JUNIPER NETWORKS | Engineering Simplicity

Juniper Connected Security Solution for Juniper Networks Devices

Published
2023-09-13

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Connected Security Solution for Juniper Networks Devices

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About this guide

This network configuration example (NCE) provides an overview and a step-by-step example for configuring and deploying Juniper Networks’ connected security solution using Junos devices. This NCE defines Juniper Connected Security deployment for an enterprise and illustrates how Juniper Connected Security secures your network.

1

CHAPTER

Network Configuration Example - Juniper Connected Security Solution for Juniper Networks Devices

About This Network Configuration Example

This network configuration example (NCE) provides an overview and a step-by-step example for configuring and deploying Juniper Connected Security solution using Junos devices. This NCE defines Juniper Connected Security deployment for an enterprise and illustrates how Juniper Connected Security secures your network.

The instructions in this NCE cover configuration scenarios for traffic blocking, infected host tracking, and monitoring using Policy Enforcer, Juniper Networks® Advanced Threat Prevention Cloud (ATP Cloud), and Security Director. The instructions also cover configuring SRX Series devices acting as a firewalls, and EX Series devices, acting as access and aggregation switches. This document is intended for security and IT engineers, as well as network architects.

RELATED DOCUMENTATION

Use Case Overview

IN THIS SECTION

Coping with Threat Landscape - An Overview

Coping with today's broad and evolving threat landscape requires threat intelligence and immediate threat enforcement, as well as a method of providing a simpler policy mechanism across multivendor security environments.

The paradigm is changing from traditional perimeter security defenses to end-to-end security solutions that can deliver comprehensive yet coordinated protection by:

- Integrating and deploying advanced security features to protect systems and data from spyware, viruses, malicious code, denial-of-service attacks, and so on.
- Enabling every part of the network to be both a detection and enforcement point, to respond to suspicious activity anywhere in the network, which is the most effective way to deal with threats and intruders.
- Closing the gap between threat intelligence and enforcement, because threat intelligence loses most of its value if it is distributed too slowly, or if it does not reach all of an enterprise's enforcement points.
- Using policy automation to adapt and enforce policy in real time, improving both compliance and business agility.
- Centralizing the security policy engine so that it can determine trust levels between network segments by collecting real-time threat information and creating a unified security policy, with distributed new policies implemented in real time from a central location.
- Providing the centralized management capabilities critical for regulatory compliance, reducing costs and streamlining operations.

Securing the Network with Juniper Connected Security Building Blocks

Juniper Connected Security provides end-to-end network visibility, allowing enterprises to secure their entire network, both physical and virtual.

Juniper Connected Security solution is comprised of the following components:

- A threat detection engine—Juniper ATP Cloud detects known and unknown malware. Known threats are detected by consolidating threat feed information from a variety of sources—command and control (C&C) servers, GeoIP—as well as information acquired from in-house log servers.

  Unknown threats are identified using various methods such as sandboxing, machine learning, and threat deception.

- Centralized policy management—Junos Space Security Director, which also manages SRX Series Devices, provides a management interface for the Juniper Connected Security solution called Policy Enforcer. Policy Enforcer communicates with Juniper devices and third-party devices across the network, globally enforcing security policies and consolidating threat intelligence from different sources. With monitoring capabilities, it can also act as a sensor, providing visibility for intra- and inter-network communications.

- Expansive policy enforcement—In a multi-vendor enterprise, Juniper Connected Security enforces security across Juniper devices, cloud-based solutions, and third-party devices. By communicating with all enforcement points, Juniper Connected Security can quickly block or quarantine threats, preventing the spread of bi-lateral attacks within the network.

  Juniper Connected Security integrates third-party capabilities, enabling users to leverage existing, trusted threat feed sources to provide consistent, automated defense across diverse environments. An open architecture and suite of APIs enables Juniper Connected Security to choose their preferred threat intelligence information sources and remediate across multivendor network infrastructure. See Juniper Connected Security Solution Using Third-Party Devices and Aruba ClearPass Policy Manager.

- User Intent-Based Policies—Juniper Connected Security supports the creation of policies according to logical business structures such as users, user groups, geographical locations, sites, tenants, applications, or threat risks. This allows network devices (switches, routers, firewalls, and other security devices) to share information, resources, and when threats are detected, remediation actions within the network.

The Juniper Connected Security solution provides the following benefits:

- Provides dynamic, automated threat remediation—Juniper Connected Security accurately detects known and unknown threats and delivers the ability to rapidly block or quarantine threats to prevent north-south or east-west threat propagation.

- Extends security to each layer of the network—Juniper Connected Security uses an inside-out security model because it leverages any network element as an enforcement point and then dynamically enforces security policy with software-defined segmentation designed to provide robust security.

- Works within a multi-vendor ecosystem—Juniper Connected Security adopts an open, multivendor ecosystem to detect and enforce security across Juniper products and solutions. This enables collaborative and comprehensive approach to complete network security.

- Provides centralized policy and security management—Juniper Connected Security communicates with all network elements and security products such as next-generation firewalls to globally enforce security policies and enables security policy administration through a single pane of glass. This reduces administrative overhead and facilitates a faster, more manageable approach to security as the network expands.

RELATED DOCUMENTATION

Technical Overview | 5

Use Case # 1: Configuring Juniper Connected Security | 11

Technical Overview

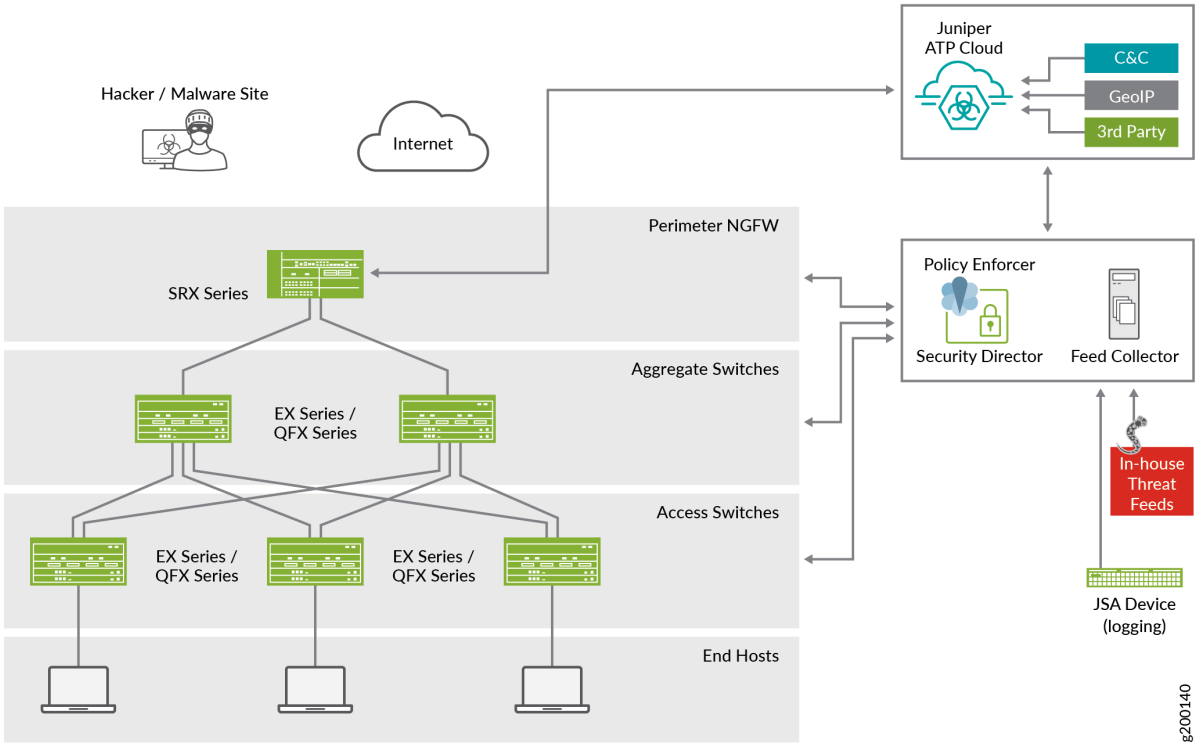
IN THIS SECTION

This section shows how the Juniper Connected Security building blocks work together to provide a comprehensive security solution for your enterprise.

Components of Juniper Connected Security Solution

Figure 1 on page 6 shows a high-level workflow of how Policy Enforcer, Security Director, Juniper Networks® Advanced Threat Prevention Cloud (ATP Cloud), and Junos devices interact to provide a secure network deployment with Juniper Connected Security.

Figure 1: Juniper Connected Security Solution Components



EX Series switches deliver switching services in branch, campus, and data center networks. QFX Series switches are high-performance, low-latency, edge devices optimized for data center environments.

In the Juniper Connected Security solution, clients/endpoints are connected to EX Series and QFX Series switches with endpoint protection software. These switches provide access security and control.

SRX Series Services gateways provide security enforcement and deep inspection across all network layers and applications.

In the context of the Juniper Connected Security solution, SRX Series devices are deployed as perimeter firewalls connected to Juniper ATP Cloud for anti-malware services.

Juniper ATP Cloud identifies varying levels of risk, and provides a higher degree of accuracy in threat protection. It integrates with SRX Series gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

Policy Enforcer uses information gathered and reported by Juniper ATP Cloud to learn about the threats and rapidly respond to new threat conditions. With this information, Policy Enforcer can automatically update policies and deploy new enforcement to firewalls and switches, quarantining and tracking infected hosts to stop the progress of threats.

Policy Enforcer identifies an infected host by its IP and MAC address, allowing tracking and continued blocking of the host even if it moves to another switch or access point on the network.

With these components working together, threats are detected more quickly by leveraging threat intelligence from multiple sources (including third-party feeds). Network security can adapt dynamically to real-time threat information so that security policies are enforced consistently.

Juniper Connected Security Workflow Overview

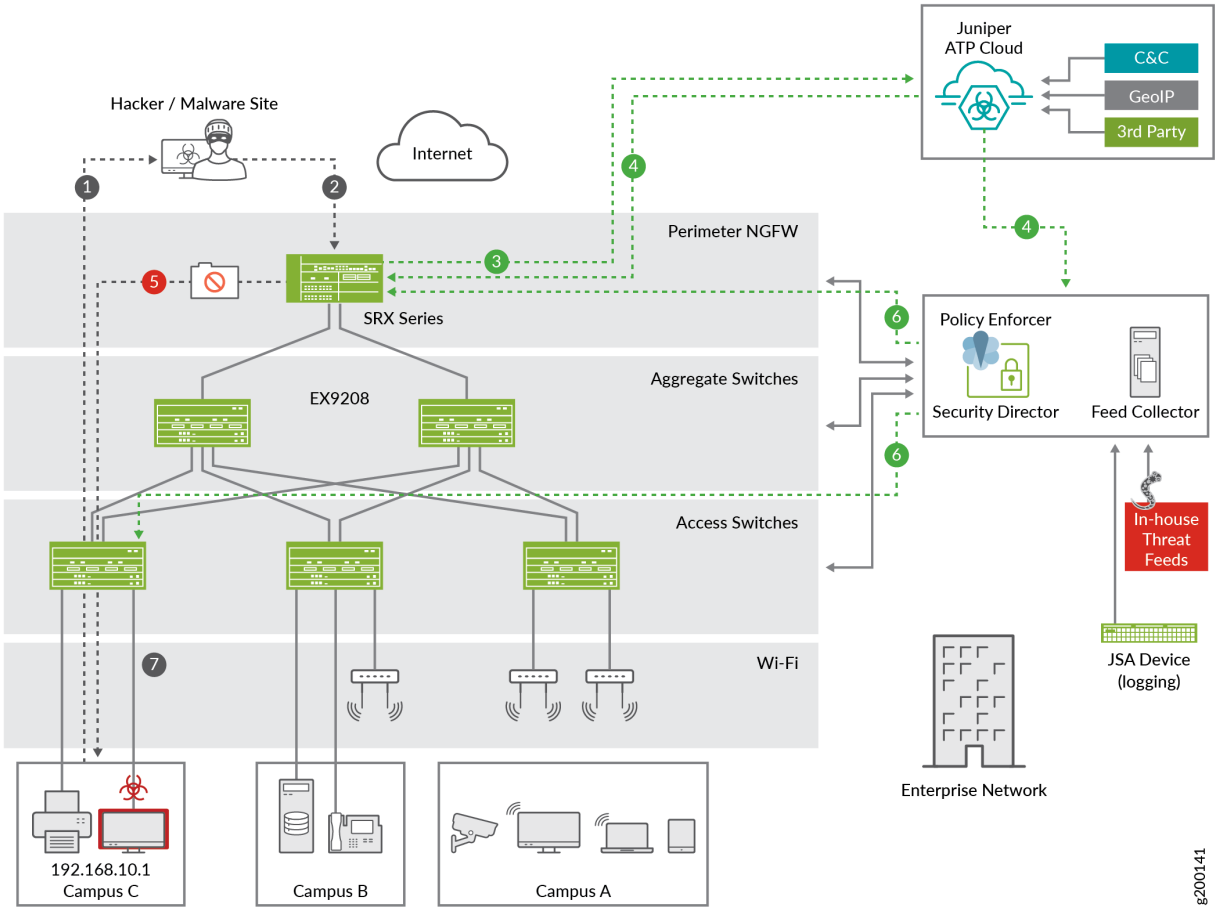
The following examples provide a high-level workflow of how Juniper Connected Security components work together to detect and block an infected endpoint, track the infected endpoint, and automatically quarantine it or block it from accessing the Internet.

Infected Host Detection and Tracking

Let's take a look at a typical enterprise with clients, endpoints, access switches, and wireless access points. When a client becomes compromised because of contact with an endpoint outside the corporate network, it becomes a threat to other hosts in the network. You must be able to control the infected host to ensure the problem doesn't spread.

Figure 2 on page 8 shows an infected host tracking workflow.

Figure 2: Juniper Connected Security Workflow - Detecting an Infected Endpoint



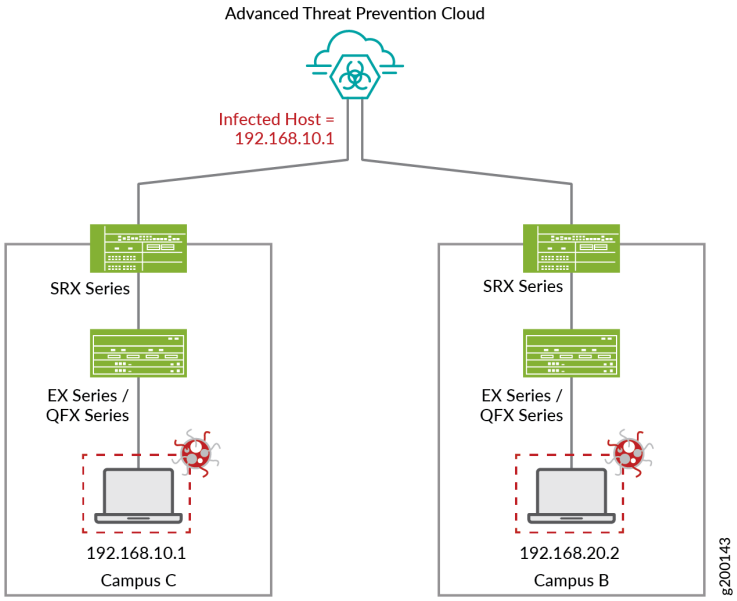
This scenario involves the following steps:

1. A user (192.168.10.1) in Campus C connects to a site on the Internet and downloads a file.
2. The file is scanned at the perimeter firewall (SRX Series device).
3. Based on user-defined policies, the firewall sends the file to an anti-malware service (Juniper ATP Cloud) for analysis.
4. Juniper ATP Cloud detects that the file contains malware, identifies 192.168.10.1 as an infected host, and notifies the SRX device and Policy Enforcer.
5. The firewall blocks the file, preventing it from being downloaded.
6. Policy Enforcer identifies the IP address and MAC address of the host that downloaded the file and pushes a security policy onto the firewalls, and firewall filters onto the switches, to prevent further threats.
7. The infected endpoint, connected to EX Series switch in Campus C, is quarantined.

The movement of infected endpoints and the resulting change in network IP addresses can easily evade security in perimeter-only protection architectures.

As the scenario continues, the infected host moves to a different location (Campus B) and receives a new IP address, as shown in Figure 3 on page 9.

Figure 3: Tracking Infected Endpoint Movement



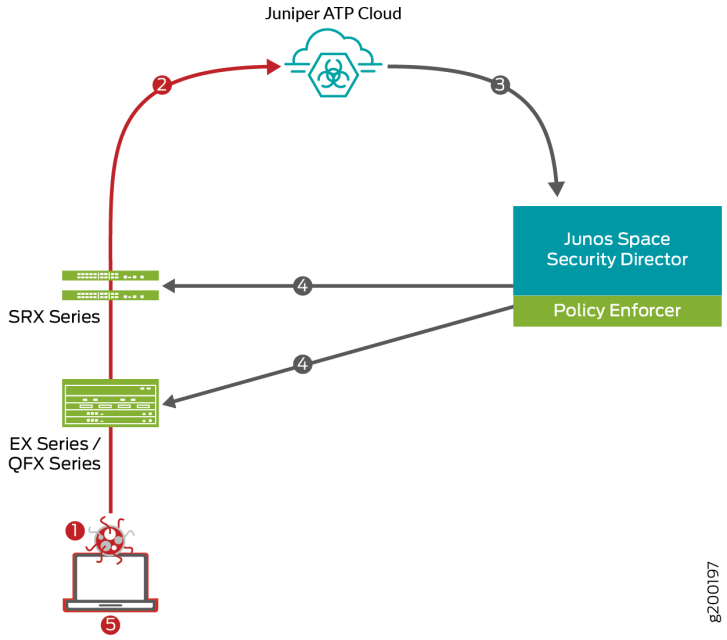
Policy Enforcer keeps track of infected host movement and informs Juniper ATP Cloud of the new MAC address-to-IP address binding. When the infected host moves to its new location (in Campus B), Policy Enforcer recognizes the host as a continuing threat and blocks it from the network.

Protection from Botnet C&C Attacks

When a host on the network tries to initiate contact with a possible command and control (C&C) server on the Internet, the SRX Series device can work with Juniper ATP Cloud, Security Director, and Policy Enforcer to intercept the traffic and perform an enforcement action based on real-time intelligence feed information that identifies the C&C server IP address and URL.

Figure 4 on page 10 shows an example of how the Juniper Connected Security solution provides protection from botnet C&C attacks.

Figure 4: Protection from Botnet C&C Attack



This scenario involves the following steps:

1. A user downloads a file from the Internet.
2. The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed. If required, it sends file to Juniper ATP Cloud for malware inspection.
3. The inspection determines this file is malware and informs Policy Enforcer of the results.
4. An enforcement policy is automatically deployed to the SRX device and EX/QFX switches.
5. The infected endpoint is quarantined.

RELATED DOCUMENTATION

Use Case Overview | 2

Use Case # 1: Configuring Juniper Connected Security | 11

Policy Enforcer

Use Case # 1: Configuring Juniper Connected Security

IN THIS SECTION

This configuration example provides step-by-step instructions to configure the Juniper Connected Security solution and help simplify security policy creation, threat detection, and policy enforcement across the network.

Requirements

This example uses the following hardware and software components:

- SRX1500 device running Junos OS Release 15.1X49-D80 or later
- EX4300 switch running Junos OS Release 15.1R5.5 or later
- Two EX2200 switches running Junos OS Release 15.1R5.5 or later
- VMware ESXi server, and vSphere client
- Juniper Networks® Advanced Threat Prevention Cloud (ATP Cloud)

- Junos Space Network Management Platform, Release 16.1R2.7 or later
- Junos Space Security Director, Release 16.2R1 or later
- Log Collector, Release 16.2R1 or later
- Policy Enforcer, Release 16.2R1 or later
- Policy Enforcer Patch for Security Director, Release 16.2R1
- VM running Windows 7 with dual NICs

For a list of supported devices, please refer to the Policy Enforcer Release Notes.

Overview and Topology

Juniper Connected Security can be deployed in three ways, as shown in Figure 5 on page 12:

Figure 5: Juniper Connected Security Implementation Options

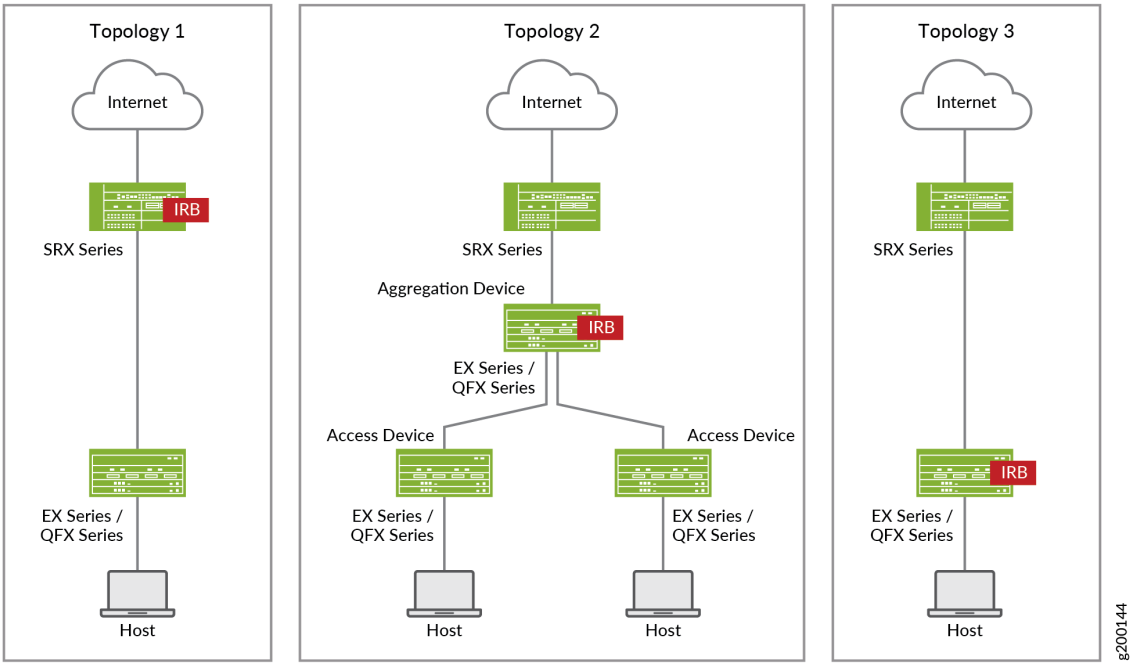


Table 1 on page 13 provides more detail on these deployment options.

Table 1: Supported Topologies for Juniper Connected Security

Topology 1	Topology 2	Topology 3
EX Series or QFX Series device as Layer 2 switch	EX Series or QFX Series device (access switch) as Layer 2 switch EX Series or QFX Series device (aggregation switch) as Layer 3 switch	EX Series or QFX Series device as Layer 2/Layer 3 switch
SRX Series device as firewall in Layer 3 mode	SRX Series device as firewall in Layer 3 mode	SRX Series device as firewall in Layer 3 mode
IRB / VLAN tagging on SRX Series device	IRB / VLAN tagging on EX Series or QFX Series device (aggregation switch)	IRB / VLAN tagging on EX Series or QFX Series switch

NOTE:

- All interconnecting switch ports (SRX/EX/QFX devices) must be configured in trunk mode, even when there is only one VLAN in use.
- All switch ports connected to end hosts must be configured in access mode.
- VLAN names and IDs must be identical on all devices.

  For more information, see Appendix 1: Configuration of SRX Series Devices and EX Series Switches.

The lab setup used for this network configuration example was built to support and test all three deployment topologies shown above. This setup is shown in Figure 6 on page 14.

Figure 6: Juniper Connected Security Topology

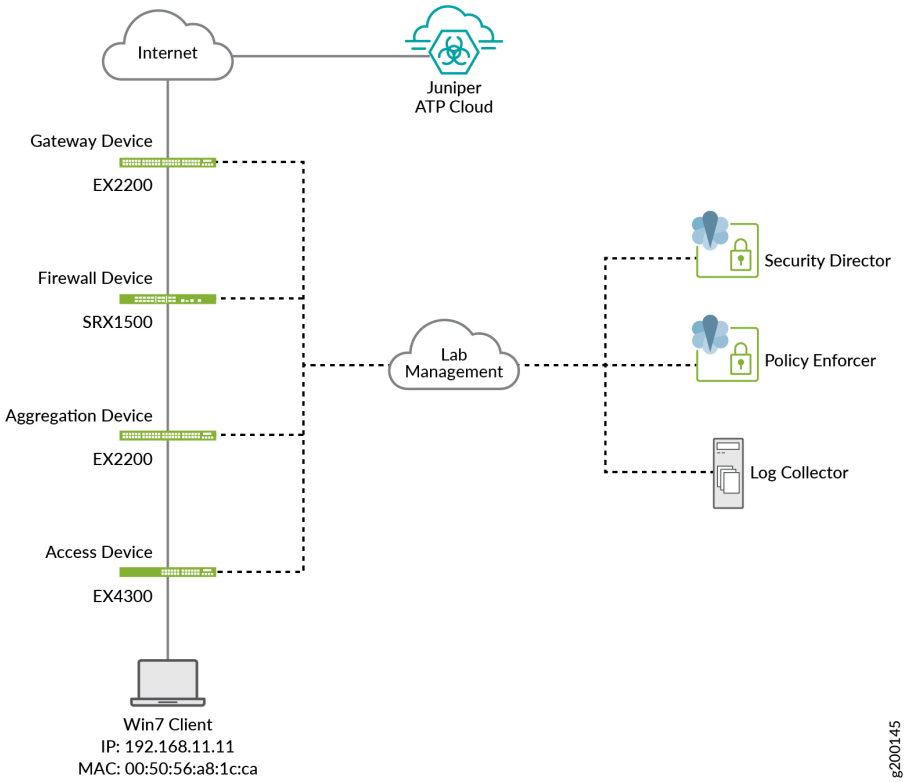


Table 2 on page 14 and Table 3 on page 15 show the details of devices, IP addresses, and parameters used in this configuration example.

Table 2: Devices and IP Addresses

Device	Function	Mgmt IP Address
SRX1500 (SRX1500-WF)	Firewall	10.13.107.186
EX4300 (EX4300-1)	Access Switch	10.13.107.181
EX2200	Aggregation Switch	10.13.107.188

Table 3: Parameters and Description

Parameter	Name	Description
Site Name	Westford-Site	A site is a grouping of network devices, including firewalls and switches, that contribute to threat prevention. An infected host with IP address 192.168.11.11 is connected to EX4300-1m which belongs to Westford-Site.
Policy Enforcement Group	JSD	A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied. In this example, Westford-site is included in policy enforcement group JSD.
Threat Prevention Policy	TPP	Threat prevention policies provide protection and monitoring for an assigned policy enforcement group. In this example, policy enforcement group JSD is assigned to threat prevention policy TPP.

The following set of installation, configuration, and verification steps are required to implement the Juniper Connected Security solution:

- Install and Configure Junos Space and Security Director
- Install and configure SRX Series devices and EX/QFX Series switches
- Download, deploy, and configure the Policy Enforcer virtual machine
- Connect Policy Enforcer to Security Director
- Obtain Juniper ATP Cloud license and create ATP Cloud portal account
- Install the root CA on your ATP Cloud-supported SRX Series devices
- Configure Juniper ATP Cloud with Policy Enforcer
- Verify the enrollment of devices on Juniper ATP Cloud
- Verify Juniper Connected Security functionality once the enrollment is successful

Install and Configure Junos Space and Security Director

IN THIS SECTION

Install Junos Space, Security Director, and Log Collector

Step-by-Step Procedure

To Install Junos Space, Security Director, and Log Collector:

1. Download the Junos Space Network Management Platform image from https://www.juniper.net/support/downloads/?p=space#sw.
2. Install Junos Space using the instructions at https://www.juniper.net/documentation/en_US/junos-space16.1/platform/information-products/topic-collections/release-notes/jd0e56.html.
3. Install Junos Security Director as per the instructions at https://www.juniper.net/documentation/en_US/junos-space16.2/information-products/topic-collections/release-notes/js-relnotes-security-design/index.html.
4. Install Log Collector as per the instructions at https://www.juniper.net/documentation/en_US/junos-space16.2/information-products/topic-collections/release-notes/js-relnotes-security-design/index.html..

Configure Networking

Step-by-Step Procedure

To configure basic networking for Junos Space and its components, perform the following tasks:

1. Configure relevant routes, netmask, gateway, DNS, and NTP so that all components except Log Collector can reach the Internet.
2. Ensure all components are in same time zone.

3. Ensure that SSH is enabled.
4. Ensure that Security Director can reach the ATP Cloud server, Policy Enforcer, and all devices.

Install Policy Enforcer Patch for Security Director, Release 16.2R1

Step-by-Step Procedure

To install the Policy Enforcer patch:

1. Download the **Policy-Enforcer-16.2R1-Patch.sh** file from https://www.juniper.net/support/downloads/?p=sdpe#sw and put it in the **/tmp** folder of the Junos Space Network Management Platform server.
2. Login to the Junos Space CLI using an SSH or console connection, and change directory to the **/tmp** folder.
3. Change the permissions of the **Policy-Enforcer-16.2R1-Patch.sh** file to allow read, write, and execute permissions for everyone, using the following command:

```
chmod 777 Policy-Enforcer-16.2R1-Patch.sh
```

4. Execute the installation script using the following command:

```
sh Policy-Enforcer-16.2R1-Patch.sh
```

It may take a few minutes for the script to complete.

Install the required DMI schemas on Security Director

Step-by-Step Procedure

You must download and install the matching Junos OS schemas to manage SRX Series devices. To download and install the correct schemas, perform the following task:

1. Install the missing DMI schemas for Junos OS Releases 15.1X49-D80 and 15.1R5.5 as per the instructions at https://www.juniper.net/documentation/en_US/junos-space16.1/platform/topics/task/configuration/junos-space-network-application-platform-schema-adding.html
2. After the schemas are installed, set them as the default schema for each relevant platform.

Install and Configure SRX Series Devices and EX Series / QFX Series Switches

IN THIS SECTION

Install and Configure SRX Series Devices

Step-by-Step Procedure

To configure SRX device devices:

1. Configure the SRX device(s) per your requirements.

> **NOTE:** Appendix 1: Configuration of SRX Series Devices and EX Series Switches of this document includes SRX device configurations for all three deployment topologies.

Install and configure EX/QFX Series switches

Step-by-Step Procedure

To configure EX (or QFX) devices:

1. Configure the EX Series and/or QFX Series switches per your requirements.

> **NOTE:** Appendix 1: Configuration of SRX Series Devices and EX Series Switches of this document includes EX device configurations for all three deployment topologies.

Configure Networking

Step-by-Step Procedure

To configure basic networking on Junos devices, perform the following tasks:

1. On all Junos devices, configure the necessary routing and DNS settings to enable Internet access, as well as connectivity to Junos Space, Policy Enforcer, and the ATP Cloud server.
2. For SRX Series devices, ensure that Internet access is enabled both in-band and out-of-band.

Device Discovery in Junos Space

Step-by-Step Procedure

To add devices to the Junos Space Network Management platform, perform the following tasks:

1. In Junos Space, discover and import the SRX Series, EX Series, and/or QFX Series devices in your environment.
2. In Security Director, assign, publish, and update any existing firewall policies to ensure Security Director and the SRX devices are in sync.

Download, Deploy, and Configure Policy Enforcer Virtual Machine

IN THIS SECTION

Procedure

Step-by-Step Procedure

To deploy and configure the Policy Enforcer virtual machine, perform the following tasks:

1. Download the Policy Enforcer virtual machine image from https://www.juniper.net/support/downloads/?p=sdpe to the management station where the vSphere client is installed.

2. On the vSphere client, select **File > Deploy OVF Template** from the menu bar.
3. Click **Browse** to locate the OVA file that was downloaded.
4. Click **Next** and follow the instructions in the installation wizard.
5. Once the installation is complete, login to the virtual machine using `root` and `abc123` as the username and password, respectively.
6. Configure the network settings, NTP information, and customer information, and finish the wizard accordingly.

   For more detailed instructions, see https://www.juniper.net/documentation/en_US/release-independent/policy-enforcer/topics/task/installation/policy-enforcer-vm-config.html.

Connect Policy Enforcer to Security Director

IN THIS SECTION

Procedure

Step-by-Step Procedure

You must identify the Policy Enforcer virtual machine in Security Director so that they can communicate with each other. To do so, follow these steps:

1. In Security Director, identify the Policy Enforcer virtual machine so that they can communicate with each other.
2. Login to Security Director and select **Administration** > **PE Settings**.
3. Enter the IP address of the Policy Enforcer virtual machine and the root password, and click **OK**.
4. Select Threat Prevention Type as **ATP Cloud with PE**.

> **NOTE**: Do not run the wizard/guided setup at this point.

Obtain Juniper ATP Cloud License and Create ATP Cloud Portal Account

IN THIS SECTION

Procedure

Step-by-Step Procedure

To obtain a Juniper ATP Cloud license and create an ATP Cloud Web portal account, follow these steps:

1. Juniper ATP Cloud has three service levels: free, basic, and premium. The free license provides limited functionality and is included with the base software. To obtain and install Juniper ATP Cloud basic or premium license, see Managing the Advanced Threat Prevention Cloud License.

   For further detail on ATP Cloud service levels and license types, see Advanced Threat Prevention Cloud License Types.

2. Create Juniper ATP Cloud Web portal account by going to https://sky.junipersecurity.net and filling in the required information.

Install the root CA on the ATP Cloud-supported SRX Series devices

IN THIS SECTION

This section is required only if you will be enabling HTTPS inspection as part of a malware profile/threat prevention policy.

Generate Root CA Certificate using Junos OS CLI or OpenSSL

Step-by-Step Procedure

To generate a root CA certificate using the Junos OS CLI on the SRX device:

1. Generate a PKI public/private key pair for a local digital certificate.

```
user@host> request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type
rsa
```

2. Using the key pair, define a self-signed certificate by providing FQDN and other details.

```
user@host> request security pki local-certificate generate-self-signed certificate-id ssl-
inspect-ca domain-name domain-name subject subject email email-id add-ca-constraint
```

OR

Step-by-Step Procedure

To generate a root CA certificate using OpenSSL on a Linux device:

1. Generate a PKI public/private key pair for a local digital certificate.

```
% openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout ssl-inspect-ca.key -out ssl-inspect-
ca.crt
```

2. Copy the key pair onto the SRX device(s).
3. On the SRX device(s), import the key pair.

```
user@host> request security pki local-certificate load key ssl-inspect-ca.key filename ssl-
inspect-ca.crt certificate-id ssl-inspect-ca
```

NOTE: Use only one of the options above.

Configure a CA Profile Group

Step-by-Step Procedure

To configure a CA profile group:

1. Create the CA profile.

```
user@host# set security pki ca-profile ssl-inspect-ca ca-identity ssl-inspect-ca
user@host# commit
```

2. The Junos OS provides a default list of trusted CA certificates that you can load on your system using the default command option.

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name All-Trusted-CA-Def filename default

Do you want to load this CA certificate ? [yes,no] (no) yes

Loading 155 certificates for group 'All-Trusted-CA-Def'.
All-Trusted-CA-Def_1: Loading done.
All-Trusted-CA-Def_2: Loading done.
All-Trusted-CA-Def_3: Loading done.
All-Trusted-CA-Def_4: Loading done.
All-Trusted-CA-Def_5: Loading done.
...
```

3. Verify that the **All-Trusted-CA-Def** certificates are loaded.

```
user@host> show security pki ca-certificate brief

...
Certificate identifier: All-Trusted-CA-Def_1
...
```

Import Root CA Certificate into a Browser

Step-by-Step Procedure

First, export the root CA certificate:

1. On the SRX device, export the certificate to a .pem file.

```
user@host> request security pki local-certificate export certificate-id ssl-inspect-ca type
pem filename /var/tmp/ssl-inspect-ca.pem
```

```
root@SRX1500-WF> request security pki local-certificate export certificate-id ssl-inspect-ca type pem filename /var/tmp/ssl-inspect-ca.pem
certificate exported successfully

root@SRX1500-WF> file list /var/tmp

/var/tmp:
TUNC2
appidd_trace_debug
cleanup-pkgs.log
eedebug_bin_file
gksdchk.log
gres-tp/
idp_license_info
install/
juniper.conf+.gz
kmdchk.log
krt_rpf_filter.txt
nsd_restart
phone-home/
pics/
pkid-new-ca-grp-profile.xml
pkid_mgd_errors
policy_status
rtsdb/
scep_cert_req
sd-upgrade/
sec-download/
spu_kmd_init
ssl-inspect-ca.pem
test1-der
```

2. Transfer the **.pem** file to your Windows client.

> **NOTE**: If you are using the Linux device with OpenSSL, the certificate is already on the device and no action is required.

Step-by-Step Procedure

Then import certificate into a browser:

1. On the Windows client, instruct the browser to trust the CA root certificate.

   Internet Explorer (version 8.0):

   - From the **Tools** menu, choose **Internet Options**.
   - On the **Content** tab, click **Certificates**.
   - Select the **Trusted Root Certification Authorities** tab and click **Import**.
   - In the **Certificate Import** Wizard, navigate to the required root CA certificate and select it.

Firefox (version 39.0):

- From the **Tools** menu, choose **Options**.
- From the **Advanced** menu, select the **Certificates** tab and click **View Certificate**.
- In the **Certificate Manager** window, select the **Authorities** tab and click **Import**.
- Navigate to the required root CA certificate and select it.

Google Chrome (version 45.0):

- From the **Settings** menu, choose **Show Advanced Settings**.
- From the **Advanced** menu, select the **Certificates** tab and click **View Certificate**.
- Under HTTPS/SSL, click **Manage Certificates**.
- In the **Certificate** window, select **Trusted Root Certification Authorities** and click **Import**.
- In the **Certificate Import** Wizard, navigate to the required root CA certificate and select it.

More details on the steps in this section can be found at: https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ssl-proxy-workflow-configuring.html

OR

Step-by-Step Procedure

1. On the Linux device, import the certificate into the browser.

```
% sudo cp ssl-inspect-ca.crt /usr/local/share/ca-certificates/ ssl-inspect-ca.crt
% sudo update-ca-certificates
```

Configure Juniper Connected Security with Juniper ATP Cloud and Policy Enforcer

IN THIS SECTION

Procedure

Step-by-Step Procedure

The tasks required to configure Juniper Connected Security include:

- Configure a secure fabric
- Define a site and add endpoints to it (switches and firewalls)
- Configure policy enforcement groups
- Create a threat prevention policy
- Apply threat prevention policies to policy enforcement groups

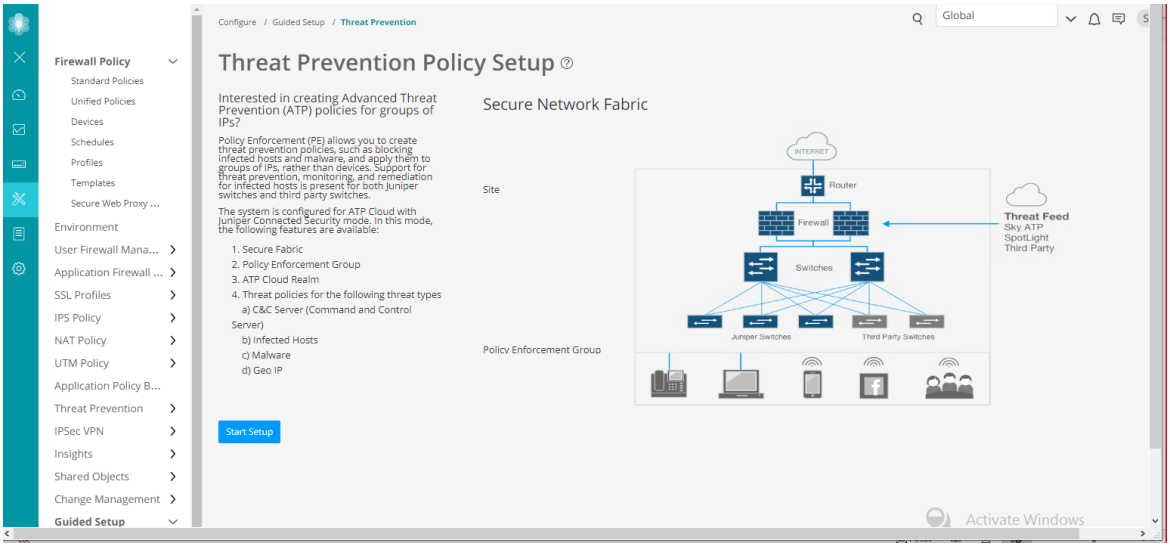
If you are using Policy Enforcer for threat prevention with Juniper ATP Cloud, Guided Setup is the most efficient way to complete the initial configuration. The Guided Setup process offers four steps for configuring Juniper Connected Security with Juniper ATP Cloud, and is used below.

To perform the configuration without the guided setup, see "Configuring Juniper Connected Security with ATP Cloud and Policy Enforcer (Without Guided Setup)" on page 75.

This configuration example implements topology 1 from "Overview and Topology" on page 12.

> **NOTE**: The screenshots used in this section have been updated to Junos Space Security Director Release 17.1R1.

1. In Security Director, go to **Configure > Guided Setup > Threat Prevention**.



2. Click **Start Setup** and follow the wizard.

3. Create a secure fabric site that includes all the relevant SRX Series and EX Series (or QFX) devices in the network.

   A secure fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices) used in policy enforcement groups.

4. Create a policy enforcement group by selecting the relevant LAN subnets for which you want to enable policy enforcement.

   A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied.

   In this step, you need to determine the type of endpoints you are including in your policy enforcement group: IP address, subnet, or location. Note that endpoints cannot belong to multiple policy enforcement groups.

5. Add the ATP Cloud realm by providing the relevant details from your ATP Cloud account.

   Before you configure the ATP Cloud realm, ensure that you:

   - Have an ATP Cloud account with an associated license.
   - Understand which type of ATP Cloud license you have: free, basic, or premium. The license controls which ATP Cloud features are available.

     See "Obtain Juniper ATP Cloud License and Create ATP Cloud Portal Account" on page 21 for more details.

   - Know which region will be covered by the realm you are creating. You must a select a region when you configure a realm.

6. Verify that the ATP Cloud realm has been added. The value **1** should appear in the **Perimeter Firewall in Sites** column, indicating that ATP Cloud has detected the SRX device.

   If the realm addition is not successful, it means there is a network issue and Security Director is unable to reach Internet. Ensure all devices/components can reach the Internet and each other.

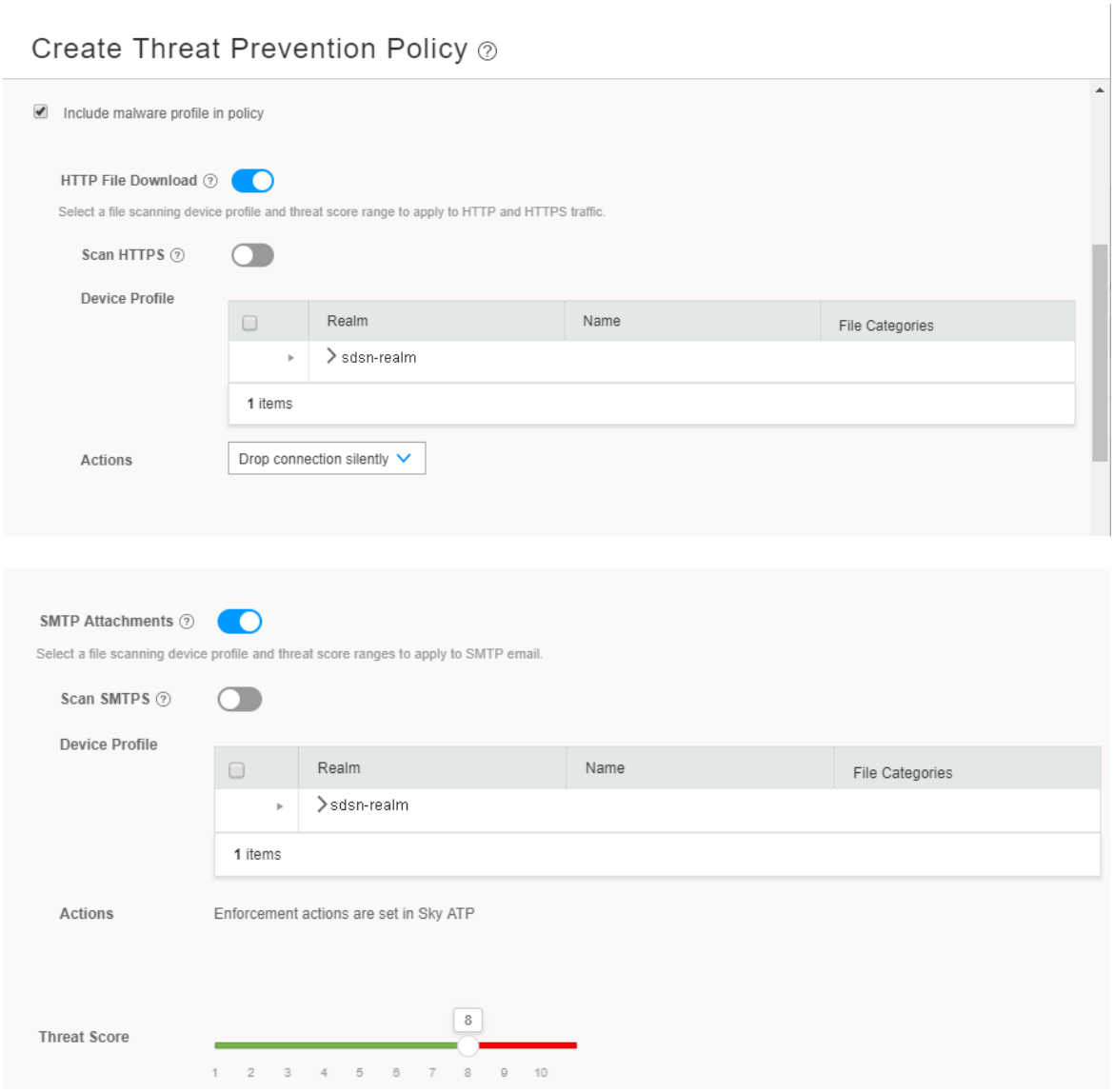
7. Create a threat prevention policy.

Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, infected hosts, and malware.

In this step, you need to:

- Determine the type of profile you will use for this policy: command & control server, infected hosts, or malware. You can select one or more threat profiles in a policy.
- Determine which action to take if a threat is found.
- Know which policy enforcement group you will add to this policy.

8. Add a profile for HTTP file downloads and SMTP attachments.



This profile indicates which file types need to be scanned for threats. In the **Device Profile** area, expand the realm and select the required profile.

9. Assign the threat prevention policy to the desired policy enforcement group by clicking **Assign to Groups**.

10. Select the policy enforcement group and click **OK**.

11. The system performs a rule analysis, and prepares device configurations that include the threat prevention policies.

12. Once the analysis is complete, instruct the system to push the updated policy to the SRX Series devices by clicking the **Update** button.

13. When the push is complete, the system returns to the **Policies** page.

Verification

IN THIS SECTION

Verify the Enrollment of Devices in Juniper ATP Cloud on SRX Series Device

Purpose

Verify that the SRX Series device is connected to the ATP Cloud server.

Action

On the SRX device, use the ***show services advanced-anti-malware status*** CLI command.

```
user@host> show services advanced-anti-malware status
 Server hostname:
 srxapi.us-west-2.sky.junipersecurity.net
  Server port: 443
    Control Plane:
      Connection time: 2017-10-15 23:53:31 UTC
      Connection status: Connected
    Service Plane:
      fpc0
```

```
        Connection active number: 11
        Connection retry statistics: 872
```

Meaning

The output displays the `Connection status` as `Connected`. The `Server hostname` field displays the ATP Cloud server hostname.

Verify the Enrollment of Policy Enforcer and SRX Series Devices in Juniper ATP Cloud

Purpose

Verify that Policy Enforcer and the SRX Series device are enrolled with Juniper ATP Cloud.

Action

In the ATP Cloud Web UI, navigate to the **Enrolled Devices** page and review the connection information for enrolled devices, including serial number, model number, tier level (free, basic, premium) enrollment status in ATP Cloud, last telemetry activity, and last activity seen.

Meaning

The `Host` field displays the enrolled firewall detail (SRX1500-WF). You can click the serial number for more details.

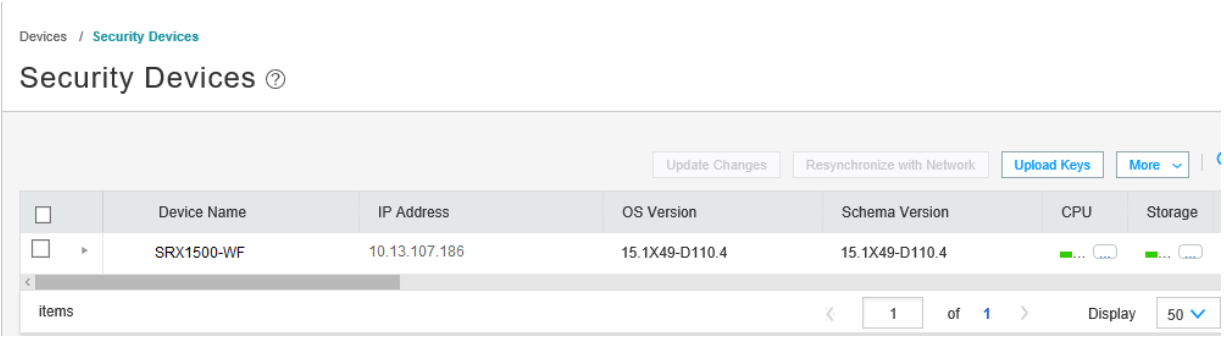
Verify the Enrollment of Devices with Juniper ATP Cloud in Security Director

Purpose

Verify that the SRX Series device is enrolled with Juniper ATP Cloud in Security Director.

Action

Navigate to **Devices > Security Devices** in Security Director.



On the **Security Devices** page, the device's name, IP address, OS version are displayed. You can scroll right to get more details such as ATP Cloud realm, serial number, assigned devices, and so on.

You can alternatively click the **Detailed View** icon next to the device name to get more details about the device.

Meaning

The ATP Cloud realm's name displayed under the **ATP Realm** field confirms enrollment of the device with the ATP Cloud realm.

Test Juniper Connected Security Functionality

Purpose

With the Juniper Connected Security solution configured, verify how it detects a problem and reacts to it.

In this scenario, an end host (192.168.11.11) on the LAN simulates a threat by contacting (pinging) a C&C server (192.0.2.1). This event is determined to exceed the threat prevention policy's threat score threshold.

Action

Verify the connectivity between end hosts to endpoints on the LAN and Internet using the Ping command before and after the attack.

Before the attack, the end host starts continuous pings to endpoints on the LAN and Internet.

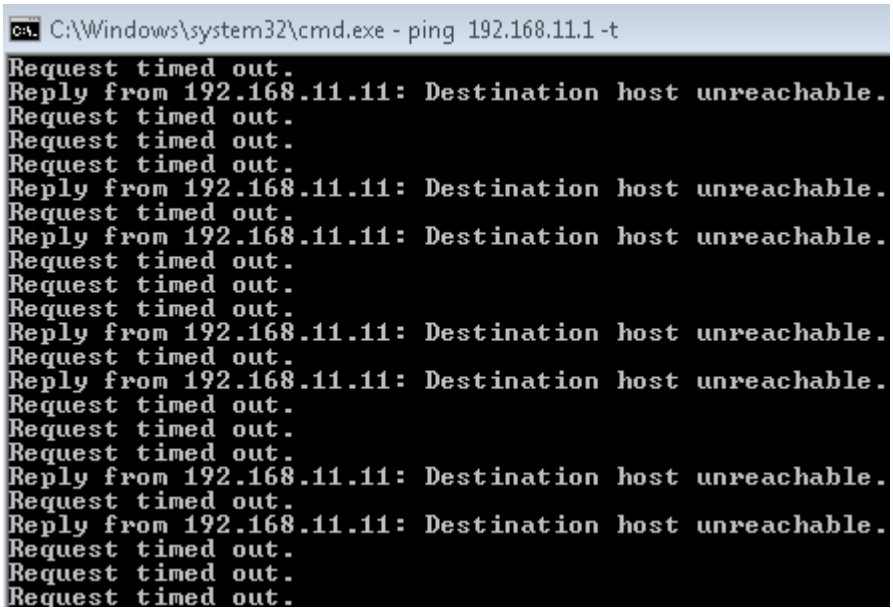
```
C:\Users\ccl>ping 192.168.11.1 -t

Pinging 192.168.11.1 with 32 bytes of data:
Reply from 192.168.11.1: bytes=32 time=2ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
Reply from 192.168.11.1: bytes=32 time<1ms TTL=64
```

```
C:\Windows\system32\cmd.exe - ping 8.8.8.8 -t
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
Reply from 8.8.8.8: bytes=32 time=12ms TTL=56
```

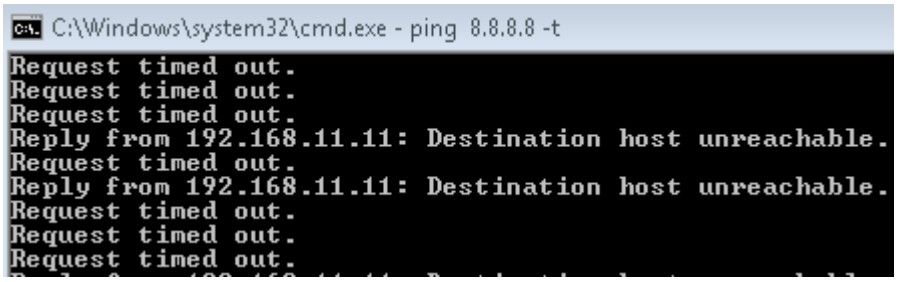
The end host pings the C&C server.

```
C:\windows\system32\cmd.exe - ping 192.0.2.1 -t

C:\Users\ccl>ping 192.0.2.1 -t

Pinging 192.0.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Verify that connectivity to the endpoint on the LAN is blocked after the attack.



Confirm that the end host can no longer reach the Internet.



Meaning

All ping sessions show that the traffic is blocked after the threat is detected, which confirms that the Juniper Connected Security solution is working properly.

Verify Juniper Connected Security Functionality Using the Security Director Logs

Purpose

Verify that the firewall filter has been created and applied to the switch where the end host is attached.

Action

Check the Security Director logs (**/var/log/jboss/servers/server1/SECI.log**).

```
<term>
<name>MAC_00:50:56:a8:1c:ca</name>
<from>
<source-mac-address>
<name>00:50:56:a8:1c:ca</name>
</source-mac-address>
</from>
<then>
<discard/>
<log/>
</then>
</term>
<term>
<name>GOOD_HOST_MAC_00:50:56:a8:1c:ca</name>
<then>
<accept/>
</then>
</term>
</filter>
<filter>
<name>SDSN_OUTPUT_EX4300-1_VLAN14</name>
<term>
<name>MAC_00:50:56:a8:1c:ca</name>
<from>
<destination-mac-address>
<name>00:50:56:a8:1c:ca</name>
</destination-mac-address>
</from>
<then>
<discard/>
</then>
</term>
<term>
<name>GOOD_HOST_MAC_00:50:56:a8:1c:ca</name>
<then>
<accept/>
</then>
</term>
</filter>
</ethernet-switching>
</family>
</firewall>
</configuration>
```

```
2017-05-29 01:11:03,415 ERROR [net.juniper.jnap.seci.infectedhost.helper.InfectedHostTrackManagementIntfImpl] (Thread-24296 (HornetQ-client-global-threads-2059323893))  T
ime taken by Space method configManager.pushConfigurationAtomically :- 21516
2017-05-29 01:11:03,415 ERROR [net.juniper.jnap.seci.infectedhost.helper.InfectedHostTrackManagementIntfImpl] (Thread-24296 (HornetQ-client-global-threads-2059323893))  F
IRST TIME BLOCKING -> updateInfectedHost SUCCESS in SETTING SDSN VACL Filter on Switch Host :- EX4300-1 vlan :- VLAN14
```

Meaning

The logs confirm that firewall filters have been automatically created and pushed to the access switch to block the end host.

Verify Juniper Connected Security Functionality on the EX Series Switch

Purpose

Verify that the firewall filters have been applied to the switch where the end host is attached.

Action

Run the `show firewall` command on the switch.

```
root@EX4300-1> show firewall

{master:0}
root@EX4300-1> show firewall

Filter: SDSN_INPUT_EX4300-1_VLAN14

Filter: SDSN_OUTPUT_EX4300-1_VLAN14

{master:0}
root@EX4300-1>
```

Meaning

The output confirms that the firewall filters are applied on the access switch to block the end host.

Verify Juniper Connected Security Functionality on the SRX Series Device

Purpose

Display the list of hosts within your network that may have been compromised and require attention.

Action

Use the **show security dynamic-address category-name Infected-Hosts** command on the SRX device.

```
[edit]
root@SRX1500-WF# run show security dynamic-address category-name Infected-Hosts
No.       IP-start        IP-end          Feed             Address
1         192.168.11.11   192.168.11.11   Infected-Hosts/1 ID-2150001a

Total number of matching entries: 1
```

Meaning

The output shows that the ATP Cloud infected host feed containing the end host's IP address has been successfully downloaded, resulting in the SRX device taking action to block Internet access for the infected host.

Verifying the Configuration on the SRX Series Device

Purpose

Verify that the threat prevention policy has been pushed to SRX Series device.

Action

Run the `show security` and `show services` commands, and verify that the following configuration elements exist on the SRX device. These configuration changes can also be seen through Security Director.

Your output may look slightly different as the outputs are dependent on your setup and location.

```
set security policies global policy PolicyEnforcer-Rule1-1 match source-address JSD_192.168.10.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match source-address JSD_192.168.11.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services security-intelligence-policy TPP
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services advanced-anti-malware-policy TPP
```

```
set security address-book global address JSD_192.168.10.1/24 192.168.10.0/24
set security address-book global address JSD_192.168.11.1/24 192.168.11.0/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-address JSD_192.168.10.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-address JSD_192.168.11.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match application any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit application-services security-intelligence-policy TPP
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit application-services advanced-anti-malware-policy TPP
```

```
set services security-intelligence profile TPP_Infected-Hosts category Infected-Hosts
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 5
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then log
set services security-intelligence policy TPP CC TPP_CC
set services security-intelligence policy TPP Infected-Hosts TPP_Infected-Hosts
set services advanced-anti-malware connection url https://srxapi.us-west-2.sky.junipersecurity.net
set services advanced-anti-malware connection authentication tls-profile aamw-ssl
set services advanced-anti-malware policy TPP http inspection-profile default_profile
set services advanced-anti-malware policy TPP http action block
set services advanced-anti-malware policy TPP http notification log
set services advanced-anti-malware policy TPP verdict-threshold 8
set services advanced-anti-malware policy TPP fallback-options action permit
set services advanced-anti-malware policy TPP fallback-options notification log
set services advanced-anti-malware policy TPP default-notification log
set services advanced-anti-malware policy TPP whitelist-notification log
set services advanced-anti-malware policy TPP blacklist-notification log
```

Meaning

The new policies, security intelligence feed points, and advanced malware URL confirm that the threat prevention policy has been pushed to SRX Series device.

Monitoring Juniper Connected Security Functionality on the SRX Series Device

Purpose

Display a summary of session information for the various profiles in use.

Action

Use the **show services security-intelligence statistics** CLI command to view a quick report.

```
user@host> show services security-intelligence statistics
Category Whitelist:
  Profile Whitelist:
    Total processed sessions: 10716
    Permit sessions:          0
Category Blacklist:
  Profile Blacklist:
    Total processed sessions: 10716
    Block drop sessions:      0
Category CC:
  Profile TPP_CC:
    Total processed sessions: 10171
    Permit sessions:          0
    Block drop sessions:      0
    Block close sessions:     0
    Close redirect sessions:  0
Category Infected-Hosts:
  Profile TPP_Infected-Hosts:
    Total processed sessions: 10716
    Permit sessions:          0
    Block drop sessions:      12
    Block close sessions:     0
```

Meaning

The `Category Infected-Hosts` field provides the data on sessions processed (blocked/dropped) through the different profiles such as `Profile TPP_CC` and `Profile TPP_Infected-Hosts`. In this sample output, the `Permit sessions` field confirms that no sessions were allowed when the threat was detected.

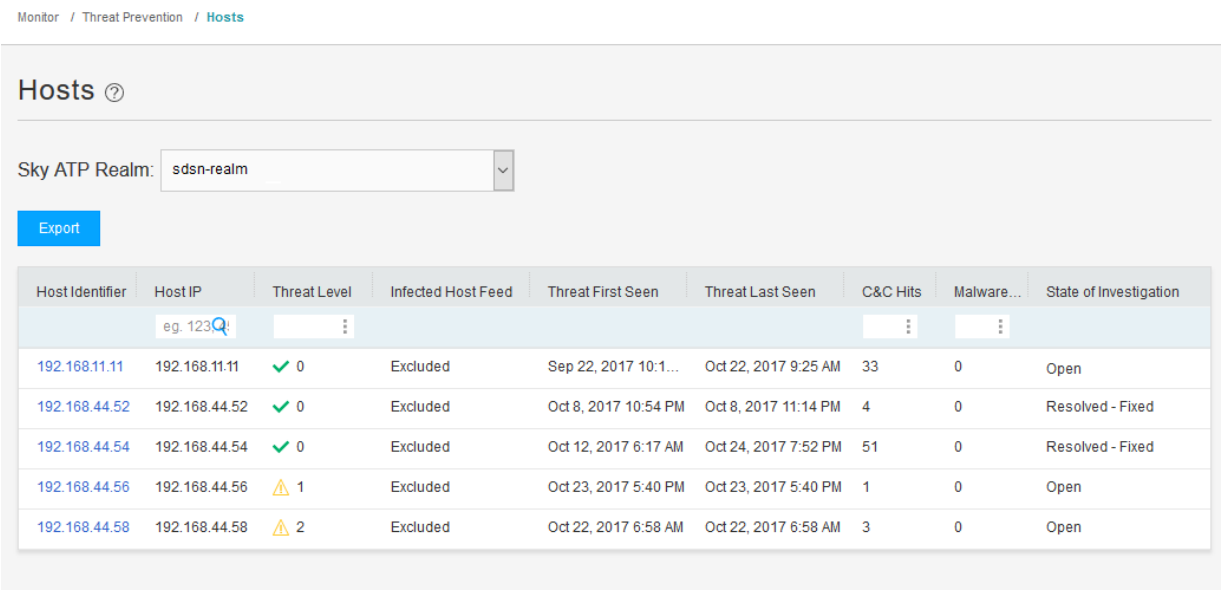
View Compromised Hosts and Other Details

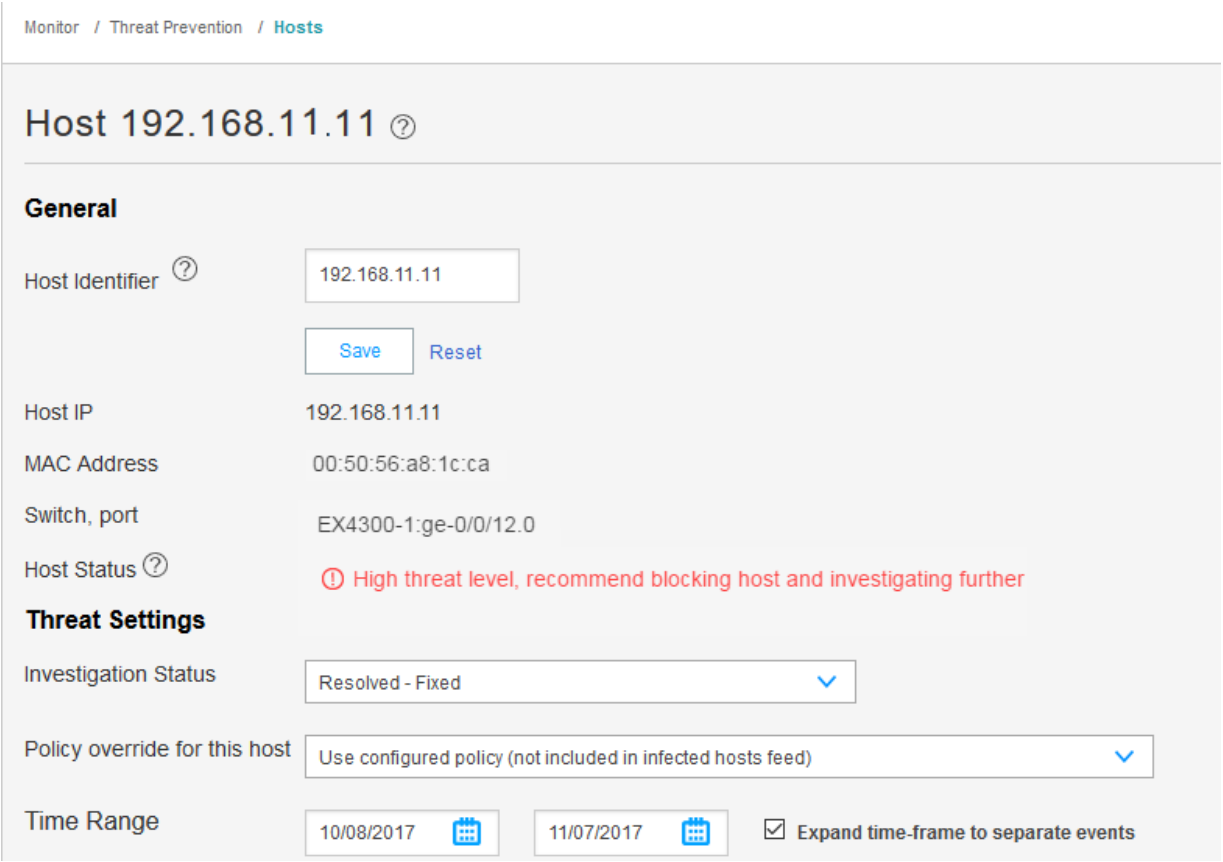
Purpose

View information about current threats to a specific host by time frame.

Action

Navigate to **Monitor > Threat Prevention > Hosts** in Security Director, or **Monitor > Hosts** in theATP portal.





Meaning

The **Hosts** page lists compromised hosts and their associated threat levels. The output confirms that ATP Cloud and Security Director have detected the infected host. From here, you can monitor and mitigate malware detections on a per host basis.

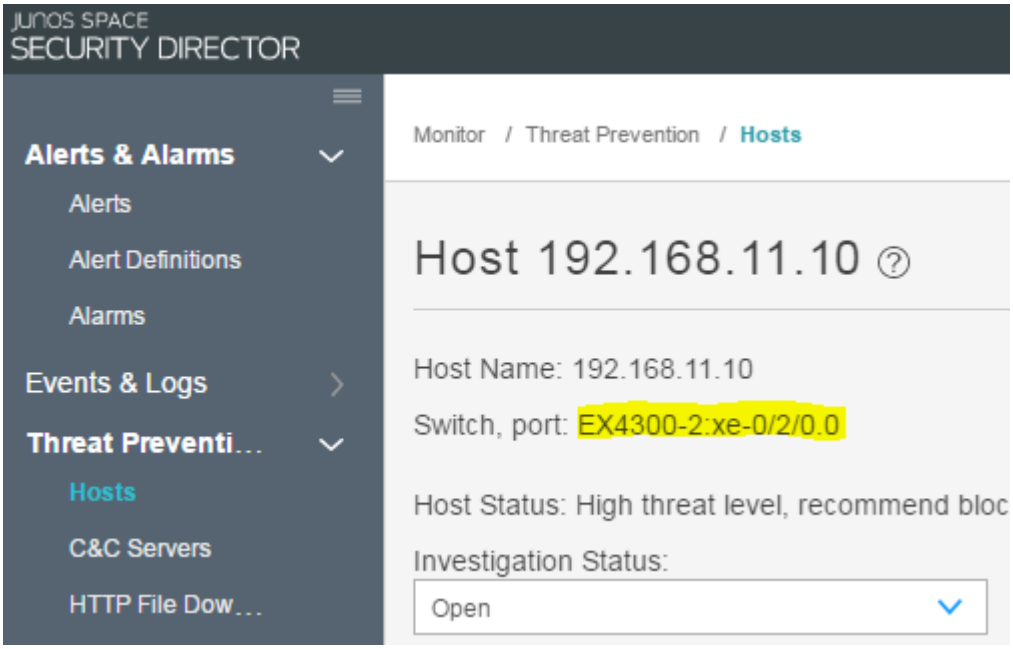
Verifying Host Tracking

Purpose

When the infected host (192.168.11.11) physically moves to another location (connected to EX4300-2), verify that the Policy Enforcer learns the new IP address of the host, updates its MAC address-to-IP address binding, and continues to quarantine the host.

Action

Navigate to **Monitor > Threat Prevention > Hosts** in Security Director.



Meaning

The screenshots confirm that the infected host has moved to new location, is attached to a different switch (EX4300-2), and has a new IP address. They also confirm that the EX4300-2 switch and ATP Cloud have detected the move, continued to recognize the host as infected, and continued to quarantine it.

NOTE: Switch EX4300-2 was not included in the earlier configuration steps, as this switch is part of the Topology 2 implementation option. Configuration information for this switch can be found at EX4300-2 Access Switch Configuration.

RELATED DOCUMENTATION

Use Case Overview | 2

Technical Overview | 5

Configuration of SRX Series Devices and EX Series Switches | 42

Configuring Juniper Connected Security with ATP Cloud and Policy Enforcer (Without Guided Setup) | 75

Configuration of SRX Series Devices and EX Series Switches

IN THIS SECTION

As discussed in "Use Case # 1: Configuring Juniper Connected Security" on page 11, Juniper Connected Security can be deployed in three ways, as shown in Figure 7 on page 42:

Figure 7: Juniper Connected Security Implementation Options

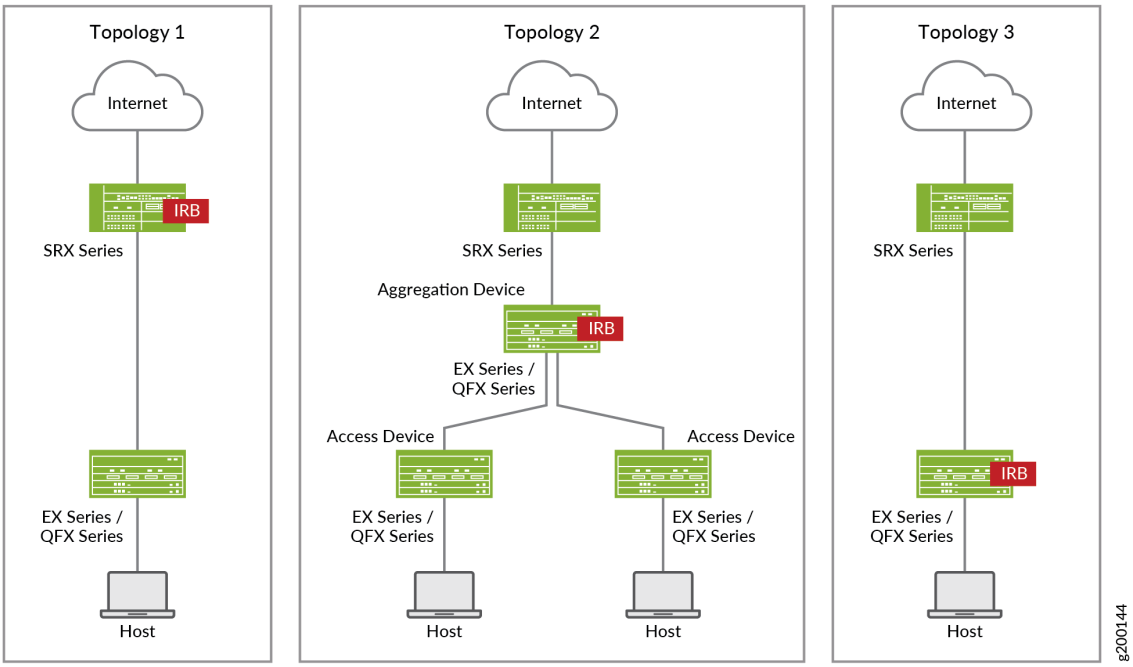


Table 4 on page 43 provides more detail on these deployment options.

Table 4: Supported Topologies for Juniper Connected Security

Topology 1	Topology 2	Topology 3
EX Series or QFX Series device as Layer 2 switch	EX Series or QFX Series device (access switch) as Layer 2 switch EX Series or QFX Series device (aggregation switch) as Layer 3 switch	EX Series or QFX Series device as Layer 2/Layer 3 switch
SRX Series device as firewall in Layer 3 mode	SRX Series device as firewall in Layer 3 mode	SRX Series device as firewall in Layer 3 mode
IRB / VLAN tagging on SRX Series device	IRB / VLAN tagging on EX Series or QFX Series device (aggregation switch)	IRB / VLAN tagging on EX Series or QFX Series switch

Configuration files for each topology are provided below.

NOTE: These configurations are captured from a lab environment, and are provided for reference only. Actual configurations may vary based on the specific requirements of your environment.

Configuration Files for Topology #1

SRX Series Firewall Configuration

```
set version 15.1X49-D80.4
set system host-name SRX1500-WF
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system name-server 8.8.8.8
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services xnm-clear-text
set system services netconf ssh
set system services dhcp-local-server group wan-dhcp interface irb.12
set system syslog user * any emergency
set system syslog host 192.168.10.4 structured-data
```

```
set system syslog file messages any any
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any info
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|GRES"
set system syslog file default-log-messages structured-data
set system max-configurations-on-flash 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set system ntp server 203.0.113.1
set services application-identification
set services ssl initiation profile aamw-ssl trusted-ca aamw-secintel-ca
set services ssl initiation profile aamw-ssl trusted-ca aamw-cloud-ca
set services ssl initiation profile aamw-ssl client-certificate aamw-srx-cert
set services ssl initiation profile aamw-ssl actions crl disable
set services security-intelligence url https://10.13.107.164:443/api/v1/manifest.xml
set services security-intelligence authentication auth-token ABC123
set services security-intelligence profile TPP_CC category CC
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_CC rule Rule-1 then action permit
set services security-intelligence profile TPP_CC rule Rule-1 then log
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 5
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 6
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_CC rule Rule-2 then action permit
set services security-intelligence profile TPP_CC rule Rule-2 then log
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 8
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 9
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 10
set services security-intelligence profile TPP_CC rule Rule-3 then action block drop
set services security-intelligence profile TPP_CC rule Rule-3 then log
set services security-intelligence profile TPP_Infected-Hosts category Infected-Hosts
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 5
```

```
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then log
set services security-intelligence policy TPP CC TPP_CC
set services security-intelligence policy TPP Infected-Hosts TPP_Infected-Hosts
set services advanced-anti-malware connection url https://srxapi.us-
west-2.sky.junipersecurity.net
set services advanced-anti-malware connection authentication tls-profile aamw-ssl
set services advanced-anti-malware policy TPP http inspection-profile default_profile
set services advanced-anti-malware policy TPP http action block
set services advanced-anti-malware policy TPP http notification log
set services advanced-anti-malware policy TPP verdict-threshold 8
set services advanced-anti-malware policy TPP fallback-options action permit
set services advanced-anti-malware policy TPP fallback-options notification log
set services advanced-anti-malware policy TPP default-notification log
set services advanced-anti-malware policy TPP whitelist-notification log
set services advanced-anti-malware policy TPP blacklist-notification log
set security log mode stream
set security log format sd-syslog
set security log source-address 192.168.10.1
set security log stream TRAFFIC category all
set security log stream TRAFFIC host 192.168.10.4
set security log stream TRAFFIC host port 514
set security pki ca-profile All-Trusted-CA-Def_1 ca-identity All-Trusted-CA-Def_1
set security pki ca-profile All-Trusted-CA-Def_2 ca-identity All-Trusted-CA-Def_2
set security pki ca-profile All-Trusted-CA-Def_3 ca-identity All-Trusted-CA-Def_3
set security pki ca-profile All-Trusted-CA-Def_4 ca-identity All-Trusted-CA-Def_4
set security pki ca-profile All-Trusted-CA-Def_5 ca-identity All-Trusted-CA-Def_5
set security pki ca-profile All-Trusted-CA-Def_6 ca-identity All-Trusted-CA-Def_6
set security pki ca-profile All-Trusted-CA-Def_7 ca-identity All-Trusted-CA-Def_7
set security pki ca-profile All-Trusted-CA-Def_8 ca-identity All-Trusted-CA-Def_8
set security pki ca-profile All-Trusted-CA-Def_9 ca-identity All-Trusted-CA-Def_9
set security pki ca-profile All-Trusted-CA-Def_10 ca-identity All-Trusted-CA-Def_10
set security pki ca-profile All-Trusted-CA-Def_11 ca-identity All-Trusted-CA-Def_11
set security pki ca-profile All-Trusted-CA-Def_12 ca-identity All-Trusted-CA-Def_12
set security pki ca-profile All-Trusted-CA-Def_13 ca-identity All-Trusted-CA-Def_13
set security pki ca-profile All-Trusted-CA-Def_14 ca-identity All-Trusted-CA-Def_14
```

```
set security pki ca-profile All-Trusted-CA-Def_15 ca-identity All-Trusted-CA-Def_15
set security pki ca-profile All-Trusted-CA-Def_16 ca-identity All-Trusted-CA-Def_16
set security pki ca-profile All-Trusted-CA-Def_17 ca-identity All-Trusted-CA-Def_17
set security pki ca-profile All-Trusted-CA-Def_18 ca-identity All-Trusted-CA-Def_18
set security pki ca-profile All-Trusted-CA-Def_19 ca-identity All-Trusted-CA-Def_19
set security pki ca-profile All-Trusted-CA-Def_20 ca-identity All-Trusted-CA-Def_20
set security pki ca-profile All-Trusted-CA-Def_21 ca-identity All-Trusted-CA-Def_21
set security pki ca-profile All-Trusted-CA-Def_22 ca-identity All-Trusted-CA-Def_22
set security pki ca-profile All-Trusted-CA-Def_23 ca-identity All-Trusted-CA-Def_23
set security pki ca-profile All-Trusted-CA-Def_24 ca-identity All-Trusted-CA-Def_24
set security pki ca-profile All-Trusted-CA-Def_25 ca-identity All-Trusted-CA-Def_25
set security pki ca-profile All-Trusted-CA-Def_26 ca-identity All-Trusted-CA-Def_26
set security pki ca-profile All-Trusted-CA-Def_27 ca-identity All-Trusted-CA-Def_27
set security pki ca-profile All-Trusted-CA-Def_28 ca-identity All-Trusted-CA-Def_28
set security pki ca-profile All-Trusted-CA-Def_29 ca-identity All-Trusted-CA-Def_29
set security pki ca-profile All-Trusted-CA-Def_30 ca-identity All-Trusted-CA-Def_30
set security pki ca-profile All-Trusted-CA-Def_31 ca-identity All-Trusted-CA-Def_31
set security pki ca-profile All-Trusted-CA-Def_32 ca-identity All-Trusted-CA-Def_32
set security pki ca-profile All-Trusted-CA-Def_33 ca-identity All-Trusted-CA-Def_33
set security pki ca-profile All-Trusted-CA-Def_34 ca-identity All-Trusted-CA-Def_34
set security pki ca-profile All-Trusted-CA-Def_35 ca-identity All-Trusted-CA-Def_35
set security pki ca-profile All-Trusted-CA-Def_36 ca-identity All-Trusted-CA-Def_36
set security pki ca-profile All-Trusted-CA-Def_37 ca-identity All-Trusted-CA-Def_37
set security pki ca-profile All-Trusted-CA-Def_38 ca-identity All-Trusted-CA-Def_38
set security pki ca-profile All-Trusted-CA-Def_39 ca-identity All-Trusted-CA-Def_39
set security pki ca-profile All-Trusted-CA-Def_40 ca-identity All-Trusted-CA-Def_40
set security pki ca-profile All-Trusted-CA-Def_41 ca-identity All-Trusted-CA-Def_41
set security pki ca-profile All-Trusted-CA-Def_42 ca-identity All-Trusted-CA-Def_42
set security pki ca-profile All-Trusted-CA-Def_43 ca-identity All-Trusted-CA-Def_43
set security pki ca-profile All-Trusted-CA-Def_44 ca-identity All-Trusted-CA-Def_44
set security pki ca-profile All-Trusted-CA-Def_45 ca-identity All-Trusted-CA-Def_45
set security pki ca-profile All-Trusted-CA-Def_46 ca-identity All-Trusted-CA-Def_46
set security pki ca-profile All-Trusted-CA-Def_47 ca-identity All-Trusted-CA-Def_47
set security pki ca-profile All-Trusted-CA-Def_48 ca-identity All-Trusted-CA-Def_48
set security pki ca-profile All-Trusted-CA-Def_49 ca-identity All-Trusted-CA-Def_49
set security pki ca-profile All-Trusted-CA-Def_50 ca-identity All-Trusted-CA-Def_50
set security pki ca-profile All-Trusted-CA-Def_51 ca-identity All-Trusted-CA-Def_51
set security pki ca-profile All-Trusted-CA-Def_52 ca-identity All-Trusted-CA-Def_52
set security pki ca-profile All-Trusted-CA-Def_53 ca-identity All-Trusted-CA-Def_53
set security pki ca-profile All-Trusted-CA-Def_54 ca-identity All-Trusted-CA-Def_54
set security pki ca-profile All-Trusted-CA-Def_55 ca-identity All-Trusted-CA-Def_55
set security pki ca-profile All-Trusted-CA-Def_56 ca-identity All-Trusted-CA-Def_56
set security pki ca-profile All-Trusted-CA-Def_57 ca-identity All-Trusted-CA-Def_57
```

```
set security pki ca-profile All-Trusted-CA-Def_58 ca-identity All-Trusted-CA-Def_58
set security pki ca-profile All-Trusted-CA-Def_59 ca-identity All-Trusted-CA-Def_59
set security pki ca-profile All-Trusted-CA-Def_60 ca-identity All-Trusted-CA-Def_60
set security pki ca-profile All-Trusted-CA-Def_61 ca-identity All-Trusted-CA-Def_61
set security pki ca-profile All-Trusted-CA-Def_62 ca-identity All-Trusted-CA-Def_62
set security pki ca-profile All-Trusted-CA-Def_63 ca-identity All-Trusted-CA-Def_63
set security pki ca-profile All-Trusted-CA-Def_64 ca-identity All-Trusted-CA-Def_64
set security pki ca-profile All-Trusted-CA-Def_65 ca-identity All-Trusted-CA-Def_65
set security pki ca-profile All-Trusted-CA-Def_66 ca-identity All-Trusted-CA-Def_66
set security pki ca-profile All-Trusted-CA-Def_67 ca-identity All-Trusted-CA-Def_67
set security pki ca-profile All-Trusted-CA-Def_68 ca-identity All-Trusted-CA-Def_68
set security pki ca-profile All-Trusted-CA-Def_69 ca-identity All-Trusted-CA-Def_69
set security pki ca-profile All-Trusted-CA-Def_70 ca-identity All-Trusted-CA-Def_70
set security pki ca-profile All-Trusted-CA-Def_71 ca-identity All-Trusted-CA-Def_71
set security pki ca-profile All-Trusted-CA-Def_72 ca-identity All-Trusted-CA-Def_72
set security pki ca-profile All-Trusted-CA-Def_73 ca-identity All-Trusted-CA-Def_73
set security pki ca-profile All-Trusted-CA-Def_74 ca-identity All-Trusted-CA-Def_74
set security pki ca-profile All-Trusted-CA-Def_75 ca-identity All-Trusted-CA-Def_75
set security pki ca-profile All-Trusted-CA-Def_76 ca-identity All-Trusted-CA-Def_76
set security pki ca-profile All-Trusted-CA-Def_77 ca-identity All-Trusted-CA-Def_77
set security pki ca-profile All-Trusted-CA-Def_78 ca-identity All-Trusted-CA-Def_78
set security pki ca-profile All-Trusted-CA-Def_79 ca-identity All-Trusted-CA-Def_79
set security pki ca-profile All-Trusted-CA-Def_80 ca-identity All-Trusted-CA-Def_80
set security pki ca-profile All-Trusted-CA-Def_81 ca-identity All-Trusted-CA-Def_81
set security pki ca-profile All-Trusted-CA-Def_82 ca-identity All-Trusted-CA-Def_82
set security pki ca-profile All-Trusted-CA-Def_83 ca-identity All-Trusted-CA-Def_83
set security pki ca-profile All-Trusted-CA-Def_84 ca-identity All-Trusted-CA-Def_84
set security pki ca-profile All-Trusted-CA-Def_85 ca-identity All-Trusted-CA-Def_85
set security pki ca-profile All-Trusted-CA-Def_86 ca-identity All-Trusted-CA-Def_86
set security pki ca-profile All-Trusted-CA-Def_87 ca-identity All-Trusted-CA-Def_87
set security pki ca-profile All-Trusted-CA-Def_88 ca-identity All-Trusted-CA-Def_88
set security pki ca-profile All-Trusted-CA-Def_89 ca-identity All-Trusted-CA-Def_89
set security pki ca-profile All-Trusted-CA-Def_90 ca-identity All-Trusted-CA-Def_90
set security pki ca-profile All-Trusted-CA-Def_91 ca-identity All-Trusted-CA-Def_91
set security pki ca-profile All-Trusted-CA-Def_92 ca-identity All-Trusted-CA-Def_92
set security pki ca-profile All-Trusted-CA-Def_93 ca-identity All-Trusted-CA-Def_93
set security pki ca-profile All-Trusted-CA-Def_94 ca-identity All-Trusted-CA-Def_94
set security pki ca-profile All-Trusted-CA-Def_95 ca-identity All-Trusted-CA-Def_95
set security pki ca-profile All-Trusted-CA-Def_96 ca-identity All-Trusted-CA-Def_96
set security pki ca-profile All-Trusted-CA-Def_97 ca-identity All-Trusted-CA-Def_97
set security pki ca-profile All-Trusted-CA-Def_98 ca-identity All-Trusted-CA-Def_98
set security pki ca-profile All-Trusted-CA-Def_99 ca-identity All-Trusted-CA-Def_99
set security pki ca-profile All-Trusted-CA-Def_100 ca-identity All-Trusted-CA-Def_100
```

```
set security pki ca-profile All-Trusted-CA-Def_101 ca-identity All-Trusted-CA-Def_101
set security pki ca-profile All-Trusted-CA-Def_102 ca-identity All-Trusted-CA-Def_102
set security pki ca-profile All-Trusted-CA-Def_103 ca-identity All-Trusted-CA-Def_103
set security pki ca-profile All-Trusted-CA-Def_104 ca-identity All-Trusted-CA-Def_104
set security pki ca-profile All-Trusted-CA-Def_105 ca-identity All-Trusted-CA-Def_105
set security pki ca-profile All-Trusted-CA-Def_106 ca-identity All-Trusted-CA-Def_106
set security pki ca-profile All-Trusted-CA-Def_107 ca-identity All-Trusted-CA-Def_107
set security pki ca-profile All-Trusted-CA-Def_108 ca-identity All-Trusted-CA-Def_108
set security pki ca-profile All-Trusted-CA-Def_109 ca-identity All-Trusted-CA-Def_109
set security pki ca-profile All-Trusted-CA-Def_110 ca-identity All-Trusted-CA-Def_110
set security pki ca-profile All-Trusted-CA-Def_111 ca-identity All-Trusted-CA-Def_111
set security pki ca-profile All-Trusted-CA-Def_112 ca-identity All-Trusted-CA-Def_112
set security pki ca-profile All-Trusted-CA-Def_114 ca-identity All-Trusted-CA-Def_114
set security pki ca-profile All-Trusted-CA-Def_115 ca-identity All-Trusted-CA-Def_115
set security pki ca-profile All-Trusted-CA-Def_116 ca-identity All-Trusted-CA-Def_116
set security pki ca-profile All-Trusted-CA-Def_117 ca-identity All-Trusted-CA-Def_117
set security pki ca-profile All-Trusted-CA-Def_118 ca-identity All-Trusted-CA-Def_118
set security pki ca-profile All-Trusted-CA-Def_119 ca-identity All-Trusted-CA-Def_119
set security pki ca-profile All-Trusted-CA-Def_120 ca-identity All-Trusted-CA-Def_120
set security pki ca-profile All-Trusted-CA-Def_121 ca-identity All-Trusted-CA-Def_121
set security pki ca-profile All-Trusted-CA-Def_122 ca-identity All-Trusted-CA-Def_122
set security pki ca-profile All-Trusted-CA-Def_123 ca-identity All-Trusted-CA-Def_123
set security pki ca-profile All-Trusted-CA-Def_124 ca-identity All-Trusted-CA-Def_124
set security pki ca-profile All-Trusted-CA-Def_125 ca-identity All-Trusted-CA-Def_125
set security pki ca-profile All-Trusted-CA-Def_126 ca-identity All-Trusted-CA-Def_126
set security pki ca-profile All-Trusted-CA-Def_127 ca-identity All-Trusted-CA-Def_127
set security pki ca-profile All-Trusted-CA-Def_128 ca-identity All-Trusted-CA-Def_128
set security pki ca-profile All-Trusted-CA-Def_129 ca-identity All-Trusted-CA-Def_129
set security pki ca-profile All-Trusted-CA-Def_130 ca-identity All-Trusted-CA-Def_130
set security pki ca-profile All-Trusted-CA-Def_131 ca-identity All-Trusted-CA-Def_131
set security pki ca-profile All-Trusted-CA-Def_132 ca-identity All-Trusted-CA-Def_132
set security pki ca-profile All-Trusted-CA-Def_133 ca-identity All-Trusted-CA-Def_133
set security pki ca-profile All-Trusted-CA-Def_134 ca-identity All-Trusted-CA-Def_134
set security pki ca-profile All-Trusted-CA-Def_135 ca-identity All-Trusted-CA-Def_135
set security pki ca-profile All-Trusted-CA-Def_136 ca-identity All-Trusted-CA-Def_136
set security pki ca-profile All-Trusted-CA-Def_137 ca-identity All-Trusted-CA-Def_137
set security pki ca-profile All-Trusted-CA-Def_138 ca-identity All-Trusted-CA-Def_138
set security pki ca-profile All-Trusted-CA-Def_139 ca-identity All-Trusted-CA-Def_139
set security pki ca-profile All-Trusted-CA-Def_140 ca-identity All-Trusted-CA-Def_140
set security pki ca-profile All-Trusted-CA-Def_141 ca-identity All-Trusted-CA-Def_141
set security pki ca-profile All-Trusted-CA-Def_142 ca-identity All-Trusted-CA-Def_142
set security pki ca-profile All-Trusted-CA-Def_143 ca-identity All-Trusted-CA-Def_143
set security pki ca-profile All-Trusted-CA-Def_144 ca-identity All-Trusted-CA-Def_144
```

```
set security pki ca-profile All-Trusted-CA-Def_145 ca-identity All-Trusted-CA-Def_145
set security pki ca-profile All-Trusted-CA-Def_146 ca-identity All-Trusted-CA-Def_146
set security pki ca-profile All-Trusted-CA-Def_147 ca-identity All-Trusted-CA-Def_147
set security pki ca-profile All-Trusted-CA-Def_148 ca-identity All-Trusted-CA-Def_148
set security pki ca-profile All-Trusted-CA-Def_149 ca-identity All-Trusted-CA-Def_149
set security pki ca-profile All-Trusted-CA-Def_150 ca-identity All-Trusted-CA-Def_150
set security pki ca-profile All-Trusted-CA-Def_151 ca-identity All-Trusted-CA-Def_151
set security pki ca-profile All-Trusted-CA-Def_152 ca-identity All-Trusted-CA-Def_152
set security pki ca-profile All-Trusted-CA-Def_153 ca-identity All-Trusted-CA-Def_153
set security pki ca-profile All-Trusted-CA-Def_154 ca-identity All-Trusted-CA-Def_154
set security pki ca-profile All-Trusted-CA-Def_155 ca-identity All-Trusted-CA-Def_155
set security pki ca-profile ssl-inspect-ca ca-identity ssl-inspect-ca
set security pki ca-profile ssl-ca ca-identity ssl-ca
set security pki ca-profile aamw-ca ca-identity deviceCA
set security pki ca-profile aamw-ca enrollment url http://ca.junipersecurity.net:8080/ejbca/
publicweb/apply/scep/SRX/pkiclient.exe
set security pki ca-profile aamw-ca revocation-check disable
set security pki ca-profile aamw-ca revocation-check crl url http://va.junipersecurity.net/ca/
deviceCA.crl
set security pki ca-profile aamw-secintel-ca ca-identity JUNIPER
set security pki ca-profile aamw-secintel-ca revocation-check crl url http://
va.junipersecurity.net/ca/current.crl
set security pki ca-profile aamw-cloud-ca ca-identity JUNIPER_CLOUD
set security pki ca-profile aamw-cloud-ca revocation-check crl url http://
va.junipersecurity.net/ca/cloudCA.crl
set security pki ca-profile-group All-Trusted-CA-Def cert-base-count 155
set security address-book global address JSD_192.168.10.1/24 192.168.10.0/24
set security address-book global address JSD_192.168.11.1/24 192.168.11.0/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.10.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.11.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match
destination-address any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match
application any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit
application-services security-intelligence-policy TPP
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit
application-services advanced-anti-malware-policy TPP
set security policies from-zone trust to-zone untrust policy t-u match source-address any
set security policies from-zone trust to-zone untrust policy t-u match destination-address any
set security policies from-zone trust to-zone untrust policy t-u match application any
```

```
set security policies from-zone trust to-zone untrust policy t-u then permit
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
JSD_192.168.10.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
JSD_192.168.11.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services
security-intelligence-policy TPP
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services
advanced-anti-malware-policy TPP
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces irb.12
set security zones security-zone trust interfaces irb.14
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces irb.13
set interfaces ge-0/0/0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members VLAN12
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN14
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members VLAN13
set interfaces fxp0 unit 0 family inet address 10.13.107.186/23
set interfaces irb unit 12 family inet address 192.168.10.1/24
set interfaces irb unit 13 family inet address 192.168.231.1/24
set interfaces irb unit 14 family inet address 192.168.11.1/24
set snmp trap-group space targets 10.13.107.162
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 0.0.0.0/0 next-hop 192.168.231.10
set routing-options static route 172.29.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.30.76.0/23 next-hop 10.13.106.1
set routing-options static route 10.163.69.44/30 next-hop 10.13.106.1
set protocols l2-learning global-mode switching
set access address-assignment pool wan-1 family inet network 192.168.10.1/24
set access address-assignment pool wan-1 family inet range wan-1-range low 192.168.10.10
set access address-assignment pool wan-1 family inet range wan-1-range high 192.168.10.20
set access address-assignment pool wan-1 family inet dhcp-attributes maximum-lease-time 86400
set access address-assignment pool wan-1 family inet dhcp-attributes name-server 8.8.8.8
set access address-assignment pool wan-1 family inet dhcp-attributes router 192.168.10.1
set vlans VLAN12 vlan-id 12
```

```
set vlans VLAN12 l3-interface irb.12
set vlans VLAN13 vlan-id 13
set vlans VLAN13 l3-interface irb.13
set vlans VLAN14 vlan-id 14
set vlans VLAN14 l3-interface irb.14
```

EX4300 Access Switch Configuration

```
set version 15.1R5.5
set system host-name EX4300-1
set system auto-snapshot
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services netconf ssh
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any any
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|CFMD_CCM_DEFECT| LFMD_3AH | RPD_MPLS_PATH_BFD|
(Master Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master Detected, Members
Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup
changed)|(interface vcp-)"
set system syslog file default-log-messages structured-data
set system ntp server 203.0.113.1
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN99
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN14
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members VLAN14
set interfaces me0 unit 0 family inet address 10.13.107.181/23
set snmp trap-group space targets 10.13.107.162
set routing-options static route 0.0.0.0/0 next-hop 10.13.106.1
set protocols l2-learning global-mac-table-aging-time 120
```

```
set protocols lldp interface all
set protocols lldp-med interface all
set protocols igmp-snooping vlan default
set vlans VLAN14 vlan-id 14
set vlans VLAN99 vlan-id 99
```

EX2200 Switch Configuration

NOTE: In this topology, the EX2200 switch acts as a simple default gateway to the Internet. It does not play any role in the Juniper Connected Security solution.

```
set version 15.1R5.5
set system host-name EX2200-INTERNET
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh
set system services telnet
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members VLAN13
set interfaces ge-0/0/47 description "to DMZ ge/0/015"
set interfaces ge-0/0/47 unit 0 family inet address 198.51.100.2/30
set interfaces me0 unit 0 family inet address 10.13.107.188/23
set interfaces vlan unit 13 family inet address 192.168.231.10/24
set routing-options static route 0.0.0.0/0 next-hop 198.51.100.1
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 192.168.0.0/16 next-hop 192.168.231.1
set protocols igmp-snooping vlan all
set protocols lldp interface all
set protocols lldp-med interface all
set vlans VLAN13 vlan-id 13
set vlans VLAN13 l3-interface vlan.13
```

Configuration Files for Topology #2

SRX Series Firewall Configuration

```
set version 15.1X49-D80.4
set system host-name SRX1500-1
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system name-server 8.8.8.8
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services xnm-clear-text
set system services netconf ssh
set system syslog user * any emergency
set system syslog host 192.168.10.4 structured-data
set system syslog file messages any any
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any info
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|GRES"
set system syslog file default-log-messages structured-data
set system max-configurations-on-flash 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set system ntp server 203.0.113.1
set services application-identification
set services ssl initiation profile aamw-ssl actions crl disable
set services security-intelligence url https://10.13.107.164:443/api/v1/manifest.xml
set services security-intelligence authentication auth-token ABC123
set services security-intelligence profile TPP_CC category CC
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_CC rule Rule-1 then action permit
set services security-intelligence profile TPP_CC rule Rule-1 then log
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 5
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 6
```

```
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_CC rule Rule-2 then action permit
set services security-intelligence profile TPP_CC rule Rule-2 then log
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 8
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 9
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 10
set services security-intelligence profile TPP_CC rule Rule-3 then action block drop
set services security-intelligence profile TPP_CC rule Rule-3 then log
set services security-intelligence profile TPP_Infected-Hosts category Infected-Hosts
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 5
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then log
set services security-intelligence policy TPP CC TPP_CC
set services security-intelligence policy TPP Infected-Hosts TPP_Infected-Hosts
set services advanced-anti-malware connection url https://srxapi.us-
west-2.sky.junipersecurity.net
set services advanced-anti-malware connection authentication tls-profile aamw-ssl
set services advanced-anti-malware policy TPP http inspection-profile default_profile
set services advanced-anti-malware policy TPP http action block
set services advanced-anti-malware policy TPP http notification log
set services advanced-anti-malware policy TPP verdict-threshold 8
set services advanced-anti-malware policy TPP fallback-options action permit
set services advanced-anti-malware policy TPP fallback-options notification log
set services advanced-anti-malware policy TPP default-notification log
set services advanced-anti-malware policy TPP whitelist-notification log
set services advanced-anti-malware policy TPP blacklist-notification log
set security log mode stream
set security log format sd-syslog
set security log source-address 192.168.1.254
set security log stream TRAFFIC category all
set security log stream TRAFFIC host 192.168.10.4
set security log stream TRAFFIC host port 514
```

```
set security pki ca-profile All-Trusted-CA-Def_1 ca-identity All-Trusted-CA-Def_1
set security pki ca-profile All-Trusted-CA-Def_2 ca-identity All-Trusted-CA-Def_2
set security pki ca-profile All-Trusted-CA-Def_3 ca-identity All-Trusted-CA-Def_3
set security pki ca-profile All-Trusted-CA-Def_4 ca-identity All-Trusted-CA-Def_4
set security pki ca-profile All-Trusted-CA-Def_5 ca-identity All-Trusted-CA-Def_5
set security pki ca-profile All-Trusted-CA-Def_6 ca-identity All-Trusted-CA-Def_6
set security pki ca-profile All-Trusted-CA-Def_7 ca-identity All-Trusted-CA-Def_7
set security pki ca-profile All-Trusted-CA-Def_8 ca-identity All-Trusted-CA-Def_8
set security pki ca-profile All-Trusted-CA-Def_9 ca-identity All-Trusted-CA-Def_9
set security pki ca-profile All-Trusted-CA-Def_10 ca-identity All-Trusted-CA-Def_10
set security pki ca-profile All-Trusted-CA-Def_11 ca-identity All-Trusted-CA-Def_11
set security pki ca-profile All-Trusted-CA-Def_12 ca-identity All-Trusted-CA-Def_12
set security pki ca-profile All-Trusted-CA-Def_13 ca-identity All-Trusted-CA-Def_13
set security pki ca-profile All-Trusted-CA-Def_14 ca-identity All-Trusted-CA-Def_14
set security pki ca-profile All-Trusted-CA-Def_15 ca-identity All-Trusted-CA-Def_15
set security pki ca-profile All-Trusted-CA-Def_16 ca-identity All-Trusted-CA-Def_16
set security pki ca-profile All-Trusted-CA-Def_17 ca-identity All-Trusted-CA-Def_17
set security pki ca-profile All-Trusted-CA-Def_18 ca-identity All-Trusted-CA-Def_18
set security pki ca-profile All-Trusted-CA-Def_19 ca-identity All-Trusted-CA-Def_19
set security pki ca-profile All-Trusted-CA-Def_20 ca-identity All-Trusted-CA-Def_20
set security pki ca-profile All-Trusted-CA-Def_21 ca-identity All-Trusted-CA-Def_21
set security pki ca-profile All-Trusted-CA-Def_22 ca-identity All-Trusted-CA-Def_22
set security pki ca-profile All-Trusted-CA-Def_23 ca-identity All-Trusted-CA-Def_23
set security pki ca-profile All-Trusted-CA-Def_24 ca-identity All-Trusted-CA-Def_24
set security pki ca-profile All-Trusted-CA-Def_25 ca-identity All-Trusted-CA-Def_25
set security pki ca-profile All-Trusted-CA-Def_26 ca-identity All-Trusted-CA-Def_26
set security pki ca-profile All-Trusted-CA-Def_27 ca-identity All-Trusted-CA-Def_27
set security pki ca-profile All-Trusted-CA-Def_28 ca-identity All-Trusted-CA-Def_28
set security pki ca-profile All-Trusted-CA-Def_29 ca-identity All-Trusted-CA-Def_29
set security pki ca-profile All-Trusted-CA-Def_30 ca-identity All-Trusted-CA-Def_30
set security pki ca-profile All-Trusted-CA-Def_31 ca-identity All-Trusted-CA-Def_31
set security pki ca-profile All-Trusted-CA-Def_32 ca-identity All-Trusted-CA-Def_32
set security pki ca-profile All-Trusted-CA-Def_33 ca-identity All-Trusted-CA-Def_33
set security pki ca-profile All-Trusted-CA-Def_34 ca-identity All-Trusted-CA-Def_34
set security pki ca-profile All-Trusted-CA-Def_35 ca-identity All-Trusted-CA-Def_35
set security pki ca-profile All-Trusted-CA-Def_36 ca-identity All-Trusted-CA-Def_36
set security pki ca-profile All-Trusted-CA-Def_37 ca-identity All-Trusted-CA-Def_37
set security pki ca-profile All-Trusted-CA-Def_38 ca-identity All-Trusted-CA-Def_38
set security pki ca-profile All-Trusted-CA-Def_39 ca-identity All-Trusted-CA-Def_39
set security pki ca-profile All-Trusted-CA-Def_40 ca-identity All-Trusted-CA-Def_40
set security pki ca-profile All-Trusted-CA-Def_41 ca-identity All-Trusted-CA-Def_41
set security pki ca-profile All-Trusted-CA-Def_42 ca-identity All-Trusted-CA-Def_42
set security pki ca-profile All-Trusted-CA-Def_43 ca-identity All-Trusted-CA-Def_43
```

```
set security pki ca-profile All-Trusted-CA-Def_44 ca-identity All-Trusted-CA-Def_44
set security pki ca-profile All-Trusted-CA-Def_45 ca-identity All-Trusted-CA-Def_45
set security pki ca-profile All-Trusted-CA-Def_46 ca-identity All-Trusted-CA-Def_46
set security pki ca-profile All-Trusted-CA-Def_47 ca-identity All-Trusted-CA-Def_47
set security pki ca-profile All-Trusted-CA-Def_48 ca-identity All-Trusted-CA-Def_48
set security pki ca-profile All-Trusted-CA-Def_49 ca-identity All-Trusted-CA-Def_49
set security pki ca-profile All-Trusted-CA-Def_50 ca-identity All-Trusted-CA-Def_50
set security pki ca-profile All-Trusted-CA-Def_51 ca-identity All-Trusted-CA-Def_51
set security pki ca-profile All-Trusted-CA-Def_52 ca-identity All-Trusted-CA-Def_52
set security pki ca-profile All-Trusted-CA-Def_53 ca-identity All-Trusted-CA-Def_53
set security pki ca-profile All-Trusted-CA-Def_54 ca-identity All-Trusted-CA-Def_54
set security pki ca-profile All-Trusted-CA-Def_55 ca-identity All-Trusted-CA-Def_55
set security pki ca-profile All-Trusted-CA-Def_56 ca-identity All-Trusted-CA-Def_56
set security pki ca-profile All-Trusted-CA-Def_57 ca-identity All-Trusted-CA-Def_57
set security pki ca-profile All-Trusted-CA-Def_58 ca-identity All-Trusted-CA-Def_58
set security pki ca-profile All-Trusted-CA-Def_59 ca-identity All-Trusted-CA-Def_59
set security pki ca-profile All-Trusted-CA-Def_60 ca-identity All-Trusted-CA-Def_60
set security pki ca-profile All-Trusted-CA-Def_61 ca-identity All-Trusted-CA-Def_61
set security pki ca-profile All-Trusted-CA-Def_62 ca-identity All-Trusted-CA-Def_62
set security pki ca-profile All-Trusted-CA-Def_63 ca-identity All-Trusted-CA-Def_63
set security pki ca-profile All-Trusted-CA-Def_64 ca-identity All-Trusted-CA-Def_64
set security pki ca-profile All-Trusted-CA-Def_65 ca-identity All-Trusted-CA-Def_65
set security pki ca-profile All-Trusted-CA-Def_66 ca-identity All-Trusted-CA-Def_66
set security pki ca-profile All-Trusted-CA-Def_67 ca-identity All-Trusted-CA-Def_67
set security pki ca-profile All-Trusted-CA-Def_68 ca-identity All-Trusted-CA-Def_68
set security pki ca-profile All-Trusted-CA-Def_69 ca-identity All-Trusted-CA-Def_69
set security pki ca-profile All-Trusted-CA-Def_70 ca-identity All-Trusted-CA-Def_70
set security pki ca-profile All-Trusted-CA-Def_71 ca-identity All-Trusted-CA-Def_71
set security pki ca-profile All-Trusted-CA-Def_72 ca-identity All-Trusted-CA-Def_72
set security pki ca-profile All-Trusted-CA-Def_73 ca-identity All-Trusted-CA-Def_73
set security pki ca-profile All-Trusted-CA-Def_74 ca-identity All-Trusted-CA-Def_74
set security pki ca-profile All-Trusted-CA-Def_75 ca-identity All-Trusted-CA-Def_75
set security pki ca-profile All-Trusted-CA-Def_76 ca-identity All-Trusted-CA-Def_76
set security pki ca-profile All-Trusted-CA-Def_77 ca-identity All-Trusted-CA-Def_77
set security pki ca-profile All-Trusted-CA-Def_78 ca-identity All-Trusted-CA-Def_78
set security pki ca-profile All-Trusted-CA-Def_79 ca-identity All-Trusted-CA-Def_79
set security pki ca-profile All-Trusted-CA-Def_80 ca-identity All-Trusted-CA-Def_80
set security pki ca-profile All-Trusted-CA-Def_81 ca-identity All-Trusted-CA-Def_81
set security pki ca-profile All-Trusted-CA-Def_82 ca-identity All-Trusted-CA-Def_82
set security pki ca-profile All-Trusted-CA-Def_83 ca-identity All-Trusted-CA-Def_83
set security pki ca-profile All-Trusted-CA-Def_84 ca-identity All-Trusted-CA-Def_84
set security pki ca-profile All-Trusted-CA-Def_85 ca-identity All-Trusted-CA-Def_85
set security pki ca-profile All-Trusted-CA-Def_86 ca-identity All-Trusted-CA-Def_86
```

```
set security pki ca-profile All-Trusted-CA-Def_87 ca-identity All-Trusted-CA-Def_87
set security pki ca-profile All-Trusted-CA-Def_88 ca-identity All-Trusted-CA-Def_88
set security pki ca-profile All-Trusted-CA-Def_89 ca-identity All-Trusted-CA-Def_89
set security pki ca-profile All-Trusted-CA-Def_90 ca-identity All-Trusted-CA-Def_90
set security pki ca-profile All-Trusted-CA-Def_91 ca-identity All-Trusted-CA-Def_91
set security pki ca-profile All-Trusted-CA-Def_92 ca-identity All-Trusted-CA-Def_92
set security pki ca-profile All-Trusted-CA-Def_93 ca-identity All-Trusted-CA-Def_93
set security pki ca-profile All-Trusted-CA-Def_94 ca-identity All-Trusted-CA-Def_94
set security pki ca-profile All-Trusted-CA-Def_95 ca-identity All-Trusted-CA-Def_95
set security pki ca-profile All-Trusted-CA-Def_96 ca-identity All-Trusted-CA-Def_96
set security pki ca-profile All-Trusted-CA-Def_97 ca-identity All-Trusted-CA-Def_97
set security pki ca-profile All-Trusted-CA-Def_98 ca-identity All-Trusted-CA-Def_98
set security pki ca-profile All-Trusted-CA-Def_99 ca-identity All-Trusted-CA-Def_99
set security pki ca-profile All-Trusted-CA-Def_100 ca-identity All-Trusted-CA-Def_100
set security pki ca-profile All-Trusted-CA-Def_101 ca-identity All-Trusted-CA-Def_101
set security pki ca-profile All-Trusted-CA-Def_102 ca-identity All-Trusted-CA-Def_102
set security pki ca-profile All-Trusted-CA-Def_103 ca-identity All-Trusted-CA-Def_103
set security pki ca-profile All-Trusted-CA-Def_104 ca-identity All-Trusted-CA-Def_104
set security pki ca-profile All-Trusted-CA-Def_105 ca-identity All-Trusted-CA-Def_105
set security pki ca-profile All-Trusted-CA-Def_106 ca-identity All-Trusted-CA-Def_106
set security pki ca-profile All-Trusted-CA-Def_107 ca-identity All-Trusted-CA-Def_107
set security pki ca-profile All-Trusted-CA-Def_108 ca-identity All-Trusted-CA-Def_108
set security pki ca-profile All-Trusted-CA-Def_109 ca-identity All-Trusted-CA-Def_109
set security pki ca-profile All-Trusted-CA-Def_110 ca-identity All-Trusted-CA-Def_110
set security pki ca-profile All-Trusted-CA-Def_111 ca-identity All-Trusted-CA-Def_111
set security pki ca-profile All-Trusted-CA-Def_112 ca-identity All-Trusted-CA-Def_112
set security pki ca-profile All-Trusted-CA-Def_114 ca-identity All-Trusted-CA-Def_114
set security pki ca-profile All-Trusted-CA-Def_115 ca-identity All-Trusted-CA-Def_115
set security pki ca-profile All-Trusted-CA-Def_116 ca-identity All-Trusted-CA-Def_116
set security pki ca-profile All-Trusted-CA-Def_117 ca-identity All-Trusted-CA-Def_117
set security pki ca-profile All-Trusted-CA-Def_118 ca-identity All-Trusted-CA-Def_118
set security pki ca-profile All-Trusted-CA-Def_119 ca-identity All-Trusted-CA-Def_119
set security pki ca-profile All-Trusted-CA-Def_120 ca-identity All-Trusted-CA-Def_120
set security pki ca-profile All-Trusted-CA-Def_121 ca-identity All-Trusted-CA-Def_121
set security pki ca-profile All-Trusted-CA-Def_122 ca-identity All-Trusted-CA-Def_122
set security pki ca-profile All-Trusted-CA-Def_123 ca-identity All-Trusted-CA-Def_123
set security pki ca-profile All-Trusted-CA-Def_124 ca-identity All-Trusted-CA-Def_124
set security pki ca-profile All-Trusted-CA-Def_125 ca-identity All-Trusted-CA-Def_125
set security pki ca-profile All-Trusted-CA-Def_126 ca-identity All-Trusted-CA-Def_126
set security pki ca-profile All-Trusted-CA-Def_127 ca-identity All-Trusted-CA-Def_127
set security pki ca-profile All-Trusted-CA-Def_128 ca-identity All-Trusted-CA-Def_128
set security pki ca-profile All-Trusted-CA-Def_129 ca-identity All-Trusted-CA-Def_129
set security pki ca-profile All-Trusted-CA-Def_130 ca-identity All-Trusted-CA-Def_130
```

```
set security pki ca-profile All-Trusted-CA-Def_131 ca-identity All-Trusted-CA-Def_131
set security pki ca-profile All-Trusted-CA-Def_132 ca-identity All-Trusted-CA-Def_132
set security pki ca-profile All-Trusted-CA-Def_133 ca-identity All-Trusted-CA-Def_133
set security pki ca-profile All-Trusted-CA-Def_134 ca-identity All-Trusted-CA-Def_134
set security pki ca-profile All-Trusted-CA-Def_135 ca-identity All-Trusted-CA-Def_135
set security pki ca-profile All-Trusted-CA-Def_136 ca-identity All-Trusted-CA-Def_136
set security pki ca-profile All-Trusted-CA-Def_137 ca-identity All-Trusted-CA-Def_137
set security pki ca-profile All-Trusted-CA-Def_138 ca-identity All-Trusted-CA-Def_138
set security pki ca-profile All-Trusted-CA-Def_139 ca-identity All-Trusted-CA-Def_139
set security pki ca-profile All-Trusted-CA-Def_140 ca-identity All-Trusted-CA-Def_140
set security pki ca-profile All-Trusted-CA-Def_141 ca-identity All-Trusted-CA-Def_141
set security pki ca-profile All-Trusted-CA-Def_142 ca-identity All-Trusted-CA-Def_142
set security pki ca-profile All-Trusted-CA-Def_143 ca-identity All-Trusted-CA-Def_143
set security pki ca-profile All-Trusted-CA-Def_144 ca-identity All-Trusted-CA-Def_144
set security pki ca-profile All-Trusted-CA-Def_145 ca-identity All-Trusted-CA-Def_145
set security pki ca-profile All-Trusted-CA-Def_146 ca-identity All-Trusted-CA-Def_146
set security pki ca-profile All-Trusted-CA-Def_147 ca-identity All-Trusted-CA-Def_147
set security pki ca-profile All-Trusted-CA-Def_148 ca-identity All-Trusted-CA-Def_148
set security pki ca-profile All-Trusted-CA-Def_149 ca-identity All-Trusted-CA-Def_149
set security pki ca-profile All-Trusted-CA-Def_150 ca-identity All-Trusted-CA-Def_150
set security pki ca-profile All-Trusted-CA-Def_151 ca-identity All-Trusted-CA-Def_151
set security pki ca-profile All-Trusted-CA-Def_152 ca-identity All-Trusted-CA-Def_152
set security pki ca-profile All-Trusted-CA-Def_153 ca-identity All-Trusted-CA-Def_153
set security pki ca-profile All-Trusted-CA-Def_154 ca-identity All-Trusted-CA-Def_154
set security pki ca-profile All-Trusted-CA-Def_155 ca-identity All-Trusted-CA-Def_155
set security pki ca-profile ssl-inspect-ca ca-identity ssl-inspect-ca
set security pki ca-profile ssl-ca ca-identity ssl-ca
set security pki ca-profile aamw-ca ca-identity deviceCA
set security pki ca-profile aamw-ca enrollment url http://ca.junipersecurity.net:8080/ejbca/
publicweb/apply/scep/SRX/pkiclient.exe
set security pki ca-profile aamw-ca revocation-check disable
set security pki ca-profile aamw-ca revocation-check crl url http://va.junipersecurity.net/ca/
deviceCA.crl
set security pki ca-profile aamw-secintel-ca ca-identity JUNIPER
set security pki ca-profile aamw-secintel-ca revocation-check crl url http://
va.junipersecurity.net/ca/current.crl
set security pki ca-profile aamw-cloud-ca ca-identity JUNIPER_CLOUD
set security pki ca-profile aamw-cloud-ca revocation-check crl url http://
va.junipersecurity.net/ca/cloudCA.crl
set security pki ca-profile-group All-Trusted-CA-Def cert-base-count 155
set security address-book global address JSD_192.168.10.1/24 192.168.10.0/24
set security address-book global address JSD_192.168.11.1/24 192.168.11.0/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-
```

```
address JSD_192.168.10.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.11.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match
destination-address any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match
application any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit
application-services security-intelligence-policy TPP
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit
application-services advanced-anti-malware-policy TPP
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then log
session-init
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then count
set security policies from-zone trust to-zone untrust policy t-u match source-address any
set security policies from-zone trust to-zone untrust policy t-u match destination-address any
set security policies from-zone trust to-zone untrust policy t-u match application any
set security policies from-zone trust to-zone untrust policy t-u then permit
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.10.1/24
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.11.1/24
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match
destination-address any
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match
application any
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 then permit
application-services security-intelligence-policy TPP
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 then permit
application-services advanced-anti-malware-policy TPP
set security policies from-zone untrust to-zone trust policy u-t match source-address any
set security policies from-zone untrust to-zone trust policy u-t match destination-address any
set security policies from-zone untrust to-zone trust policy u-t match application any
set security policies from-zone untrust to-zone trust policy u-t then permit
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
JSD_192.168.10.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
JSD_192.168.11.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services
security-intelligence-policy TPP
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services
```

```
advanced-anti-malware-policy TPP
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.12
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/2.13
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 unit 12 vlan-id 12
set interfaces ge-0/0/0 unit 12 family inet address 192.168.1.254/24
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 unit 13 vlan-id 13
set interfaces ge-0/0/2 unit 13 family inet address 192.168.231.1/24
set interfaces fxp0 description MGMT
set interfaces fxp0 unit 0 family inet address 10.13.107.186/23
set snmp trap-group space targets 10.13.107.162
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 0.0.0.0/0 next-hop 192.168.231.10
set routing-options static route 192.168.10.0/24 next-hop 192.168.1.1
set routing-options static route 192.168.11.0/24 next-hop 192.168.1.1
set routing-options static route 192.168.99.0/24 next-hop 192.168.1.1
set routing-options static route 172.29.64.0/20 next-hop 10.13.106.1
set routing-options static route 172.29.80.0/20 next-hop 10.13.106.1
```

EX4300-1 Access Switch Configuration

```
set version 15.1R5.5
set system host-name EX4300-1
set system auto-snapshot
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services netconf ssh
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any any
```

```
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|CFMD_CCM_DEFECT| LFMD_3AH | RPD_MPLS_PATH_BFD|
(Master Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master Detected, Members
Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup
changed)|(interface vcp-)"
set system syslog file default-log-messages structured-data
set system ntp server 203.0.113.1
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN11
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN99
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members VLAN11
set interfaces me0 unit 0 family inet address 10.13.107.181/23
set snmp trap-group space targets 10.13.107.162
set routing-options static route 0.0.0.0/0 next-hop 10.13.106.1
set protocols l2-learning global-mac-table-aging-time 120
set protocols lldp interface all
set protocols lldp-med interface all
set protocols igmp-snooping vlan default
set vlans VLAN11 vlan-id 11
set vlans VLAN99 vlan-id 99
```

EX4300-2 Access Switch Configuration

```
set version 15.1R5.5
set system host-name EX4300-2
set system auto-snapshot
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services netconf ssh
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any any
```

```
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|CFMD_CCM_DEFECT| LFMD_3AH | RPD_MPLS_PATH_BFD|
(Master Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master Detected, Members
Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup
changed)|(interface vcp-)"
set system syslog file default-log-messages structured-data
set system ntp server 203.0.113.1
set interfaces ge-0/0/0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members VLAN10
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members VLAN99
set interfaces xe-0/2/0 unit 0 family ethernet-switching interface-mode access
set interfaces xe-0/2/0 unit 0 family ethernet-switching vlan members VLAN10
set interfaces me0 unit 0 family inet address 10.13.107.180/23
set snmp trap-group space targets 10.13.107.162
set routing-options static route 0.0.0.0/0 next-hop 10.13.106.1
set protocols l2-learning global-mac-table-aging-time 120
set protocols lldp interface all
set protocols lldp-med interface all
set protocols igmp-snooping vlan default
set vlans VLAN10 vlan-id 10
set vlans VLAN99 vlan-id 99
```

EX2200 Aggregation Switch Configuration

```
set version 15.1R5.5
set system host-name EX2200-LAN
set system arp aging-timer 2
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh max-sessions-per-connection 32
set system services netconf ssh
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any any
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
```

```
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|cm_device|(Master Unchanged, Members Changed)|
(Master Changed, Members Changed)|(Master Detected, Members Changed)|(vc add)|(vc delete)|
(Master detected)|(Master changed)|(Backup detected)|(Backup changed)|(interface vcp-)"
set system syslog file default-log-messages structured-data
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members VLAN10
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members VLAN99
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN11
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN99
set interfaces ge-0/0/12 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members VLAN12
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members VLAN12
set interfaces me0 unit 0 family inet address 10.13.107.182/23
set interfaces vlan unit 10 family inet address 192.168.10.1/24
set interfaces vlan unit 11 family inet address 192.168.11.1/24
set interfaces vlan unit 12 family inet address 192.168.1.1/24
set interfaces vlan unit 99 family inet address 192.168.99.1/24
set snmp trap-group space targets 10.13.107.162
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 0.0.0.0/0 next-hop 192.168.1.254
set routing-options static route 172.29.64.0/20 next-hop 10.13.106.1
set routing-options static route 172.29.80.0/20 next-hop 10.13.106.1
set protocols igmp-snooping vlan all
set protocols lldp interface all
set protocols lldp-med interface all
set vlans VLAN10 vlan-id 10
set vlans VLAN10 l3-interface vlan.10
set vlans VLAN11 vlan-id 11
set vlans VLAN11 l3-interface vlan.11
set vlans VLAN12 vlan-id 12
set vlans VLAN12 l3-interface vlan.12
set vlans VLAN99 vlan-id 99
set vlans VLAN99 l3-interface vlan.99
```

EX2200 Internet Gateway Switch Configuration

NOTE: In this topology, the EX2200 switch acts as a simple default gateway to the Internet. It does not play any role in the Juniper Connected Security solution.

```
set version 15.1R5.5
set system host-name EX2200-INTERNET
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh
set system services telnet
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set interfaces ge-0/0/12 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members VLAN13
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members VLAN13
set interfaces ge-0/0/47 description "to DMZ ge/0/015"
set interfaces ge-0/0/47 unit 0 family inet address 198.51.100.2/30
set interfaces me0 unit 0 family inet address 10.13.107.188/23
set interfaces vlan unit 13 family inet address 192.168.231.10/24
set routing-options static route 0.0.0.0/0 next-hop 198.51.100.1
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 192.168.0.0/16 next-hop 192.168.231.1
set protocols igmp-snooping vlan all
set protocols lldp interface all
set protocols lldp-med interface all
set vlans VLAN13 vlan-id 13
set vlans VLAN13 l3-interface vlan.13
```

Configuration Files for Topology #3

SRX Series Firewall Configuration

```
set version 15.1X49-D80.4
set system host-name SRX1500-1
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system name-server 8.8.8.8
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services xnm-clear-text
set system services netconf ssh
set system syslog user * any emergency
set system syslog host 192.168.10.4 structured-data
set system syslog file messages any any
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any info
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|GRES"
set system syslog file default-log-messages structured-data
set system max-configurations-on-flash 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set system ntp server 203.0.113.1
set services application-identification
set services ssl initiation profile aamw-ssl trusted-ca aamw-secintel-ca
set services ssl initiation profile aamw-ssl trusted-ca aamw-cloud-ca
set services ssl initiation profile aamw-ssl client-certificate aamw-srx-cert
set services ssl initiation profile aamw-ssl actions crl disable
set services security-intelligence url https://10.13.107.164:443/api/v1/manifest.xml
set services security-intelligence authentication auth-token ABC123
set services security-intelligence profile TPP_CC category CC
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_CC rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_CC rule Rule-1 then action permit
```

```
set services security-intelligence profile TPP_CC rule Rule-1 then log
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 5
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 6
set services security-intelligence profile TPP_CC rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_CC rule Rule-2 then action permit
set services security-intelligence profile TPP_CC rule Rule-2 then log
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 8
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 9
set services security-intelligence profile TPP_CC rule Rule-3 match threat-level 10
set services security-intelligence profile TPP_CC rule Rule-3 then action block drop
set services security-intelligence profile TPP_CC rule Rule-3 then log
set services security-intelligence profile TPP_Infected-Hosts category Infected-Hosts
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 5
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile TPP_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile TPP_Infected-Hosts rule Rule-2 then log
set services security-intelligence policy TPP CC TPP_CC
set services security-intelligence policy TPP Infected-Hosts TPP_Infected-Hosts
set services advanced-anti-malware connection url https://srxapi.us-
west-2.sky.junipersecurity.net
set services advanced-anti-malware connection authentication tls-profile aamw-ssl
set services advanced-anti-malware policy TPP http inspection-profile default_profile
set services advanced-anti-malware policy TPP http action block
set services advanced-anti-malware policy TPP http notification log
set services advanced-anti-malware policy TPP verdict-threshold 8
set services advanced-anti-malware policy TPP fallback-options action permit
set services advanced-anti-malware policy TPP fallback-options notification log
set services advanced-anti-malware policy TPP default-notification log
set services advanced-anti-malware policy TPP whitelist-notification log
set services advanced-anti-malware policy TPP blacklist-notification log
set security log mode stream
set security log format sd-syslog
set security log source-address 192.168.1.254
```

```
set security log stream TRAFFIC category all
set security log stream TRAFFIC host 192.168.10.4
set security log stream TRAFFIC host port 514
set security pki ca-profile All-Trusted-CA-Def_1 ca-identity All-Trusted-CA-Def_1
set security pki ca-profile All-Trusted-CA-Def_2 ca-identity All-Trusted-CA-Def_2
set security pki ca-profile All-Trusted-CA-Def_3 ca-identity All-Trusted-CA-Def_3
set security pki ca-profile All-Trusted-CA-Def_4 ca-identity All-Trusted-CA-Def_4
set security pki ca-profile All-Trusted-CA-Def_5 ca-identity All-Trusted-CA-Def_5
set security pki ca-profile All-Trusted-CA-Def_6 ca-identity All-Trusted-CA-Def_6
set security pki ca-profile All-Trusted-CA-Def_7 ca-identity All-Trusted-CA-Def_7
set security pki ca-profile All-Trusted-CA-Def_8 ca-identity All-Trusted-CA-Def_8
set security pki ca-profile All-Trusted-CA-Def_9 ca-identity All-Trusted-CA-Def_9
set security pki ca-profile All-Trusted-CA-Def_10 ca-identity All-Trusted-CA-Def_10
set security pki ca-profile All-Trusted-CA-Def_11 ca-identity All-Trusted-CA-Def_11
set security pki ca-profile All-Trusted-CA-Def_12 ca-identity All-Trusted-CA-Def_12
set security pki ca-profile All-Trusted-CA-Def_13 ca-identity All-Trusted-CA-Def_13
set security pki ca-profile All-Trusted-CA-Def_14 ca-identity All-Trusted-CA-Def_14
set security pki ca-profile All-Trusted-CA-Def_15 ca-identity All-Trusted-CA-Def_15
set security pki ca-profile All-Trusted-CA-Def_16 ca-identity All-Trusted-CA-Def_16
set security pki ca-profile All-Trusted-CA-Def_17 ca-identity All-Trusted-CA-Def_17
set security pki ca-profile All-Trusted-CA-Def_18 ca-identity All-Trusted-CA-Def_18
set security pki ca-profile All-Trusted-CA-Def_19 ca-identity All-Trusted-CA-Def_19
set security pki ca-profile All-Trusted-CA-Def_20 ca-identity All-Trusted-CA-Def_20
set security pki ca-profile All-Trusted-CA-Def_21 ca-identity All-Trusted-CA-Def_21
set security pki ca-profile All-Trusted-CA-Def_22 ca-identity All-Trusted-CA-Def_22
set security pki ca-profile All-Trusted-CA-Def_23 ca-identity All-Trusted-CA-Def_23
set security pki ca-profile All-Trusted-CA-Def_24 ca-identity All-Trusted-CA-Def_24
set security pki ca-profile All-Trusted-CA-Def_25 ca-identity All-Trusted-CA-Def_25
set security pki ca-profile All-Trusted-CA-Def_26 ca-identity All-Trusted-CA-Def_26
set security pki ca-profile All-Trusted-CA-Def_27 ca-identity All-Trusted-CA-Def_27
set security pki ca-profile All-Trusted-CA-Def_28 ca-identity All-Trusted-CA-Def_28
set security pki ca-profile All-Trusted-CA-Def_29 ca-identity All-Trusted-CA-Def_29
set security pki ca-profile All-Trusted-CA-Def_30 ca-identity All-Trusted-CA-Def_30
set security pki ca-profile All-Trusted-CA-Def_31 ca-identity All-Trusted-CA-Def_31
set security pki ca-profile All-Trusted-CA-Def_32 ca-identity All-Trusted-CA-Def_32
set security pki ca-profile All-Trusted-CA-Def_33 ca-identity All-Trusted-CA-Def_33
set security pki ca-profile All-Trusted-CA-Def_34 ca-identity All-Trusted-CA-Def_34
set security pki ca-profile All-Trusted-CA-Def_35 ca-identity All-Trusted-CA-Def_35
set security pki ca-profile All-Trusted-CA-Def_36 ca-identity All-Trusted-CA-Def_36
set security pki ca-profile All-Trusted-CA-Def_37 ca-identity All-Trusted-CA-Def_37
set security pki ca-profile All-Trusted-CA-Def_38 ca-identity All-Trusted-CA-Def_38
set security pki ca-profile All-Trusted-CA-Def_39 ca-identity All-Trusted-CA-Def_39
set security pki ca-profile All-Trusted-CA-Def_40 ca-identity All-Trusted-CA-Def_40
```

```
set security pki ca-profile All-Trusted-CA-Def_41 ca-identity All-Trusted-CA-Def_41
set security pki ca-profile All-Trusted-CA-Def_42 ca-identity All-Trusted-CA-Def_42
set security pki ca-profile All-Trusted-CA-Def_43 ca-identity All-Trusted-CA-Def_43
set security pki ca-profile All-Trusted-CA-Def_44 ca-identity All-Trusted-CA-Def_44
set security pki ca-profile All-Trusted-CA-Def_45 ca-identity All-Trusted-CA-Def_45
set security pki ca-profile All-Trusted-CA-Def_46 ca-identity All-Trusted-CA-Def_46
set security pki ca-profile All-Trusted-CA-Def_47 ca-identity All-Trusted-CA-Def_47
set security pki ca-profile All-Trusted-CA-Def_48 ca-identity All-Trusted-CA-Def_48
set security pki ca-profile All-Trusted-CA-Def_49 ca-identity All-Trusted-CA-Def_49
set security pki ca-profile All-Trusted-CA-Def_50 ca-identity All-Trusted-CA-Def_50
set security pki ca-profile All-Trusted-CA-Def_51 ca-identity All-Trusted-CA-Def_51
set security pki ca-profile All-Trusted-CA-Def_52 ca-identity All-Trusted-CA-Def_52
set security pki ca-profile All-Trusted-CA-Def_53 ca-identity All-Trusted-CA-Def_53
set security pki ca-profile All-Trusted-CA-Def_54 ca-identity All-Trusted-CA-Def_54
set security pki ca-profile All-Trusted-CA-Def_55 ca-identity All-Trusted-CA-Def_55
set security pki ca-profile All-Trusted-CA-Def_56 ca-identity All-Trusted-CA-Def_56
set security pki ca-profile All-Trusted-CA-Def_57 ca-identity All-Trusted-CA-Def_57
set security pki ca-profile All-Trusted-CA-Def_58 ca-identity All-Trusted-CA-Def_58
set security pki ca-profile All-Trusted-CA-Def_59 ca-identity All-Trusted-CA-Def_59
set security pki ca-profile All-Trusted-CA-Def_60 ca-identity All-Trusted-CA-Def_60
set security pki ca-profile All-Trusted-CA-Def_61 ca-identity All-Trusted-CA-Def_61
set security pki ca-profile All-Trusted-CA-Def_62 ca-identity All-Trusted-CA-Def_62
set security pki ca-profile All-Trusted-CA-Def_63 ca-identity All-Trusted-CA-Def_63
set security pki ca-profile All-Trusted-CA-Def_64 ca-identity All-Trusted-CA-Def_64
set security pki ca-profile All-Trusted-CA-Def_65 ca-identity All-Trusted-CA-Def_65
set security pki ca-profile All-Trusted-CA-Def_66 ca-identity All-Trusted-CA-Def_66
set security pki ca-profile All-Trusted-CA-Def_67 ca-identity All-Trusted-CA-Def_67
set security pki ca-profile All-Trusted-CA-Def_68 ca-identity All-Trusted-CA-Def_68
set security pki ca-profile All-Trusted-CA-Def_69 ca-identity All-Trusted-CA-Def_69
set security pki ca-profile All-Trusted-CA-Def_70 ca-identity All-Trusted-CA-Def_70
set security pki ca-profile All-Trusted-CA-Def_71 ca-identity All-Trusted-CA-Def_71
set security pki ca-profile All-Trusted-CA-Def_72 ca-identity All-Trusted-CA-Def_72
set security pki ca-profile All-Trusted-CA-Def_73 ca-identity All-Trusted-CA-Def_73
set security pki ca-profile All-Trusted-CA-Def_74 ca-identity All-Trusted-CA-Def_74
set security pki ca-profile All-Trusted-CA-Def_75 ca-identity All-Trusted-CA-Def_75
set security pki ca-profile All-Trusted-CA-Def_76 ca-identity All-Trusted-CA-Def_76
set security pki ca-profile All-Trusted-CA-Def_77 ca-identity All-Trusted-CA-Def_77
set security pki ca-profile All-Trusted-CA-Def_78 ca-identity All-Trusted-CA-Def_78
set security pki ca-profile All-Trusted-CA-Def_79 ca-identity All-Trusted-CA-Def_79
set security pki ca-profile All-Trusted-CA-Def_80 ca-identity All-Trusted-CA-Def_80
set security pki ca-profile All-Trusted-CA-Def_81 ca-identity All-Trusted-CA-Def_81
set security pki ca-profile All-Trusted-CA-Def_82 ca-identity All-Trusted-CA-Def_82
set security pki ca-profile All-Trusted-CA-Def_83 ca-identity All-Trusted-CA-Def_83
```

```
set security pki ca-profile All-Trusted-CA-Def_84 ca-identity All-Trusted-CA-Def_84
set security pki ca-profile All-Trusted-CA-Def_85 ca-identity All-Trusted-CA-Def_85
set security pki ca-profile All-Trusted-CA-Def_86 ca-identity All-Trusted-CA-Def_86
set security pki ca-profile All-Trusted-CA-Def_87 ca-identity All-Trusted-CA-Def_87
set security pki ca-profile All-Trusted-CA-Def_88 ca-identity All-Trusted-CA-Def_88
set security pki ca-profile All-Trusted-CA-Def_89 ca-identity All-Trusted-CA-Def_89
set security pki ca-profile All-Trusted-CA-Def_90 ca-identity All-Trusted-CA-Def_90
set security pki ca-profile All-Trusted-CA-Def_91 ca-identity All-Trusted-CA-Def_91
set security pki ca-profile All-Trusted-CA-Def_92 ca-identity All-Trusted-CA-Def_92
set security pki ca-profile All-Trusted-CA-Def_93 ca-identity All-Trusted-CA-Def_93
set security pki ca-profile All-Trusted-CA-Def_94 ca-identity All-Trusted-CA-Def_94
set security pki ca-profile All-Trusted-CA-Def_95 ca-identity All-Trusted-CA-Def_95
set security pki ca-profile All-Trusted-CA-Def_96 ca-identity All-Trusted-CA-Def_96
set security pki ca-profile All-Trusted-CA-Def_97 ca-identity All-Trusted-CA-Def_97
set security pki ca-profile All-Trusted-CA-Def_98 ca-identity All-Trusted-CA-Def_98
set security pki ca-profile All-Trusted-CA-Def_99 ca-identity All-Trusted-CA-Def_99
set security pki ca-profile All-Trusted-CA-Def_100 ca-identity All-Trusted-CA-Def_100
set security pki ca-profile All-Trusted-CA-Def_101 ca-identity All-Trusted-CA-Def_101
set security pki ca-profile All-Trusted-CA-Def_102 ca-identity All-Trusted-CA-Def_102
set security pki ca-profile All-Trusted-CA-Def_103 ca-identity All-Trusted-CA-Def_103
set security pki ca-profile All-Trusted-CA-Def_104 ca-identity All-Trusted-CA-Def_104
set security pki ca-profile All-Trusted-CA-Def_105 ca-identity All-Trusted-CA-Def_105
set security pki ca-profile All-Trusted-CA-Def_106 ca-identity All-Trusted-CA-Def_106
set security pki ca-profile All-Trusted-CA-Def_107 ca-identity All-Trusted-CA-Def_107
set security pki ca-profile All-Trusted-CA-Def_108 ca-identity All-Trusted-CA-Def_108
set security pki ca-profile All-Trusted-CA-Def_109 ca-identity All-Trusted-CA-Def_109
set security pki ca-profile All-Trusted-CA-Def_110 ca-identity All-Trusted-CA-Def_110
set security pki ca-profile All-Trusted-CA-Def_111 ca-identity All-Trusted-CA-Def_111
set security pki ca-profile All-Trusted-CA-Def_112 ca-identity All-Trusted-CA-Def_112
set security pki ca-profile All-Trusted-CA-Def_114 ca-identity All-Trusted-CA-Def_114
set security pki ca-profile All-Trusted-CA-Def_115 ca-identity All-Trusted-CA-Def_115
set security pki ca-profile All-Trusted-CA-Def_116 ca-identity All-Trusted-CA-Def_116
set security pki ca-profile All-Trusted-CA-Def_117 ca-identity All-Trusted-CA-Def_117
set security pki ca-profile All-Trusted-CA-Def_118 ca-identity All-Trusted-CA-Def_118
set security pki ca-profile All-Trusted-CA-Def_119 ca-identity All-Trusted-CA-Def_119
set security pki ca-profile All-Trusted-CA-Def_120 ca-identity All-Trusted-CA-Def_120
set security pki ca-profile All-Trusted-CA-Def_121 ca-identity All-Trusted-CA-Def_121
set security pki ca-profile All-Trusted-CA-Def_122 ca-identity All-Trusted-CA-Def_122
set security pki ca-profile All-Trusted-CA-Def_123 ca-identity All-Trusted-CA-Def_123
set security pki ca-profile All-Trusted-CA-Def_124 ca-identity All-Trusted-CA-Def_124
set security pki ca-profile All-Trusted-CA-Def_125 ca-identity All-Trusted-CA-Def_125
set security pki ca-profile All-Trusted-CA-Def_126 ca-identity All-Trusted-CA-Def_126
set security pki ca-profile All-Trusted-CA-Def_127 ca-identity All-Trusted-CA-Def_127
```

```
set security pki ca-profile All-Trusted-CA-Def_128 ca-identity All-Trusted-CA-Def_128
set security pki ca-profile All-Trusted-CA-Def_129 ca-identity All-Trusted-CA-Def_129
set security pki ca-profile All-Trusted-CA-Def_130 ca-identity All-Trusted-CA-Def_130
set security pki ca-profile All-Trusted-CA-Def_131 ca-identity All-Trusted-CA-Def_131
set security pki ca-profile All-Trusted-CA-Def_132 ca-identity All-Trusted-CA-Def_132
set security pki ca-profile All-Trusted-CA-Def_133 ca-identity All-Trusted-CA-Def_133
set security pki ca-profile All-Trusted-CA-Def_134 ca-identity All-Trusted-CA-Def_134
set security pki ca-profile All-Trusted-CA-Def_135 ca-identity All-Trusted-CA-Def_135
set security pki ca-profile All-Trusted-CA-Def_136 ca-identity All-Trusted-CA-Def_136
set security pki ca-profile All-Trusted-CA-Def_137 ca-identity All-Trusted-CA-Def_137
set security pki ca-profile All-Trusted-CA-Def_138 ca-identity All-Trusted-CA-Def_138
set security pki ca-profile All-Trusted-CA-Def_139 ca-identity All-Trusted-CA-Def_139
set security pki ca-profile All-Trusted-CA-Def_140 ca-identity All-Trusted-CA-Def_140
set security pki ca-profile All-Trusted-CA-Def_141 ca-identity All-Trusted-CA-Def_141
set security pki ca-profile All-Trusted-CA-Def_142 ca-identity All-Trusted-CA-Def_142
set security pki ca-profile All-Trusted-CA-Def_143 ca-identity All-Trusted-CA-Def_143
set security pki ca-profile All-Trusted-CA-Def_144 ca-identity All-Trusted-CA-Def_144
set security pki ca-profile All-Trusted-CA-Def_145 ca-identity All-Trusted-CA-Def_145
set security pki ca-profile All-Trusted-CA-Def_146 ca-identity All-Trusted-CA-Def_146
set security pki ca-profile All-Trusted-CA-Def_147 ca-identity All-Trusted-CA-Def_147
set security pki ca-profile All-Trusted-CA-Def_148 ca-identity All-Trusted-CA-Def_148
set security pki ca-profile All-Trusted-CA-Def_149 ca-identity All-Trusted-CA-Def_149
set security pki ca-profile All-Trusted-CA-Def_150 ca-identity All-Trusted-CA-Def_150
set security pki ca-profile All-Trusted-CA-Def_151 ca-identity All-Trusted-CA-Def_151
set security pki ca-profile All-Trusted-CA-Def_152 ca-identity All-Trusted-CA-Def_152
set security pki ca-profile All-Trusted-CA-Def_153 ca-identity All-Trusted-CA-Def_153
set security pki ca-profile All-Trusted-CA-Def_154 ca-identity All-Trusted-CA-Def_154
set security pki ca-profile All-Trusted-CA-Def_155 ca-identity All-Trusted-CA-Def_155
set security pki ca-profile ssl-inspect-ca ca-identity ssl-inspect-ca
set security pki ca-profile ssl-ca ca-identity ssl-ca
set security pki ca-profile aamw-ca ca-identity deviceCA
set security pki ca-profile aamw-ca enrollment url http://ca.junipersecurity.net:8080/ejbca/
publicweb/apply/scep/SRX/pkiclient.exe
set security pki ca-profile aamw-ca revocation-check disable
set security pki ca-profile aamw-ca revocation-check crl url http://va.junipersecurity.net/ca/
deviceCA.crl
set security pki ca-profile aamw-secintel-ca ca-identity JUNIPER
set security pki ca-profile aamw-secintel-ca revocation-check crl url http://
va.junipersecurity.net/ca/current.crl
set security pki ca-profile aamw-cloud-ca ca-identity JUNIPER_CLOUD
set security pki ca-profile aamw-cloud-ca revocation-check crl url http://
va.junipersecurity.net/ca/cloudCA.crl
set security pki ca-profile-group All-Trusted-CA-Def cert-base-count 155
```

```
set security address-book global address JSD_192.168.10.1/24 192.168.10.0/24
set security address-book global address JSD_192.168.11.1/24 192.168.11.0/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.10.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.11.1/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match
destination-address any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match
application any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit
application-services security-intelligence-policy TPP
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit
application-services advanced-anti-malware-policy TPP
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then log
session-init
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then count
set security policies from-zone trust to-zone untrust policy t-u match source-address any
set security policies from-zone trust to-zone untrust policy t-u match destination-address any
set security policies from-zone trust to-zone untrust policy t-u match application any
set security policies from-zone trust to-zone untrust policy t-u then permit
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.10.1/24
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match source-
address JSD_192.168.11.1/24
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match
destination-address any
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 match
application any
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 then permit
application-services security-intelligence-policy TPP
set security policies from-zone untrust to-zone trust policy PolicyEnforcer-Rule1-1 then permit
application-services advanced-anti-malware-policy TPP
set security policies from-zone untrust to-zone trust policy u-t match source-address any
set security policies from-zone untrust to-zone trust policy u-t match destination-address any
set security policies from-zone untrust to-zone trust policy u-t match application any
set security policies from-zone untrust to-zone trust policy u-t then permit
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
JSD_192.168.10.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
JSD_192.168.11.1/24
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match application any
```

```
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services
security-intelligence-policy TPP
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services
advanced-anti-malware-policy TPP
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.12
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/2.13
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 unit 12 vlan-id 12
set interfaces ge-0/0/0 unit 12 family inet address 192.168.1.254/24
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 unit 13 vlan-id 13
set interfaces ge-0/0/2 unit 13 family inet address 192.168.231.1/24
set interfaces fxp0 description MGMT
set interfaces fxp0 unit 0 family inet address 10.13.107.186/23
set snmp trap-group space targets 10.13.107.162
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 0.0.0.0/0 next-hop 192.168.231.10
set routing-options static route 172.29.64.0/20 next-hop 10.13.106.1
set routing-options static route 172.29.80.0/20 next-hop 10.13.106.1
set routing-options static route 192.168.10.0/24 next-hop 192.168.1.1
set routing-options static route 192.168.11.0/24 next-hop 192.168.1.3
```

EX4300 Access Switch Configuration

```
set version 15.1R5.5
set system host-name EX4300-1
set system auto-snapshot
set system time-zone America/New_York
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh max-sessions-per-connection 32
set system services telnet
set system services netconf ssh
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
```

```
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any any
set system syslog file default-log-messages match "(requested 'commit' operation)|(requested
'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|
ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|
transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU
Online)|(FRU Offline)|(plugged in)|(unplugged)|CFMD_CCM_DEFECT| LFMD_3AH | RPD_MPLS_PATH_BFD|
(Master Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master Detected, Members
Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup
changed)|(interface vcp-)"
set system syslog file default-log-messages structured-data
set system ntp server 203.0.113.1
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN99
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN12
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members VLAN11
set interfaces irb unit 11 family inet address 192.168.11.1/24
set interfaces irb unit 12 family inet address 192.168.1.3/24
set interfaces me0 unit 0 family inet address 10.13.107.181/23
set snmp trap-group space targets 10.13.107.162
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.29.64.0/20 next-hop 10.13.106.1
set routing-options static route 172.29.80.0/20 next-hop 10.13.106.1
set routing-options static route 0.0.0.0/0 next-hop 192.168.1.254
set protocols l2-learning global-mac-table-aging-time 120
set protocols lldp interface all
set protocols lldp-med interface all
set protocols igmp-snooping vlan default
set vlans VLAN11 vlan-id 11
set vlans VLAN11 l3-interface irb.11
set vlans VLAN12 vlan-id 12
set vlans VLAN12 l3-interface irb.12
set vlans VLAN99 vlan-id 99
set vlans VLAN99 l3-interface irb.99
```

EX2200 Internet Gateway Switch Configuration

NOTE: In this topology, the EX2200 switch acts as a simple default gateway to the Internet. It does not play any role in the Juniper Connected Security solution.

```
set version 15.1R5.5
set system host-name EX2200-INTERNET
set system root-authentication encrypted-password "$ABC123"
set system services ftp
set system services ssh
set system services telnet
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set interfaces ge-0/0/12 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members VLAN13
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members VLAN13
set interfaces ge-0/0/47 description "to DMZ ge/0/015"
set interfaces ge-0/0/47 unit 0 family inet address 198.51.100.2/30
set interfaces me0 unit 0 family inet address 10.13.107.188/23
set interfaces vlan unit 13 family inet address 192.168.231.10/24
set routing-options static route 0.0.0.0/0 next-hop 198.51.100.1
set routing-options static route 10.13.0.0/16 next-hop 10.13.106.1
set routing-options static route 172.28.0.0/16 next-hop 10.13.106.1
set routing-options static route 192.168.0.0/16 next-hop 192.168.231.1
set protocols igmp-snooping vlan all
set protocols lldp interface all
set protocols lldp-med interface all
set vlans VLAN13 vlan-id 13
set vlans VLAN13 l3-interface vlan.13
```

RELATED DOCUMENTATION

Use Case # 1: Configuring Juniper Connected Security | 11

Configuring Juniper Connected Security with ATP Cloud and Policy Enforcer (Without Guided Setup) | 75

Configuring Juniper Connected Security with ATP Cloud and Policy Enforcer (Without Guided Setup)

IN THIS SECTION

This section provides details of the tasks required to configure Juniper Connected Security without guided setup.

Requirements

See "Use Case # 1: Configuring Juniper Connected Security" on page 11 for topology, system requirements, and verification steps.

Overview

The following tasks are required to configure Juniper Connected Security:

- Create ATP Cloud realms
- Create secure fabric by adding a site and endpoint devices
- Configure policy enforcement groups
- Create threat prevention policies
- Apply threat prevention policies to policy enforcement groups

Configuring Juniper Connected Security with ATP Cloud and Policy Enforcer (Without Guided Setup)

IN THIS SECTION

Create ATP Cloud Realms

Step-by-Step Procedure

Create one or more ATP Cloud realms and enroll SRX Series devices in the appropriate realm. (Enroll devices by clicking **Add Devices** in the list view once the realm is created.)

To create ATP Cloud realms:

1. In the UI, navigate to **Configure > Threat Prevention >ATP Cloud Realms**.
2. Click the + icon to add a new ATP Cloud realm.
3. Complete the following configuration:
   a. Enter the location by selecting a region of the world from the available choices.
   b. Enter a username. Your username for ATP Cloud is your e-mail address.
   c. Enter a password. It should be a unique string at least 8 characters long, and include uppercase and lowercase letters, at least one number, and at least one special character.
   d. Enter a name for the security realm. The name can contain alphanumeric characters and the dash symbol, and should be a name that is meaningful to your organization.
   e. Click **OK**.

Create Sites and Add Devices

Step-by-Step Procedure

A Secure Fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices) used in policy enforcement groups.

1. In the UI, navigate to **Devices > Secure Fabric**.
2. Click the + icon to create a new site.
3. Enter the following details for the new site:
   a. Site name.
   b. Description (Optional).
4. Click **OK**.
5. Assign or reassign devices to a site.
   a. Click an existing device to edit it or click **Add Enforcement Points**.
   b. On the Add Enforcement Points page, select the check box beside a device in the **Available** list and click the > icon to move it to the **Selected** list.
   c. Click **OK**.

Create a Policy Enforcement Group

Step-by-Step Procedure

Create a policy enforcement group by adding endpoints under one common group name and later applying a threat prevention policy to that group.

To create a policy enforcement group:

1. In the UI, navigate to **Configure > Shared Objects > Policy Enforcement Groups** .
2. Click the + icon to create a new policy enforcement group.
3. Enter the following details:
   a. Name.
   b. Description (Optional).
   c. Select a group type from the available choices: IP address/subnet or location.

d. Select the check box beside the IP address of the endpoint devices in the **Available** list and click the > icon to move them to the **Selected** list. The endpoints in the **Selected** list will be included in the policy enforcement group.

e. If the endpoint you want does not appear in the list, add it as an Additional IP and click the **Add** button.

f. Click **OK**.

Create a Threat Prevention Policy

Step-by-Step Procedure

Add the threat prevention policy, including profiles for one or more threat types: C&C server, infected host, malware.

1. In the UI, navigate to **Configure > Threat Prevention > Policies**.
2. Click the + icon to create a new threat prevention policy.
3. Enter the following details:
   a. Name.
   b. Description.
   c. Select the desired profile(s). Table 5 on page 78 provides details of available profiles and respective actions.

Table 5: Profiles Available for Threat Prevention Policy

Profiles	Selecting Profile	Policy Action
Command and Control Server	Select the check box to include management for this threat type in the policy.	Use the slider to change the action to be taken based on the threat score. Select one of the following actions: • Drop connection silently (This is the default and recommended setting.) • Close connection and do not send a message.

Table 5: Profiles Available for Threat Prevention Policy *(Continued)*

Profiles	Selecting Profile	Policy Action
Infected Host	Include infected host profile in policy.	Select one of the following actions: • Drop connection silently (This is the default and recommended setting.) • Quarantine—In the field provided, enter a VLAN to which quarantined files are sent. (Note that the fallback option is to block and drop the connection silently.)
Malware (HTTP file download and SMTP File attachment)	Include malware profile in policy: • HTTP file download • SMTP File Attachment	Select one of the following actions: • For HTTP file download: Drop connection silently and Close connection and do not send a message. • For SMTP File Attachment: Quarantine, Deliver malicious messages with warning headers added, and Permit.

d. Select a log setting (Policy setting for all profiles).

e. Click **OK**.

4. Click **OK**.

Apply Threat Prevention Policy to Policy Enforcement Groups

Step-by-Step Procedure

Apply your threat prevention policies to policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong.

1. In the UI, navigate to **Configure >Threat Prevention > Policies** and find the appropriate policy.
2. In the Policy Enforcement Groups column, click the **Assign to Groups** link that appears here when there are no policy enforcement groups assigned, or click the group name that appears in this column to edit the existing list of assigned groups. You can also select the check box beside a policy and click the **Assign to Groups** button at the top of the page.

3. On the Assign to Policy Enforcement Groups page, select the check box beside a group in the **Available list** and click the > icon to move it to the **Selected** list. The groups in the **Selected** list will inherit the policy.

4. Click **OK**.

   The system performs a rule analysis, and prepares device configurations that include the threat prevention policies.

5. Once the analysis is complete, instruct the system to push the updated policy to the SRX devices by clicking **Update** button.

6. When the push is complete, the system returns to the **Policies** page.

RELATED DOCUMENTATION

Use Case Overview | 2

Technical Overview | 5

Use Case # 1: Configuring Juniper Connected Security | 11

Configuration of SRX Series Devices and EX Series Switches | 42