with 10.6.16.46 port 48128: no matching MAC found. Their offer: hmac-sha1-96 [preauth]* *Bad Kex Alg:* *<date> <time> <host> sshd[12992]: Unable to negotiate with 10.6.16.46 port 48538: no matching key exchange method found. Their offer: ecdh-sha2-nistp256,ext-info-c [preauth]*
	Successful SSH rekey	*{date-time} {hostname}* sshd[27951]: Outbound-ReKey for *{ip-address}:36598*
FCS_TLSC_EXT.2	Failure to establish an TLS Session	**Syslog** *Bad Cipher and General Failure:*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
		<date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:ssl3_read_bytes:sslv3 alert handshake failure', location='/etc/syslog-ng.d/syslog-tls.conf:17:9' *Invalid Purpose:* *<date> <time> <host> syslog-ng[6506]: X509 Certificate Validation; depth='0', ok='0', errnum='26', error='unsupported certificate purpose'* *Unknown/Wrong Cipher:* *<date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:set_client_ciphersuite:unknown cipher returned', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Invalid TLS version:* *<date> <time> <host> syslog-ng[23039]: SSL error while writing stream; tls_error='SSL routines:ssl_choose_client_version:unsupported protocol', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Wrong Curve:* *<date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:tls_process_ske_ecdhe:wrong curve', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'* *Certificate Verification Failure:* *<date> <time> <host> syslog-ng[17342]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed'* *ITT:* *{date-time} {hostname}* SF-IMS[9173]: [9545] sftunnelId:sf_ssl [ERROR] Connect:SSL handshake failed ***Invalid EKU:*** *<date> <time> <host> SF-IMS[27670]: [31809] sftunnelId:sf_ssl [WARN] Peer Certificate from 6658e980-71ee-11ed-8615-81a820744594 does not meet Cisco Common Criteria, Upgrade it to 6.1.0 and re-register to the manager.* ***Invalid Identifier:*** *<date> <time> <host> SF-IMS[4627]: [2604] sftunnelId:sf_ssl [ERROR] CERT subject_title(6658e980-71ee-11ed-8615-81a820744594*) did not match connected peer uuid(6658e980-71ee-11ed-8615-81a820744594)*
FCS_TLSS_EXT.1	Failure to establish an TLS Session	**HTTPS** *No Shared Cipher/Invalid Key Exchange:* *<date> <time> <host> [ssl:info] [pid 20165] SSL Library Error: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate?* *Digest Check Failed:* *<date> <time> <host> [ssl:info] [pid 15536:tid 22427868288768] SSL Library Error: error:1416C095:SSL routines:tls_process_finished:digest check failed* *Wrong Version:*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
		<date> <time> <host> [ssl:info] [pid 15536:tid 22427857782528] SSL Library Error: error:142090FC:SSL routines:tls_early_post_process_client_hello:unknown protocol *General Failure:* *<date> <time> <host> [ssl:info] [pid 17833:tid 22427853580032] [client 172.16.16.91:50570] AH02008: SSL library error 1 in handshake (server 172.16.16.116:443)* *ITT:* *<date> <time> <host> SF-IMS[19567]: [11420] sftunneld:sf_ssl [ERROR] Accept:SSL handshake failed*
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	*TLS:* *<date> <time> fmc1600 mojo_server.pl: fmc1600: testuser@127.0.0.1, Login, Login Failed* *<date> <time> mc1600 mojo_server.pl: fmc1600: Invalid User@127.0.0.1, Login, Login Failed*
FIA_PMG_EXT.1	Resetting Password	**Audit log Web GUI** *{date-time}<host> {username}* System > Local > User Management > Users, Edited user - admin19#000x0a#000x00
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Console Login Success: <date> <time> <host> login[7684]: pam_unix(login:session): session opened for user admin by LOGIN(uid=0) Console Login Failure: <date> <time> <host> login[7684]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/ttyS0 ruser= rhost= user=admin <date> <time> <host>login[7684]: FAILED LOGIN (1) on '/dev/ttyS0' FOR 'admin', Authentication failure SSH Login Success: <date> <time> <host> sshd[6518]: Accepted keyboard-interactive/pam for admin from 10.6.16.46 port 47680 ssh2 <date> <time> <host> sshd[6518]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Login Failure: <date> <time> <host> sshd[6354]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.6.16.46 user=admin <date> <time> <host> sshd[6351]: error: PAM: Authentication failure for admin from 10.6.16.46 SSH Public Key Success: <date> <time> <host> sshd[23895]: Accepted publickey for admin from 10.6.16.46 port 52474 ssh2: RSA SHA256:f0h+AIMnU4GtMnLhx4+l1TsjNL78E1XSdTZVGl6AdFU <date> <time> <host> sshd[23895]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Public Key Failure: <date> <time> <host> sshd[24147]: Operating in CiscoSSL FIPS mode\n <date> <time> <host> sshd[24147]: Postponed keyboard-interactive for admin from 10.6.16.46 port 52476 ssh2 [preauth] WebUI Success:

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
		<date> <time> <host> login.cgi: <host>: <user>@10.6.16.45, Login, Login Success WebUI Failure: <date> <time> <host> login.cgi: <host>: <user>@10.6.16.45, Login, Login Failed
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	See FIA_UIA_EXT.1
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	*TLS:* *Trust Anchor Addition:* *<date> <time> <host> SF-IMS[14865]: HTTPSCert:InstallCertificate [INFO] Cert Added: F5_client-TOE-00-rsa_rootca-rsa* *Trust Anchor Deletion:* *<date> <time> <host> SF-IMS[13985]: HTTPSCert:DeleteCertificate [INFO] Cert Deleted: F1_client-TOE-00-rsa_rootca-rsa* *Expired cert:* *<date> <time> <host> syslog-ng[5115]: X509 Certificate Validation; depth='0', ok='0', errnum='10', error='certificate has expired'* *Corrupt ASN.1:* *<date> <time> <host> syslog-ng[5403]: SSL error while writing stream; tls_error='asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag'* *Invalid Signature:* *<date> <time> <host> syslog-ng[5697]: X509 Certificate Validation; depth='0', ok='0', errnum='7', error='certificate signature failure'* *Invalid CA:* *<date> <time> <host> syslog-ng[10519]: X509 Certificate Validation; depth='1', ok='0', errnum='24', error='invalid CA certificate'* *Revoked cert:* *<date> <time> <host> syslog-ng[9301]: X509 Certificate Validation; depth='0', ok='0', errnum='23', error='certificate revoked'* *Invalid Chain:* *<date> <time> <host> syslog-ng[15124]: X509 Certificate Validation; depth='1', ok='0', errnum='19', error='self signed certificate in certificate chain'*
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate	*Trust Anchor Addition:* *<date> <time> <host> SF-IMS[14865]: HTTPSCert:InstallCertificate [INFO] Cert Added: F5_client-TOE-00-rsa_rootca-rsa* *Trust Anchor Deletion:* *<date> <time> <host> SF-IMS[13985]: HTTPSCert:DeleteCertificate [INFO] Cert Deleted: F1_client-TOE-00-rsa_rootca-rsa* *Expired cert:*

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
		<date> <time> <host> SF-IMS[28844]: [25530] sftunneld:sf_ssl [ERROR] err 10:certificate has expired *<u>Corrupt ASN.1:</u>* *<date> <time> <host> SF-IMS[28844]: [25959] sftunneld:sf_ssl [ERROR] SSL_renegotiate error: 1: error:00000001:lib(0):func(0):reason(1)* *<u>Invalid Signature:</u>* *<date> <time> <host> SF-IMS[28844]: [25984] sftunneld:sf_ssl [ERROR] err 7:certificate signature failure* *<u>Invalid CA:</u>* *<date> <time> <host> SF-IMS[28844]: [26310] sftunneld:sf_ssl [ERROR] err 24:invalid CA certificate* *<u>Invalid Chain:</u>* *<date> <time> <host> SF-IMS[1278]: [1285] sftunneld:sf_ssl [ERROR] err 20:unable to get local issuer certificate*
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	*<date> <time> <host> SF-IMS[27507]: [27507] Cisco_Firepower_Mgmt_Center_Patch-7.0.1-55 17:000_start/100_start_messages.sh [INFO] Upgrade starting*
FMT_SMF.1	All management activities of TSF data.	<date> <time> <host> platformSettingEdit.cgi: <host>: <user>@172.16.16.90, System > Local > User Management > Users, Enable user – testuser Jan 6 16:31:38 fmc1600 mojo_server.pl: fmc1600: testuser@127.0.0.1, Login, Login Success <date> <time> <host> platformSettingEdit.cgi: <host>: <user>@10.6.16.45, Devices > Platform Settings > Login Banner > Modified: Custom Login Banner This is a GCT banner to test FTA_TAB.1. > This is a GCT banner to test FTA_TAB.1 <date> <time> <host> platformSettingEdit.cgi: <host>: <user>@10.6.16.45, Shell Timeout, Browser/Shell timeout changed Ability to verify updates: <date> <time> <host> sudo: www : TTY=unknown ; PWD=/usr/local/sf/htdocs/admin ; USER=root ; COMMAND=/usr/local/sf/bin/verify_signed_image.sh -m -s /var/tmp/sigstatus_ujPyp8Pv -i /var/sf/updates/Cisco_Firepower_Mgmt_Center_Hotfix_BG-6.4.0.10-2.sh.REL.tar <date> <time> <host> user.cgi: <host>: <user>@10.6.16.45, System > Local > User Management > Users, Edited user – testuser <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: SSL IKE SA lifetime: <date> <time> <host> sfdccsm: <host>: <user>@172.16.16.81, Objects > Object Management > Ike2, edit test_policy ESP SA lifetime: <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Device > VPN > FTD S2S, Update VPN Topology Entry gct-vpn <date> <time> <host> SF-IMS[2124]: HTTPSCert:InstallCertificate [INFO] Certificate Chain added <date> <time> <host> SF-IMS[2124]: HTTPSCert:InstallCertificate [INFO] Cert Added: 010D_client-TOE-00-rsa_rootca-rsa <date> <time> <host> sudo:

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
		<date> <time> <host> platformSettingEdit.cgi: <host>: <user>@172.16.16.91, Command Line, Executed expert- command
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	*Initiation:* *<date> <time> <host> SF-IMS[27507]: [27507] Cisco_Firepower_Mgmt_Center_Patch-6.4.0.1-17:000_start/100_start_messages.sh [INFO] Upgrade starting* *Success:* *<date> <time> <host> SF-IMS[32329]: [32329] Cisco_Firepower_Mgmt_Center_Patch-6.4.0.1-17:999_finish/999_z_complete_upgrade_message.sh [INFO] Upgrade complete* *Failure:* *<date> <time> <host> SF-IMS[27569]: update.cgi:ProcessUpdateUpload [ERROR] update failed signature verification: file = Cisco_Firepower_Mgmt_Center_Patch-6.4.0.10-95.sh.REL-modified.tar* *<date> <time> <host> SF-IMS[15473]: update.cgi:ProcessUpdateUpload [ERROR] update is not a signed package: file = Cisco_Firepower_Threat_Defense_Virtual-7.0.5-72.tar.gz*
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	*<date> <time> <host> mojo_server.pl: <host>: <user>@10.6.16.47, Updated time to Thu 31 Jan 2019 04:30:00 AM EST from Wed 03 Jun 2020 02:05:31 PM EDT, Save*
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	**Console (audit log on Web GUI)** *<date> <time> <host> expire-session.pl: <host>: <user>@local, Session Expiration, Session terminated on ttyS0 due to inactivity (admin)*
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	WebUI Session Lock: <date> <time> <host> expire-session.pl: <host>: <user>@Default User IP, Session Expiration, Session expired due to inactivity (admin) SSH Session Lock: <date> <time> <host> SyslogTag:expire-session.pl: SyslogMessage:<15>Dec 27 17:57:40 fmcv expire-session.pl: fmcv: admin@172.16.16.91, Session Expiration, Session terminated on pts/0 due to inactivity (admin)
FTA_SSL.4	The termination of an interactive session.	WebUI Logout: <date> <time> <host> login.cgi: <host>: <user>@127.0.0.1, Logout, Logout Success Console Logout: <date> <time> <host> login[5660]: pam_unix(login:session): session closed for user admin SSH Logout: <date> <time> <host> sshd[7843]: Received disconnect from 10.6.16.46 port 47538:11: disconnected by user

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
		<date> <time> <host> sshd[20745]: Disconnected from user admin 172.16.16.91 port 59290
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Initiation/Establishment of Syslog over TLS sessions: <date> <time> <host> syslog-ng[4946]: Syslog connection established; fd='17', server='AF_INET(10.6.16.46:6514)', local='AF_INET(0.0.0.0:0)' Termination of Syslog over TLS sessions: <date> <time> <host> syslog-ng[4946]: Syslog connection broken; fd='17', server='AF_INET(10.6.16.46:6514)', time_reopen='60'
FTP_TRP.1/Admin	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	**Initiation** See FIA_UIA_EXT.1 **Termination** See FTA_SSL.4 **Failure** See FCS_HTTPS_EXT.1 and FCS_SSHS_EXT.1.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Initiation: <date> <time> <host> SF-IMS[19106]: [19420] sfmbservice:sfmb_service [INFO] Established connection to peer 10.6.16.221 Termination: <date> <time> <host> SF-IMS[22235]: [25609] sfmbservice:sfmb_service [INFO] Connection closed to host 10.6.16.221 Failure: <date> <time> <host> SF-IMS[9336]: [2438] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed
FMT_SMF.1/IPS	Modification of an IPS policy element.	<date> <time> <host> TR:2022-04-20T19:29:45-04:00 MSG:ActionQueueScrape.pl:<14>Apr 20 19:29:45 fmcv ActionQueueScrape.pl: fmcv: admin@127.0.0.1, Intrusion Policy > SBD.1.2 String Match Rules > rule_configs, Changed ICMP String match (1:1000039) to "Generate events" (from "Drop and generate events")
IPS_ABD_EXT.1	Inspected traffic matches an anomaly-based IPS policy.	<date> <time> <host> (null) %NGIPS-1-430003: EventPriority: High, DeviceUUID: ee5eb176-a726-11ed-82c8-bb1c5e1ba303, InstanceID: 3, FirstPacketSecond: 2023-02-15T11:46:15Z, ConnectionID: 12174, AccessControlRuleAction: Block, AccessControlRuleReason: Intrusion Block, SrcIP: 172.16.8.82, DstIP: 172.16.8.15, SrcPort: 58799, DstPort: 21, Protocol: tcp, IngressInterface: eth1, EgressInterface: eth2, IngressZone: Internal, EgressZone: External, ACPolicy: ABD.1 Anomaly Detection - THROUGHPUT, AccessControlRuleName: ABD THROUGHPUT, ConnectionDuration: 0, IPSCount: 1, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 82, ResponderBytes: 0, NAPPolicy: Net Access Policy - Common <date> <time> <host> (null) %NGIPS-0-430001: DeviceUUID: ee5eb176-a726-11ed-82c8-bb1c5e1ba303, InstanceID: 3, FirstPacketSecond: 2023-02-15T11:46:15Z, ConnectionID: 12183, SrcIP: 172.16.8.82, DstIP: 172.16.8.15, SrcPort: 5565, DstPort: 21, Protocol: tcp, IngressInterface: eth1, EgressInterface: eth2, IngressZone: Internal, EgressZone: External, Priority: 1, GID: 1, SID: 1000031, Revision: 1, Message: FTP USER ANOMALY, Classification: ABD.1 Anomaly Detection, IntrusionPolicy: ABD.1 Anomaly Detections, ACPolicy: ABD.1 Anomaly Detection - THROUGHPUT, AccessControlRuleName: ABD THROUGHPUT, NAPPolicy: Net Access Policy - Common, InlineResult: Dropped
IPS_IPB_EXT.1	Inspected traffic matches a list of known-good or	<date> <time> <host> (null) %NGIPS-1-430002: EventPriority: High, DeviceUUID: ee5eb176-a726-11ed-82c8-bb1c5e1ba303, InstanceID: 1,

© 2023 Cisco Systems, Inc. All rights reserved.

SFR	Auditable Event	Audit Messages Generated by FMC
	known-bad addresses applied to an IPS policy.	FirstPacketSecond: 2023-02-15T12:00:13Z, ConnectionID: 3133, AccessControlRuleAction: Block, AccessControlRuleReason: IP Block, SrcIP: 50.50.51.120, DstIP: 104.237.139.111, SrcPort: 59864, DstPort: 80, Protocol: tcp, IngressInterface: eth1, EgressInterface: eth2, IngressZone: Internal, EgressZone: External, ACPolicy: IPB Configuration, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 60, ResponderBytes: 0, NAPPolicy: No Rules Active, SecIntMatchingIP: Source, IPReputationSICategory: BAD_RANGE
IPS_NTA_EXT.1	Modification of which IPS policies are active on a TOE interface. Enabling/disabling a TOE interface with IPS policies applied. Modification of which mode(s) is/are active on a TOE interface.	<date> <time> <host>: admin@172.16.16.81, Policies > Access Control > Access Control, Page View#000x0a#000x00 <date> <time> 172.16.16.223 ActionQueueScrape.pl: FMCv: Default User@Default User IP, High Availability, Synchronization - Save SensorPolicy#000x0a#000x00 <date> <time> 172.16.16.223 mojo_server.pl: FMCv: admin@172.16.16.81, Devices > Device Management > Devices, Page View#000x0a#000x00 <date> <time> 172.16.16.223 mojo_server.pl: FMCv: admin@127.0.0.1, Devices > Device Management > Device Edit > Interfaces, Save#000x0a#000x00
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS rule with logging enabled.	<date> <time> <host>: (null) %NGIPS-7-430001: DeviceUUID: 278c5002-b2df-11ed-8409-d0ff4adbbdd5, ConnectionID: 0, SrcIP: ::, DstIP: ::, IngressInterface: eth1, EgressInterface: eth2, IngressZone: Internal, EgressZone: External, Priority: 3, GID: 116, SID: 2, Revision: 2, Message: DECODE_IPV4_INVALID_HEADER_LEN, Classification: Generic Protocol Command Decode, IntrusionPolicy: SBD.1.1 Header Rules, ACPolicy: SBD.1.1 Header Access Pol, NAPPolicy: Net Access Pol - Verify Checksums, InlineResult: Dropped

4.3 Restrict Access and Enable CC Mode

The system by default only supports SSH and HTTPS security protocols for management. Telnet and HTTP are not supported for management and cannot be enabled. SNMPv3 is supported but is not permitted for management—only for sending SNMP traps for alerting. The system is required to support only the cipher suites, version, and protocols claimed in the Security Target. HTTPS, TLS, and SSH connection settings are configured automatically when CC mode is enabled. While not required by the NDcPP, the administrator should configure access list to control which computers can access the appliances on specific ports.

IMPORTANT! By default, access to the appliance is **not** restricted. To operate the appliance in a more secure environment, consider adding access to the appliance for specific IP addresses and then deleting the default **any** option.

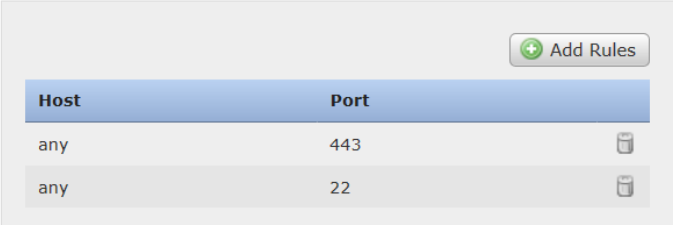
By default, port 443 (HTTPS), which is used to access the web interface, and port 22 (SSH), which is used to access the command line, are enabled for any IP address. The access list is part of the system policy. Administrator can specify the access list either by creating a new system policy or by editing an existing system policy. In either case, the access list does not take effect until the system policy is applied.

1. Login with Administrator Role.

© 2023 Cisco Systems, Inc. All rights reserved.

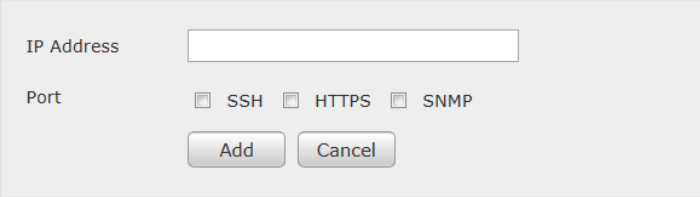
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
    - Management Center—Choose **System > Configuration.**
    - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click **Access List**.

    The Access List page appears.



4. Click **Add Rules**.

    The Add IP Address page appears.



5. In the IP Address field, you have the following options, depending on the IP addresses you want to add:
    - An exact IP address (for example, 172.16.16.81)
    - An IP address range using CIDR (for example, 192.168.0.0/16)
    - Any IP address using **any** term
6. Select **SSH** or **HTTPS** or both of these options to specify which ports you want to enable for these IP addresses.

    WARNING! SNMP management must not be enabled in the evaluated configuration. SNMP cannot be used for management. However, encrypted SNMPv3 traps are allowed for alerting only.
7. Click **Add**.
8. Click the delete icon ( ) to remove the permissive rules.

    IMPORTANT! If you delete access for the IP address that you are currently using to connect to the appliance interface, and there is no entry for “IP=any port=443”, you will lose access to the system when you save (for FMC) or deploy (for device) the setting.
9. Click **Save**.

© 2023 Cisco Systems, Inc. All rights reserved.

10. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

Note: The Source IP field in the audit event above is cut off.

© 2023 Cisco Systems, Inc. All rights reserved.

Enable CC Compliance (also known as CC Mode)

Enabling CC mode will restrict the SSH algorithms, SSH rekey, TLS versions and TLS cipher suites (including elliptical curves) to the Approved ones claimed in the Security Target. There are additional features such as enabling the power-up integrity HMAC-SHA-512 self-test, enabling FIPS mode to ensure the TOE uses the correct DRBG method, and other TLS required checks such as the ones specified in section 6 of RFC 6125. To be in the evaluated configuration, you must enable CC Mode.

IMPORTANT! After you enable this setting, you cannot disable it. If you need to do so, contact Support for assistance.

IMPORTANT! The FMC will not receive data from a managed device unless both are operating in CC mode. Therefore, you must enable CC mode on the FMC first, then its managed devices.

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
   - Management Center—Choose **System > Configuration.**
   - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click **UCAPL/CC Compliance**.
4. Choose **CC** from the drop-down list.
5. Click **Save**.
6. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again. Remember, you need to enable CC Mode first on the FMC!

NOTE! System automatically reboots when you enable CC compliance. The FMC reboots when you save the system configuration; managed devices reboot when you deploy the configuration.

Audit Record:

2016-11-15 19:54:52	admin	Enable UCAPL/CC Compliance	Enable CC mode	10.128.120.41

Configure SSH Public-Key Authentication

Perform the following steps on a remote workstation:

1. Log into the remote machine as root.
2. Regenerate the SSH keypair and follow instructions below

```
ssh-keygen -t rsa
```

© 2023 Cisco Systems, Inc. All rights reserved.

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): [leave it blank]
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
1e:54:c7:09:14:29:f5:32:b8:81:c4:99:e2:a8:5d:b8 root@cc-auto
```

3. Copy the public key to the system.

IMPORTANT! Use step 3 for configuring FMC only.

```
cat ~/.ssh/id_rsa.pub | ssh admin@<IP address of System> "mkdir -p ~/.ssh && cat >>
~/.ssh/authorized_keys"
```

4. Copy the public key to the system.

IMPORTANT! Use step 4 for configuring Device only.

```
# After generating the RSA keys, login to Device and type 'expert'
mkdir –p ~/.ssh
touch ~/.ssh/authorized_keys
scp <username>@<IP address of remote machine>:~/.ssh/id_rsa.pub .
mv id_rsa.pub ~/.ssh/authorized_keys
exit
exit
```

[Enter the admin password to authorized the copy of public keys to system authorized keys]

5. Log into the system without providing a password

Audit Record:

May 25 2016 15:33:27 FMCv sshd[14076]: Accepted publickey for admin from 172.18.153.143 port 35698 ssh2: RSA SHA256:PLdSQVED/mXpzRl59rHp4+dL5lbSktFiEfmAUBoTLMs

Configure SSH ReKey Configuration (Optional)

When CC mode is enabled, the SSH rekeying will occur approximately at 1 hour of time or after 1 GB of data has been transmitted, whichever occurs first. To change these values to be smaller, the administrator can configure these during the pre-operational state **ONLY** using the local management connection:

© 2023 Cisco Systems, Inc. All rights reserved.

1. Login locally to shell with the default **admin** account using the password created during the initial setup process.

   NOTE! If you are on a sensor, the **>** will be displayed. Type the command ***expert*** to access the shell from the CLI.

2. The shell prompt **<username>@<hostname>:~$** is displayed.
3. Type command ***sudo -i*** to gain root access.

   A warning message is displayed about root privilege (first time only).

4. Enter the same password as in step 1.
5. The shell prompt **<username>@<hostname>:~#** is displayed.
6. Type the command ***vi /etc/ssh/sshd_config*** to modify the SSH daemon configuration file.
7. Modify "RekeyLimit 1G 1h" to the desired values. For example, "RekeyLimit 1G 30m"

   WARNING! Do not set the time to be greater than one hour or the volume to be greater than 1 GB.

8. Type ***/etc/rc.d/init.d/sshd restart*** to restart the SSH server.

Generate Certificate Request and RSA Keypair

1. Login locally to shell with the default **admin** account using the password created during the initial setup process.
2. Type command ***expert*** to gain expert mode.
3. The shell prompt **<username>@<hostname>:~$** is displayed.
4. Type command ***sudo -i*** to gain root access.

   A warning message is displayed about root privilege (first time only).

5. Enter the same password as in step 1.
6. The shell prompt **<username>@<hostname>:~#** is displayed.
7. Change to 'ssl' dir using command ***cd /etc/ssl***.
8. Type the command ***openssl genrsa –out audit.key 2048*** to generate the RSA key.
9. Type the command ***chmod 700 audit.key***
10. Type the command ***openssl req –new –key audit.key –subj "/C=<Country>/ST=<State>/L=<City>/O=<Company>/<OU>=<Unit>/CN=<CommonName>" –out CSR.pem***

    Replace <*Country*> with "US" (for example, /C=US/ST=NC/L=RTP/O=…)

11. Send the CSR.pem to the external CA to sign and generate certificate.

© 2023 Cisco Systems, Inc. All rights reserved.

IMPORTANT! The audit client certificate is expected to have the cA flag set to FALSE and critical. Other expected fields include: TLS Web Client Authentication (for X509v3 Extended Key Usage) and Digital Signature, Non Repudiation, Key Encipherment (for X509v3 Key Usage).

12. Exit expert mode.
13. Use the command ***configure audit_cert import*** to import the certificate, private key (i.e., audit.key), and CA or CA chain.
14. Use the command ***configure audit_cert delete*** to zeroize the existing certificate chain and associated keys.
15. Use the command ***configure audit_cert import*** to zeroize and replace the existing certificate chain and associated keys.

© 2023 Cisco Systems, Inc. All rights reserved.

4.4 Configure Secure Connection with Audit Server

Administrator can configure the system so it can transmit audit and syslog records securely to an external audit server (Suggestion: syslog-ng, version 3.7 or later) while storing the audit and syslog records locally. The audit server must be functional and accessible before the appliance can send the audit records. The system does not send the audit records until you save the setting.

If you stream the logs to an audit server, you can use Transport Layer Security (TLS) to secure the channel between the system and the syslog-ng server. To securely send the logs to a trusted audit server, there are two requirements:

- Import a signed audit client certificate for the system. You can generate a certificate request based on your system information and the identification information you supply. Send the resulting request to a certificate authority to request a client certificate. After you have a signed certificate from a certificate authority (CA), you can import it.
- Configure the communication channel with the audit server (i.e., syslog-ng) to use TLS.

To verify the certificate status, configure the system to load one of more certificate revocation lists (CRLs). The system compares the server certificate against those listed in the CRLs. If a server offers a certificate that is listed in a CRL as a revoked certificate, the connection fails.

NOTE! If you choose to verify certificates using CRLs, the system uses the same CRLs to validate both the audit client and audit server certificates.

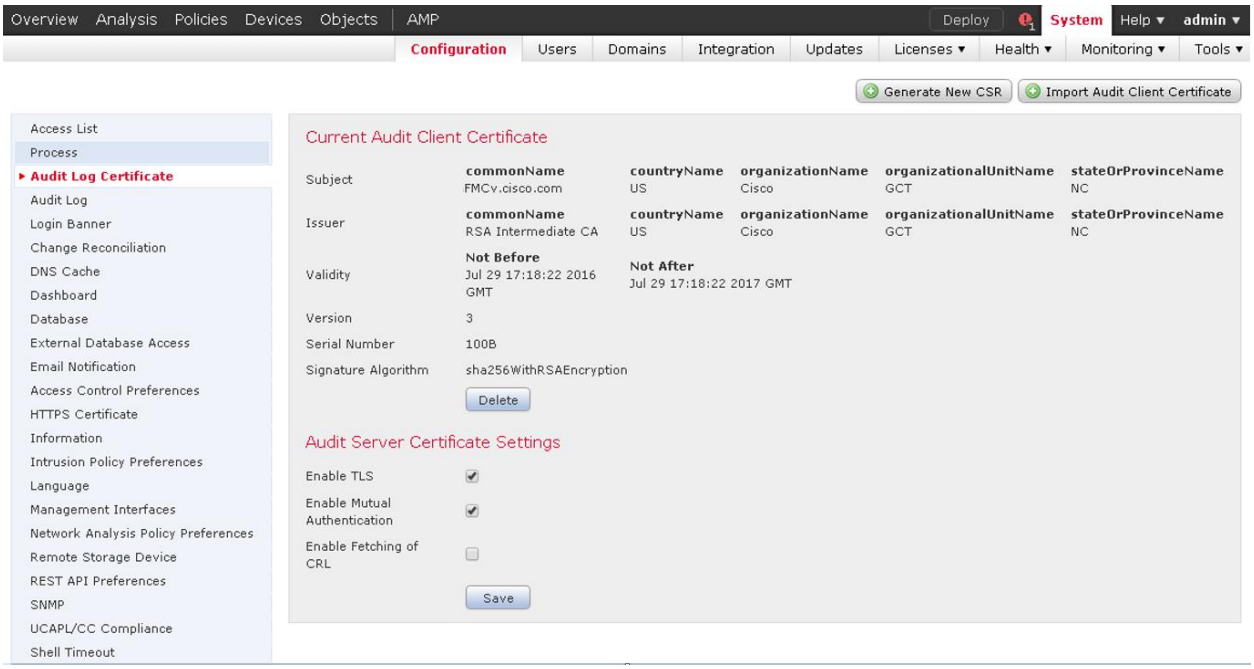
Audit log connection fails if the audit server certificate that does not meet either one of the following criteria:

- The certificate is not signed by the CA with cA flag set to TRUE.
- The certificate is not signed by a trusted CA in the certificate chain.
- The certificate Common Name (CN) or Subject Alternative Name (SAN) does not match the expected hostname (i.e., reference identifier).
- The certificate has been revoked or modified.

To view the client audit certificate:

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
    - Management Center—Choose **System > Configuration.**
    - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select **Audit Log Certificate**.

© 2023 Cisco Systems, Inc. All rights reserved.



Audit Record:

2016-11-15 20:22:55	admin	System > Configuration > Configuration > /admin/audit_cert.cgi	Page View	10.128.120.41

To delete the client audit certificate:

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
    - Management Center—Choose **System > Configuration.**
    - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select **Audit Log Certificate**.
4. Clicking **Delete** will zeroize the existing certificate chain and associated keys.
5. Clicking **Import Audit Client Certificate** will zeroize and replace the existing certificate chain and associated keys.

To generate a Certificate Signing Request (CSR):

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
    - Management Center—Choose **System > Configuration.**

© 2023 Cisco Systems, Inc. All rights reserved.

- Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.

3. Select **Audit Log Certificate**.
4. Click **Generate New CSR**.
5. Enter a country code in the **Country Name (two-letter code)** field.
6. Enter a state or province postal abbreviation in the **State or Province** field.
7. Enter a **Locality or City**.
8. Enter an **Organization** name.
9. Enter an **Organization Unit (Department)** name.
10. Enter the fully qualified domain name for which you want to request a certificate in the **Common Name** field.

NOTE! If the SAN and DNS hostname do not match, or if the SAN is not present and the CN and the DNS hostname do not match, the secure audit log connection will fail.

---

11. Click **Generate**.
12. Open a new blank file with a text editor.
13. Copy the entire block of text in the certificate request, including the *BEGIN CERTIFICATE REQUEST* and *END CERTIFICATE REQUEST* lines, and paste it into a blank text file.
14. Save the file with extensions .csr.
15. Click **Close**.

IMPORTANT! This method will automatically generate a RSA 2048-bits key pair and embed the public key in the CSR. In this case, you do not need to import the private key. However, if you generate the RSA key pair externally, then you will need to import the private RSA key.

To import the audit client certificate

(On the NGIPSv, use the command “configure audit_cert import”.)

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
   - Management Center—Choose **System > Configuration.**
   - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select **Audit Log Certificate**.
4. Click **Import Audit Client Certificate**.
5. Open the client certificate in a text editor, copy the entire block of text, including the *BEGIN CERTIFICATE* and *END CERTIFICATE* lines. Paste this text into the **Client Certificate** field.

© 2023 Cisco Systems, Inc. All rights reserved.

IMPORTANT! The audit client certificate is expected to have the cA flag set to FALSE and critical. Other expected fields include: TLS Web Client Authentication (for X509v3 Extended Key Usage) and Digital Signature, Non Repudiation, Key Encipherment (for X509v3 Key Usage).

6. To import a private RSA key, open the private key file and copy the entire block of text, including the *BEGIN <KEY TPYE> PRIVATE KEY* and *END <KEY TYPE> PRIVATE KEY* lines. Paste this text into the **Private Key** field. If the key pair is generated internally, this field is not required.
7. Open each intermediate CA certificate and the root CA certificate, and copy the entire block of text for each, and paste it into the **Certificate Chain** field (concatenate as needed). The audit server certificate is signed by one of these CA in the chain.

IMPORTANT! The CA certificate must have the cA flag set to TRUE and critical.

WARNING! The audit client certificate is validated against the CA or CA certificates in the chain. The import will fail if the validation fails.

8. Click **Save**.
9. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

The system supports validating audit server certificates using imported CRLs in Distinguished Encoding Rules (DER) format.

If you choose to use CRLs, to ensure that the list of revoked certificates stays current, you can create a scheduled task to update the CRLs. The system displays the most recent refresh of the CRLs.

If you choose CRLs, the system uses the same CRLs to validate both audit client certificates and HTTPS certificate to secure the HTTPS connection between the system and a web browser.

Enable TLS and mutual authentication with the audit server (i.e., syslog-ng):

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
   - Management Center—Choose **System > Configuration.**
   - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select **Audit Log Certificate**.
4. Choose **Enable TLS** to use Transport Layer Security to send the audit and syslog log to an external audit server.

© 2023 Cisco Systems, Inc. All rights reserved.

WARNING! This setting is required in the evaluated configuration.

5. Choose **Enable Mutual Authentication**.

WARNING! This setting is required in the evaluated configuration.

NOTE! If you enable mutual authentication without importing a valid audit client certificate, the secure audit log connection will fail.

6. You have two options:
   - To verify server certificate using one or more CRLs, select **Enable Fetching of CRL** and continue with Step 6. This setting is required in the evaluated configuration.
   - To accept server certificate without revocation check, skip to Step 9.
7. Enter a valid URL to an existing CRL file and click **Add CRL**. Repeat to up to 25 CRLs.

NOTE! Do not copy and paste the URL. Enter the URL manually.

8. Click **Refresh CRL** to load the current CRL or CRLs from the specified URL or URLs. Enabling fetching of the CRL creates a scheduled task to regularly update the CRL or CRLs. Edit the task to set the frequency of the update.
9. Click **Save**.
10. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

Specify the external audit server:

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
   - Management Center—Choose **System > Configuration.**
   - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select **Audit Log**.
4. Select **Enabled** from the **Send Audit Log to Syslog** drop-down menu.
5. Specify the destination host for the audit information by using the IP address or the fully qualified name (reference identifier, e.g., syslog.cisco.com) of the syslog server in the **Host** field. The default port (514) is used but if TLS is enabled, port 6514 will be used. For NGIPSv and FMC the reference identifier used for the syslog-over-TLS connection to the remote syslog server is the syslog server's hostname or IP address as entered by the Firepower administrator when adding the syslog host to the configuration.
6. Click **Save**.

© 2023 Cisco Systems, Inc. All rights reserved.

7. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

2016-11-15 20:34:07	admin	Devices > Platform Settings > Audit Log Settings > Modified: Send Audit Log to Syslog Disabled > enabled	Save	10.128.120.41
2016-11-15 20:34:07	admin	Devices > Platform Settings > Audit Log Settings > Modified: Host > 172.18.152.193	Save	10.128.120.41

Configure the external audit server (i.e., syslog-ng daemon):

1. Login as authorized administrator.
2. Install syslog-ng with version 3.7[2] or later.
3. Edit the syslog-ng configuration file by adding the following section below.
   vi /etc/syslog-ng/syslog-ng.conf

   # It maybe a different path depending on OS.

   Or you can search for it. “find / -name syslog-ng.conf”

```
source s_network_TLS {
  tcp( port(6514)
        tls(
            key-file(“/etc/ssl/server.key.pem”)   # Private key of audit server certificate
            cert-file(“/etc/ssl/server.cert.pem”)  # Audit server certificate
            ca-dir(“/etc/ssl”) # Location of the CA certificates and symbolic links. See below
                ###  openssl x509 -noout -hash -in rootCA.pem
                ###   ln -s rootCA.pem 2e286222.0
                ###   This is the CA that signed the audit client certificate and other CA(s) in the chain.
                ###   All CA certs must have basic constraints CA flag set to TRUE and critical
            cipher-suite(AES128-SHA) # e.g., TLS Ciphersuite to be supported by the server
            ssl-options(no-sslv2, no-sslv3, no-tlsv1)  # no-sslv2, no-sslv3, no-tlsv1, no-tlsv11, no-tlsv12
            peer-verify(required-trusted)  # required-trusted for mutual auth, optional-trusted for no auth
         )
  );
};

destination d_local {
  file("/var/log/remote_messages" ts-format(iso));   # The remote syslog file location can be configured here
};
```

[2] Another option is rsyslog with stunnel but this configuration is not described in this document.

© 2023 Cisco Systems, Inc. All rights reserved.

```
log {
   source(s_network_TLS); destination(d_local);
};
```

NOTE! When CC mode is enabled, the TLS version and cipher suites will be limited to the ones claimed in the Security Target. The audit server setting must include those versions and cipher suites, or the secure audit log connection will fail.

4. Restart the syslog-ng server and make sure there is no error message.
   /etc/rc.d/init.d/syslog-ng restart # Command may be different depending on the OS.

5. Use netstat to make sure the syslog-ng is listening.
   netstat -an | grep 6514
6. Make sure port 6514 is opened by the firewall to allow the connection.

The administrator is responsible for maintaining the connection between the system and audit server. If the connection is unintentionally broken, the administrator should perform the following steps to diagnose and fix the problem:

- Check the physical network cables.
- Check that the audit server is still running.
- Reconfigure the audit log settings.
- If all else fail, reboot the system and audit server.

© 2023 Cisco Systems, Inc. All rights reserved.

4.5 Configure Access Control Policy

An access control policy determines how the system handles traffic on the monitored network. Administrators can configure one or more access control policies, which they can then apply to one or more managed devices. Each device can have only one applied policy though. Access control rules can be added to a policy to provide granular control how traffic is handled and logged. To associate the access control policy and all rules under the policy to an interface, you first need to create the interface sets for the device using “Configure Inline Interface” and “Configure Inline Set” sections from the general System User Guide. Then you can target the policy to a certain device using the target tab.

For each rule, administrator can specify a rule *action*, that is, whether to trust, block, or inspect matching traffic with an intrusion policy. Each rule contains a set of conditions that identify the specific traffic you want to control. Rules can be simple or complex, matching traffic by any combination of security zone, IP address, application, protocols, ports, etc.

The system matches traffic to access control rules in order; the first matched rule handles the traffic.

4.5.1 Access Control Policy

On the Access Control Policy page (**Policies > Access Control**) administrator can view all the current access control policies by name and optional description and the following status information:

- When a policy is up to date on targeted devices, in green text.
- When a policy is out of date on targeted devices, in red text.

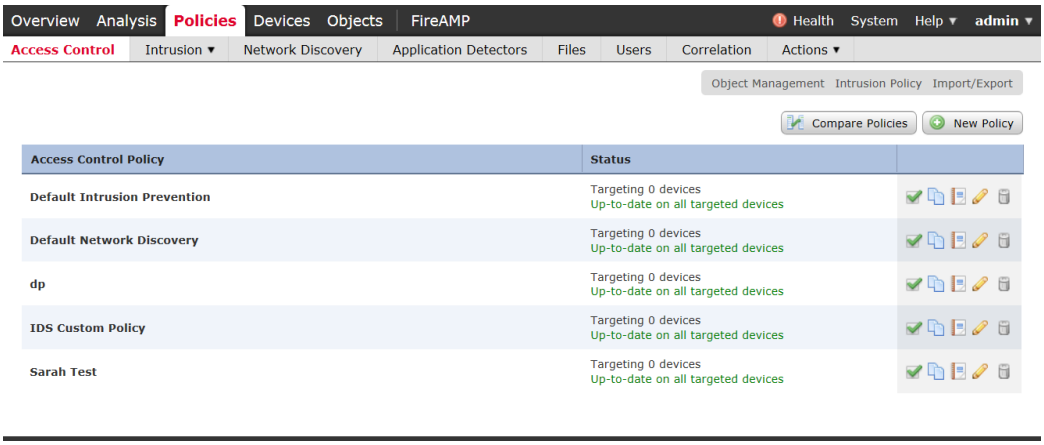
The default access control policy blocks all traffic from entering your network.

Creating Access Control Policy

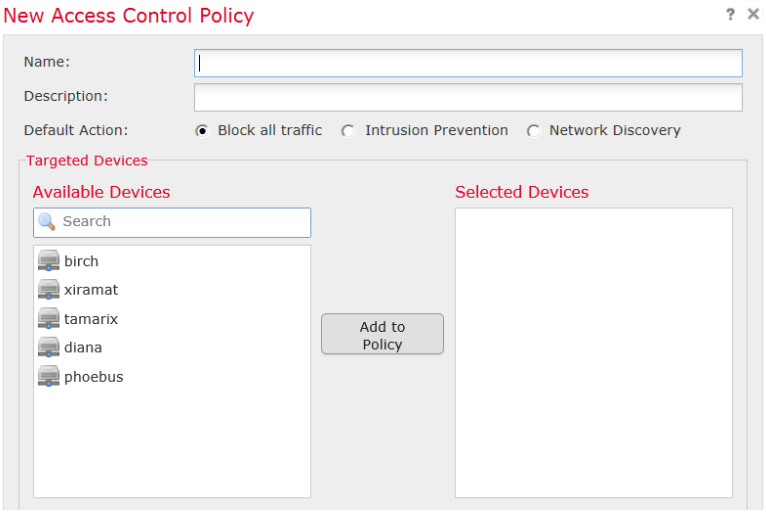
When you create a new access control policy you must, at minimum, give it a unique name and specify a default action. Although you are not required to identify the policy targets at policy creation time, you must perform this step before you can apply the policy.

1. Login with Administrator Role or Access Admin.
2. Select **Policies > Access Control**.

© 2023 Cisco Systems, Inc. All rights reserved.



3. Click **New Policy**.



4. In the **Name:** field, type a unique name for the new policy. Optionally, type a description in the **Description:** field.
5. Specify the default action.

WARNING! Leave the default **Block all traffic** in the evaluated configuration.

6. Select the devices where you want to apply the policy. Click on the managed Device(s) you want the policy to applied to. Then click on **Add to Policy** button.
7. Specify the initial **Default Action**:
   - **Block all traffic** creates a policy with the **Access Control: Block All Traffic** default action.
   - **Intrusion Prevention** creates a policy with the **Intrusion Prevention: Balanced Security and Connectivity** default action, associated with the default intrusion variable set.
8. Click **Save**.
9. Click **Deploy** and select the device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

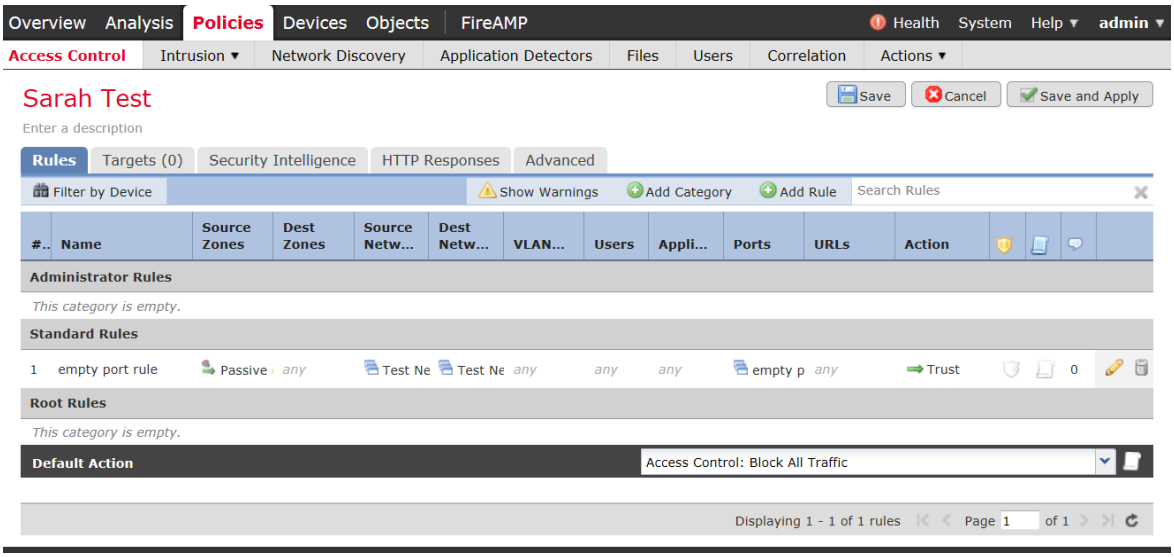
© 2023 Cisco Systems, Inc. All rights reserved.

2013-07-02 15:52:56	admin	Policies > Access Control > Access Control Policy > cctest	Create Policy	10.4.10.26

Editing Access Control Policy

1. Login with Administrator Role.
2. Select **Policies > Access Control**.
3. Click the edit icon ( ) next to the access control policy you want to configure.

   The Policy Edit page appears.



4. Make changes to the policy and click **Save**.
5. Click **Deploy** and select the device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

2013-07-02 16:07:47	admin	Policies > Access Control > Access Control Policy > cctest	Save Policy	10.4.10.26
2017-02-24 17:30:41	System	Task Queue	Successful task completion : Policy Deployment to 172.18.152.193	

Delete Access Control Policy

1. Login with Administrator Role.
2. Select **Policies > Access Control**.
3. Click the delete icon ( ) next to the policy you want to delete.
4. Click **OK** to confirm.

© 2023 Cisco Systems, Inc. All rights reserved.

Audit Record:

2013-07-02 16:10:29	admin	Policies > Access Control > Access Control Policy > cctest	Delete Policy	10.4.10.26

Enabling Syslog Messages (Do-Not-Block List)

To allow known-good source addresses:

- If you do *__not__* want the connections to be logged, either:
  - Add the known-good addresses to the Do-Not-Block List; or
  - Add a rule to the top of the Access Control Policy with the source addresses set to the known-good addresses and the action set to “Trust” and leave logging for that rule disabled (the default setting).
- If you *__do__* want the connections to be logged:
  - Ensure the known-good addresses are *__not__* in the Do-Not-Block List, *__nor__* in the Block List.
  - Add a rule to the top of the Access Control Policy with the source addresses set to the known-good addresses and the action set to “Trust” and *__enable__* logging on that rule.

    [Warning, logging this activity can have a negative impact on performance when the connection rate from the known-good addresses is high.]

© 2023 Cisco Systems, Inc. All rights reserved.

4.5.2 Access Control Rule

A set of access control rules is a key component of an access control policy. Access control rules allow administrator to manage, in a granular fashion, which traffic can enter the network, exit it, or cross from within without leaving it. Within an access control policy, the system matches traffic to rules in top-down order by rule number. Firepower access-control rules can be reordered via the FMC GUI by clicking dragging any rule up or down within its access-control rule listing.

In addition to its rule order and some other basic attributes, each rule has the following major components:

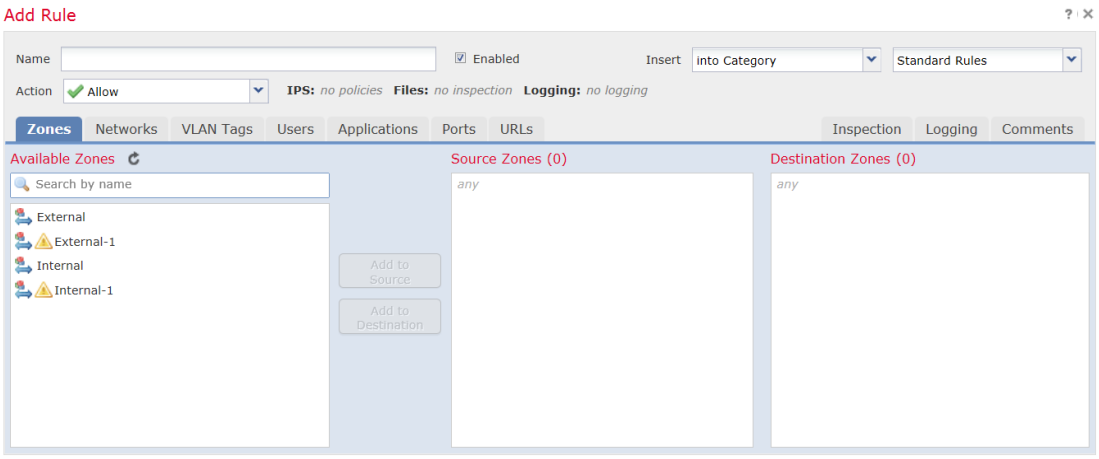
- A set of rule *conditions* that identifies the specific traffic you want to control.
- A rule *action*, which determines how the system handles traffic that meets the rule's conditions.
- Intrusion *inspection* option, which allow you to examine allowed traffic with intrusion policy.
- The *logging* option, which allow you to keep a record (event log) of the matching traffic.

The access control policy's default action defines the default action (for example, block all traffic) for the policy.

Creating and Editing Access Control Rules

1. Login with Administrator Role or Access Admin.
2. Select **Policies > Access Control**.
3. Click the edit icon ( ) next to the access control policy you want to configure.
4. Add a new rule or edit an existing rule:
   - To add a new rule, click **Add Rule**.
   - To edit an existing rule, click the edit icon ( ) next to the rule you want to edit.

   Either the Add Rule or Editing Rule page appears.



5. Configure the following rule components:

© 2023 Cisco Systems, Inc. All rights reserved.

- You must provide a unique rule **Name**.
- Specify whether the rule is **Enabled**.
- Specify the rule position.
- Select a rule **Action**[3].
- Configure the rule's conditions[4].
- Configure the rule's **Inspection** option.
- Specify **Logging** option.
- Add **Comments**.

6. Click **Add** or **Save**.

   Your changes are saved. You must apply the access control policy for your changes to take effect.

Audit Record:

2013-07-02 16:07:47	admin	Policies > Access Control > Access Control Policy > cctest	Save Policy	10.4.10.26
2013-07-02 16:27:29	admin	Policies > Access Control > Access Control Policy > test	Save Policy	10.4.10.26

Click on the compare ( ) icon to see what rule(s) were added, removed, or modified and how.

For example, the following AC rule "cc rule" has been added to AC policy "test" by admin.

test (2013-07-01 09:31:02 by ahepburn)	
Policy Information	
Modified	2013-07-01 09:31:02 by ahe
Rules	
Category 2	
Name	Standard Rules

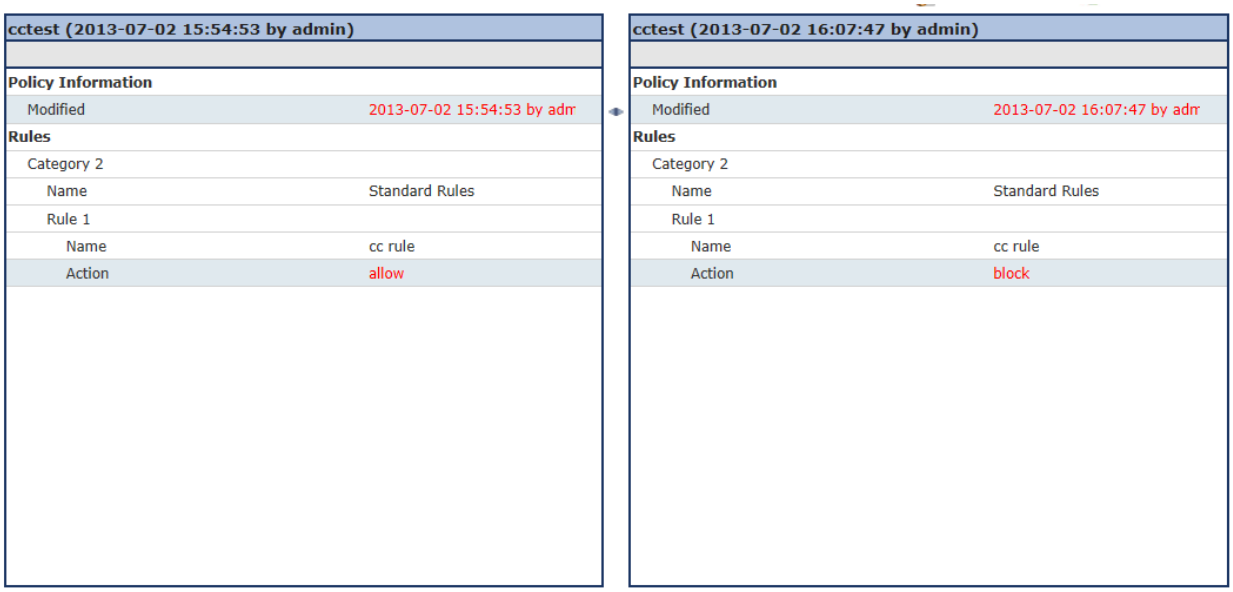
test (2013-07-02 16:12:57 by admin)	
Policy Information	
Modified	2013-07-02 16:12:57 by adm
Security Intelligence	
Blacklist Logging	
Send to Defense Center	Disabled
Rules	
Category 2	
Name	Standard Rules
Rule 1	
Name	cc rule
Action	allow
Destination Ports	
"TCP (6):123"	
Source Ports	
"TCP (6):123"	
Logging	
Log at beginning	Disabled
Log at end	Disabled
Log Files	Disabled
Send to Defense Center	Disabled

[3] The evaluated actions are Allow and Block.

[4] The evaluated conditions are Zones, Networks, Applications, and Ports. The other conditions are presented for completeness only.

© 2023 Cisco Systems, Inc. All rights reserved.

For example, the following AC rule “cc rule” has the new action set to block, from allow.



Understanding Rule Conditions

Administrator can set an access control rule to match traffic meeting any of the conditions described in the following table:

Condition	Description
Zones	A configuration of one or more interfaces where you can apply policies. Zones provide a mechanism for classifying traffic on source and destination interfaces, and you can add source and destination zone conditions to rules.
Networks	Any combination of individual IPv4 and IPv6 addresses, CIDR blocks, and/or networks (by default, any). The system also supports Network Objects as described in Section 4, page 148 in the Cisco 3D System User Guide.
VLAN Tags	A number from 0 to 4094 that identifies traffic on your network by VLAN.
Users	Individual LDAP users and user groups retrieved from a Microsoft Active Directory Server.
Applications	Applications provided by Cisco, user-defined applications, and application filters you create using the object manager.
Ports	Source and Destination ports. ICMPv4 and ICMPv6 type and code. Transport protocol ports, including individual and group port objects you create based on transport protocols[5]. The system supports Port Objects as described in Section 4, page 170 in the Cisco 3D System User Guide.
URLs	Cisco-provided URLs grouped by category and reputation, literal URLs, and any individual and group URL objects you create using the object manager.

[5] We support all the protocol-specific attributes required in the FWPP.

© 2023 Cisco Systems, Inc. All rights reserved.

IMPORTANT! Note that to use the Application tab for the access control rules, CONTROL license is required which requires PROTECTION license. This is needed to detect FTP and FTP data connections for dynamic rule. The CONTROL license is only supported for series 3 appliances.

To support the dynamic session establishment capability for FTP, you first need to create an access control rule that allows both FTP and FTP data. You can also configure the logging for this rule. This will enable the FTP application detector which has understanding of the application-level protocol so that FTP data connection will be allowed without additional rule.

Deleting Access Control Rules

1. Login with Administrator Role.
2. Select **Policies > Access Control**.
3. Click the edit icon ( ) next to the access control policy you want to configure.
4. Click the delete icon ( ) next to the access control rule you want to delete.
5. Click **OK** to confirm.
6. Click **Save**.

Audit Record:

2013-07-02 16:07:47	admin	Policies > Access Control > Access Control Policy > cctest	Save Policy	10.4.10.26
2013-07-02 16:27:29	admin	Policies > Access Control > Access Control Policy > test	Save Policy	10.4.10.26

Click on the compare ( ) icon to see what rule was added, deleted, or modified and how.

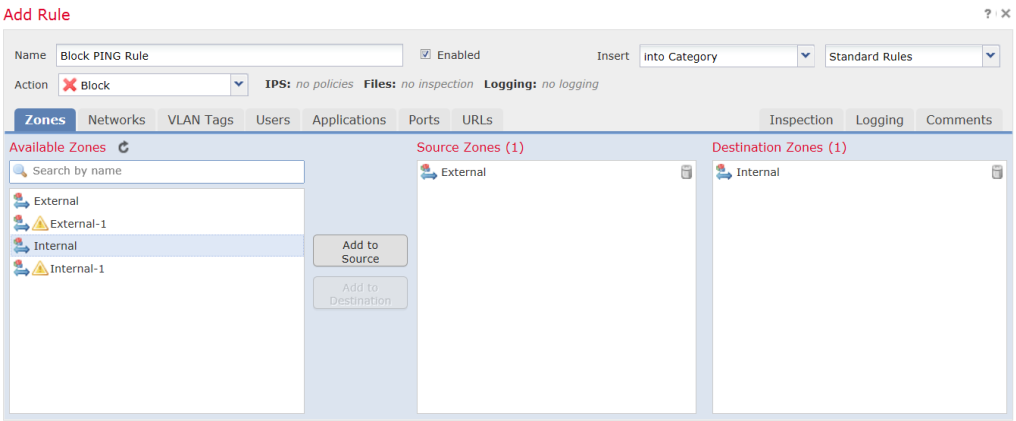
For example, the following AC rule “cc rule” has been deleted in AC policy “test” by admin.

© 2023 Cisco Systems, Inc. All rights reserved.

test (2013-07-02 16:12:57 by admin)		test (2013-07-02 16:27:29 by admin)	
Policy Information		**Policy Information**	
Modified	2013-07-02 16:12:57 by adm	Modified	2013-07-02 16:27:29 by adm
Rules		**Rules**	
Category 2		Category 2	
Name	Standard Rules	Name	Standard Rules
Rule 1			
Name	cc rule		
Action	allow		
Destination Ports			
"TCP (6):123"			
Source Ports			
"TCP (6):123"			
Logging			
Log at beginning	Disabled		
Log at end	Disabled		
Log Files	Disabled		
Send to Defense Center	Disabled		

The following example demonstrates how to block all Ping (ICMP echo request) from the external network to internal network and log the connection attempt.

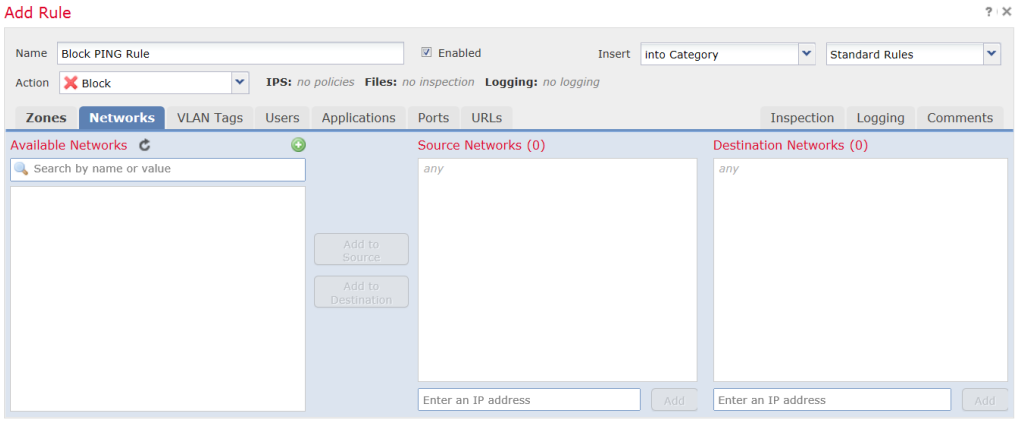
1. Login with Administrator Role.
2. Select **Policies > Access Control**.
3. Click the edit icon ( ) next to the access control policy you want to configure.
4. Click **Add Rule**.
5. Type a name for the rule.
6. Leave the **Enabled** checkbox selected.
7. Let the rule get inserted into standard rules.
8. Select **Block** from drop-down list for the rule action.
9. On the **Zones** tab, select the **External** zone as the source zone and the **Internal** zone as the destination zone. You can click and drag or use the buttons.



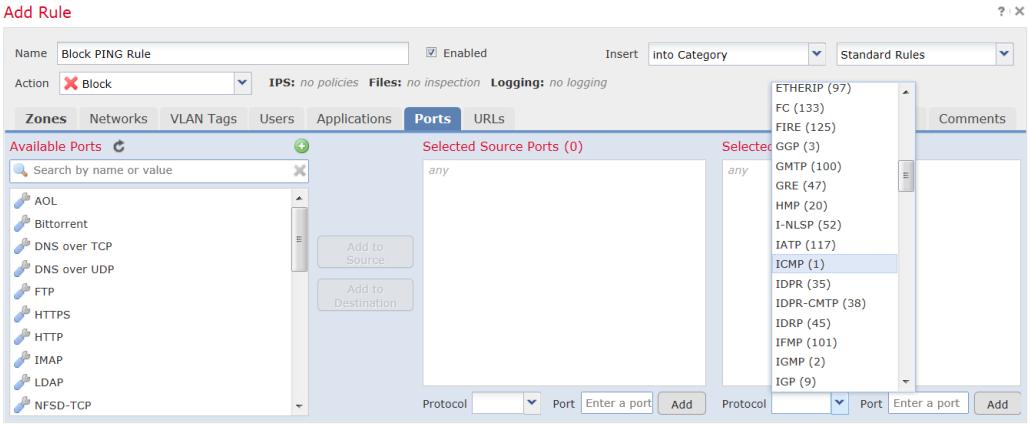
© 2023 Cisco Systems, Inc. All rights reserved.

10. On the **Networks** tab, select **any** as the source network and **any** as the destination network.

    For granular control, you can enter IP address or range of IP addresses for source and destination networks. The system also supports IPv6 addresses as well.

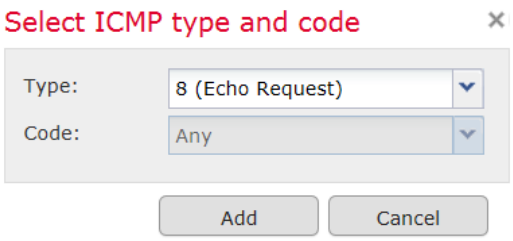


11. On the **Ports** tab, in the second **Protocol** fields, select **ICMP(1)**.



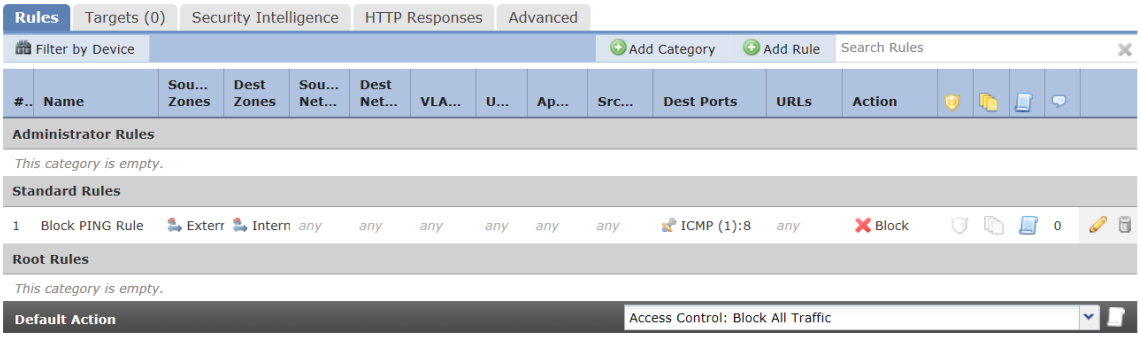
    The Select ICMP type and code pop-up window appears.

12. In the **Type:** field, select **8 (Echo Request)**.



13. Click **Add**.
14. On the **Logging** tab, check **Log at Beginning of Connection**.
15. In the **Send Connection Events to:** field, check the **FMC**.
16. Click **Add**.

© 2023 Cisco Systems, Inc. All rights reserved.



17. Click **Save**.

The Intrusion and Network Analysis Policy (NAP) policies are associated with the Access Control (AC) policy which is then assigned to one or more sensors. However, only one AC policy can be assigned to any one sensor at a time (for example, if admin assigns AC policy 'XYZ' to a sensor with another policy assigned, the old AC policy will be unassigned automatically). Finally, when an AC policy is assigned to a sensor, that policy will be active on **all** the enabled interfaces on the sensor.

Modification of which Intrusion Policy is Active on Device's Interfaces

Create an IPS Policy and associate it with an AC Policy

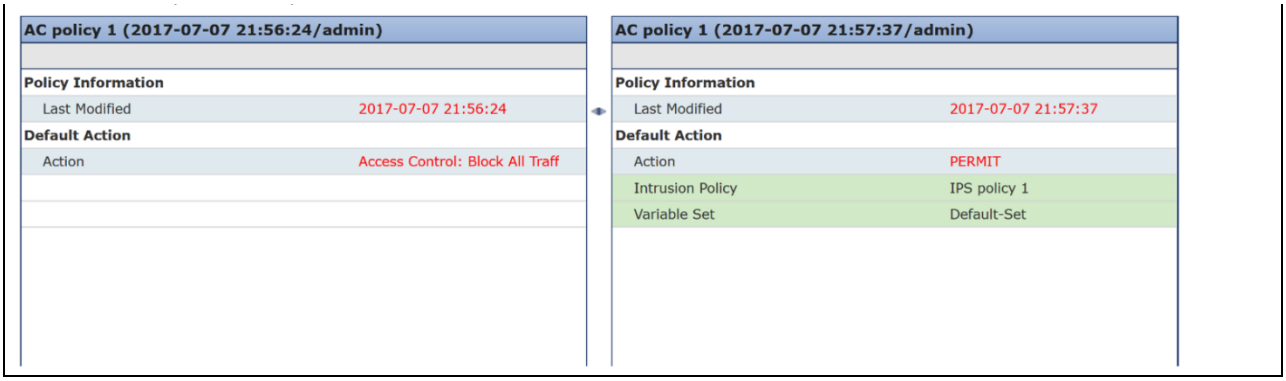
1. Login with Administrator Role.
2. Select **Policies > Access Control > Intrusion**.
3. Click **Create Policy** and create the Intrusion policy.
4. Select **Policies > Access Control**.
5. Assign a device (i.e., sensor) to the AC policy. Select the device and click on **Add to Policy**.
6. Click **Save**.
7. Associate the Intrusion policy with the AC policy either through the default action or AC rule.
8. Click **Save**.

Audit Record:

2017-07-07 17:57:38	admin	Policies > Access Control > Access Control > Firewall Policy Editor	Save Policy AC policy 1:367
2017-07-07 17:56:28	admin	Policies > Access Control > Access Control > Firewall Policy Editor	Page View
2017-07-07 17:56:24	admin	Policies > Access Control > Access Control > Firewall Policy Editor	Create Policy AC policy 1;Assigned to device(s) : 172.18.152.1
2017-07-07 17:55:02	admin	Policies > Access Control > Access Control	Page View
2017-07-07 17:54:39	admin	Policies > Access Control > Intrusion	Page View
2017-07-07 17:54:38	admin	Policies > Intrusion > Intrusion Policy > IPS policy 1	Policy Committed - "Create initial policy"
2017-07-07 17:54:06	admin	Policies > Access Control > Intrusion	Page View

Click on the compare ( ) icon to see what change.

© 2023 Cisco Systems, Inc. All rights reserved.



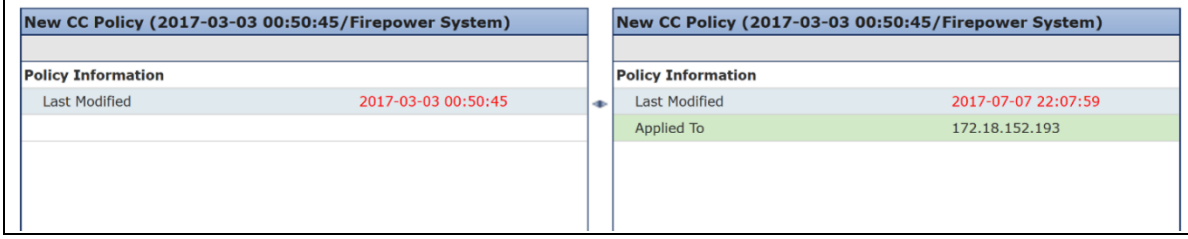
Assign a Different AC Policy to the Device

1. Login with Administrator Role.
2. Select **Policies > Access Control**.
3. Edit a different AC policy.
4. Click on **Policy Assignments**.
5. Assign a device to the AC policy. Select the device and click on **Add to Policy**. Click **OK** and confirm.
6. Click **Save**.

Audit Record:

2017-07-07 18:08:00 admin Policies > Access Control > Access Control > Firewall Policy Editor Save Policy New CC Policy:368

Click on the compare ( ) icon to see what change.



Associate AC Policy with Different Intrusion Policy

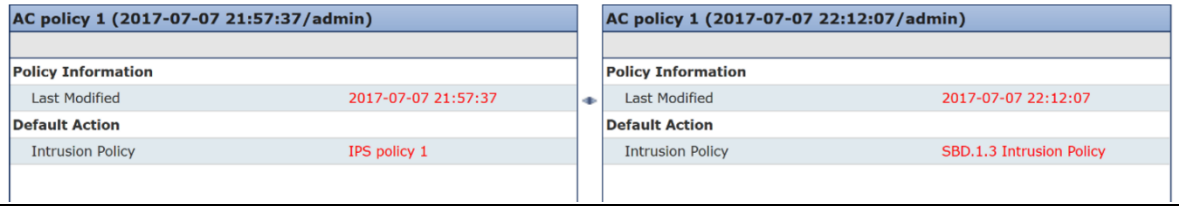
1. Login with Administrator Role.
2. Select **Policies > Access Control**.
3. Edit a AC policy.
4. Associate a different Intrusion policy either through the default action or AC rule.
5. Click **Save**.

Audit Record:

© 2023 Cisco Systems, Inc. All rights reserved.

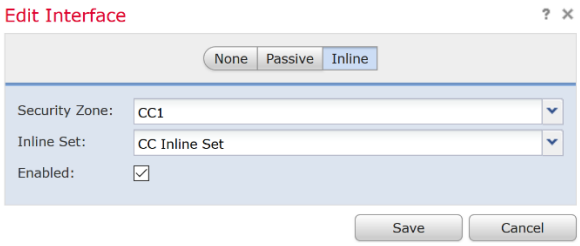
2017-07-07 18:12:07 admin Policies > Access Control > Access Control > Firewall Policy Editor Save Policy AC policy 1:369

Click on the compare ( ) icon to see what change.



Enabling/Disabling a Device Interface with Intrusion Policy Applied

1. Login with Administrator Role.
2. Select **Device > Device Management**.
3. Edit an interface (e.g., eth1).

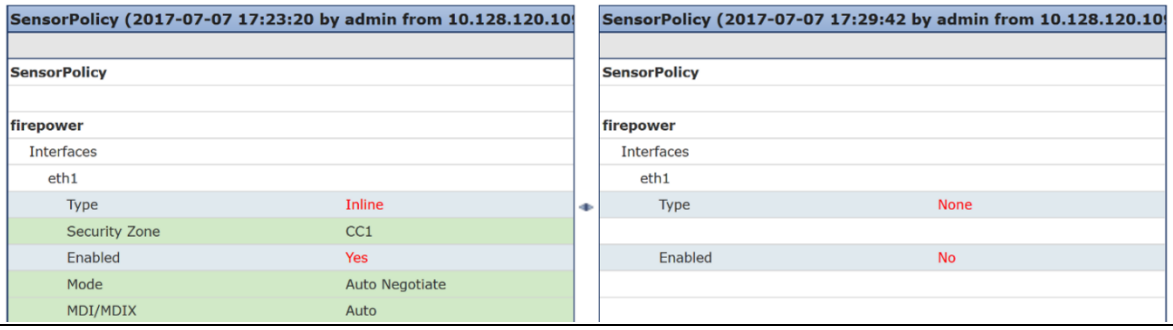


4. To disable an interface, change the interface from **Inline** to **None**.
5. Click **Save**.

Audit Record:

2017-07-07 17:29:42 admin Devices > Device Management > Device Edit > Interfaces Save:365 10.128.120.109

Click on the compare ( ) icon to see what change.

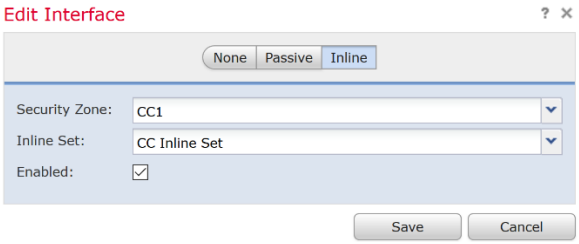


Modification of which Mode(s) is/are Active on Device Interface

1. Login with Administrator Role.
2. Select **Device > Device Management**.

© 2023 Cisco Systems, Inc. All rights reserved.

3. Edit an interface (e.g., eth1).



4. To change an interface mode, change the interface from **Inline** to **Passive**.
5. Click **Save**.

Audit Record:

2017-07-07 17:14:57	admin	Devices > Device Management > Device Edit > Interfaces	Save:362	10.128.120.109

Click on the compare ( ) icon to see what change.

SensorPolicy (2017-06-22 17:41:21 by admin from 127.0.0.1)		SensorPolicy (2017-07-07 17:14:57 by admin from 10.128.120.10	
SensorPolicy		**SensorPolicy**	
firepower		**firepower**	
Interfaces		Interfaces	
eth1		eth1	
Type	Inline	Type	Passive
Security Zone	CC1		
		MTU	1518
		Load Balancing Mode	Use Inner IP Headers
eth2		eth2	
Type	Inline	Type	None
Security Zone	CC2		
Enabled	Yes	Enabled	No
Mode	Auto Negotiate		
MDI/MDIX	Auto		
Inline Sets			
CC Inline Set			
Interfaces	eth1<->eth2		

Note: eth1 and eth2 used to be inline and now eth1 is passive and eth2 is not active (i.e., disabled).

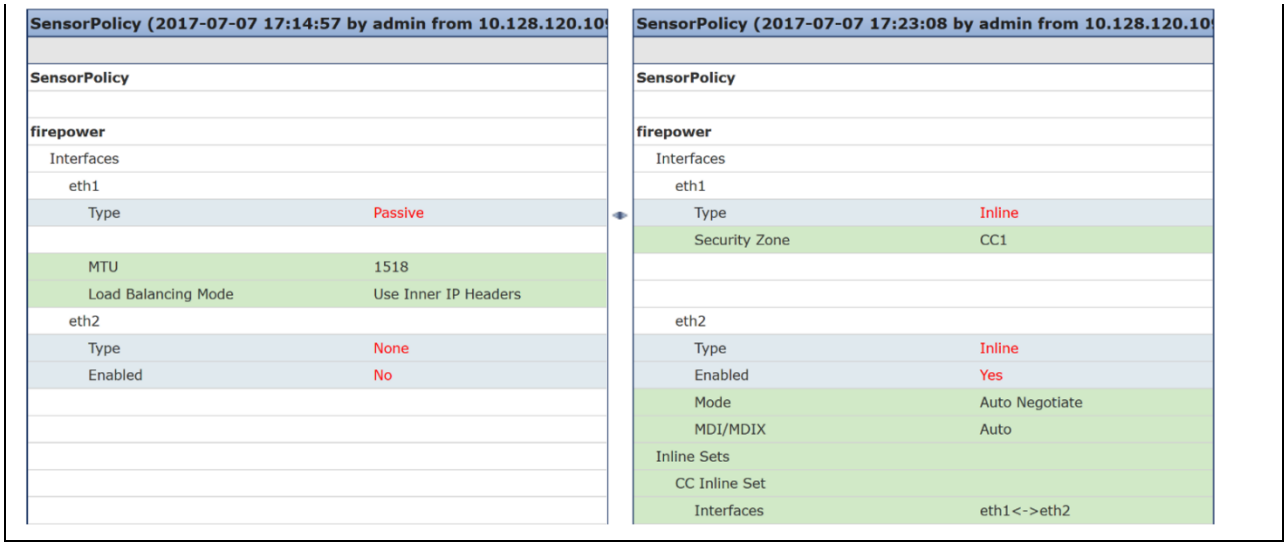
6. Change eth1 and eth2 back to inline mode. Doing this also enables eth2.

Audit Record:

2017-07-07 17:23:20	admin	Devices > Device Management > Device Edit > Interfaces	Save:364	10.128.120.109

Click on the compare ( ) icon to see what change.

© 2023 Cisco Systems, Inc. All rights reserved.



SensorPolicy (2017-07-07 17:14:57 by admin from 10.128.120.10	
SensorPolicy	
firepower	
Interfaces	
eth1	
Type	Passive
MTU	1518
Load Balancing Mode	Use Inner IP Headers
eth2	
Type	None
Enabled	No

SensorPolicy (2017-07-07 17:23:08 by admin from 10.128.120.10	
SensorPolicy	
firepower	
Interfaces	
eth1	
Type	Inline
Security Zone	CC1
eth2	
Type	Inline
Enabled	Yes
Mode	Auto Negotiate
MDI/MDIX	Auto
Inline Sets	
CC Inline Set	
Interfaces	eth1<->eth2

4.6 Configure Security Intelligence

If you want to always allow, block, or monitor specific IP addresses, URLs, or domain names, you must configure custom objects, lists, or feeds. For your convenience, Cisco provides feeds containing IP addresses, domain names, and URLs with poor reputation, as determined by Talos:

- The *Intelligence Feed*, which comprises several regularly updated collections of IP addresses.
- The *DNS and URL Intelligence Feed*, which comprises several regularly updated collection of domain names and URLs.

You can also customize the feature to suit the unique needs of your organization, for example:

- **Global Block List and custom Block List** —the system allows you to manually customize a Block List with specific IP addresses, URLs, or domain names in many ways depending on your needs.
- **Using the Block List to eliminate false negatives**—when a Do-Not-Block List is too broad in scope, or incorrectly allows traffic that you want blocked, you can override a Do-Not-Block List with a custom Block List.
- **Monitoring instead of using Block List** —especially useful in passive deployments and for testing feeds before you implemented them; you can merely monitor and log the violating sessions instead of blocking them.

By default, Security Intelligence filtering is not constrained by zone, that is, Security Intelligence objects have an associated zone of Any. You can constrain by only one zone. To enforce Security Intelligence filtering for an object on multiple zones, you must add the object to the Do-Not-Block List or Block List separately for each zone. Also, the default Do-Not-Block List or Block List cannot be constrained by zone.

1. Login with Administrator Role or Access Admin.

   NOTE: You must be ‘admin’ or ‘access admin’ role to configure this.

2. Select **Policies > Access Control**.

© 2023 Cisco Systems, Inc. All rights reserved.

3. Click the edit icon () next to the access control policy you want to configure.
4. Click on the **Security Intelligence** tab.
5. You have the following options:
    - Click the **Networks** tab to add network objects.
    - Click the **URLs** tab to add URL objects.
6. Find the **Available Objects** you want to add to the Do-Not-Block List or Block List.
7. Select one or more **Available Objects** to add.
8. Optionally, constrain the selected objects by zone by selecting an **Available Zone**.

NOTE: You cannot constrain system-provided Security Intelligence lists by zone.

9. Click **Add to Do-Not-Block List** or **Add to Block List**, or click and drag the selected objects to either list.
10. Optionally, set blocked objects to monitor-only by right-clicking the object under **Block List**, then selecting **Monitor-only (do not block)**.
11. Choose a DNS policy from the **DNS Policy** drop-down list.
12. Click **Save**.

The policy hierarchy order is not configurable and follows this order: Security Intelligence (Block List takes precedence over Do-Not-Block List), anomaly-based rules, then signature-based rules.

4.7 Managing Intrusion Policies

Intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic. Intrusion policies are invoked by your access control policy and are the system's last line of defense before traffic is allowed to its destination.

At the heart of each intrusion policy are the intrusion rules. An enabled rule causes the system to generate intrusion events for (and optionally block) traffic matching the rule. Disabling a rule stops processing of the rule.

The Firepower System delivers several base intrusion policies, which enable you to take advantage of the experience of the Cisco Talos Security Intelligence and Research Group (Talos). For these policies, Talos sets intrusion and preprocessor rule states (enabled or disabled), as well as provides the initial configurations for other advanced settings.

For intrusion rules to affect traffic, you must correctly configure drop rules and rules that replace content, as well as well as correctly deploy managed devices inline, that is, with inline interface sets. Finally, you must enable the intrusion policy's *drop behavior*, or **Drop when Inline** setting.

4.7.1 Create Intrusion Policy

When you create a new intrusion policy you must give it a unique name, specify a base policy, and specify drop behavior.

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click **Create Policy**.
4. Enter a unique **Name** and, optionally, a **Description**.

© 2023 Cisco Systems, Inc. All rights reserved.

5. Specify the initial **Base Policy**.

   You can use either a system-provided or another custom policy as your base policy.

6. Set the policy's drop behavior:
   - Check the **Drop when Inline** check box to allow intrusion rules to affect traffic and generate events.
   - Clear the **Drop when Inline** check box to prevent intrusion rules from affecting traffic while still generating events.
7. Create the policy:
   - Click **Create Policy** to create the new policy and return to the Intrusion Policy page. The new policy has the same settings as its base policy.
   - Click **Create and Edit Policy** to create the policy and open it for editing in the advanced intrusion policy editor.

Audit Record:

2016-11-22 18:07:08	admin	Policies > Intrusion > Intrusion Policy > Test	Policy Committed - "Create initial policy"	10.128.120.41

4.7.2 Viewing Intrusion Rules in an Intrusion Policy

You can adjust how rules are displayed in the intrusion policy, and can sort rules by several criteria. You can also display the details for a specific rule to see rule settings, rule documentation, and other rule specifics.

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click the edit icon ( ) next to the intrusion policy.
4. Click **Rules** under **Policy Information** in the navigation panel.
5. Check the rule whose rule details you want to view.
6. Click **Show details** button.

4.7.3 Intrusion Rule States

Intrusion rule states allow you to enable or disable the rule within an individual intrusion policy, as well as specify which action the system takes if monitored conditions trigger the rule.

In an intrusion policy, you can set a rule's state to the following values:

Generate Events

You want the system to detect a specific intrusion attempt and generate an intrusion event when it finds matching traffic. When a malicious packet crosses your network and triggers the rule, the packet is sent to its destination and the system generates an intrusion event. The malicious packet reaches its target, but you are notified via the event logging.

© 2023 Cisco Systems, Inc. All rights reserved.

Drop and Generate Events

You want the system to detect a specific intrusion attempt, drop the packet containing the attack, and generate an intrusion event when it finds matching traffic. The malicious packet never reaches its target, and you are notified via the event logging.

Note that rules set to this rule state generate events but do not drop packets in a passive deployment, including deployments where a 7000 or 8000 Series device inline interface set is in tap mode. For the system to drop packets, you must also enable the **Drop when Inline** in your intrusion policy and deploy your device inline.

Disable

You do not want the system to evaluate matching traffic.

NOTE: Choosing either the **Generate Events** or **Drop and Generate Events** options enables the rule. Choosing **Disable** disables the rule.

---

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click the edit icon () next to the intrusion policy.
4. Click **Rules** under **Policy Information** in the navigation panel.
5. Choose the rule or rules where you want to set the rule state.
6. Choose one of the following:
   - **Rule State** > **Generate Events**
   - **Rule State** > **Drop and Generate Events**
   - **Rule State** > **Disable**
7. To save changes you made in this policy since the last policy commit, click **Policy Information** in the navigation panel, then click **Commit Changes**.

   If you leave the policy without committing changes, changes since the last commit are discarded if you edit a different policy.

Audit Record:

2016-11-22 18:11:26	admin	Intrusion Policy > default > rule_configs	Added "Drop and generate events" to APP-DETECT 12P DNS request attempt (1:3706

4.7.4 Adding and Modifying Intrusion Event Thresholds

You can set a threshold for one or more specific rules in an intrusion policy. You can also separately or simultaneously modify existing threshold settings. You can set a single threshold for each. Adding a threshold overwrites any existing threshold for the rule.

© 2023 Cisco Systems, Inc. All rights reserved.

You can also modify the global threshold that applies by default to all rules and preprocessor-generated events associated with the intrusion policy. Please see the “Global Rule Threshold” section for more details.

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click the edit icon () next to the intrusion policy.
4. Click **Rules** under **Policy Information** in the navigation panel.
5. Choose the rule or rules where you want to set a threshold.
6. Choose **Event Filtering** > **Threshold**. To remove the threshold, choose **Event Filtering** > **Remove Thresholds**.
7. Choose a threshold type from the **Type** drop-down list.
8. From the **Track By** drop-down list, choose whether you want the event instances tracked by **Source** or **Destination** IP address.
9. Enter a value in the **Count** field.
10. Enter a value in the **Seconds** field.
11. Click **OK**.
12. To save changes you made in this policy since the last policy commit, click **Policy Information** in the navigation panel, then click **Commit Changes**.

    If you leave the policy without committing changes, changes since the last commit are discarded if you edit a different policy.

Audit Record:

2016-11-22 18:14:53	admin	Intrusion Policy > Test > rule_configs > APP-DETECT 12P DNS request attempt (1:37062) > threshold	Added "Threshold" to Type
2016-11-22 18:14:53	admin	Intrusion Policy > Test > rule_configs > APP-DETECT 12P DNS request attempt (1:37062) > threshold	Added "Source" to Track By
2016-11-22 18:14:53	admin	Intrusion Policy > Test > rule_configs > APP-DETECT 12P DNS request attempt (1:37062) > threshold	Added "12" to Count
2016-11-22 18:14:53	admin	Intrusion Policy > Test > rule_configs > APP-DETECT 12P DNS request attempt (1:37062) > threshold	Added "60" to Seconds

4.7.5 Intrusion Rules Editor

An *intrusion rule* is a set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities on your network. As the system analyzes network traffic, it compares packets against the conditions specified in each rule. If the packet data matches all the conditions specified in a rule, the rule triggers. If a rule is an *alert rule*, it generates an intrusion event. If it is a *pass rule*, it ignores the traffic. For a *drop rule* in an inline deployment, the system drops the packet and generates an event. You can view and evaluate intrusion events from the Firepower Management Center web interface.

All rules contain two logical sections: the rule header and the rule options. The rule header contains:

- the rule's action or type

© 2023 Cisco Systems, Inc. All rights reserved.

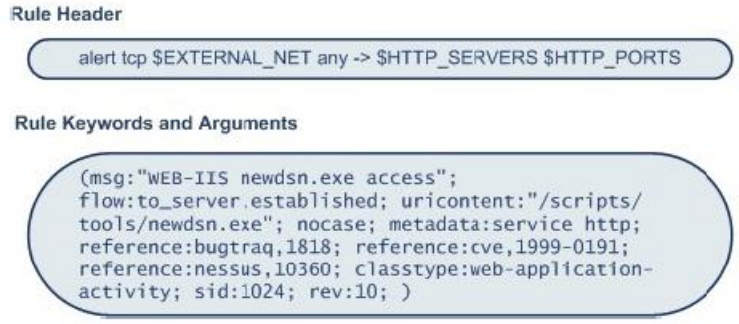
- the protocol
- the source and destination IP addresses and netmasks
- direction indicators showing the flow of traffic from source to destination
- the source and destination ports

The rule options section contains:

- event messages
- keywords and their parameters and arguments
- patterns that a packet's payload must match to trigger the rule
- specifications of which parts of the packet the rules engine should inspect

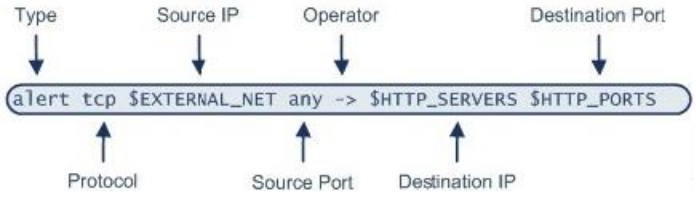
The following diagram illustrates the parts of a rule:

For example,



Intrusion Rule Header

Every rule has a rule header containing parameters and arguments. The following illustrates parts of a rule header:



Action (*alert*) – Generates an intrusion event when triggered. Other actions include pass or drop.
Protocol (*tcp*) – Tests TCP traffic only. ICMP, IP, TCP, and UDP protocols are also supported.
Source IP (*$EXTERNAL_NET*) – Tests traffic coming from any host that is not on your internal network.
Source Port (*any*) – Tests traffic coming from any port on the originating host.
Operate (->) – Tests external traffic destined for the web servers on your network.
Destination IP (*$HTTP_SERVERS*) - Tests traffic to be delivered to any host specified as a web server on your internal network. Both IP and IPv6 addresses and ranges are supported.
Destination Port (*$HTTP_PORTS*) - Tests traffic delivered to an HTTP port on your internal network.

Intrusion Rule Options and Keywords

Rule options follow the rule header and are enclosed inside a pair of parentheses. There may be one option or many and the options are separated with a semicolon. If you use multiple options, these options form a logical AND. The action in the rule header is invoked only when all criteria in the options are true. In general, an option may have two parts: a keyword and an argument.

© 2023 Cisco Systems, Inc. All rights reserved.

The *message* keyword: Specify meaningful text that appears as a message when the rule triggers.

The *ack* keyword: Specify the acknowledgement value. For example, (flags: A; ack: 0; msg: "TCP ping detected";)means receive a TCP packet with the A flag set and the acknowledgement contains a value of 0.

The *content* keyword: Specify data pattern inside a packet. The pattern may be presented in the form of an ASCII string or as binary data in the form of hexadecimal characters.

The *offset* keyword: Specify a certain offset from the start of the data part of the packet to search.

The *dsize* keyword: Specify the length of the data part of a packet.

The *flags* keyword: Find out which flag bits are set inside the TCP header of a packet.

The *fragbits* keyword: Find out which three frag bits (Reserved, Don't Frag, More Frag) in the IP headers.

The *fragoffset* keyword: Tests the offset of a fragmented packet.

The *itype* keyword: Specify the ICMP type.

The *icode* keyword: Specify the ICMP code.

The *icmp_id* keyword: Specify the ICMP identification number.

The *icmp_seq* keyword: Specify the ICMP sequence number.

The *ipopts* keyword: Specify the IP Options. Record Route, Loose Source Routing, Strict Source Routing.

The *ip_proto* keyword: Specify the IP protocol number.

The *id* keyword: Specify the IP header fragment identification field

The *nocase* keyword: Its only purpose is to make a case insensitive search of a pattern within the data part of a packet. It is used in conjunction with the *content* keyword.

The *seq* keyword: Specify the sequence number of a TCP packet.

The *window* keyword: Specify the TCP window size.

The *flow* keyword: Apply a rule on TCP sessions to packets flowing in a particular direction.

The *tos* keyword: Detect a specific value in the Type of Service (TOS) field of the IP header.

The *ttl* keyword: Detect Time to Live value in the IP header of the packet.

Required Header Field Inspection	Intrusion Rule Keyword or Rule

© 2023 Cisco Systems, Inc. All rights reserved.

IPv4:	
Version	alert (msg:"DECODE_NOT_IPV4_DGRAM"; sid:1; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
Header Length	alert (msg:"DECODE_IPV4_INVALID_HEADER_LEN"; sid:2; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
Packet Length	alert (msg:"DECODE_IPV4_DGRAM_LT_IPHDR"; sid:3; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;) alert (msg:"DECODE_IPV4_DGRAM_GT_CAPLEN"; sid:6; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
ID	*id*
IP Flags	*fragbits*
Fragment Offset	*fragoffset*
Time to Live (TTL)	*ttl*
Protocol	*ip_proto*
Header Checksum	Inspected by “Checksum Verification” preprocessor.
Source Address	*Source IP* OR alert (msg:"DECODE_IP4_SRC_MULTICAST"; sid:410; gid:116; rev:1; metadata:rule-type decode; classtype:misc-activity;)
Destination Address	*Destination IP* OR alert (msg:"DECODE_IP4_DST_RESERVED"; sid:412; gid:116; rev:1; metadata:rule-type decode; classtype:misc-activity;)
IP Options.	*ipopts*
IPv6:	
Version	alert (msg:"DECODE_IPV6_IS_NOT"; sid:271; gid:116; rev:1; metadata:rule-type decode; classtype: protocol-command-decode;)
payload length	*dsize* OR alert (msg:"DECODE_IPV6_TRUNCATED_EXT"; sid:272; gid:116; rev:1; metadata:rule-type decode; classtype:bad-unknown;)

© 2023 Cisco Systems, Inc. All rights reserved.

next header	alert (msg:"DECODE_IPV6_BAD_NEXT_HEADER"; sid:281; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
hop limit	alert (msg:"DECODE_IPV6_MIN_TTL"; sid:270; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
source address	*Source IP* OR alert (msg:"DECODE_IPV6_SRC_MULTICAST"; sid:277; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
destination address	*Destination IP* OR alert (msg:"DECODE_IPV6_DST_RESERVED_MULTICAST"; sid:278; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;) alert (msg:"DECODE_IPV6_DST_ZERO"; sid:276; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
routing header	alert (msg:"DECODE_IPV6_ROUTE_AND_HOPBYHOP"; sid:282; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;) alert (msg:"DECODE_IPV6_TWO_ROUTE_HEADERS"; sid:283; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
ICMP:	
Type	*itype*
Code	*icode*
Header Checksum	Inspected by “Checksum Verification” preprocessor.
Rest of Header(varies based on the ICMP type and code)	*icmp_id, icmp_seq*
ICMPv6:	
Type	*itype*
Code	*icode*
Header Checksum	Inspected by “Checksum Verification” preprocessor.
TCP:	

© 2023 Cisco Systems, Inc. All rights reserved.

source port	*Source Port*
destination port	*Destination Port*
sequence number	*seq*
acknowledgement number	*ack*
offset	alert (msg:"DECODE_TCP_INVALID_OFFSET"; sid:46; gid:116; rev:1; metadata:rule-type decode; reference:cve,2004-0816; classtype:bad-unknown;)
reserved	Inspected and normalized by preprocessor, if configured.
TCP flags	*flags*
window	*window*
checksum	Inspected by “Checksum Verification” preprocessor.
urgent pointer	alert (msg:"DECODE_TCP_BAD_URP"; sid:419; gid:116; rev:1; metadata:rule-type decode; classtype: misc-activity;) OR Inspected and normalized by preprocessor, if configured.
TCP options	alert (msg:"DECODE_TCPOPT_TRUNCATED"; sid:55; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
UDP:	
Source port	*Source Port*
destination port	*Destination Port*
length;	alert (msg:"DECODE_UDP_DGRAM_INVALID_LENGTH"; sid:96; gid:116; rev:1; metadata:rule-type decode; classtype:protocol-command-decode;)
UDP checksum	Inspected by “Checksum Verification” preprocessor.

Writing New Rules

1. Login with Administrator Role or Intrusion Admin.
2. Access the intrusion rules using either of the following methods:
    - Choose **Policies > Access Control > Intrusion** then click **Intrusion Rules**.
    - Choose **Objects** > **Intrusion Rules**.
3. Click **Create Rule**.
4. Enter a value in the **Message** field.
5. Choose a value from each of the following drop-down lists:

© 2023 Cisco Systems, Inc. All rights reserved.

- **Classification**
- **Action**
- **Protocol**
- **Direction**

6. Enter values in the following fields:
   - **Source IPs**
   - **Destination IPs**
   - **Source Port**
   - **Destination Port**

   NOTE: The system uses the value '*any*' if you do not specify a value for these fields.
7. Click **Add Option**.
8. Enter any arguments for the keyword you added.
9. Optionally, repeat steps 6 to 8.
10. If you added multiple keywords, you can:
    - Reorder keywords – Click the up or down arrow next to the keyword you want to move.
    - Delete a keyword – Click the **X** next to that keyword.
11. Click **Save As New**.

Audit Record:

2016-11-17 18:40:22	admin	Policies > Intrusion > Rule Editor > Create	save 1.1000000.1	10.128.120.41

4.7.6 Intrusion Rules Import

As new vulnerabilities become known, the Cisco Talos Security Intelligence and Research Group (Talos) releases intrusion rule updates that you can import onto your Firepower Management Center, and then implement by deploying the changed configuration to your managed devices. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules.

Intrusion rule updates are cumulative, and Cisco recommends you always import the latest update.

For changes made by an intrusion rule update to take effect, you must redeploy configurations. When importing a rule update, you can configure the system to automatically redeploy to affected devices. This approach is especially useful if you allow the intrusion rule update to modify system-provided base intrusion policies.

1. Manually download the update from the Cisco Support Site (http://www.cisco.com/cisco/web/support/index.html).
2. Login with Administrator Role.
3. Choose **System** > **Updates**, then click the **Rule Updates** tab.

© 2023 Cisco Systems, Inc. All rights reserved.

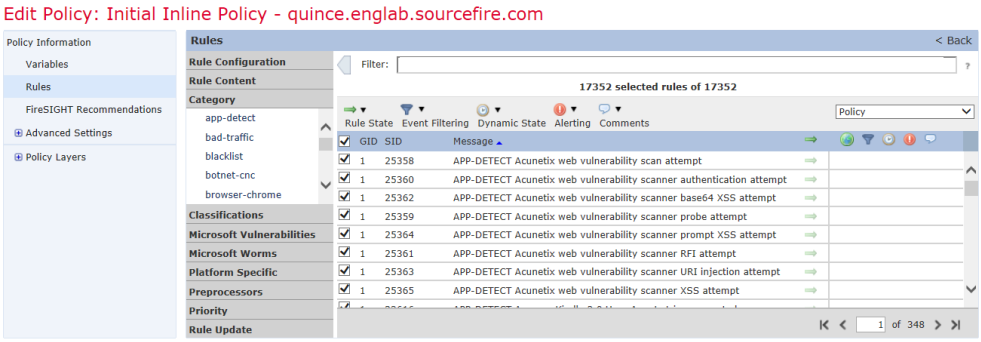
4. If you want to move all user-defined rules that you have created or imported to the deleted folder, you must click **Delete All Local Rules** in the toolbar, then click **OK**.
5. Choose **Rule Update or text rule file to upload and install** and click **Browse** to navigate to and choose the rule update file.
6. If you want to automatically re-deploy policies to your managed devices after the update completes, choose **Reapply all policies after the rule update import completes**.
7. Click **Import**. The system installs the rule update and displays the Rule Update Log detailed view.

NOTE: Contact Support if you receive an error message while installing the rule update.

4.7.7 Configure Dynamic Rule State

The administrator can configure traffic bandwidth control at the policy level to stop excessive traffic from a specific source or network, to a specific destination or network, or all detected traffic.

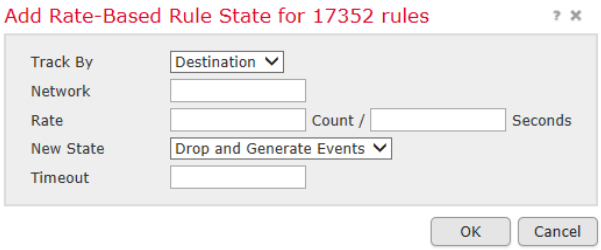
1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click the edit icon ( ) next to the policy you want to configure.
4. Click **Rules** under **Policy Information** in the navigation panel.
5. Select the rule or rules where you want to add a dynamic rule state. You have the following options:
   - To select a specific rule, select the check box next to the rule.
   - To select all the rules, select the check box at the top of the column.



6. Select **Dynamic State > Add Rate-Based Rule State**.

   The Add Rate-Based Rule State dialog box appears.

© 2023 Cisco Systems, Inc. All rights reserved.



7. Select the appropriate **Track By** option to indicate how you want the rule matches tracked:
    - Select **Source** to track the number of hits for that rule from a specific source or set of sources.
    - Select **Destination** to track the number of hits for that rule to a specific destination or set of destinations.
    - Select **Rule** to track all matches for that rule.
8. When you set **Track By** to **Source** or **Destination**, enter the address of each host you want to track in the **Network** field.

    You can specify a single IP address, address block, variable, or a comma-separated list comprised of any combination of these.
9. Indicate the number of rule matches per time period to set the attack rate:
    - In the **Count** field, using an integer between 1 and 2147483647, specify the number of rule matches you want to use as your threshold.
    - In the **Seconds** field, using an integer between 1 and 2147483647, specify the number of seconds that make up the time period for which attacks are tracked.
10. Select a **New State** radio button to specify the action to be taken when the conditions are met:
    - Select **Drop and Generate Events** to generate an event and drop the packet that triggered the event in inline deployments or generate an event in passive deployments.
11. In the **Timeout** field, type the number of seconds you want the action to remain in effect. After the timeout occurs, the rule reverts to its original state. Specify 0 or leave the field blank to prevent the action from timing out.
12. Click **OK**.
13. Select **Commit Changes**.
14. Deploy the policy.

Audit Record:

2013-03-19 18:03:50	admin	Intrusion Policy > CC Test > advanced_configs > rate_based_attacks > control_connections > connect > Control Simultaneous Connections 1	Added "Source" to Track By
2013-03-19 18:03:50	admin	Intrusion Policy > CC Test > advanced_configs > rate_based_attacks > control_connections > connect > Control Simultaneous Connections 1	Added "10.1.1.1" to Network
2013-03-19 18:03:50	admin	Intrusion Policy > CC Test > advanced_configs > rate_based_attacks > control_connections > connect > Control Simultaneous Connections 1	Added "1000" to Count
2013-03-19 18:03:50	admin	Intrusion Policy > CC Test > advanced_configs > rate_based_attacks > control_connections > connect > Control Simultaneous Connections 1	Added "No" to Drop
2013-03-19 18:03:50	admin	Intrusion Policy > CC Test > advanced_configs > rate_based_attacks > control_connections > connect > Control Simultaneous Connections 1	Added "1" to Timeout

© 2023 Cisco Systems, Inc. All rights reserved.

4.7.8 Global Rule Threshold

The global rule threshold sets limits for event logging by an intrusion policy. You can set a global rule threshold across all traffic to limit how often the policy logs events from a specific source or destination and displays those events per specified time period. You can also set thresholds per rule, or preprocessor rule in the policy. When you set a global threshold, that threshold applies for each rule in the policy that does not have an overriding specific threshold. Thresholds can prevent you from being overwhelmed with a large number of events.

Every intrusion policy contains a default global rule threshold that applies by default to all intrusion rules and preprocessor rules. This default threshold limits the number of events on traffic going to a destination to one event per 60 seconds.

You can:

- Change the global threshold.
- Disable the global threshold.
- Override the global threshold by setting individual thresholds for specific rules.

  For example, you might set a global limit threshold of five events every 60 seconds, but then set a specific threshold of ten events for every 60 seconds for SID1315. All other rules generate no more than five events in each 60-second period, but the system generates up to ten events for each 60-second period for SID1315.

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click the edit icon ( ) next to the policy you want to configure.
4. Click **Advanced Setting** in the navigation panel.
5. If **Global Rule Thresholding** under **Intrusion Rule Thresholds** is disabled, click **Enabled**.
6. Click the edit icon ( ) next to **Global Rule Thresholding**.
7. Using the **Type** radio buttons, specify the type of threshold that will apply over the time you specify in the **Seconds** field.
   - **Limit**

     Logs and displays events for the specified number of packets (specified by the count argument) that trigger the rule during the specified time period.

     For example, if you set the type to **Limit**, the **Count** to *10*, and the **Seconds** to *60*, and 14 packets trigger the rule, the system stops logging events for the rule after displaying the first 10 that occur within the same minute.
   - **Threshold**
     Logs and displays a single event when the specified number of packets (specified by the count argument) trigger the rule during the specified time period. Note that the counter for the time restarts after you hit the threshold count of events and the system logs that event.

© 2023 Cisco Systems, Inc. All rights reserved.

For example, you set the type to **Threshold**, **Count** to *10*, and **Seconds** to *60*, and the rule triggers 10 times by second 33. The system generates one event, then resets the Seconds and Count counters to 0.

- **Both**
  Logs and displays an event once per specified time period, after the specified number (count) of packets trigger the rule.

  For example, if you set the type to **Both**, **Count** to *2*, and **Seconds** to *10*, the following event counts result:
  - If the rule is triggered once in 10 seconds, the system does not generate any events (the threshold is not met).
  - If the rule is triggered twice in 10 seconds, the system generates on eevent (the threshold is met when the rule triggers the second time).
  - If the rule is triggered four times in 10 seconds, the system generates one event (the threshold is met when the rule triggered the second time and following events are ignored).

8. Using the **Track By** radio buttons, specify the tracking method. This determines whether the event in stance count is calculated per source or destination IP address.
9. Enter a value in the **Count** field.
10. Enter a value in the **Seconds** field.
11. To save changes you made in this policy since the last policy commit, click **Policy Information**, then click **Commit Changes**.

Audit Record:

2016-11-17 19:48:46	admin	Intrusion Policy > default > advanced_configs > threshold_global	Changed Count to "2" (from "1")	10.128.120.41
2016-11-17 19:48:46	admin	Intrusion Policy > default > advanced_configs > threshold_global	Changed Seconds to "65" (from "60")	10.128.120.41

4.8 Stateful Session Behaviors

The system implements packet decoders and preprocessors to detect anomalous traffic that might signal an intrusion attempt and, when the appropriate enabled accompanying decoder and preprocessor rules, report on detected anomalies. Next, intrusion rules examine the decoded packets for attacks based on patterns. Used together, intrusion rules and preprocessors provide broader and deeper packet inspection than a signature-based system and help to identify intrusions more effectively.

Before packets can be inspected, the packets must be captured from the network. As the system captures packets, it sends them to the packet decoder. The packet decoder converts the packet headers and payloads into a format that can be easily used by the preprocessors and the rules engine. Each layer of the TCP/IP stack is decoded in turn, beginning with the data link layer and continuing through the network and transport layers, as described in the following table.

TCP/IP Layer	Decoded Packets
Data Link	Ethernet

© 2023 Cisco Systems, Inc. All rights reserved.

	Virtual local area network (VLAN)
Network	Internet Protocol version 4 (IPv4)
	Internet Protocol version 6 (IPv6)
	Internet Control Message Protocol version 4 (ICMPv4)
	Internet Control Message Protocol version 6 (ICMPv6)
Transport	Transmission Control Protocol (TCP)
	User Datagram Protocol (UDP)

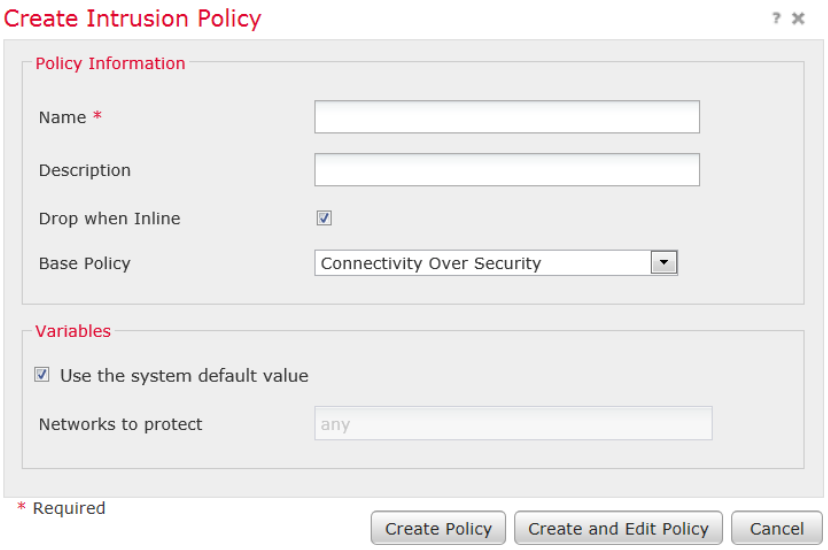
After the packets are decoded through the first three TCP/IP layers, they are sent to preprocessors, which normalize traffic at the application layer and detect protocol anomalies. The following three preprocessors must be enabled and configured in the evaluated configuration (be default, all three preprocessors are enabled):

- TCP Streaming Preprocessor - Administrators can configure the system so that the preprocessor detects any TCP traffic that cannot be identified as part of an established TCP session. Stateful inspection allows administrators to ignore these packets because they are not part of an established TCP session and do not provide meaningful information.
- UDP Streaming Preprocessor - UDP data streams are not typically thought of in terms of sessions. However, the stream preprocessor uses the source and destination IP address fields in the encapsulating IP datagram header and the port fields in the UDP header to determine the direction of flow and identify a session.
- IP Defragmentation Preprocessor - When an IP datagram is broken into two or more smaller IP datagrams because it is larger than the maximum transmission unit (MTU), it is fragmented. A single IP datagram fragment may not contain enough information to identify a hidden attack. Attackers may attempt to evade detection by transmitting attack data in fragmented packets or attempt to crash the system when reassembling the fragmented packets. The IP defragmentation preprocessor reassembles fragmented IP datagrams, and if fragmented datagrams cannot be reassembled, it will be rejected (i.e., dropped) and logged with certain intrusion rules enabled.

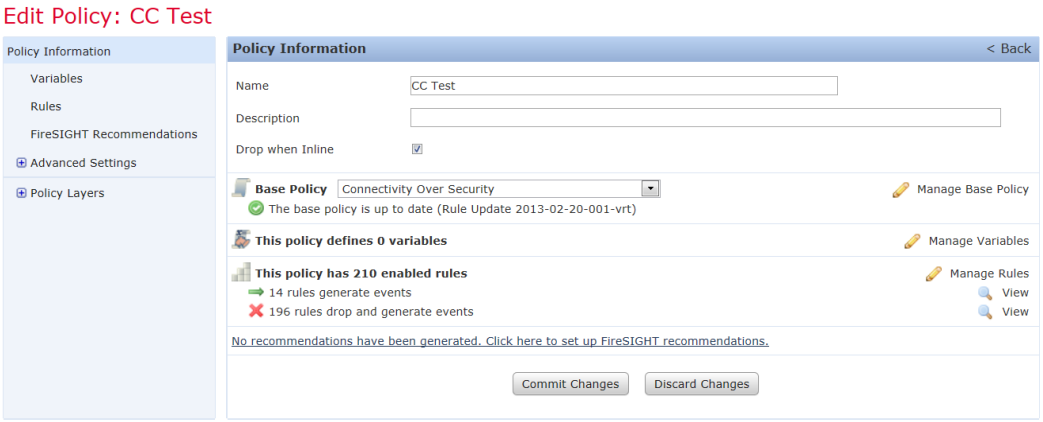
4.8.1 Verify Enabled Preprocessors

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click **Create Policy**.

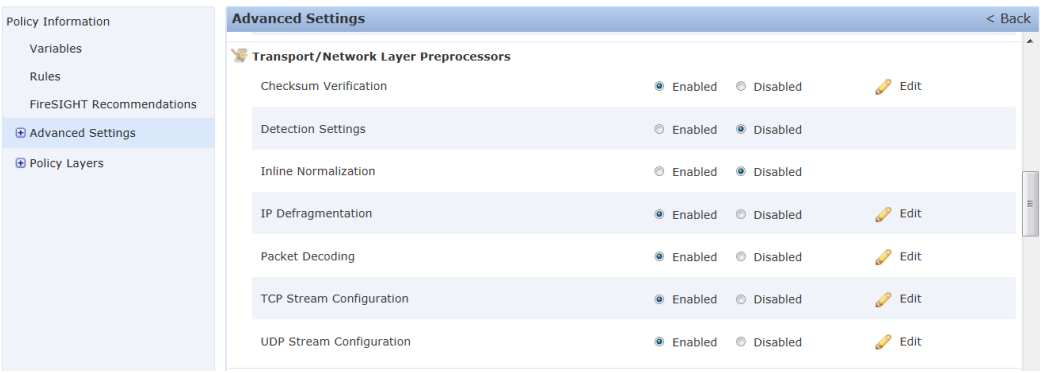
© 2023 Cisco Systems, Inc. All rights reserved.



4. In the **Name** field, enter a unique name and optionally a description.
5. Click **Create and Edit Policy**.



6. Click **Advanced Settings**.
7. Verify that IP Defragmentation, TCP Stream and UDP Stream are enabled.



8. Click on **Policy Information** and **Commit Changes**.

© 2023 Cisco Systems, Inc. All rights reserved.

9. Optionally, enter a comment and click **OK**.
10. Associate the intrusion policy with the access control policy.

NOTE! You cannot apply the intrusion policy until it is associated with an access control policy or rule.

Audit Record:

2013-03-19 19:26:14	admin	Policies > Intrusion > Intrusion Policy > CC Test	Policy Committed: "Create initial policy"	10.4.11.248
2013-03-19 19:28:10	admin	Intrusion Policy > CC Test > advanced_configs > normalize	Added "Enabled" to Normalize TCP	10.4.11.248
2013-03-19 19:28:10	admin	Intrusion Policy > CC Test > advanced_configs > normalize	Added "Enabled" to Normalize TCP Payload	10.4.11.248

4.8.2 Configure Anomaly Detection

Preprocessors prepare traffic to be further inspected by normalizing traffic and identifying protocol anomalies. Preprocessors can generate preprocessor events when packets trigger preprocessor options that you configure. The base policy for your network analysis policy determines which preprocessors are enabled by default and the default configuration for each.

The FTP/Telnet decoder analyzes FTP and telnet data streams, normalizing FTP and telnet commands before processing by the rules engine. You can enable rule126:3 to generate an event when this anomaly is detected in Telnet traffic, and rule125:9 when it is detected on the FTP command channel.

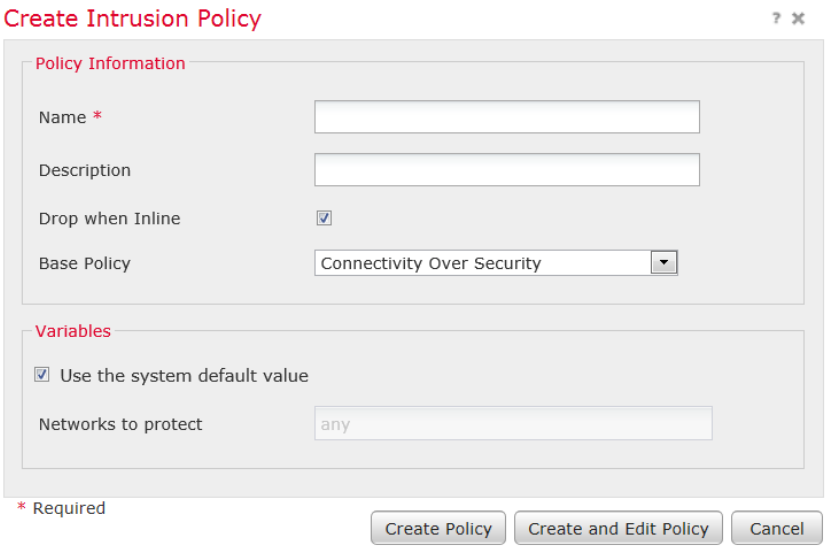
The inline normalization preprocessor normalizes traffic to minimize the chances of attackers evading detection in inline deployments. You can specify normalization of any combination of IPv4, IPv6, ICMPv4, ICMPv6, and TCP traffic. When the packet decoding **Detect Protocol Header Anomalies** option is enabled, you can enable the following rules in the decoder rule category to generate events for this option:

- You can enable rule 116:428 to generate an event when the system detects an IPv4 packet with a TTL less than the specified minimum.
- You can enable rule 116:270 to generate an event when the system detects an IPv6 packet with a hop limit that is less than the specified minimum.

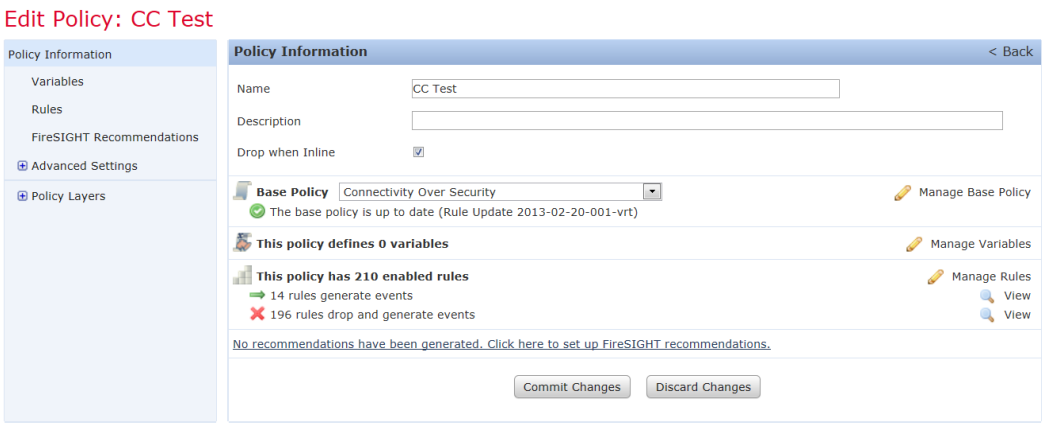
The system can detect, drop, and log anomaly fragmented packets if the IP Defragmentation Preprocessor is enabled and certain intrusion rules are enabled.

1. Login with Administrator Role or Intrusion Admin.
2. Select **Policies > Access Control > Intrusion**.
3. Click **Create Policy**.

© 2023 Cisco Systems, Inc. All rights reserved.

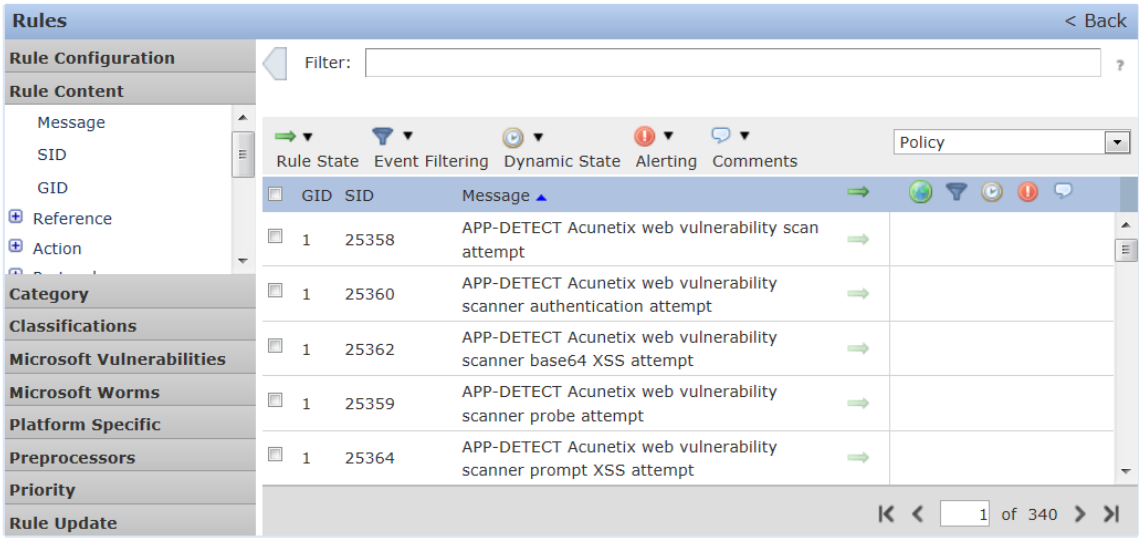


4. In the **Name** field, enter a unique name and optionally a description.
5. Click **Create and Edit Policy**.



6. Click **Manage Rules**.

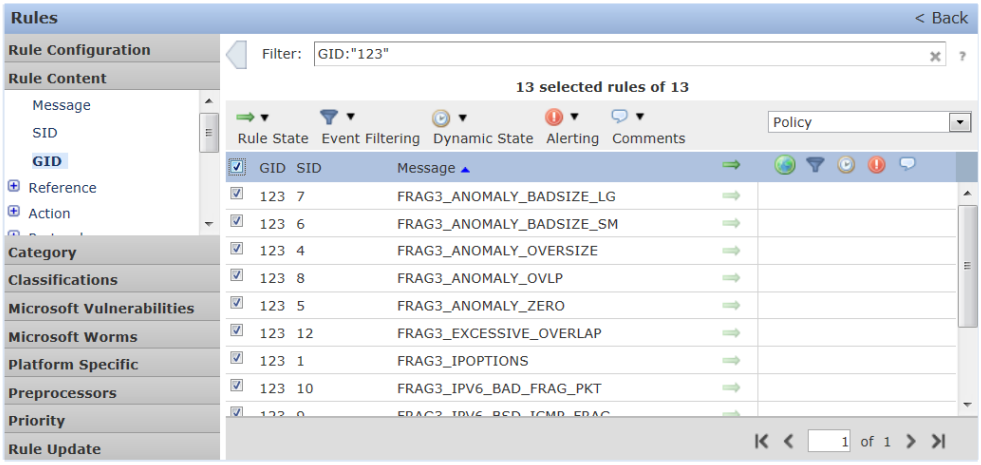
© 2023 Cisco Systems, Inc. All rights reserved.



7. Click **Rule Content** and select **GID**.

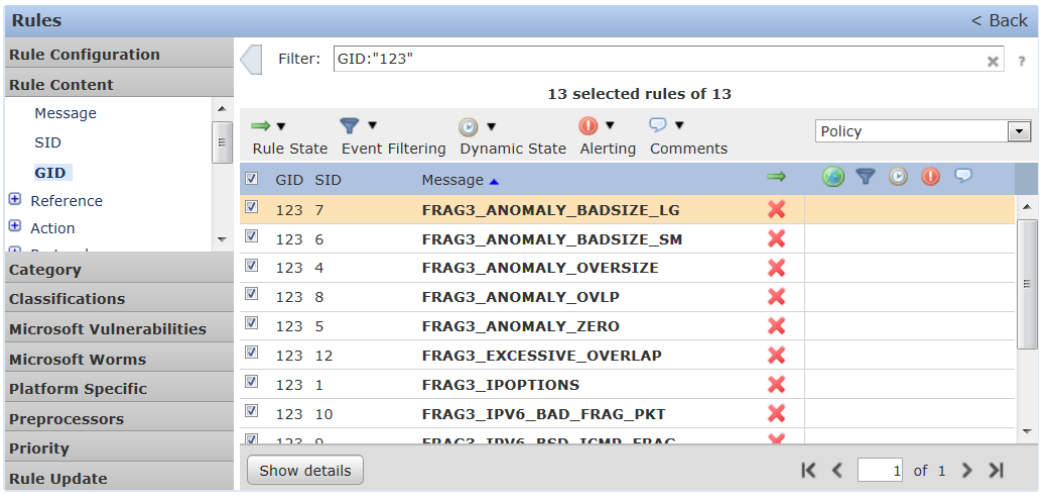
   The Enter the GID filter pop-up window appears.

8. Enter **123** and click **OK**.
9. Select all the rules. Hint: Click the top checkbox.

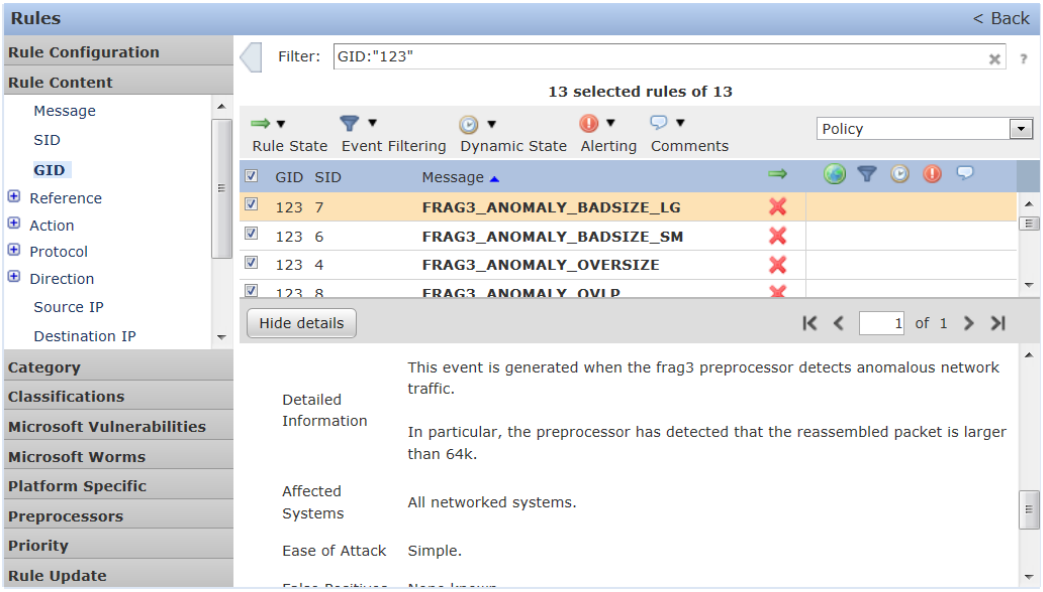


10. In the **Rule State** field, click and select **Drop and Generate Events**.

© 2023 Cisco Systems, Inc. All rights reserved.



11. For more details on each rule, click on a rule and select **Show details**.



11. Click on **Policy Information** and **Commit Changes**.
12. Optionally, enter a comment and click **OK**.
13. Associate the intrusion policy with the access control policy.

NOTE! You cannot apply the intrusion policy until it is associated with an access control policy or rule.

Audit Record:

2013-03-01 13:36:21	admin	Intrusion Policy > test2 > advanced configs > normalize	Added "Enabled" to Normalize TCP	10.4.10.223
2013-03-01 13:36:21	admin	Intrusion Policy > test2 > advanced configs > normalize	Added "Enabled" to Normalize TCP Payload	10.4.10.223
2013-03-01 13:36:20	admin	Policies > Intrusion > Intrusion Policy	Page View	10.4.10.223
2013-03-01 13:36:19	admin	Policies > Intrusion > Intrusion Policy > test2	Policy Committed: ""	10.4.10.223

© 2023 Cisco Systems, Inc. All rights reserved.

4.8.3 Portscan Detection

A portscan is a form of network reconnaissance that is often used by attackers as a prelude to an attack. In a portscan, an attacker sends specially crafted packets to a targeted host. By examining the packets that the host responds with, the attacker can often determine which ports are open on the host and, either directly or by inference, which application protocols are running on these ports.

By itself, a portscan is not evidence of an attack. In fact, some of the port scanning techniques used by attackers can also be employed by legitimate users on your network. Cisco's portscan detector is designed to help you determine which portscans might be malicious by detecting patterns of activity.

Protocol Types

Protocol	Description
TCP	Detects TCP probes such as SYN scans, ACK scans, TCP connect() scans, and scans with unusual flag combinations such as Xmas tree, FIN, and NULL.
UDP	Detects UDP probes such as zero-byte UDP packet.
ICMP	Detects ICMP echo requests (pings).
IP	Detects IP protocol scans. These scans differ from TCP and UDP scans because the attacker, instead of looking for open ports, is trying to discover which IP protocols are supported on a target host.

When portscan detection is enabled, you must enable rules with GeneratorID (GID)122 and a SnortID (SID) from among SIDs 1 through 27 to generate events for each enabled portscan type.

Portscan Event Packet View

When you enable the a accompanying preprocessor rules, the portscan detector generates intrusion events that you can view just as you would any other intrusion event. However, the information presented on the packet view is different from the other types of intrusion events.

Begin by using the intrusion event views to drill down to the packet view for a ports can event. Note that you cannot download a portscan packet because single port scan events are based on multiple packets; however, the portscan packet view provides all usable packet information.

For any IP address, you can click the address to view the context menu and select **whois** to perform a lookup on the IP address or **View Host Profile** to view the host profile for that host.

Portscan Packet View

Information	Description
Device	The device that detected the event.
Time	The time when the event occurred.
Message	The event message generated by the preprocessor.
Source IP	The IP address of the scanning host.

© 2023 Cisco Systems, Inc. All rights reserved.

Destination IP	The IP address of the scanned host.
Port/Proto Count	For TCP and UDP portscans, the number of times that the port being scanned changes. For example, if the first port scanned is 80, the second port scanned is 8080, and the third port scanned is again 80, then the port count is 3. For IP protocol portscans, the number of times that the protocol being used to connect to the scanned host changes.
Port/Proto Range	For TCP and UDP portscans, the range of the ports that were scanned. For IP protocol portscans, the range of IP protocol numbers that were used to attempt to connect to the scanned host.
Open Ports	The TCP ports that were open on the scanned host. This field appears only when the portscan detects one or more open ports.

1 Login with Administrator Role or Intrusion Admin.

2 Select **Policies > Access Control > Intrusion** then click on **Network Analysis Policy**.

3 Click the edit icon ( ) next to the policy you want to edit.

4 Click **Settings**.

5 If **Portscan Detection** under **Specific Threat Detection** is disabled, click **Enabled**.

6 Click the edit icon ( ) next to **Portscan Detection**.

7 In the **Protocol** field, specify protocols to enable.

NOTE! You must ensure TCP stream processing is enabled to detect scans over TCP, and that UDP stream processing is enabled to detect scans over UDP. Also make sure you do not enable “Packet Size Performance Boost” and “Packet Type Performance Boost”.

8 In the **Scan Type** field, specify portscan types you want to detect.

9 Choose a level from the **Sensitivity Level** list.

NOTE! If you are encountering inconsistent detection (especially on the virtual Sensor), try disabling the “Latency-based performance setting”.

10 To save changes you made in this policy since the last policy commit, click **Policy Information**, then click **Commit Changes**.

Audit Record:

2016-11-29 13:20:15	admin	Network Analysis Policy > default > settings	Changed Portscan Detection to "Enabled" (from "Disabled")	10.128.120.136
2016-11-29 13:20:15	admin	Network Analysis Policy > default > settings > portscan	Changed Protocol to "TCP" (from "TCP, UDP")	10.128.120.136

© 2023 Cisco Systems, Inc. All rights reserved.

4.8.4 Rate-Based Attack Prevention

Rate-based attacks (i.e., flooding attacks) are attacks that depend on frequency of connection or repeated attempts to perpetrate the attack. You can use rate-based detection criteria to detect a rate-based attack as it occurs and respond to it when it happens, then return to normal detection settings after it stops.

You can configure your network analysis policy to include rate-based filters that detect excessive activity directed at hosts on your network. You can use this feature on managed devices deployed in inline mode to block rate-based attacks for a specified time, then revert to only generating events and not drop traffic.

The SYN attack prevention option helps you protect your network hosts against SYN floods. You can protect individual hosts or whole networks based on the number of packets seen over a period of time. If your device is deployed passively, you can generate events. If your device is placed inline, you can also drop the malicious packets. After the timeout period elapses, if the rate condition has stopped, the event generation and packet dropping stops.

For example, you could configure a setting to allow a maximum of 10 SYN packets from anyone IP address, and block further connections from that IP address for 60 seconds.

You can also limit TCP/IP connections to or from hosts on your network to prevent denial of service (DoS) attacks or excessive activity by users. When the system detects the configured number of successful connections to or from a specified IP address or range of addresses, it generates events on additional connections. The rate-based event generation continues until the timeout period elapses without the rate condition occurring. In an inline deployment you can choose to drop packets until the rate condition times out.

For example, you could configure a setting to allow a maximum of 10 successful simultaneous connections from anyone IP address, and block further connections from that IP address for 60 seconds.

Rate-based attack prevention identifies abnormal traffic patterns and attempts to minimize the impact of that traffic on legitimate requests. Rate-based attacks usually have one of the following characteristics:

- Any traffic containing excessive incomplete connections to hosts on the network, indicating a SYN flood attack
- Any traffic containing excessive complete connections to hosts on the network, indicating a TCP/IP connection flood attack
- Excessive rule matches in traffic going to a particular destination IP address or addresses or coming from a particular source IP address or addresses.
- Excessive matches for a particular rule across all traffic.

In a network analysis policy, you can either configure SYN flood or TCP/IP connection flood detection for the entire policy; in an intrusion policy, you can set rate-based filters for individual intrusion or preprocessor rules. Note that you cannot manually add a rate-based filter to GID135 rules or modify their rule state. Rules with GID135 use the client as the source value and the server as the destination value.

The *detection_filter* keyword prevents a rule from triggering until a threshold number of rule matches occur within a specified time. When a rule includes the *detection_filter* keyword, the system tracks the number of incoming packets matching the pattern in the rule per timeout period. The system can count

© 2023 Cisco Systems, Inc. All rights reserved.

hits for that rule from particular source or destination IP addresses. After the rate exceeds the rate in the rule, event notification for that rule begins.

You can configure rate-based attack prevention at the policy level to stop SYN flood attacks. You can also stop excessive connections from a specific source or to a specific destination.

1 Login with Administrator Role or Intrusion Admin.

2 Select **Policies > Access Control > Intrusion** then click on **Network Analysis Policy**.

3 Click the edit icon () next to the policy you want to edit.

4 Click **Settings**.

5 If **Rate-Based Attack Prevention** under **Specific Threat Detection** is disabled, click **Enabled**.

6 Click the edit icon () next to **Rate-Based Attack Prevention**.

7 You have two choices:

- To prevent incomplete connections intended to flood a host, click **Add** under **SYN Attack Prevention**.
- To prevent excessive numbers of connections, click **Add** under **Control Simultaneous Connections**.

8 Specify how you want to track traffic:

- To track all traffic from a specific source or range of sources, choose **Source** from the **Track By** drop-down list, and enter a single IP address or address block in the **Network** field.
- To track all traffic to a specific destination or range of destinations, choose **Destination** from the **Track By** drop-down list, and enter an IP address or address block in the **Network** field.

NOTE! To load-balance the traffic for maximum performance, the source and destination address and port are used to determine which Snort Instance the traffic is sent to.

9 Specify the triggering rate for the rate tracking setting:

- For SYN attack configuration, enter the number of SYN packets per number of seconds in the **Rate** fields.
- For simultaneous connection configuration, enter the number of connections in the **Count** field.

NOTE! The recommended setting is between 600 - 6,000 TCP SYN/connection requests per minute per IP address. However, the exact number will vary and will depend on the host(s) and/or network configuration.

10 To drop packets matching the rate-based attack prevention settings, check the **Drop** check box.

11 In the **Timeout** field, enter the time period after which to stop generating events (and if applicable, dropping) for traffic with the matching pattern of SYNs or simultaneous connections.

12 Click **OK**.

© 2023 Cisco Systems, Inc. All rights reserved.

13 To save changes you made in this policy since the last policy commit, click **Policy Information**, then click **Commit Changes**.

4.8.5 Specific Attacks

To detect these specific attacks, enable each of the rules listed in the table below:

Attack	Attack Category	Rule
Teardrop	IP Attack	Rule 123:2 “FRAG2_TEARDROP”
Bonk	IP Attack	Rule 123:4 “FRAG3_ANOMALY_OVERSIZE”
Boink	IP Attack	Rule 123:4 “FRAG3_ANOMALY_OVERSIZE”
Land	IP Attack	Rule 116:151 “DECODE_BAD_TRAFFIC_SAME_SRCDST”
Nuke	ICMP Attack	alert tcp $EXTERNAL_NET any -> $HOME_NET 135:139 (msg:"SERVER-OTHER Winnuke attack"; flow:stateless; flags:U+; metadata:ruleset community; reference:bugtraq,2010; reference:cve,1999-0153; classtype:attempted-dos; sid:1257000; rev:15; gid:1001;)
Ping of Death	ICMP Attack	Rule 123:7 “FRAG3_ANOMALY_BADSIZE_LG”
Null flags	TCP Attack	alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Null TCP attack"; flags:0; classtype:attempted-dos; sid:269; rev:3;)
SYN+FIN flags	TCP Attack	Rule 116:420 “DECODE_TCP_SYN_FIN”
FIN only flags	TCP Attack	alert tcp any any -> any any (sid:1000003; gid:1; flags:F*; msg:"FIN only"; classtype:attempted-dos; rev:3;)
SYN+RST flags	TCP Attack	Rule 116:421 “DECODE_TCP_SYN_RST”
Bomb	UDP Attack	Rule 116:98 “DECODE_UDP_DGRAM_LONG_PACKET”
Chargen DoS	UDP Attack	Rule 1:271 “SERVER-OTHER echo+chargen bomb”

The default behavior for each rule is determined by which “Base Policy” is used to create a custom-defined Intrusion Policy that’s deployed to a Firepower device. The available pre-configured Base Policies are: No Rules Active; Connectivity Over Security; Balanced Security and Connectivity; Security Over Connectivity; and Maximum Detection. Regardless of which Base Policy is used to create the Intrusion Policy that’s deployed to the Firepower device, each Base Policy contains the same set of default rules and the behavior of each rule can be modified as desired by editing any Intrusion Policy.

© 2023 Cisco Systems, Inc. All rights reserved.

Attack	Default Rule Behavior (Rule State) in each type of Base Policy				
	No Rules Active	Connectivity Over Security	Balanced Security and Connectivity	Security Over Connectivity	Maximum Detection
Teardrop	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Bonk	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Boink	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Land	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Nuke	Undefined	Undefined	Undefined	Undefined	Undefined
Ping of Death	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Null flags	Undefined	Undefined	Undefined	Undefined	Undefined
SYN+FIN flags	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
FIN only flags	Undefined	Undefined	Undefined	Undefined	Undefined
SYN+RST flags	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Bomb	Disabled	Disabled	Disabled	Disabled	Drop and Generate Events
Chargen DoS	Disabled	Disabled	Disabled	Disabled	Disabled

The FTP/Telnet decoder analyzes FTP and telnet data streams, normalizing FTP and telnet commands before processing by the rules engine.

You can set options for decoding on multiple FTP servers. Each server profile you create contains the server IP address and the ports on the server where traffic should be monitored. You can specify which FTP commands to validate and which to ignore for a particular server, and set maximum parameter lengths for commands. You can also set the specific command syntax the decoder should validate against for particular commands and set alternate maximum command parameter lengths.

Networks

Use this option to specify one or more IP addresses of FTP servers.

Ports

Use this option to specify the ports on the FTP server where the managed device should monitor traffic. In the interface, list multiple ports separated by commas. Port21 is the well-known port for FTP traffic.

File Get Commands

Use this option to define the FTP commands used to transfer files from server to client. Do not change these values unless directed to do so by Support.

File Put Commands

Use this option to define the FTP commands used to transfer files from client to server. Do not change these values unless directed to do so by Support.

© 2023 Cisco Systems, Inc. All rights reserved.

Additional FTP Commands

Use this line to specify the additional commands that the decoder should detect. Separate additional commands by spaces.

The HTTP Inspect preprocessor is responsible for:

- Decoding and normalizing HTTP requests sent to and HTTP responses received from web servers on your network.
- Separating messages sent to web servers into URI, non-cookie header, cookie header, method, and message body components to improve performance of HTTP-related intrusion rules.

Networks

Use this option to specify the IP address of one or more servers. You can specify a single IP address or address block, or a comma-separated list comprised of either or both.

Ports

The ports whose HTTP traffic the preprocessor engine normalizes. Separate multiple port numbers with commas.

HTTP Methods

Specifies HTTP request methods in addition to GET and POST that you expect the system to encounter in traffic. Use a comma to separate multiple values.

Intrusion rules use the *content* or *protected_content* keyword with the HTTP Method argument to search for content in HTTP methods. You can enable rule 119:31 to generate events when a method other than GET, POST, or a method configured forth is option is encountered in traffic.

The SMTP preprocessor instructs the rules engine to normalize SMTP commands. The preprocessor can also extract and decode email attachments in client-to-server traffic and, depending on the software version, extract email filenames, addresses, and header data to provide context when displaying intrusion events triggered by SMTP traffic.

Ports

Specifies the ports whose SMTP traffic you want to normalize. You can specify a value greater than or equal to 0. Separate multiple ports with commas.

Stateful Inspection

When selected, causes SMTP decoder to save state and provide session context for individual packets and only inspects reassembled sessions. When cleared, analyze seach individual packet without session context.

Custom Commands

When **Normalize** is set to *Cmds*, normalizes the listed commands.

Detect Unknown Commands

Detects unknown commands in SMTP traffic.

© 2023 Cisco Systems, Inc. All rights reserved.

You can enable rules124:5 to generate events for this option.

4.8.6 Checksum Verification

The system can verify all protocol-level checksums to ensure that complete IP, TCP, UDP, and ICMP transmissions are received and that, at a basic level, packets have not been tampered with or accidentally altered in transit. A checksum uses an algorithm to verify the integrity of a protocol in the packet. The packet is considered to be unchanged if the system computes the same value that is written in the packet by the end host.

Disabling checksum verification may leave your network susceptible to insertion attacks. Note that the system does not generate checksum verification events. In an inline deployment, you can configure the system to drop packets with invalid checksums.

NOTE! Do not disable checksum verification in the evaluated configuration.

Portscan Event Packet View

You can set any of the following options to **Enabled** or **Disabled** in a passive or inline deployment, or to **Drop** in an inline deployment:

- **ICMP Checksums**
- **IP Checksums**
- **TCP Checksums**
- **UDP Checksums**

To drop offending packets, in addition to setting an option to **Drop** you must also enable **Inline Mode** in the associated network analysis policy and ensure that the device is deployed inline.

Setting these options to **Drop** in a passive deployment, or in an inline deployment in tap mode, is the same as setting them to **Enabled**.

The default for all checksum verification options is **Enabled**.

1 Login with Administrator Role or Intrusion Admin.

2 Select **Policies > Access Control > Intrusion** then click on **Network Analysis Policy**.

3 Click the edit icon ( ) next to the policy you want to edit.

4 Click **Settings**.

5 If **Checksum Verification** under **Transport/Network Layer Preprocessors** is disabled, click **Enabled**.

6 Click the edit icon ( ) next to **Checksum Verification**.

7 For each protocol, click **Drop**.

8 To save changes you made in this policy since the last policy commit, click **Policy Information**, then click **Commit Changes**.

© 2023 Cisco Systems, Inc. All rights reserved.

Audit Record:

2017-02-28 20:19:19	admin	Network Analysis Policy > default > settings > checksum mode	Changed ICMP Checksums to "Drop and Generate Events" (from "Enabled")	10.128.120.150
2017-02-28 20:19:19	admin	Network Analysis Policy > default > settings > checksum mode	Changed IP Checksums to "Drop and Generate Events" (from "Enabled")	10.128.120.150
2017-02-28 20:19:19	admin	Network Analysis Policy > default > settings > checksum mode	Changed TCP Checksums to "Drop and Generate Events" (from "Enabled")	10.128.120.150
2017-02-28 20:19:19	admin	Network Analysis Policy > default > settings > checksum mode	Changed UDP Checksums to "Drop and Generate Events" (from "Enabled")	10.128.120.150

4.8.7 Passive vs Inline

You can configure your device in either a passive or inline IPS deployment. In a passive deployment, you deploy the system out of band from the flow of network traffic. In an inline deployment, you configure the system transparently on a network segment by binding two ports together.

Passive Deployment

In a passive IPS deployment, the Firepower System monitors traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally, and no traffic received on these interfaces is retransmitted.

You can configure one or more physical ports on a managed device as passive interfaces.

IMPORTANT! When you disable a passive interface, users can no longer access it for security purposes.

1. Login with Administrator Role.
2. Select **Device > Device Management**.
3. Next to the device where you want to configure the passive interface, click the edit icon ( ).
4. Next to the interface where you want to configure it as a passive interface, click the edit icon ( ).
5. Click **Passive**.
6. Associate a security zone with the passive interface
7. Check the **Enabled** check box.
8. Click **Save**.

Audit Record:

2016-11-23 17:50:36	admin	Devices > Device Management > Device Edit > Interfaces	Save:82	10.128.120.41

Inline Deployment

In an inline IPS deployment, you configure the Firepower System transparently on a network segment by binding two ports together. This allows the system to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

© 2023 Cisco Systems, Inc. All rights reserved.

You can configure one or more physical ports on a managed device as inline interfaces. You must assign a pair of inline interfaces to an inline set before they can handle traffic in an inline deployment.

1. Login with Administrator Role.
2. Select **Device > Device Management**.
3. Next to the device where you want to configure the inline interface, click the edit icon ( ).
4. Next to the interface where you want to configure it as an inline interface, click the edit icon ( ).
5. Click **Inline**.
6. Associate a security zone with the inline interface
7. Check the **Enabled** check box.
8. Click **Save**.
9. Select **Device > Device Management**.
10. Next to the device where you want to add the inline set, click the edit icon ( ).
11. Click the **Inline Sets** tab.
12. Click **Add Inline Set**.
13. Enter a **Name**.
14. Next to **Interfaces**, choose one or more inline interface pairs, then click the add selected icon ( ).
15. If you want to specify that traffic is allowed to bypass detection and continue through the device, choose Failopen (default). If you want Failsafe, please click on the **FailSafe** check box.

    IMPORTANT! Failsafe option will prevent traffic from flowing through the appliance if a failure occurs for inline deployment. This can potentially cause a Denial of Service (DoS) attack on the monitored network.
16. Click **OK**.

Audit Record:

2016-11-23 18:07:40	admin	Devices > Device Management > Device Edit > Interfaces	Save:83	10.128.120.41

© 2023 Cisco Systems, Inc. All rights reserved.

4.9 Management Functions

4.9.1 View Audit Log

FMCs and managed devices log read-only auditing information for user activity. Audit logs are presented in a standard event view that allows administrator to view, sort, and filter audit log messages based on any item in the audit view. Administrator can delete and report on audit information and can view detailed reports of the changes that users make.

The audit log stores a maximum of 100,000 entries. When the number of audit log entries greatly exceeds 100,000, the appliance overwrites the oldest records from the database to reduce the number to 100,000.

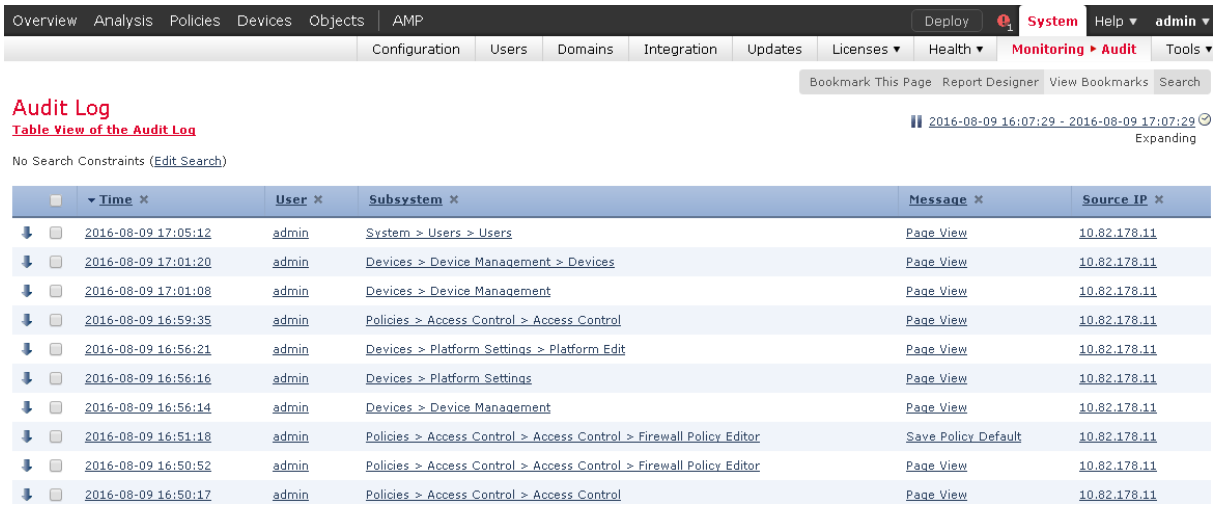
NOTE! To change the maximum number of entries, go to System > Configuration > Database > Audit Event Database > Maximum Audit Events

The syslog is not stored in the same database as the audit logs. The number of syslog entries is based on the disk space so it varies based on the model. However, when the syslog storage space is full, it will overwrite the oldest logs with the newest logs via 'logrotate' implementation.

NOTE! To prevent losing audit records, set up an audit server to send a copy of the audit and syslog records to.

View Audit Log and Syslog via GUI

1. Login with Administrator Role.
2. Select **System > Monitoring > Audit**.

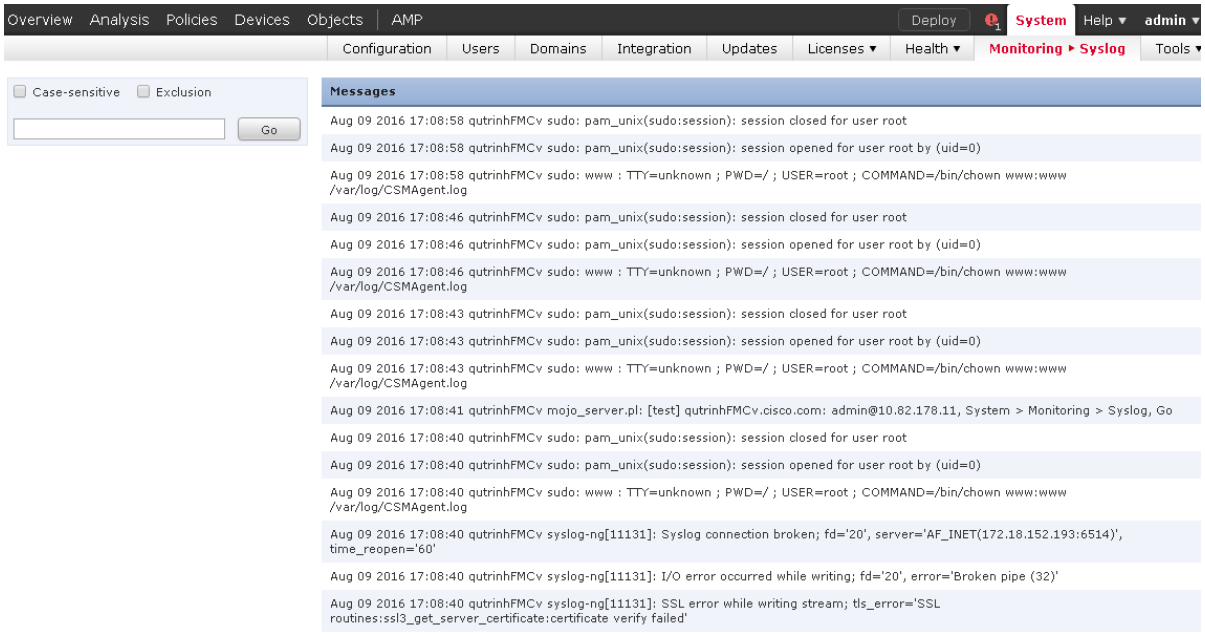


3. The System log (syslog) page provides administrator with system log information for the appliance. The system log displays each message generated by the system. The following items are listed in order:
    - Date that the message was generated.
    - Time that the message was generated.

© 2023 Cisco Systems, Inc. All rights reserved.

- Host that generated the message.
- The message itself[6].

4. Select **System > Monitoring > Syslog**.



Audit Record:

2013-02-26 18:28:08	admin	System > Monitoring > Audit	Page View	10.4.10.227
2013-02-26 18:31:28	admin	System > Monitoring > Syslog	Page View	10.4.10.227

View Audit Log and Syslog via CLI

The command ***show audit-log*** and ***show syslog [filter] [number of lines]***displays the audit log in reverse chronological order; the most recent audit log events are listed first.

Access

Basic

Syntax

show audit-log

Example

[6] The message includes the user or source IP only if applicable. In most cases, the system generated the system log not the user and most of the time, the source IP address is the IP address of the appliance (i.e., system process resides on the system).

© 2023 Cisco Systems, Inc. All rights reserved.

- show audit-log

Audit Record:

```
Audit Log Output:
 time                  :  1361905822 (Tue Feb 26 19:10:22 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- show audit-log
 result                :  Success
 action_source_ip      :  10.4.10.227
 action_destination_ip :  Default Target IP
-------------------------------------------------------------
 time                  :  1361901223 (Tue Feb 26 17:53:43 2013)
 event_type            :  Session terminated due to inactivity (admin)
 subsystem             :  Session Expiration
 actor                 :  admin
 message               :  Session terminated due to inactivity (admin)
 result                :  Success
 action_source_ip      :  10.4.33.204
 action_destination_ip :  10.5.60.81
-------------------------------------------------------------
 time                  :  1361900652 (Tue Feb 26 17:44:12 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
>
```

4.9.2 Management of Intrusion Events

When the system identifies a possible intrusion, it generates an *intrusion event*, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded. Managed devices transmit their events to the Firepower Management Center where you can view the aggregated data and gain a greater understanding of the attacks against your network assets.

You can also deploy a managed device as an inline, switched, or routed intrusion system, which allows you to configure the device to drop or replace packets that you know to be harmful.

The only accounts able to view intrusion events are accounts that have been assigned the “Administrator” or “Intrusion Admin” roles, and intrusion events can only be viewed via the FMC GUI, they cannot be viewed via CLI on either NGIPSv or FMC. The initial intrusion events view differs depending on the workflow you use to access the page. You can use one of the predefined workflows, which includes one or more drill-down pages, at able view of intrusion events, and a terminating packet view, or you can create your own workflow. You can also view workflows based on custom tables, which may include intrusion events.

Viewing Intrusion Events

1. Login with Administrator Role or Security Analyst.
2. Select **Analysis > Intrusions > Events**.

Audit Record:

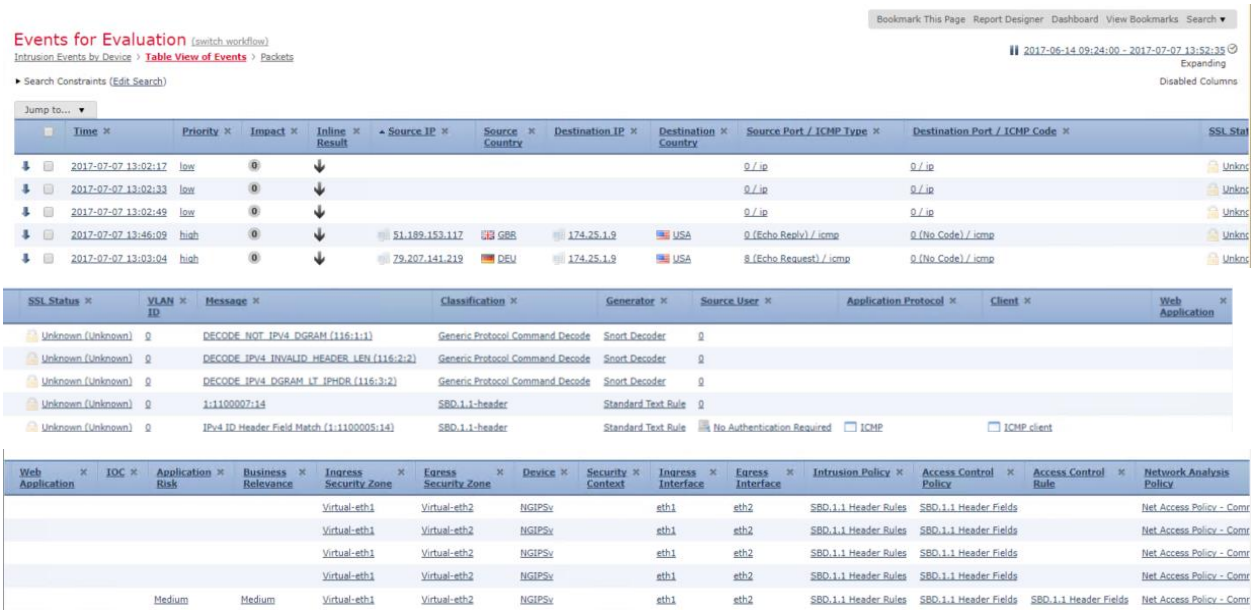
2016-11-17 19:56:43	admin	Analysis > Intrusion Events > Events	Page View	10.128.120.41

© 2023 Cisco Systems, Inc. All rights reserved.

The list below describes the intrusion event information that can be viewed, searched, filtered, and sorted by the system. In addition, basic contents such as date, time, and type can also be used to filter and sort. Note only Administrators and Intrusion Admins have access to the intrusion events.

NOTE! Some fields in the table view of intrusion events are disabled by default. To enable a field for the duration of your session, expand the search constraints, then click the column name under **Disabled Columns**.

Samples of Intrusion Event (split into 3 parts)



Access Control Policy

The access control policy associated with the intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event is enabled.

Access Control Rule

The access control rule that invoked the intrusion policy that generated the event. Default Action indicates that the intrusion policy where the rule is enabled is not associated with a specific access control rule but, instead, is configured as the default action of the access control policy.

This field is blank if intrusion inspection was associated with neither an access control rule nor the default action, for example, if the packet was examined by the default intrusion policy.

Application Protocol

The application protocol, if available, which represents communications between hosts detected in the traffic that triggered the intrusion event.

Application Risk

© 2023 Cisco Systems, Inc. All rights reserved.

The risk associated with detected applications in the traffic that triggered the intrusion event: Very High, High, Medium, Low, and Very Low. Each type of application detected in a connection has an associated risk; this field displays the highest risk of those.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows. This field is not searchable.

Destination Continent

The continent of the receiving host involved in the intrusion event.

Destination Country

The country of the receiving host involved in the intrusion event.

Destination IP

The IP address used by the receiving host involved in the intrusion event.

Destination Port / ICMP Code

The port number for the host receiving the traffic. For ICMP traffic, where there is no port number, this field displays the ICMP code.

Destination User

The User ID for any known user logged in to the destination host.

Device

The managed Sensor where the access control policy was deployed.

Domain

The domain of the Sensor that detected the intrusion. This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Egress Interface

The egress interface of the packet that triggered the event. This interface column is not populated for a passive interface.

Egress Security Zone

The egress security zone of the packet that triggered the event. This security zone field is not populated in a passive deployment.

Email Attachments

The MIME attachment filename that was extracted from the MIME Content-Disposition header. To display attachment file names, you must enable the SMTP preprocessor **Log MIME Attachment Names** option. Multiple attachment filenames are supported.

Email Headers (search only)

The data that was extracted from the email header. To associate email headers with intrusion events for SMTP traffic, you must enable the SMTP preprocessor **Log Headers** option.

© 2023 Cisco Systems, Inc. All rights reserved.

Generator

The component that generated the event.

HTTP Hostname

The hostname, if present, that was extracted from the HTTP request Host header. Note that request packets do not always include the hostname.

To associate hostnames with intrusion events for HTTP client traffic, you must enable the HTTP Inspect preprocessor **Log Hostname** option.

In table views, this column displays the first fifty characters of the extracted host name. You can hover your pointer over the displayed portion of an abbreviated host name to display the complete name, up to 256 bytes. You can also display the complete host name, up to 256 bytes, in the packet view.

HTTP Response Code

The HTTP status code sent in response to a client's HTTP request over the connection that triggered the event.

HTTP URI

The raw URI, if present, associated with the HTTP request packet that triggered the intrusion event. Note that request packets do not always include a URI.

To associate URIs with intrusion events for HTTP traffic, you must enable the HTTP Inspect preprocessor **Log URI** option.

To see the associated HTTP URI in intrusion events triggered by HTTPresponses, you should configure HTTP server ports in the **Perform Stream Reassembly on Both Ports** option; note, however, that this increases resource demands for traffic reassembly.

This column displays the first fifty characters of the extracted URI. You can hover your pointer over the displayed portion of an abbreviated URI to display the complete URI, up to 2048bytes. You can also display the complete URI, up to 2048 bytes, in the packet view.

Ingress Interface

The ingress interface of the packet that triggered the event. Only this interface column is populated for a passive interface.

Ingress Security Zone

The ingress security zone of the packet that triggered the event. Only this security zone field is populated in a passive deployment.

Inline Result

Actions

Intrusion Policy

The intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event was enabled.

Message

The explanatory text for the event. For rule-based intrusion events, the event message is pulled from the rule.

© 2023 Cisco Systems, Inc. All rights reserved.

Priority

The event priority as determined by the Cisco Talos Security Intelligence and Research Group (Talos). The priority corresponds to either the value of the priority keyword or the value for the classtype keyword.

For other intrusion events, the priority is determined by the decoder or preprocessor. Valid values are high, medium, and low.

Protocol (search only)

The name or number of the transport protocol used in the connection.

Snort ID (search only)

Specify the Snort ID (SID) of the rule that generated the event or, optionally, specify the combination Generator ID (GID) and SID of the rule, where the GID and SID are separated with a colon (:) in the format GID:SID.

Source Continent

The continent of the sending host involved in the intrusion event.

Source Country

The country of the sending host involved in the intrusion event.

Source IP

The IP address used by the sending host involved in the intrusion event.

Source Port / ICMP Type

The port number on the sending host. For ICMP traffic, where there is no port number, this field displays the ICMP type.

Source User

The User ID for any known user logged in to the source host.

The intrusion events cannot be modified but they can be deleted by the Administrators or Intrusion Admins who have restricted access. When the intrusion events storage is full, the newest data will overwrite the oldest data.

The intrusion event database stores a maximum of 100,000 entries. When the number of intrusion event entries greatly exceeds 100,000, the appliance overwrites the oldest records from the database to reduce the number to 100,000.

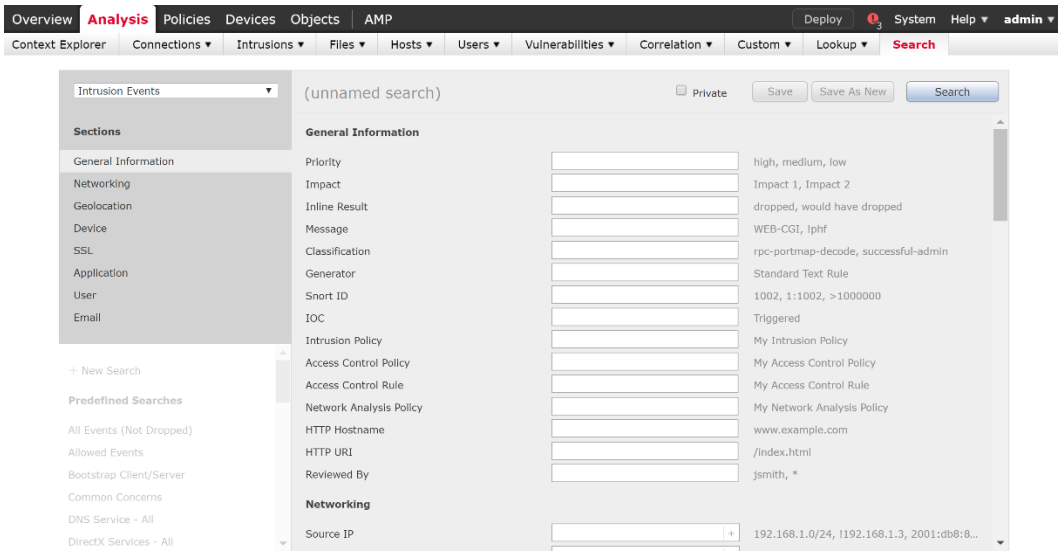
NOTE! To change the maximum number of entries, go to System > Configuration > Database > Intrusion Event Database > Maximum Intrusion Events

---

Searching Intrusion Events

1. Login with Administrator Role.
2. Select **Analysis > Intrusions > Events**.
3. Click on the **Edit Search** link.

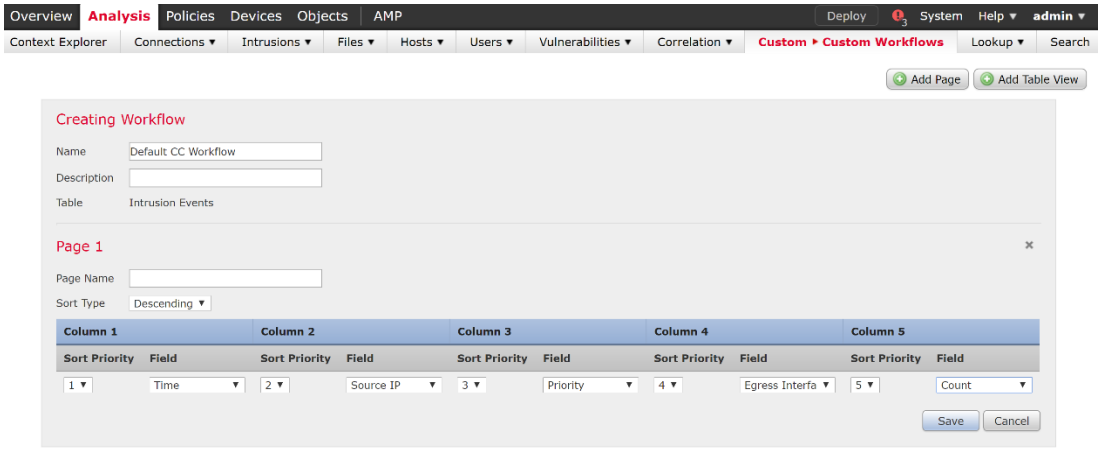
© 2023 Cisco Systems, Inc. All rights reserved.



4. Enter the value you want to search for then click **Search**.

Sorting and filtering Intrusion Events

1. Login with Administrator Role.
2. Select **Analysis > Intrusions > Events**.
3. Click on the column name to sort the intrusion events based on that column.
4. To configure (i.e., filter) different column names, create a workflow via **Analysis** > **Custom** > **Custom Workflows**.
5. Click **Create Custom Workflow**.
6. Give your workflow a descriptive name. In the **Table** drop-down, select **Intrusion Events**.
7. Click **Add Page**.
8. Set the **Sort Priority** and **Field** for each column. There are five columns to configure.



9. Click **Save**.
10. Go back to intrusion events via **Analysis > Intrusions > Events**.

© 2023 Cisco Systems, Inc. All rights reserved.

Click on the **switch workflow** link and choose the workflow you created.

4.9.3 Device Registration

Before you manage a device with a Firepower Management Center, you must make sure that the network settings are configured correctly on the device. This is usually completed as part of the installation process. In addition, the management network should be an internal, trusted network separated physically or logically from the monitored network.

Note that if you registered a Firepower Management Center and a device using IPv4 and want to convert them to IPv6, you must delete and re-register the device.

The registration process requires: a) manually setting a registration key on the device to be registered, and setting the hostname or IP address of the FMC that will be managing the device; and b) manually setting the same registration key on the FMC, as well as the hostname or IP address of the device being registered. When the key and FMC IP address are set on the device, the device will periodically attempt to establish a TLS connection with the FMC, and will listen for TLS connections from the FMC. Likewise, when the registration key and device hostname or IP address are set on the FMC, the FMC will attempt to initiate a TLS connection to the device and will listen for a TLS connection from that device. When the initial TLS connection is established the device and FMC will authenticate each other using the registration key, and will each generate and exchange new X.509v3 certificates. Those certificates will be used for authentication of all subsequent TLS connections between the device and the FMC. The FMC and NGIPSv generate unique certificates with distinct UUIDs at install and as part of the registration process. Those certificates are only used for communications between NGIPSv and FMC, are not configurable, and do not provide interoperability with non-Firepower devices.

During device registration if there's an interruption to the TLS connection between the FMC and the device being registered the registration will fail, and will be automatically reattempted when connectivity is resumed.

Follow the procedures below to proceed with device registration.

<u>On NGIPSv appliances:</u>

1. Login to the CLI with Administrator Role.
2. Use the "configure manager add" command. The syntax is shown below.

   configure manager add {hostname | IPv4_address | IPv6_address} [registration key]

   where {hostname | IPv4_address | IPv6_address} specifies the DNS hostname or IP address (IPv4 or IPv6) of the Firepower Management Center that manages this device.
3. To de-register a manager, just enter "configure manager delete" command. Please sure you delete the Device from the FMC first.

<u>On FMC</u>

1. Login with Administrator Role.
2. Select **Device > Device Management**.
3. From the **Add** drop-down menu, choose **Add Device**.

© 2023 Cisco Systems, Inc. All rights reserved.

NOTE! To de-register a Device, just click on the trash can icon next to the Device you want to remove.

4. In the **Host** field, enter the IP address or the hostname of the device you want to add.
5. In the **Display Name** field, enter a name for the device as you want it to display in the Firepower Management Center.
6. In the **Registration Key** field, enter the same registration key that you used when you configured the device to be managed by the Firepower Management Center.
7. Choose licenses to apply to the device.
8. Click **Register** to add the device to the Firepower Management Center.

4.9.4 Custom Web Server Certificate

Transport Layer Security (TLS) certificates enable Firepower Management Centers and 7000 and 8000 Series devices to establish an encrypted channel between the system and a web browser. A default certificate is included with all Firepower devices, but it is not generated by a certificate authority (CA) trusted by any globally known CA. For this reason, consider replacing it with a custom certificate signed by a globally known or internally trusted CA.

You can generate a certificate request based on your system information and the identification information you supply. You can use it to self-sign a certificate if you have an internal certificate authority(CA) installed that is trusted by your browser. You can also send the resulting request to a certificate authority to request a server certificate. After you have a signed certificate from a certificate authority (CA), you can import it.

Generating an HTTPS Server Certificate Signing Request

When you generate a certificate request through the local configuration HTTPS Certificate page using this procedure, you can only generate a certificate for a single system. If you install a certificate that is not signed by a globally known or internally trusted CA, you receive a security warning when you connect to the system.

1. Login with Administrator Role.
2. Select **System > Configuration**.
3. Click **HTTPS Certificate**.
4. Click **Generate New CSR**.
5. Enter a country code in the **Country Name (two-letter code)** field.
6. Enter a state or province postal abbreviation in the **State or Province** field.
7. Enter a **Locality or City**.
8. Enter an **Organization** name.
9. Enter an **Organization Unit (Department)** name.
10. Enter the fully qualified domain name of the server for which you want to request a certificate in the **Common Name** field.

© 2023 Cisco Systems, Inc. All rights reserved.

NOTE! Enter the fully qualified domain name of the server exactly as it should appear in the certificate in the **Common Name** field. If the common name and the DNS hostname do not match, you receive a warning when connecting to the appliance.

11. Click **Generate**.
12. Open a text editor.
13. Copy the entire block of text in the certificate request, including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines, and paste it into a blank text file.
14. Save the file as servername.csr, where servername is the name of the server where you plan to use the certificate.
15. Click **Close**.

Importing HTTPS Server Certificate

If the signing authority that generated the certificate requires you to trust an intermediate CA, you must also supply a certificate chain (or certificate path). Please note only PEM format is supported.

1. Login with Administrator Role.
2. Select **System > Configuration**.
3. Click **HTTPS Certificate**.
4. Click **Import HTTPS Certificate**.
5. Open the server certificate in a text editor, copy the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines. Paste this text into the **Server Certificate** field.
6. If you want to upload a private key, open the private key file and copy the entire block of text, including the BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY lines. Paste this text into the **Private Key** field.
7. Open any required intermediate certificates, copy the entire block of text for each, and paste it into the **Certificate Chain** field.
8. Click **Save**.

4.9.5 User and Role Management

If you have Administrator Role, you can use the web interface to view and manage user accounts on a FMC or a managed device, including adding, modifying, and deleting accounts. User accounts without Administrator Role are restricted from accessing user management functions. The CLI has “show users” and “configure users” commands but they are only available for the virtual appliances. Management of the user and role is performed via web interface only. Note that all users created are TOE administrators.

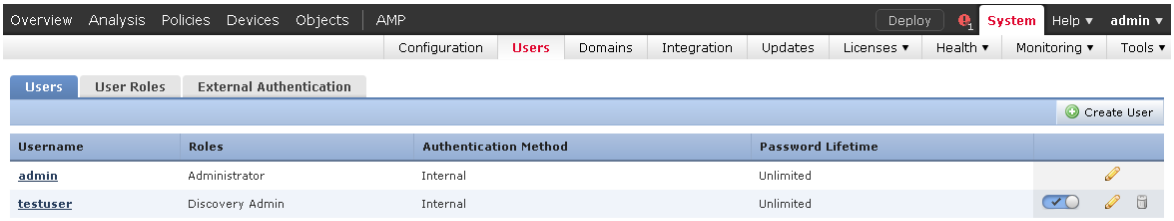
Viewing User Accounts

© 2023 Cisco Systems, Inc. All rights reserved.

From the User Management page, you can view, edit, and delete existing accounts.

1. Login with Administrator Role.
2. Select **System > Users**

   The User Management page appears, showing each user, with options to activate, deactivate, edit, or delete the user account.



Audit Record:

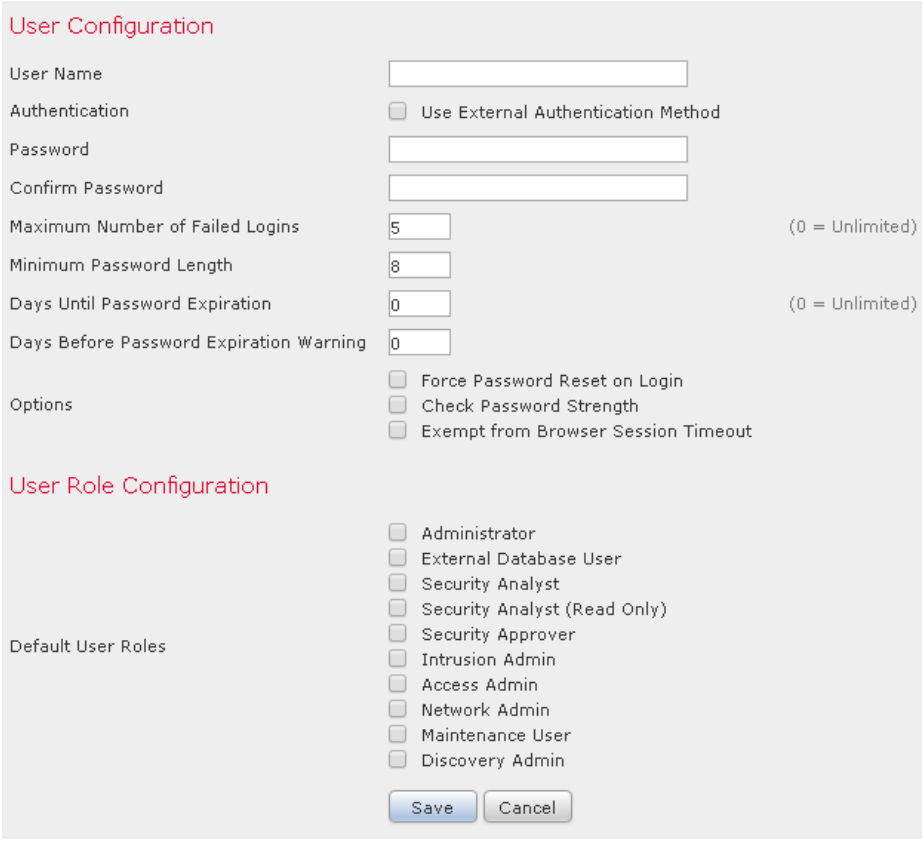
2013-02-26 18:33:35	admin	System > Local > User Management > Users	Page View	10.4.10.227

Adding New User Accounts

When you set up a new user account, you can control which parts of the system the account can access. You can set password expiration and strength settings for the user account during creation. For a local account on an 8000 Series device, you can also configure the level of command line access the user will have. On the NGIPSv, use the command “configure user add <username> [*basic* | *configure*]”. To get more CLI options, use the command “configure user ?”.

1. Login with Administrator Role.
2. Select **System > Users**.
3. Click **Create User**.

© 2023 Cisco Systems, Inc. All rights reserved.



4. In the **User Name** field, type a name for the new user.

   New user names must contain alphanumeric or hyphen characters with no spaces, and must be no more than 32 characters.

5. Do **NOT** check the **Use External Authentication Method** checkbox.

6. In the **Password** and **Confirm Password** fields, type a password (up to 32 alphanumeric characters).

   Strong Password Composition:

   The password must be at least eight alphanumeric characters of mixed case and must include at least one numeric character and one special character. It cannot be a word that appears in a dictionary or include consecutive repeating characters.

7. Set the **Maximum number of Failed Logins** to 3 to 7 (recommended). The default setting is 5.

   When the maximum number of failed login attempts is reached for any account, that account will be locked. Accounts can be unlocked by another account with the "Administrator" role by resetting the account activation switch ( ), and optionally editing the account properties to check the "Force Password Reset on Login" checkbox (see screenshot above at step 3).

   If all accounts with the "Administrator" role become locked the default "admin" account can be unlocked using password recovery procedures available here: https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118631-technote-firesight-00.html

© 2023 Cisco Systems, Inc. All rights reserved.

8. Configure the user account password options. For example, set the **Minimum Password Length** to 15. The default setting is 8 and the maximum allowable is 32.
9. If you are creating a local user through the web interface of an 8000 Series device, you can assign the level of **Command-Line Interface Access** for the user:
    - Select **None** to disable access to the command line for the user.
    - Select **Basic** to allow the user to log into the shell and to access a specific subset of commands.
    - Select **Configuration** to allow the user to log into the shell and use any command line option, including expert mode if that is allowed on the appliance.
10. Check the **Check Password Strength** checkbox. By default, this is not selected.

WARNING! This is a recommended evaluated configuration setting.

11. Do **NOT** click on the **Exempt from GUI Session Timeout** checkbox.
12. Select the access roles to grant the user.

NOTE! The screenshot above shows multiple roles that exist by default. The only role evaluated under Common Criteria (CC) for administration of the entire set of CC-certified functionality is the "Administrator" role, while the other default roles listed below are relevant only to the CC-certified IPS functionality.

- "IPS Administrator" (or Administrator): Have all privileges and access.
- "IPS Analyst" (or Intrusion Admin): Have all access to intrusion policies and network analysis privileges but cannot deploy policies
- Access Admin: Have all access to access control policies but cannot deploy policies
- Discovery Admin: Have all access to network discovery, application detection, and correlation features but cannot deploy policies
- Security Analyst: Have all access to security event analysis feature

13. Click **Save**.

Audit Record:

2013-02-26 18:36:08 admin System > Local > User Management > Users Added user - CCuser:134 10.4.10.227

time : 1488331638 (Wed Mar 1 01:27:18 2017)
event_type : Default Action
subsystem : Command Line
actor : admin
message : Executed root-view- configure user add tester1 config
result : Success

© 2023 Cisco Systems, Inc. All rights reserved.

action_source_ip : 10.128.120.150

action_destination_ip : Default Target IP

Modifying and Deleting User Accounts

Administrator can modify or delete user accounts from the system at any time, with the exception of the **admin** account, which cannot be deleted. On the NGIPSv, use the command “configure user delete <username>”. To get more CLI options, use the command “configure user ?”.

1. Login with Administrator Role.
2. Select **System > Users**.
3. Click the edit icon () next to the user you want to modify.
4. Modify the settings you choose and click **Save**.
5. To delete a user account, click the delete icon () next to the user you want to delete.
6. Click **OK** to confirm.
7. The user account is deleted.

Audit Record:

2013-02-26 18:38:33	admin	System > Local > User Management > Users	Edited user - CCuser:135	10.4.10.227
2013-02-26 18:38:44	admin	System > Local > User Management > Users	Deleted user - CCuser:136	10.4.10.227

time : 1488331670 (Wed Mar 1 01:27:50 2017)

event_type : Default Action

subsystem : Command Line

actor : admin

message : Executed root-view- configure user delete tester1

result : Success

action_source_ip : 10.128.120.150

action_destination_ip : Default Target IP

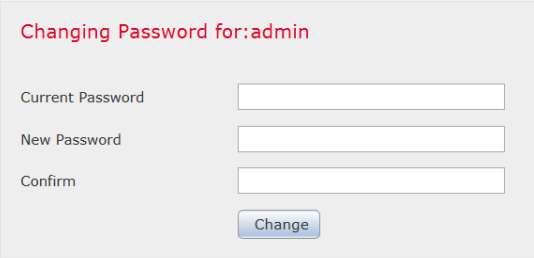
© 2023 Cisco Systems, Inc. All rights reserved.

4.9.6 Change Password

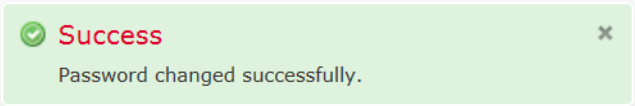
All user accounts are protected with a password. You can change your password[7] at any time, and depending on the settings for your user account, you may have to change your password periodically due to password expiration. You can use either the web page or the CLI[8] to change your password.

Note that if password strength checking is enabled, passwords must be at least eight alphanumeric characters of mixed case and must include at least one number and one special character. When creating or changing passwords, the passwords must be composed of upper and lower case letters, numbers and special characters including blank space and !@#$%^&*() ‘(double or single quote/apostrophe), + (plus), - (minus), = (equal), , (comma), . (period), / (forward-slash), \ (back-slash), | (vertical-bar or pipe), : (colon), ; (semi-colon), < > (less-than, greater-than inequality signs), [ ] (square-brackets), { } (braces or curly-brackets),? (question-mark), (underscore), and ~ (tilde). Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.

1. From the drop-down list under your username, select **User Preferences**.



2. In the **Current Password** field, type your current password.
3. In the **New Password** and **Confirm** fields, type your new password.
4. Click **Change**.
5. The Success message appears.



Audit Record:

2013-02-26 18:40:19	admin	User Preferences > Change Password	Change	10.4.10.227

Configure Password via CLI

The command ***configure password*** allows the current user to change their password.

After issuing the command, the CLI prompts the user for their current password, then prompts the user to enter the new password twice.

---

[7] Only user with Administrator Role can change other user password.

[8] Available on Series-3 managed devices only.

© 2023 Cisco Systems, Inc. All rights reserved.

Access

Basic

Syntax

configure password

Example

- configure password

Enter current password:

Enter new password:

Confirm new password:

Audit Record:

```
Enter current password:
Enter new password:
Confirm new password:

> show audit-log
Audit Log Output:
 time                  :  1361900652 (Tue Feb 26 17:44:12 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- show audit-log
 result                :  Success
 action_source_ip      :  10.4.10.227
 action_destination_ip :  Default Target IP
-----------------------------------------------------------
 time                  :  1361900637 (Tue Feb 26 17:43:57 2013)
 event_type            :  Default Action
 subsystem             :  Command Line
 actor                 :  admin
 message               :  Executed root-view- configure password
 result                :  Success
 action_source_ip      :  10.4.10.227
 action_destination_ip :  Default Target IP
-----------------------------------------------------------
```

4.9.7 Configure Time Synchronization

Administrator can manage time synchronization on the managed appliance (NGIPSv) using the Time Synchronization page. To adhere to the Common Criteria requirements, the clock on the FMC must be set manually, but the managed device can synchronize its clock with the FMC (the connection between the managed device and FMC will use NTP over TLS).

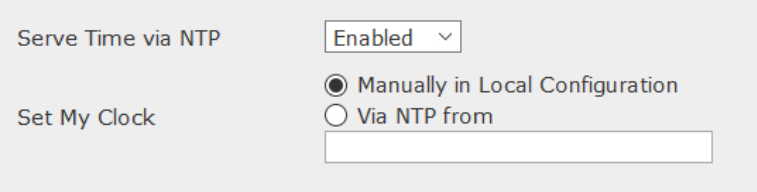
Time settings are part of the system policy. Administrator can specify the time settings either by creating a new system policy or by editing an existing policy. In either case, the time setting is not used until you apply the system policy.

Note that time settings are displayed on most pages on the appliance in local time using the time zone you set on the Time Zone page (America/New York by default), but are stored on the appliance itself using UTC time. In addition, the current time appears in UTC at the top of the Time Synchronization page (local time is displayed in the Manual clock setting option, if enabled).

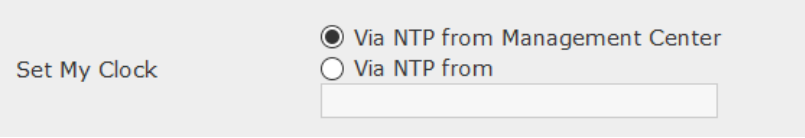
© 2023 Cisco Systems, Inc. All rights reserved.

To configure the FMC system clock, and configure how the managed device's clock will be set:

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
    - Management Center—Choose **System > Configuration.**
    - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click **Time Synchronization** on the left side of the page.
4. On the FMC:
    - Set the time manually by selecting **Manually in Local Configuration**. For more details see the "Setting the Time Manually" section below.
    - Optional and recommended: If you want to serve time from the FMC to your managed devices, in the **Serve Time via NTP** drop-down list, select **Enabled**.



5. For the managed device:
    - Click "**Time Synchronization**" on the left side of the page (under **Devices > Platform Settings**), then set the "Set My Clock" option to "Via NTP from Management Center."



6. Click **Save**.
7. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

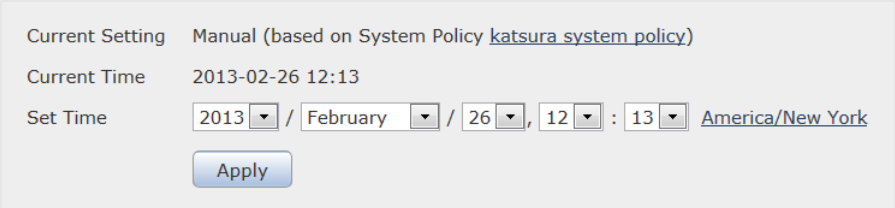
Audit Record:

2013-02-26 12:11:54	admin	System > Local > System Policy > Time Synchronization > Settings on Defense Center, Master Defense Center > Mod
2013-02-26 12:11:54	admin	System > Local > System Policy > Time Synchronization > Settings on 3D Sensor > Modified: Set My Clock Via NTP fr

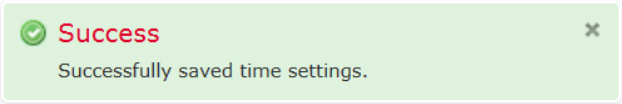
Setting the Time Manually

1. Login with Administrator Role.
2. Select **System > Configuration**.
3. Click **Time**.

© 2023 Cisco Systems, Inc. All rights reserved.



4. Select the following from the **Set Time** drop-down lists:
    - Year
    - Month
    - Day
    - Hour
    - Minute
5. Click **Apply**.
6. The Success message appears.



Audit Record:

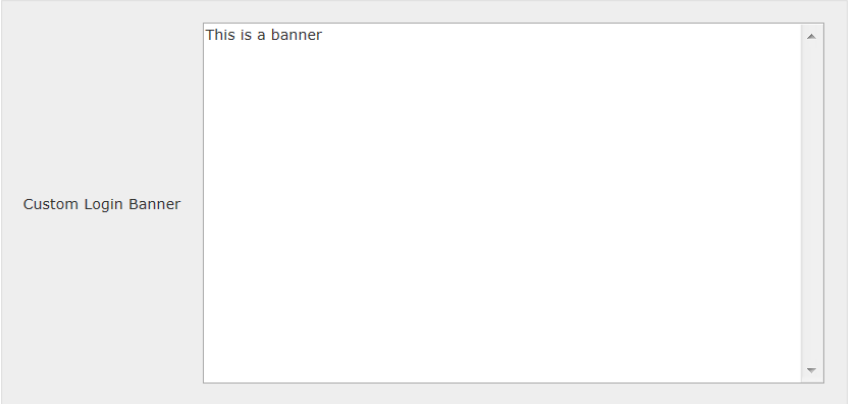
2013-02-26 17:41:02	admin	System > Local > Configuration > Time	Page View	10.4.10.227
2013-02-26 17:41:01	admin	Updated time to Tue 26 Feb 2013 05:41:00 PM EST from Tue 26 Feb 2013 06:41:47 PM EST	Save	10.4.10.227

4.9.8 Configure Login Banner

Administrator can create a custom login banner that appears when users log into the appliance using SSH and on the login page of the web interface. Banners can contain any printable characters except the less-than symbol (<) and the greater-than symbol (>).

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
    - Management Center—Choose **System > Configuration.**
    - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click **Login Banner**.

© 2023 Cisco Systems, Inc. All rights reserved.



4. In the **Custom Login Banner** field, enter the login banner you want to use with this system policy.
5. Click **Save**.
6. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

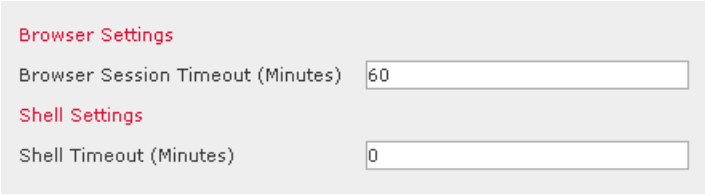
Audit Record:

2013-02-26 17:44:19	admin	System > Local > System Policy > Login Banner > Modified: Custom Login Banner New Banner > This is a banner	Save	10.4.10.227

4.9.9 Inactivity Timeout Setting

By default, all user sessions (web-based and CLI) automatically log out after 60 minutes (1 hour) of inactivity, unless you are otherwise configured to be exempt from session timeout. Users with Administrator Role can change the inactivity timeout value in the system policy to meet their security needs.

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a Classic managed device:
   - Management Center—Choose **System > Configuration.**
   - Managed device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click **Shell Timeout**.



4. In the **Browser Session Timeout (Minutes)** and **Shell Timeout (Minutes)** fields, enter a value from 1 – 1440 (24 hours) max. The value of 0 will disable this feature. Note that FMC checks multiple times per minute for idle sessions and terminates those sessions when they're

© 2023 Cisco Systems, Inc. All rights reserved.

detected, so sessions may not be terminated until 20-40 seconds after the configured inactivity limit has been reached.

WARNING! This is a required evaluated configuration setting and must NOT be disabled.

6. Click **Save**.
7. Click **Deploy** if you are configuring these settings for the managed devices. Select the device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

2013-02-26 18:11:53	admin	System > Local > System Policy > User Interface > Modified: Shell Timeout (Minutes) 0 > 15	Save	10.4.10.227

Session Timeout Record

The system will record in the audit log when a user is logged out due to inactivity.

Audit Record:

2013-02-26 18:02:26	admin	Session Expiration	Session terminated due to inactivity (admin)	10.2.100.250

```
Audit Log Output:
time                  :  1362178064 (Fri Mar  1 22:47:44 2013)
event_type            :  Default Action
subsystem             :  Command Line
actor                 :  admin
message               :  Executed root-view- show audit-log
result                :  Success
action_source_ip      :  10.4.10.223
action_destination_ip :  Default Target IP
-------------------------------------------------------------
time                  :  1362177449 (Fri Mar  1 22:37:29 2013)
event_type            :  Session terminated on pts/0 due to inactivity (admin)

subsystem             :  Session Expiration
actor                 :  admin
message               :  Session terminated on pts/0 due to inactivity (admin)

result                :  Success
action_source_ip      :  10.4.10.223
action_destination_ip :  10.5.60.81
```

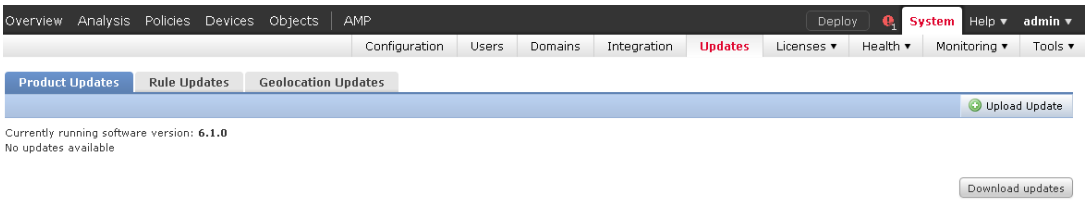
4.9.10Product Upgrade

Cisco electronically distributes several different types of updates, including major and minor updates to the system software itself, as well as intrusion rule updates and VDB updates. Administrator must update the FMC before you can update the devices they manage. Cisco recommends that you use the FMC's web interface to update not only itself, but also the devices it manages.

As upgrade files are uploaded to FMC, FMC will automatically verify the integrity of the files using digital signature to ensure they have not been modified since they were created by Cisco, and that they were properly signed by Cisco. If any upgrade file fails the automatic integrity verification the file will be automatically deleted and will not be available to install to the FMC or any managed device. Any upgrade file listed on FMC's Product Updates page has been verified and can be installed by an authorized administrator.

The Product Updates page (**System > Updates**) shows the version of each update, as well as the date and time it was generated. It also indicates whether a reboot is required as part of the update.

© 2023 Cisco Systems, Inc. All rights reserved.



When administrator install or uninstall updates from a managed device, the following capabilities may be affected:

- Traffic inspection and connection logging
- Traffic flow including switching, routing, and related functionality
- Link state

WARNING! To ensure absolutely no packets pass through the appliance without inspection, please disconnect the managed devices from the network during the upgrade process. Once the process has been completed and upgrade version has been verified, reconnect the managed devices to the network.

Therefore, upgrading and regular maintenance should be performed during off-peak hours only.

To Update the FMC:

Update the FMC in one of two ways, depending on the type of update and whether your FMC has access to the Internet:

- Administrator can use the FMC to obtain the update directly from the Cisco Support Site, if your FMC has constant access to the Internet. This option is not supported for major updates and is not allowed in the evaluated configuration.
- Administrator can manually download the update from the Cisco Support Site and then upload it to the FMC. Choose this option if your FMC does not have access to the Internet or if you are performing a major update.

1. Login with Administrator Role.
2. Upload the update to the FMC. You have two options, depending on the type of update and whether your FMC has access to the Internet:
    - For all except major updates, and if your FMC has access to the Internet, select **System > Updates**, then click **Download Updates** to check for the latest updates on the Cisco Support Site (https://software.cisco.com/).

© 2023 Cisco Systems, Inc. All rights reserved.

- For major updates, or if your FMC does not have access to the Internet, you must first manually download the update from the Cisco Support Site. Select **System > Updates**, then click **Upload Update**. Browse to the update and click **Upload**.

The update is uploaded to the FMC.

WARNING! Make sure you have a valid Support account. The Cisco Support Site requires authentication and is protected using HTTPS. Click on **Downloads** and find the appropriate version of the software, Rules, or VDB. Download the upgrade version (extension .sh) and the corresponding SHA-512 hash. Using a trusted hash utility tool[9], compute the SHA-512 hash of the downloaded *.sh. If the hashes do not match, discard the upgrade version and contact Cisco Support (e-mail tac@cisco.com or call us at 1-800-553-2447 or 1-408-526-7209).

3. Make sure that the appliances in your deployment are successfully communicating and that there are no issues being reported by the health monitor.
4. Select **System > Updates**.
5. Click the install icon ( ) next to the update you uploaded.
6. Select the FMC and click **Install**. If prompted, confirm that you want to install the update and reboot the FMC.
7. After the update finishes, if necessary, log into the FMC.
8. Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
9. Select **Help > About** and confirm that the software version is listed correctly.
10. Re-deploy the access control policies.

To Update Managed Devices:

1. Login with Administrator Role.
2. Download the update from the Cisco Support Site.
3. Make sure that the appliances in your deployment are successfully communicating and that there are no issues being reported by the health monitor.
4. On the managing FMC, select **System > Updates**.

   The Product Updates page appears.
5. Click **Upload Update** to browse to the update you downloaded, then click **Upload**.

   The update is uploaded to the FMC. The Product Updates tab shows the type of update you just uploaded, its version number, and the date and time when it was generated. The page also indicates whether a reboot is required as part of the update.
6. Click the install icon ( ) next to the update you uploaded.

[9] This tool is not part of the TOE. Examples of such tool include MD5 & SHA-1 Checksum Utility v2.1, DP Hash, File Checksum Tool, BD File Hash, etc.

© 2023 Cisco Systems, Inc. All rights reserved.

7. Select the devices where you want to install the update, then click **Install**; you can update multiple devices at once if they use the same update. If prompted, confirm that you want to install the update and reboot the devices.
8. On the FMC, select **Devices > Device Management** and confirm that the devices you updated have the correct version listed.
9. Verify that the devices you updated are successfully communicating with the FMC.

Audit Record:

2013-02-27 17:40:07	admin	System > Updates > Product Updates	Update Install	10.4.11.59

Successful task completion : Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-139 : Successful VDB Installation

4.9.11 Self-Tests

Cisco products perform a suite of FIPS 140-2 self-tests during power-up and re-boot. If any of the self-test fails, the product will not enter operational state. If this occurs, please re-boot the appliance. If the product still does not enter operational state, please contact Cisco Support (e-mail support@Cisco.com or call us at 1-800-917-4134 or 1-410-423-1901).

In the CC-certified configuration, the Firepower Management Center (FMC) and its managed Firepower devices are considered 'distributed' components. If any self-test fails on the FMC the failure error will be displayed at the FMC console and the FMC will automatically reboot. If any self-test fails for a managed Firepower device that device will lose connectivity to FMC and thus will appear in FMC (under Devices > Device Management) to be in an error state. To view the details of device error states, view the health monitor (System > Health > Monitor) for a summary of errors for each device, and optionally click on the icon for any device to see more details, which should include "Process Status: All processes are running correctly." If the error state continues for longer than required for the device to reboot, view the output at the device's console port for any errors indicating whether any self-tests have failed.

The following possible errors that can occur during this self-test are:

- Known Answer Test (KAT) failures, including AES encryption/decryption KAT, RSA key generation and encryption/decryption KAT, SHA hash KATs, HMAC-SHA hash KATs, PRNG KATs.
- Zeroization Test failure (key overwriting tests)
- Software integrity failure (HMAC-SHA512 integrity tests)

The actual output of FIPS 140-2 self-tests can only be accessed using the shell access[10] with root permission. The status output is located in **/var/log/openssl-selftest.log** and is displayed below:

```
Running test fips_randtest
FIPS PRNG test 1 done
FIPS PRNG test 2 done
FIPS PRNG test 3 done
----------
Running test fips_test_suite
    FIPS-mode test application
```

[10] Accessing the shell access with root access takes the products out of the evaluated configuration.

© 2023 Cisco Systems, Inc. All rights reserved.

```
    CiscoSSL FOM 6.0

        DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
1. Non-Approved cryptographic operation test...
    a. Included algorithm (D-H)……successful
2. Automatic power-up self test...successful
3a. AES encryption/decryption...successful
3b. AES-GCM encryption/decryption...successful
        Pairwise Consistency RSA test started
        Pairwise Consistency RSA test OK
        Pairwise Consistency RSA test started
        Pairwise Consistency RSA test OK
        Pairwise Consistency RSA test started
        Pairwise Consistency RSA test OK
4. RSA key generation and encryption/decryption...successful
5. DES-ECB encryption/decryption...successful
        Pairwise Consistency DSA test started
        Pairwise Consistency DSA test OK
6. DSA key generation and signature validation...successful
7a. SHA-1 hash...successful
7b. SHA-256 hash...successful
7c. SHA-512 hash...successful
7d. HMAC-SHA-1 hash...successful
7e. HMAC-SHA-224 hash...successful
7f. HMAC-SHA-256 hash...successful
7g. HMAC-SHA-384 hash...successful
7h. HMAC-SHA-512 hash...successful
8a. CMAC-AES-128 hash...successful
8b. CMAC-AES-192 hash...successful
8c. CMAC-AES-256 hash...successful
8e. CMAC-TDEA-3 hash...successful
8f. ECDSA key pairwise consistency check...
  Testing ECDSA pairwise consistency
    ECDSA key generated OK, pairwise test passed.
    successful as expected
9. Non-Approved cryptographic operation test...
    a. Included algorithm (D-H)...successful as expected
        Pairwise Consistency RSA test started
        Pairwise Consistency RSA test OK
        Pairwise Consistency RSA test started
        Pairwise Consistency RSA test OK
        Pairwise Consistency RSA test started
        Pairwise Consistency RSA test OK
 Generated 384 byte RSA private key
    BN key before overwriting:
072483096b927ac74678ffb6d1eba3732231e2bdd1062c6528906b25e75fbd4b7619fc81a204ce5cf000e96b07e5a21e40186bc81beb1d8b9a5a0c
ac5bf48591251020084cfbc8f461b1bf00c4aff06b638095b3165a0fc1874ba894bce15204379c778680a8b600fd7c4d82f9de2a1c67cdcfc6eefb643
81c3503ecc366f4ecb26f26fd7045022353024c5ec3f109669813d7f5788ed64b91b07a8bd44a44639f41c136aa45f0a1619c10a6d7192d8291ce74
1aa1ccb3fa94466966453823b4047fd116a473ae64ae3b805df2c3be288c94a62311dc8ea21b62cfc849ea5b57407a1f2c5a3d0d4dbe4de8344165
16303703335894d728c8e38ac1fad3ddaf5f158bfbc50b08895bd1bdf56f25e57a55f5ed9d02599528ea7d83b947d7496c8af35bfc179ccddce8ade3
d18ecedb3dbb70d990b92c808887fc6f08f0ae4a1be9ebaca42f68520346d2df236a538814a534224bc466f777d1ec9bc4ac852e96e9535e8a5c610
91036bf6da4920f8da5bec1562cd46f8d329d30b6685644965019      BN key after overwriting:
2202b71a6fa4bdc65b48fe63e18059f56f9848698a1dae246c071e4aa9250d7db50270c056b0665adcb57e135f019dc698dcb5b3595f911d45ff0c4
473fef26bb2cd6702fc1d2b94472215f0766218f63b6566097eabdb30de1573f8ad82f53a05231880a4cb75d85a0a939f87a8b4 ecd4d411fd566f6b
973a439e7df22511af41b45495aefb819c8d918aafee55a97d1c3682c0ef20d5d31f19641d7433c512276dced929f23d47fc78f90bb9168473fbe3c4
29e1be474eb420c44b43d9a2a909f96645eee2b9c05fa23a33828b67d756493cc121644cfd473b6095a873a06cef74078d11185dbd144e1a64229d
dfceffc8f88f297117da0822cb60e9d945f960eed3a5fd29bf43b1f594bdcce5d57910f03b1231ac14da99592339b7887f07dcadd355fb6a113d6ddd
d4f543cca6083ad9c326900e03c542c9df06547f04e1480712e218ea01f3780e0a457a87fef6dbbcbfbcf2d5f5de59938c72de180dbd29b4663cb936
ec42809b7b9c6f4780d2db0e1edf58298c0290f988e35676fabe      char buffer key before overwriting:
        4850f0a33aedd3af6e477f8302b10968
    char buffer key after overwriting:
        bf1e0ff9f86e6f39b5966cfd3b2d7394
10. Zero-ization...
    successful as expected
11. Complete DRBG health check...
```

© 2023 Cisco Systems, Inc. All rights reserved.

```
        DRBG AES-128-CTR DF test started
        DRBG AES-128-CTR DF test OK
        DRBG AES-192-CTR DF test started
        DRBG AES-192-CTR DF test OK
        DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
        DRBG AES-128-CTR test started
        DRBG AES-128-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-256-CTR test started
        DRBG AES-256-CTR test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
        DRBG SHA256 test started
        DRBG SHA256 test OK
        DRBG SHA384 test started
        DRBG SHA384 test OK
        DRBG SHA512 test started
        DRBG SHA512 test OK
        DRBG HMAC-SHA1 test started
        DRBG HMAC-SHA1 test OK
        DRBG HMAC-SHA224 test started
        DRBG HMAC-SHA224 test OK
        DRBG HMAC-SHA256 test started
        DRBG HMAC-SHA256 test OK
        DRBG HMAC-SHA384 test started
        DRBG HMAC-SHA384 test OK
        DRBG HMAC-SHA512 test started
        DRBG HMAC-SHA512 test OK
    successful as expected
12. DRBG generation check...
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA1 test started
        DRBG SHA1 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
        DRBG SHA224 test started
        DRBG SHA224 test OK
```

© 2023 Cisco Systems, Inc. All rights reserved.

DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK

© 2023 Cisco Systems, Inc. All rights reserved.

```
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
```

© 2023 Cisco Systems, Inc. All rights reserved.

```
        DRBG AES-128-CTR test started
        DRBG AES-128-CTR test OK
        DRBG AES-128-CTR test started
        DRBG AES-128-CTR test OK
        DRBG AES-128-CTR test started
        DRBG AES-128-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-192-CTR test started
        DRBG AES-192-CTR test OK
        DRBG AES-256-CTR test started
        DRBG AES-256-CTR test OK
        DRBG AES-256-CTR test started
        DRBG AES-256-CTR test OK
DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
        DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
        DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
        DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
        DRBG AES-256-CTR DF test started
        DRBG AES-256-CTR DF test OK
    successful as expected
13. Induced test failure check...
  Testing induced failure of Integrity test
    POST started
        Integrity  test failure induced
        Integrity  test failed as expected
    POST Failed
  Testing induced failure of AES test
    POST started
        Cipher AES-128-ECB test failure induced
        Cipher AES-128-ECB test failed as expected
    POST Failed
  Testing induced failure of DES3 test
    POST started
        Cipher DES-EDE3-ECB test failure induced
        Cipher DES-EDE3-ECB test failed as expected
    POST Failed
  Testing induced failure of AES-GCM test
    POST started
        GCM  test failure induced
        GCM  test failed as expected
    POST Failed
  Testing induced failure of AES-CCM test
    POST started
        CCM  test failure induced
        CCM  test failed as expected
    POST Failed
  Testing induced failure of AES-XTS test
    POST started
        XTS AES-128-XTS test failure induced
        XTS AES-128-XTS test failed as expected
        XTS AES-256-XTS test failure induced
```

© 2023 Cisco Systems, Inc. All rights reserved.

```
        XTS AES-256-XTS test failed as expected
    POST Failed
Testing induced failure of Digest test
    POST started
        Digest SHA1 test failure induced
        Digest SHA1 test failed as expected
        Digest SHA1 test failure induced
        Digest SHA1 test failed as expected
        Digest SHA1 test failure induced
        Digest SHA1 test failed as expected
    POST Failed
Testing induced failure of HMAC test
    POST started
        HMAC SHA1 test failure induced
        HMAC SHA1 test failed as expected
        HMAC SHA224 test failure induced
        HMAC SHA224 test failed as expected
        HMAC SHA256 test failure induced
        HMAC SHA256 test failed as expected
        HMAC SHA384 test failure induced
        HMAC SHA384 test failed as expected
        HMAC SHA512 test failure induced
        HMAC SHA512 test failed as expected
    POST Failed
Testing induced failure of CMAC test
    POST started
        CMAC AES-128-CBC test failure induced
        CMAC AES-128-CBC test failed as expected
        CMAC AES-192-CBC test failure induced
        CMAC AES-192-CBC test failed as expected
        CMAC AES-256-CBC test failure induced
        CMAC AES-256-CBC test failed as expected
        CMAC DES-EDE3-CBC test failure induced
        CMAC DES-EDE3-CBC test failed as expected
    POST Failed
Testing induced failure of DRBG test
    POST started
        DRBG AES-256-CTR test failure induced
        DRBG AES-256-CTR DF test failed as expected
        DRBG AES-256-CTR test failure induced
        DRBG AES-256-CTR test failed as expected
        DRBG SHA256 test failure induced
        DRBG SHA256 test failed as expected
        DRBG HMAC-SHA256 test failure induced
        DRBG HMAC-SHA256 test failed as expected
    POST Failed
Testing induced failure of RSA test
    POST started
        Signature RSA test failure induced
        Signature RSA test failed as expected
    POST Failed
Testing induced failure of DSA test
    POST started
        Signature DSA test failure induced
        Signature DSA test failed as expected
    POST Failed
Testing induced failure of ECDSA test
    POST started
        Signature ECDSA P-256 test failure induced
        Signature ECDSA P-256 test failed as expected
    POST Failed
Testing induced failure of ECDH test
    POST started
        ECDH P-256 test failure induced
        ECDH P-256 test failed as expected
        ECDH P-384 test failure induced
```

© 2023 Cisco Systems, Inc. All rights reserved.

```
        ECDH P-384 test failed as expected
        ECDH P-521 test failure induced
        ECDH P-521 test failed as expected
    POST Failed
  Testing induced failure of RSA keygen test
    POST started
    POST Success
        Pairwise Consistency RSA test failure induced
        Pairwise Consistency RSA test failed as expected
    RSA key generation failed as expected.
  Testing induced failure of DSA keygen test
    POST started
    POST Success
Pairwise Consistency DSA test failure induced
        Pairwise Consistency DSA test failed as expected
    DSA key generation failed as expected.
    POST started
    POST Success
  Testing induced failure of ECDSA keygen test
        Pairwise Consistency  test failure induced
    ECDSA key generation failed as expected.
    POST started
    POST Success
  Testing induced failure of DRBG CPRNG test
    DRBG continuous PRNG failed as expected
    POST started
    POST Success
  Testing induced failure of DRBG entropy CPRNG test
    DRBG continuous PRNG entropy failed as expected
    POST started
    POST Success
    POST started
    POST Success
  Testing operation failure with DRBG entropy failure
    DSA key generated OK as expected.
    DRBG entropy instantiate fail failed as expected
    DRBG entropy generate fail failed as expected
    DRBG reseed entropy fail failed as expected
    DSA signing failed as expected
    ECDSA key generation failed as expected.
 Induced failure test completed with 0 errors
    successful as expected

All tests completed with 0 errors
```

© 2023 Cisco Systems, Inc. All rights reserved.

4.10 Vulnerability Mitigation

The following steps need to be followed to ensure that the TOE is operating with all potential vulnerabilities mitigated -

- Cisco VDB Fingerprint Database version needs to be up to date. The “Update the Vulnerability Database (VDB) Manually” section of the FMC-CG lists the instructions to update the Cisco VDB Fingerprint Database.
- ESXi v6.7 and 7.0 should be updated in the FMCv TOE to include the latest patches – ESXi670-202210101-SG for ESXi 6.7 and ESXi70U3si-20841705 for ESXi 7.0 respectively.
- The default credentials for ESXi need to be updated.
- The “Allow External Database Access” option in the FMC should not be enabled to avoid the FMC connecting to an external SQL database. This connection is disabled by default.

© 2023 Cisco Systems, Inc. All rights reserved.