Juniper Networks | Engineering Simplicity

Juniper Advanced Threat Prevention Cloud

Juniper ATP Cloud Administrator Guide

Published
2026-02-05

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

Juniper Advanced Threat Prevention Cloud Juniper ATP Cloud Administrator Guide

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

Use this guide to configure, monitor, and manage the Juniper Advanced Threat Prevention (ATP) Cloud features in Junos OS NFX Series and SRX Series Firewalls to secure the network from viruses, malware, or malicious attachments and protect the users from security threats.

1

PART

Set Up

CHAPTER 1

Juniper Advanced Threat Prevention Cloud Overview

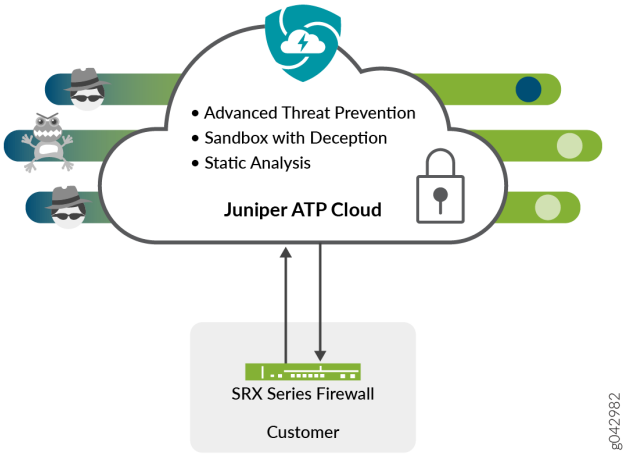
IN THIS CHAPTER

About Juniper ATP Cloud

IN THIS SECTION

Juniper® Advanced Threat Prevention Cloud (Juniper ATP Cloud) is a security framework that protects all hosts in your network against evolving security threats by employing cloud-based threat detection software with a next-generation firewall system. See Figure 1 on page 3.

Figure 1: Juniper ATP Cloud Overview



Juniper ATP Cloud protects your network by performing the following tasks:

- The SRX Series Firewall extracts potentially malicious objects and files and sends them to the cloud for analysis.
- Known malicious files are quickly identified and dropped before they can infect a host.
- Multiple techniques identify new malware, adding it to the known list of malware.
- Correlation between newly identified malware and known Command and Control (C&C) sites aids analysis.
- The SRX Series Firewall blocks known malicious file downloads and outbound C&C traffic.

Juniper ATP Cloud supports the following modes:

- Layer 3 (L3) mode
- Tap mode
- Transparent mode using MAC address

  For more information, see Transparent mode on SRX Series Firewalls.
- Secure wire mode (high-level transparent mode using the interface to directly passing traffic, not by MAC address.) For more information, see Understanding Secure Wire.

Juniper ATP Cloud Features

Juniper ATP Cloud is a cloud-based solution. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your

sensitive data is secured even though it is in a cloud shared environment. Security analysts can update their defense when new attack techniques are discovered and distribute the threat intelligence with very little delay.

In addition, Juniper ATP Cloud offers the following features:

- Integrated with the SRX Series Firewall to simplify deployment and enhance the anti-threat capabilities of the firewall.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats
- AI-Predictive Threat Prevention, an intelligent and fast malware detection and prevention solution, protects your network wherever users connect from. This solution leverages flow-based antivirus and machine learning-based zero-day threat detection to protect users from malware attacks and to prevent spreading of malware in your system. See Configure Flow-Based Antivirus Policy and Configure Machine Learning-Based Threat Detection.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.
- High availability to provide uninterrupted service.
- Scalable to handle increasing loads that require more computing resources, increased network bandwidth to receive more customer submissions, and a large storage for malware.
- Provides deep inspection, actionable reporting, and inline malware blocking
- API for C&C feeds, allowlist and blocklist operations, and file submission. See the Threat Intelligence Open API Setup Guide for more information.
- Domain Name System (DNS), Encrypted Traffic Insights (ETI) and Internet of Things (IoT) security. For licensing information specific to these features, see Software Licenses for ATP Cloud.

Figure 2 on page 5 lists the Juniper ATP Cloud components.

Figure 2: Juniper ATP Cloud Components

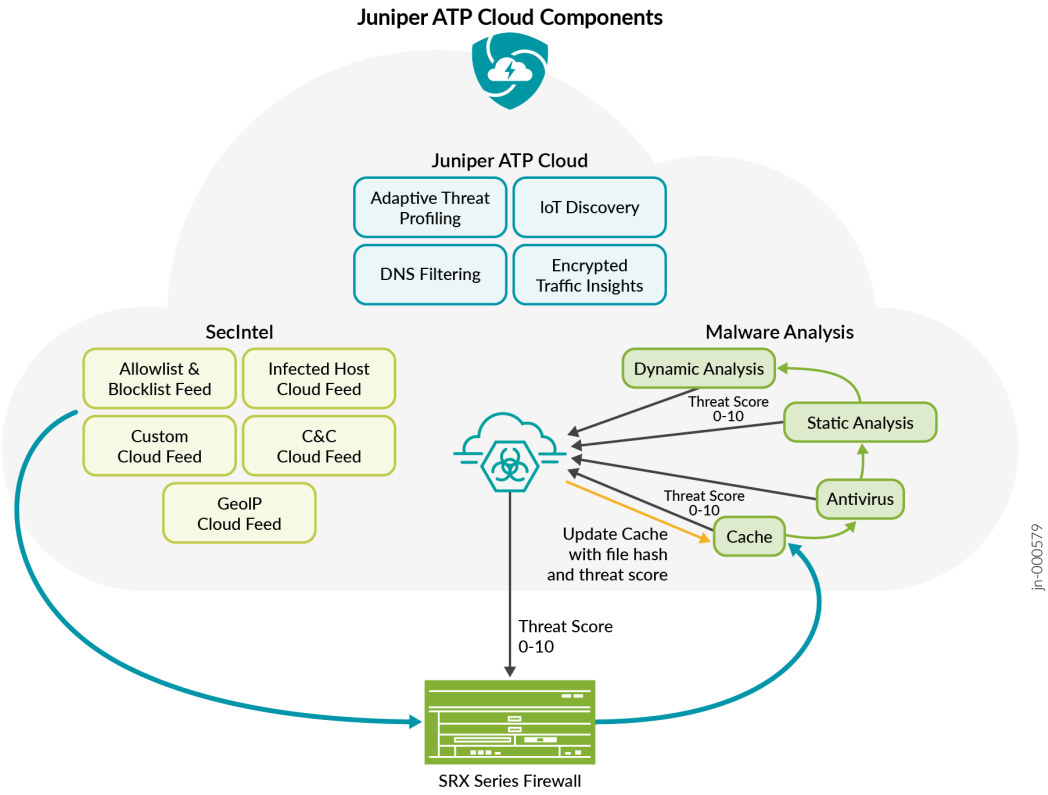


Table 1 on page 5 briefly describes each Juniper ATP Cloud component's operation.

Table 1: Juniper ATP Cloud Components

Component	Operation
C&C cloud feeds	C&C feeds are essentially a list of servers that are known C&C for botnets. The list also includes servers that are known sources for malware downloads.
GeoIP cloud feeds	GeoIP feeds is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.
Infected host cloud feeds	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or other exhibit other symptoms.

Table 1: Juniper ATP Cloud Components *(Continued)*

Component	Operation
Allowlist, blocklists and custom cloud feeds	An allowlist is simply a list of known IP addresses that you trust and a blocklist is a list that you do not trust.
SRX Series Firewall	Submits extracted file content for analysis and detected C&C hits inside the customer network. Performs inline blocking based on file signature database provided by Juniper ATP Cloud.
Malware inspection pipeline	Performs malware analysis and threat detection
Internal compromise detection	Inspects files, metadata, and other information.
Service portal (Web UI)	Graphics interface displaying information about detected threats inside the customer network. Configuration management tool where customers can refine which file categories can be submitted into the cloud for processing.
Encrypted Traffic Insights	Encrypted Traffic Insights restores visibility lost due to encrypted traffic without the heavy burden of full TLS/SSL decryption.
SecIntel	Provides curated SecIntel in the form of threat feeds that include malicious domains, URLs, and IP addresses used in known attack campaigns. SecIntel also enables customers to feed and distribute their own threat intelligence for inline blocking.
Adaptive Threat Profiling	Automatically create SecIntel threat feeds based on who and what is currently attacking the network to combat the continuous onslaught of new threats. Adaptive Threat Profiling leverages Juniper Security Services to classify endpoint behavior and build custom threat intelligence feeds that can be used for further inspection or blocking at multiple enforcement points.

Table 1: Juniper ATP Cloud Components *(Continued)*

Component	Operation
DNS Security	Provides threat prevention from attacks that utilize DGA and DNS tunneling techniques. Protect against DNS exploits for C&C communications, data exfiltration, phishing attacks, and ransomware that commonly exploit DNS using a variety of techniques.
IoT Threat Prevention	ATP Cloud allows customers to control the IoT attack surface on their network by providing an easy way to identify and categorize the IoT devices

How the SRX Series Firewall Remediates Traffic

The SRX Series Firewalls use intelligence provided by Juniper ATP Cloud to remediate malicious content through the use of security policies. If configured, security policies might block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series Firewall look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper ATP Cloud cloud for inspection. The SRX Series Firewall holds the last few KB of the file from the destination client while Juniper ATP Cloud checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper ATP Cloud performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see How is Malware Analyzed and Detected?.

Figure 3 on page 8 shows an example flow of a client requesting a file download with Juniper ATP Cloud.

Figure 3: Inspecting Inbound Files for Malware

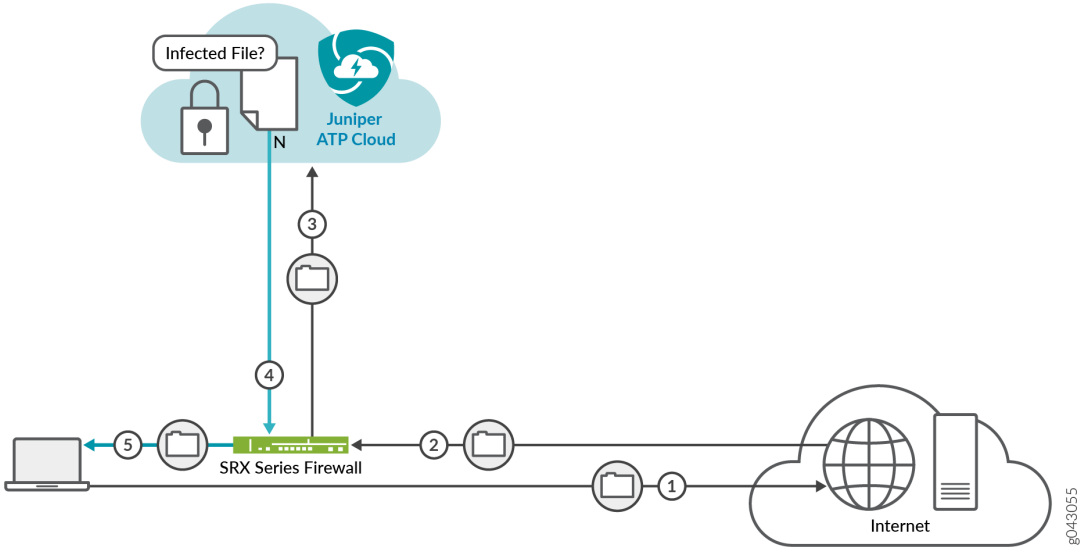


Table 2: Malware Inspection Workflow

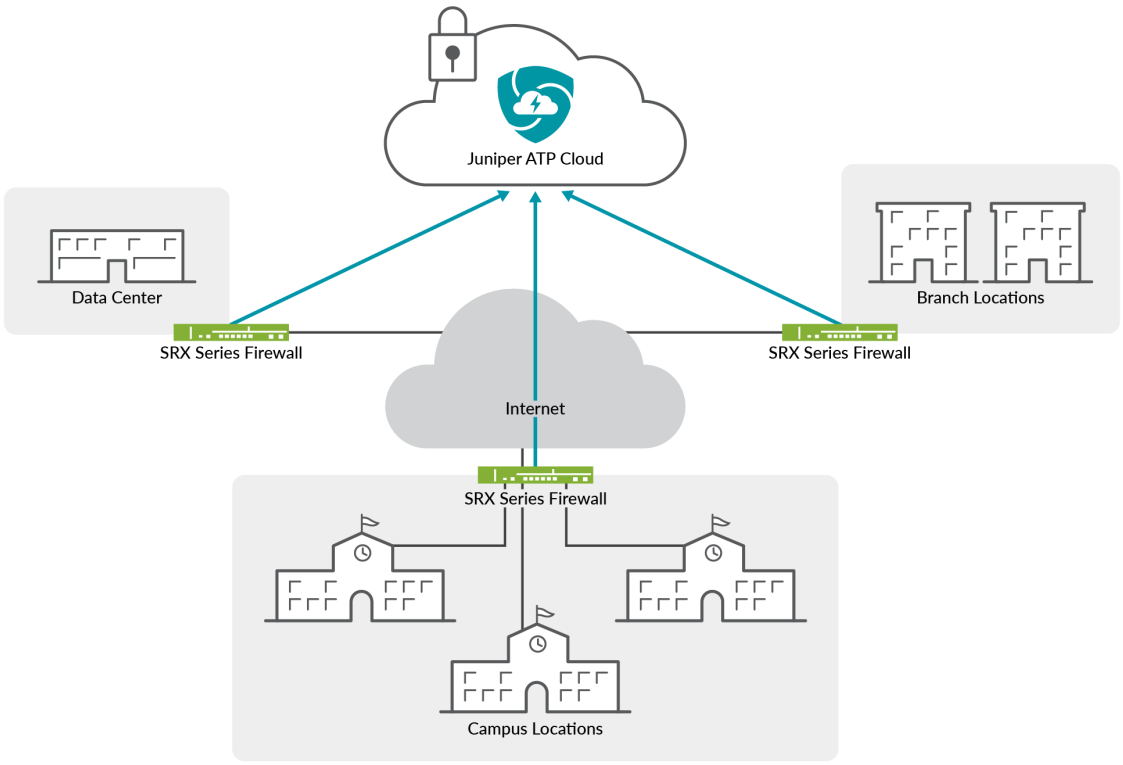
Step	Description
1	A client system behind an SRX Series Firewalls requests a file download from the Internet. The SRX Series Firewall forwards that request to the appropriate server.
2	The SRX Series Firewall receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.
4	Juniper ATP Cloud has inspected this file before and has the analysis stored in cache. In this example, the file is not malware and the threat level verdict is sent back to the SRX Series Firewall.
5	Based on user-defined policies and threat level verdict, the SRX Series Firewall sends the file to the client.

For outbound traffic, the SRX Series Firewall monitors traffic that matches C&C feeds it receives, blocks these C&C requests, and reports them to Juniper ATP Cloud. A list of infected hosts is available so that the SRX Series Firewall can block inbound and outbound traffic.

Juniper ATP Cloud Use Cases

Juniper ATP Cloud can be used anywhere in an SRX Series deployment. See Figure 4 on page 9

Figure 4: Juniper ATP Cloud Use Cases



- Campus edge firewall—Juniper ATP Cloud analyzes files downloaded from the Internet and protects end-user devices.
- Data center edge—Like the campus edge firewall, Juniper ATP Cloud prevents infected files and application malware from running on your computers.
- Branch router—Juniper ATP Cloud provides protection from split-tunneling deployments. A disadvantage of split-tunneling is that users can bypass security set in place by your company's infrastructure.

CHAPTER 2

Enroll SRX Series Firewalls to Juniper Advanced Threat Prevention Cloud

IN THIS CHAPTER

Enroll an SRX Series Firewall Using the CLI

Starting in Junos OS Release 19.3R1, you can use the `request services advanced-anti-malware enroll` command on the SRX Series Firewall to enroll a device to the Juniper ATP Cloud Web Portal. With this command, you do not have to perform any enrollment tasks on the Web Portal. All enrollment is done from the CLI on the SRX Series Firewall.

Before You Begin

- Check whether the device is already enrolled. For more information, see Search for SRX Series Firewalls Within Juniper ATP Cloud.
- If the IPv6 dual-stack (both IPv4 and IPv6) support is enabled on your SRX Series Firewall, run the following CLI commands:

  1. `set services advanced-anti-malware connection protocol-family inet6`—Configure the IPv6 protocol for AAMW connection.
  2. (Optional) `set services advanced-anti-malware connection proxy-profile` *`proxy-profile-name`*—Configure a proxy profile name if you have configured a proxy server and your Internet access goes through it.
  3. (Optional) `set services advanced-anti-malware connection routing-instance` *`routing-instance-name`*—Configure a routing instance name if you plan to route using a specific routing instance.

Enrollment establishes a secure connection between the Juniper ATP Cloud cloud server and the SRX Series Firewall. It also performs basic configuration tasks such as:

- Downloads and installs certificate authorities (CAs) onto your SRX Series Firewall.

NOTE:

- You must allow traffic to the junipersecurity.net domain on ports 8444 and 7444 since the Trusted Platform Module (TPM)-based certificates are used for connections between the SRX Series Firewall and Juniper ATP Cloud. To determine if a feature is supported by a specific platform or Junos OS release, see Feature Explorer. For more information about using TPM on SRX Series Firewalls, see Trusted Platform Module Overview.
- For newly enrolled TPM and non-TPM-based devices, traffic must be allowed to the junipersecurity.net domain only on port 443.

- Creates local certificates and enrolls these certificates with the cloud server.
- Establishes a secure connection to the cloud server.

NOTE: Juniper ATP Cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet. You do not need to open any ports on the SRX Series Firewall to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have port 443 open.

Also note, the SRX Series Firewall must be configured with DNS servers in order to resolve the cloud URL.

Using the device enrollment command `request services advanced-anti-malware enroll` on the SRX Series Firewall, you can enroll the device to an existing realm or create a realm and then enroll to it.

Here is a sample that creates a realm and then enrolls to that realm.

NOTE: You must log in as `root (super user)` to perform the following operations.

```
request services advanced-anti-malware enroll
```

1. Enroll the SRX Series Firewall to Juniper ATP Cloud (CLI only):

```
request services advanced-anti-malware enroll

Please select geographical region from the list:

1. North America

2. European Region

3. Canada
```

```
4. Asia Pacific

Your choice: 1
```

2. Select an existing realm or create a realm:

```
Enroll SRX to:

1. A new SkyATP security realm (you will be required to create it first)

2. An existing SkyATP security realm
```

If you select option 1 to create a realm, the steps are as follows:

- You are going to create a new Sky ATP realm, please provide the required information:
- Please enter a realm name (This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once a realm is created, it cannot be changed):

  Real name: example-company-a
- Please enter your company name:

  Company name: Example Company A
- Please enter your e-mail address. This will be your username for your Sky ATP account:

  Email: me@example-company-a.com
- Please setup a password for your new Sky ATP account (It must be at least 8 characters long and include both uppercase and lowercase letters, at least one number, at least one special character):

  Password: **********

  Verify: **********
- Please review the information you have provided:

  Region: North America

  New Realm: example-company-a

  Company name: Example Company A

  Email: me@example-company-a.com
- Create a new realm with the above information? [yes,no]

  yes

  Device enrolled successfully!

If you select option 2 to use an existing realm, the steps are as follows:

NOTE: You must enter a valid username and password for the existing realm as part of the enrollment procedure.

- Enter the name of the existing realm:

  ```
  Please enter a realm name.

  Realm name: example-company-b
  ```

- ```
  Please enter your company name:

  Company name: Example Company B
  ```

- Enter your email address/username for the realm. This is the email address that was previously created when setting up the realm.

  ```
  Please enter your e-mail address. This will be your username for your Sky ATP account:
  ```

- Enter the password for the realm. This is the password that was previously created when setting up the realm.

  ```
  Password:********
  ```

- ```
  Enroll device to the realm above? [yes,no] yes

  Device enrolled successfully!
  ```

You can use the `show services advanced-anti-malware status` CLI command on your SRX Series Firewall to verify that a connection has been made to the cloud server from the SRX Series Firewall.

Once enrolled, the SRX Series Firewall communicates to the cloud through multiple, persistent connections established over a secure channel (TLS 1.2) and the SRX Series Firewall is authenticated using SSL client certificates.

Use the CLI command `request services advanced-anti-malware disenroll` to disenroll a device from the Juniper ATP Cloud Web Portal.

Cloud Feeds for Juniper ATP Cloud

IN THIS SECTION

The cloud feed URL is set up automatically for you when your SRX Series Firewall is enrolled to the Juniper ATP Cloud. For more information, see "Enroll an SRX Series Firewall Using the CLI" on page 10 and Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal. There are no further steps you need to do to configure the cloud feed URL.

If you want to check the cloud feed URL on your SRX Series Firewall, run the `show services security-intelligence URL` CLI command. Your output should look similar to the following:

```
show services security-intelligence url
https://cloudfeeds.sky.junipersecurity.net/api/manifest.xml
```

If you do not see a URL listed, run the ops script again as it configures other settings in addition to the cloud feed URL.

Once you configure your SRX Series Firewall, the cloud feeds are automatically sent from Juniper ATP Cloud to the device.

Table 3: Cloud Feed Regions

Region	URL	Source
United States	*https://cloudfeeds.sky.junipersecurity.net*	Oregon, USA
European Union	*https://cloudfeeds.sky.junipersecurity.net*	Oregon, USA
APAC	*https://cloudfeeds-tokyo.sky.junipersecurity.net*	Tokyo, Japan
Canada	*https://cloudfeeds-canada.sky.junipersecurity.net*	Montreal, Canada

SRX Series Update Intervals for Cloud Feeds

The following table provides the update intervals for each feed type. Note that when the SRX Series Firewall makes requests for new and updated feed content, if there is no new content, no updates are downloaded at that time.

NOTE: Run the following commands only for troubleshooting purposes:

- The `request services security-intelligence uninstall` command uninstalls the SecIntel service from the device.
- The `request services security-intelligence download` command is used to manually initiate the download of the latest SecIntel updates before the next interval.

Table 4: Feed Update Intervals

Category	Feeds	SRX Series Firewall Update Intervals (in Seconds)
Command and Control (C&C)	Juniper Feeds	1,800
	Integrated Feeds	86,400
	Customer Feeds	60
GeoIP	geoip_country	86,400
Allowlist	Juniper Feeds (whitelist_dns)	1,800
	Juniper Feeds (whitelist_dns_umbrella)	86,400
	Customer Feeds (domain, IP and Domain Name System (DNS))	1,800
	Customer Feeds (reverse shell)	300
Blocklist	Customer Feeds (domain and IP)	1800
Infected Hosts	Infected Hosts	60
Suspicious Hosts	Suspicious Hosts	60
DNS	Juniper Feeds	1800
	Customer Feeds	60

Table 4: Feed Update Intervals *(Continued)*

Category	Feeds	SRX Series Firewall Update Intervals (in Seconds)
Dynamic Address Group (DAG)	Customer Feeds	1,800
	Third party DAG Feeds. For example, Office 365	1,800

CHAPTER 3

Configure Security Zones and Policies on SRX Series Firewall

IN THIS CHAPTER

Juniper ATP Cloud Policy Overview

The connection to the Juniper ATP Cloud cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series Firewall compares this verdict number to the Juniper ATP Cloud policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

Juniper ATP Cloud policies are an extension to the Junos OS security policies. Table 5 on page 18 shows the additions.

NOTE:

- Starting in Junos OS Release 15.1X49-D80, the match-then condition has been deprecated from the Juniper ATP Cloud policy configuration. The examples below are for Junos OS Release 15.1X49-D80 and later.

- Advanced anti-malware (AAMW) file inspection is supported for file download operation from server to client. File upload operation is not supported.

Table 5: Juniper ATP Cloud Security Policy Additions

Addition	Description

Action and notification based on the verdict number and threshold	Defines the threshold value and what to do when the verdict number is greater than or equal to the threshold. For example, if the threshold is 7 (the recommended value) and Juniper ATP Cloud returns a verdict number of 8 for a file, then that file is blocked from being downloaded and a log entry is created.
	
	`set services advanced-anti-malware policy aamwpolicy1 verdict-threshold recommended`
	
	`set services advanced-anti-malware policy aamwpolicy1 http action block notification log`

Default action and notification	Defines what to do when the verdict number is less than the threshold. For example, if the threshold is 7 and Juniper ATP Cloud returns a verdict number of 3 for a file, then that file is downloaded and a log file is created. `set services advanced-anti-malware policy aamwpolicy1 default-notification log`
Name of the inspection profile	Name of the Juniper ATP Cloud profile that defines the types of file to scan. `set services advanced-anti-malware policy aamwpolicy1 http inspection-profile default_profile`

Table 5: Juniper ATP Cloud Security Policy Additions *(Continued)*

Addition	Description

Fallback options	Defines what to do when error conditions occur or when there is a lack of resources. The following fallback options are available:
	• action—Permit or block the file regardless of its threat level.
	• notification—Add or do not add this event to the log file.
	`set services advanced-anti-malware policy aamwpolicy1 fallback-options action permit`
	`set services advanced-anti-malware policy aamwpolicy1 fallback-options notification log`
	NOTE: The above actions assume a valid session is present. If no valid session is present, Juniper ATP Cloud permits the file, regardless of whether you set the fallback option to block.

Blocklist notification	Defines whether to create a log entry when attempting to download a file from a site listed in the blocklist file. `set services advanced-anti-malware policy aamwpolicy1 blacklist-notification log`
Allowlist notification	Defines whether to create a log entry when attempting to download a file from a site listed in the allowlist file. `set services advanced-anti-malware policy aamwpolicy1 whitelist-notification log`
Name of smtp inspection profile	Name of the inspection profile for SMTP email attachments. The “actions to take” are defined in the Web UI and not through CLI commands. `set services advanced-anti-malware policy aamwpolicy1 smtp inspection-profile my_smtp_profile`

Use the `show services advanced-anti-malware policy` CLI command to view your Juniper ATP Cloud policy settings.

```
show services advanced-anti-malware policy aamwpolicy1
Advanced-anti-malware configuration:
Policy Name: aamwpolicy1
```

```
  Default-notification  : No Log
  Whitelist-notification: Log
  Blacklist-notification: Log
  Fallback options:
    Action: permit
    Notification: Log
  Protocol: HTTP
  Verdict-threshold: recommended (7)
    Action: block
    Notification: Log
    Inspection-profile: default_profile
  Protocol: SMTP
  Verdict-threshold: recommended (7)
    Action: User-Defined-in-Cloud (permit)
    Notification: No Log
    Inspection-profile: my_smtp_profile
```

Use the `show security policies` CLI command to view your firewall policy settings.

```
show security policies
from-zone trust to-zone untrust {
    policy 1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy SecIntel;
                }
            }
        }
    }
    policy firewall-policy1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
```

```
            permit {
                application-services {
                    ssl-proxy {
                        profile-name ssl-inspect-profile;
                    }
                    advanced-anti-malware-policy aamwpolicy1;
                }
            }
        }
    }
}
```

Configure Juniper ATP Cloud Policy

IN THIS SECTION

This configuration shows how to create a Juniper ATP Cloud policy using the CLI. It assumes you understand configuring security zones and security policies. See Example: Creating Security Zones.

Requirements

This configuration uses the following hardware and software components:

- An SRX1500 device with traffic through packet forwarding
- Junos OS Release 15.1X49-D80 or later

NOTE: Starting in Junos OS Release 15.1X49-D80, the match-then condition has been deprecated from the Juniper ATP Cloud policy configuration. This configuration includes those updates.

NOTE: Junos OS Release 18.2R1 or later adds explicit web proxy support for anti-malware and security-intelligence policies using the following statements: `set services advanced-anti-malware connection proxy-profile proxy_name` and `set services security-intelligence proxy-profile proxy_name`. First use the set services command to configure the web proxy profile, including the proxy host IP address and port number. See "Explicit Web Proxy for Juniper ATP Cloud" on page 29 for details.

Overview

The following configuration creates a Juniper ATP Cloud policy that has the following properties:

- Policy name is aamwpolicy1.
- Profile name is default_profile.
- Block any file if its returned verdict is greater than or equal to 7 and create a log entry.
- Create a log entry only if a file has a verdict more than 7.
- When there is an error condition, allow files to be downloaded and create a log entry.
- Create a log entry when attempting to download a file from a site listed in the blocklist or allowlist files.

Configuration

The following configuration requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the Junos OS CLI User Guide.

NOTE: Starting in Junos OS Release 15.1X49-D80, the `match-then` condition has been deprecated from the Juniper ATP Cloud policy configuration. Configurations made before 15.1X49-D80 will continue to work but we recommend you do not use these statements going forward.

1. Create the Juniper ATP Cloud policy.

- Set the policy name to aamwpolicy1 and block any file if its returned verdict is greater than or equal to 7.

  ```
  set services advanced-anti-malware policy aamwpolicy1 verdict-threshold 7
  ```

- Associate the policy with the `default_profile` profile.

  ```
  set services advanced-anti-malware policy aamwpolicy1 http inspection-profile default_profile
  ```

- Block any file if its returned verdict is greater than or equal to 7 and create a log entry.

  ```
  set services advanced-anti-malware policy aamwpolicy1 http action block notification log
  ```

- When there is an error condition, allow files to be downloaded and create a log entry.

  ```
  set services advanced-anti-malware policy aamwpolicy1 fallback-options action permit
  ```

  ```
  set services advanced-anti-malware policy aamwpolicy1 fallback-options notification log
  ```

- Create a log entry when attempting to download a file from a site listed in the blocklist or allowlist files.

  ```
  set services advanced-anti-malware policy aamwpolicy1 blacklist-notification log
  ```

  ```
  set services advanced-anti-malware policy aamwpolicy1 whitelist-notification log
  ```

- For smtp, you only need to specify the profile name. The user-defined action-to-take is defined in the Juniper ATP Cloud portal.

  ```
  set services advanced-anti-malware policy aamwpolicy1 smtp inspection-profile my_smtp_profile
  ```

2. Configure the firewall policy to enable the advanced anti-malware (AAMW) application service.

```
set security policies from-zone trust to-zone untrust policy firewall-policy1 match source-
address any
set security policies from-zone trust to-zone untrust policy firewall-policy1 match
destination-address any
set security policies from-zone trust to-zone untrust policy firewall-policy1 match
application any
set security policies from-zone trust  to-zone untrust  policy firewall-policy1  then permit
application-services advanced-anti-malware aamwpolicy1
```

3. Configure the SSL proxy profile to inspect HTTPs traffic.

```
set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
```

4. Configure the SSL forward proxy to inspect HTTPs traffic.

   Note that this command assumes you have already configured ssl-inspect-ca which is used for ssl forward proxy. If you have not already done so, an error occurs when you commit this configuration. See "Enable Juniper ATP Cloud for Encrypted HTTPS Connections" on page 26 for more information on configuring ssl-inspect-ca.

```
set security policies from-zone trust  to-zone untrust  policy firewall-policy1  then permit
application-services ssl-proxy profile-name ssl-inspect-profile
```

5. Review your policy. It should look similar as shown below.

```
show services advanced-anti-malware policy
Advanced-anti-malware configuration:
Policy Name: aamwpolicy1
  Default-notification  : No Log
  Whitelist-notification: Log
  Blacklist-notification: Log
  Fallback options:
    Action: permit
    Notification: Log
  Protocol: HTTP
    Verdict-threshold: 7
    Action: block
    Notification: Log
    Inspection-profile: default_profile
  Protocol: SMTP
    Verdict-threshold: 7
    Action: User-Defined-in-Cloud (permit)
    Notification: No Log
    Inspection-profile: my_smtp_profile
```

Verification

First, verify that your SRX Series Firewall is connected to the cloud.

```
show services advanced-anti-malware status
```

Next, clear the statistics to make it easier to read your results.

```
clear services advanced-anti-malware statistics
```

After some traffic has passed through your SRX Series Firewall, check the statistics to see how many sessions were permitted, blocked, and so on according to your profile and policy settings.

```
show services advanced-anti-malware statistics
```

Configure Interfaces and Security Zones

This configuration shows how to configure network interfaces and assign these interfaces to security zones.

Before you begin, make sure you have an SSH connection to an Internet-connected SRX Series Firewall.

To configure interfaces and security zones:

1. Configure root authentication.

   ```
   set system root-authentication plain-text-password
   New password:
   Retype new password:
   ```

   The password is not displayed on the screen.
2. Configure the system hostname.

   ```
   set system host-name user@host.example.com
   ```
3. Configure interfaces.

   ```
   set interfaces ge-0/0/0 unit 0 family inet address 10.10.2.1/24
   set interfaces ge-0/0/1 unit 0 family inet address 10.10.2.1/24
   ```
4. Configure security zones.

You need to assign each interface to a zone to pass traffic through it. To configure security zones, enter the following commands:

```
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
```

For the untrust or internal security zone, enable only the services required by the infrastructure for each specific service.

5. Configure DNS.

```
set system name-server 10.10.2.2
```

6. Configure Network Time Protocol (NTP).

```
set system processes ntp
set system ntp boot-server 10.10.2.3
set system ntp server 10.10.2.3
```

7. Commit the configuration.

```
commit
```

Enable Juniper ATP Cloud for Encrypted HTTPS Connections

If you have not already done so, you need to configure ssl-inspect-ca which is used for ssl forward proxy and for detecting malware in HTTPs. Shown below is just one example for configuring ssl forward proxy. For complete information, see Configuring SSL Proxy.

1. From operational mode, generate a PKI public/private keypair for a local digital certificate.

```
request security pki generate-key-pair certificate-id certificate-id size size type type
```

For example:

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

2. From operational mode, define a self-signed certificate. Specify certificate details such as the certificate ID (generated in the previous step), a fully qualified domain name (FQDN) for the certificate, and an e-mail address of the entity owning the certificate.

```
request security pki local-certificate generate-self-signed certificate-id certificate-id domain-name
domain-name subject subject email email-id
```

For example:

```
request security pki local-certificate generate-self-signed                    certificate-id ssl-
inspect-ca domain-name www.juniper.net subject "CN=www.juniper.net,OU=IT,O=Juniper
Networks,L=Sunnyvale,ST=CA,C=US" email security-admin@juniper.net
```

Once done, you can configure the SSL forward proxy to inspect HTTPs traffic. For example:

```
set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-caset security policies
from-zone trust  to-zone untrust  policy firewall-policy1  then permit application-services ssl-
proxy profile-name ssl-inspect-profile
```

For a more complete example, see "Configure Juniper ATP Cloud Policy" on page 21.

RELATED DOCUMENTATION

Configure Juniper ATP Cloud Policy | 21

Unified Policies for Juniper ATP Cloud

Starting in Junos OS Release 18.2R1, unified policies are supported on SRX Series Firewalls, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy. See the Junos 18.2R1 documentation for more details on Unified Policies.

Overview

Unified policies are security policies where you can use dynamic applications as match conditions, along with existing 5-tuple or 6-tuple matching conditions, to detect application changes over time, and allow you to enforce a set of rules for the transit traffic. Unified policies allow you to use dynamic applications as one of the policy match criteria in each application. For more information about united policies, see Unified Security Policies.

By adding dynamic application to the matching conditions, the data traffic is classified based on the Layer 7 application inspection results. AppID identifies dynamic or real-time Layer 4-Layer 7 applications, and after a particular application is identified, actions are performed as per the security policy. (Before identifying the final application, if the policy cannot be matched precisely, a potential policy list is made available, and the traffic is permitted using the potential policy from the list.) After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect is applied on the traffic as per the policy rules.

Juniper ATP Cloud is supported for unified policies. The `set services security-intelligence default-policy` and `set services advanced-anti-malware default-policy` commands are introduced to create default policies for each. During the initial policy lookup phase, before identifying a dynamic application, the SRX Series Firewall can apply the default policy, if the potential policy list contains multiple policies with different security intelligence (SecIntel) or anti-malware rules.

Here are the possible completions for the SecIntel default-policy:

```
set services security-intelligence default-policy ?
Possible completions:
<category>             Name of security intelligence category
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  description          Text description of policy
```

Here are the possible completions for the anti-malware default-policy:

```
set services advanced-anti-malware default-policy ?
Possible completions:
  <[Enter]>            Execute this command
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> blacklist-notification  Blacklist notification logging option
> default-notification  Notification action taken for action
> fallback-options     Fallback options for abnormal conditions
> http                 Configure HTTP options
> imap                 Configure IMAP options
> smtp                 Configure SMTP options
```

```
  verdict-threshold    Verdict threshold
> whitelist-notification  Whitelist notification logging option
  |                    Pipe through a command
```

Explicit Web Proxy for Juniper ATP Cloud

With release Junos OS 18.2R1, you can configure explicit web proxy support for SRX Series services Juniper ATP Cloud connections.

If your network uses a web proxy for access and authentication for HTTP(S) outbound sessions, you can configure your Juniper ATP Cloud connections on the SRX Series Firewall to go through a specified web proxy host. To configure HTTP(S) connections to use a web proxy, you create one or more proxy profiles and see those profiles in your anti-malware and security intelligence (SecIntel) policies.

NOTE: Support starting in Junos OS 18.2R1

Note that authentication to the proxy host is not supported in this release. Therefore an allowlist rule might be needed for the proxy host, with no authentication for Juniper ATP Cloud tunnel traffic.

WARNING: If you are using a web proxy, you must enroll SRX Series Firewalls using a slightly different process, as follows:

For the first part, get the enrollment op script from the Juniper ATP Cloud Web UI like you normally would.

1. Click the **Enroll** button on the **Devices** page.
2. Copy the command to your clipboard and click **OK**.
3. Take only the URL portion (none of the text in front of it) and enter it into the Junos OS CLI of the SRX Series Firewall you want to enroll using the following command:

   ```
   > request services advanced-anti-malware enroll https://amer.Juniper Sky.junipersecurity.net/v1/skyatp/ui_api/bootstrap/enroll/5vhcfia9y18nn98v/k2ygewjwm6c0ap4s.slax
   ```

4. Press `Enter`. (Note that this command must be run in operational mode.)

On the SRX Series Firewall, use the set services command to set the web proxy profile by entering the proxy host IP address and port number as follows:

```
set services proxy profile proxy_name protocol http host x.x.x.x port xxxx
```

NOTE: Optionally configure proxy authentication within the proxy profile. By setting a username and password, you can ensure secure access to external feeds and services.

```
[edit]
user@host# set services proxy profile proxy_name protocol http username <username>
user@host# set services proxy profile proxy_name protocol http password <password>
```

Add the web proxy profile you created to your Juniper ATP Cloud policies using the following commands:

```
set services advanced-anti-malware connection proxy-profile proxy_name
set services security-intelligence proxy-profile proxy_name
```

Use the `show services advanced-anti-malware status` command to view the web proxy IP address and port number. For example:

```
show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.dep4.test.testsystem.net
Server port: 443
+  Proxy hostname: x.x.x.x
+  Proxy port: 3128
    Control Plane:
      Connection time: 2018-5-02 17:03:09 PDT
      Connection status: Connected.
    Service Plane:
      fpc0
        Connection active number: 12
        Connection retry statistics: 0
```

RELATED DOCUMENTATION

Configure Juniper ATP Cloud Policy | 21

CHAPTER 4

Configure SRX Series Firewall

IN THIS CHAPTER

Configure the SRX Series Firewall to Block Outbound Requests to a C&C Host

The C&C feed lists devices that attempt to contact a C&C host. If an outbound request to a C&C host is attempted, the request is blocked and logged or just logged, depending on the configuration. Currently, you configure C&C through CLI commands and not through the Web interface.

To create the C&C profile and policy and firewall policy:

1. Configure the C&C profile. In this example the profile name is `cc_profile` and threat levels 8 and above are blocked.

```
set services security-intelligence profile cc_profile category CC
set services security-intelligence profile cc_profile rule CC_rule match threat-level [8
9 10]
set services security-intelligence profile cc_profile rule CC_rule then action block drop
set services security-intelligence profile cc_profile rule CC_rule then logset services
security-intelligence profile cc_profile default-rule then action permit
```

2. Verify your profile is correct using the `show services security-intelligence` CLI command. Your output should look similar to this.

```
root@host# show services security-intelligence profile cc_profile
category CC;
rule CC_rule {
    match {
        threat-level [ 8 9 10 ];
    }
    then {
        action {
            block {
                drop;
            }
        }
        log;
    }
}
default-rule {
    then {
        action {
            permit;
        }
        log;
    }
}
```

3. Configure your C&C policy to point to the profile created in Step 1. In this example, the C&C policy name is `cc_policy`.

```
set services security-intelligence policy cc_policy CC cc_profile
```

4. Verify your policy is correct using the `show services security-intelligence` CLI command. Your output should look similar to this.

```
root@host# show services security-intelligence policy cc_policy
CC {
    cc_profile;
}
```

```
[edit]
```

5. Configure the firewall policy to include the C&C policy. This example sets the trust-to-untrust zone.

```
set security policies from-zone trust to-zone untrust policy p2 match source-address any
destination-address any application any
set security policies from-zone trust to-zone untrust policy p2 then permit application-
services security-intelligence-policy cc_policy
```

6. Verify your command using the `show security policies` CLI command. It should look similar to this:

```
root@host# show security policies
...
from-zone trust to-zone untrust {
    policy p2 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                     security-intelligence-policy cc_policy;
                }
            }
        }
    }
}
...
[edit]
```

7. Commit your changes.

RELATED DOCUMENTATION

- Command and Control Servers: More Information

Configure the SRX Series Firewall to Block Infected Hosts

An Infected-Host feed lists the hosts that have been compromised and need to be quarantined from communicating with other devices. The feed is in the format of IP addresses all with a threat level of 10, for example xxx.xxx.xxx.133 with threat level 10. You can configure security policies to take enforcement actions on the inbound and outbound traffic to and from a host whose IP address is listed in the feed. The Infected-Host feed is downloaded to the SRX Series Firewall only when the infected host profile is configured and enabled in a firewall policy.

NOTE: Once the Juniper ATP Cloud global threshold for is met for an infected host (see Configuration for Infected Hosts), that host is added to the infected hosts feed and assigned a threat level of 10 by the cloud. Therefore all IP addresses in the infected hosts feed are threat level 10.

To create the infected host profile and policy and firewall policy:

1. Define a profile for both the infected host and CC. In this example, the infected host profile is named `ih-profile` and the action is block drop anything with a threat level of 10. The CC host profile is named `cc-profile` and is based on outbound requests to a C&C host, so add C&C rules to the profile (threat levels 8 and above are blocked.)

```
set services security-intelligence profile ih-profile category Infected-Hosts rule if-rule
match threat-level 10
set services security-intelligence profile ih-profile category Infected-Hosts rule if-rule
then log
set services security-intelligence profile ih-profile category Infected-Hosts default-rule
then action block drop
set services security-intelligence profile cc-profile category CCset services security-
intelligence profile cc-profile rule CC_rule match threat-level [8 9 10]
set services security-intelligence profile cc-profile rule CC_rule then action block drop
set services security-intelligence profile cc-profile rule CC_rule then log
set services security-intelligence profile cc-profile default-rule then action permit
```

If you did not configure any threat level, use the below command to configure the default rule.

```
set services security-intelligence profile ih-profile category Infected-Hosts default rule if-
rule then action block drop
```

As of Junos 18.1R1, there is support for the block action with HTTP URL redirection for Infected Hosts. During the processing of a session IP address, if the IP address in on the infected hosts list and

HTTP traffic is using ports 80 or 8080, infected hosts HTTP redirection can be done. If HTTP traffic is using dynamic ports, HTTP traffic redirection cannot be done. See command below.

2. Verify your command using the `show services security-intelligence` CLI command. It should look similar to this:

```
root@host# show services security-intelligence profile ih-profile
category Infected-Hosts;
rule if-rule {
    match {
        threat-level 10;
    }
    then {
        action {
            block {
                drop;
            }
        }
        log;
    }
}

root@host# show services security-intelligence profile cc-profile
category CC;
rule CC_rule {
    match {
        threat-level [ 10 9 8 ];
    }
    then {
        action {
            block {
                drop;
            }
        }
        log;
    }
}
default-rule {
    then {
        action {
            permit;
        }
```

```
    }
}
```

3. Configure the security intelligence policy to include both profiles created in Step 1. In this example, the policy is named `infected-host-cc-policy`.

```
set services security-intelligence policy infected-host-cc-policy Infected-Hosts ih-
profileset services security-intelligence policy infected-host-cc-policy CC cc-profile
```

4. Configure the firewall policy to include the security intelligence policy. This example sets the trust-to-untrust zone.

```
set security policies from-zone trust to-zone untrust policy p2 match source-address any
destination-address any application any
set security policies from-zone trust to-zone untrust policy p2 then permit application-
services security-intelligence-policy infected-host-cc-policy
```

5. Verify your command using the `show security policies` CLI command. It should look similar to this:

```
root@host# show security policies
...
from-zone trust to-zone untrust {
    policy p2 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                     security-intelligence-policy infected-host-cc-policy;
                }
            }
        }
    }
}
...
[edit]
```

6. Commit your changes.

Configure Reverse Proxy on the SRX Series Firewall

Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, the SRX Series Firewall acts as a proxy, so it can downgrade SSL negotiation to RSA. Other changes are shown in Table 6 on page 38.

Table 6: Comparing Reverse Proxy Before and After Junos OS Release 15.1X49-D80 and 17.3R1

Feature	Prior to 15.1X49-D80	After 15.1X49-D80 and 17.3R1
Proxy model	Runs only in tap mode Instead of participating in SSL handshake, it listens to the SSL handshake, computes session keys and then decrypts the SSL traffic.	Terminates client SSL on the SRX Series Firewall and initiates a new SSL connection with a server. Decrypts SSL traffic from the client/server and encrypts again (after inspection) before sending to the server/client.
Protocol version	Does not support TLS Version 1.1 and 1.2.	Supports all current protocol versions.
Key exchange methods	Supports RSA.	Supports RSA.
Echo system	Tightly coupled with IDP engine and its detector.	Uses existing SSL forward proxy with TCP proxy underneath.
Security services	Decrypted SSL traffic can be inspected only by IDP.	Just like forward proxy, decrypted SSL traffic is available for all security services.
Ciphers supported	Limited set of ciphers are supported.	All commonly used ciphers are supported.

The remainder of this topic uses the term *SSL proxy* to denote both forward proxy and reverse proxy.

Like forward proxy, reverse proxy requires a profile to be configured at the firewall rule level. In addition, you must also configure server certificates with private keys for reverse proxy. During an SSL handshake, the SSL proxy performs a lookup for a matching server private key in its server private key hash table database. If the lookup is successful, the handshake continues. Otherwise, SSL proxy terminates the hand shake. Reverse proxy does not prohibit server certificates. It forwards the actual server certificate/

chain as is to the client without modifying it. Intercepting the server certificate occurs only with forward proxy. The following shows example forward and reverse proxy profile configurations.

```
# show services ssl
...
proxy {
    profile ssl-inspect-profile-dut { # For forward proxy. No server cert/key is needed.
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-1 {
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-2 {
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-server-protection { # For reverse proxy. No root-ca is needed.
        server-certificate ssl-server-protection;
        actions {
            log {
                all;
            }
        }
    }
```

```
}
...
```

You must configure either `root-ca` or `server-certificate` in an SSL proxy profile. Otherwise the commit check fails. See Table 7 on page 40.

Table 7: Supported SSL Proxy Configurations

server-certificate configured	root-ca configured	Profile type
No	No	Commit check fails. You must configure either `server-certificate` or `root-ca`.
Yes	Yes	Commit check fails. Configuring both `server-certificate` and `root-ca` in the same profile is not supported.
No	Yes	Forward proxy
Yes	No	Reverse proxy

Configuring multiple instances of forward and reverse proxy profiles are supported. But for a given firewall policy, only one profile (either a forward or reverse proxy profile) can be configured. Configuring both forward and reverse proxy on the same device is also supported.

You cannot configure the previous reverse proxy implementation with the new reverse proxy implementation for a given firewall policy. If both are configured, you will receive a commit check failure message.

The following are the minimum steps to configure reverse proxy:

1. Load the server certificates and their keys into the SRX Series Firewall certificate repository using the CLI command `request security pki local-certificate load filename` *`filename`* `key key certificate-id` *`certificate-id`* `passphrase` *`exmample@1234`*. For example:

```
request security pki local-certificate load filename /cf0/cert1.pem key /cf0/key1.pem
certificate-id server1_cert_id passphrase example@1234
```

2. Attach the server certificate identifier to the SSL Proxy profile using the CLI command `set services ssl proxy profile` *`profile`* `server-certificate` *`certificate-id`* `passphrase` *`exmample@1234`*. For example

```
set services ssl proxy profile server-protection-profile server-certificate server2_cert_id
passphrase example@1234
```

3. Use the `show services ssl` CLI command to verify your configuration. For example:

```
show services ssl
profile server-protection-profile {
     server-certificate [server1_cert_id , server2_cert_id];
     actions {
          logs {
               all;
               }
             }
}
```

Configure the IMAP Emails Policy on the SRX Series Firewall

Unlike file scanning policies where you define an action permit or action block statement, with IMAP email management the action to take is defined in the **Configure > Emails > IMAP** window. All other actions are defined with CLI commands as before.

NOTE: In the IMAP window on Juniper ATP Cloud, you can select all IMAP servers or specific IMAP servers and list them. Therefore the IMAP configuration sent to the SRX Series Firewall has a flag called “process_all_traffic” which defaults to True, and a list of IMAP servers, which may be empty. In the case where “process_all_traffic” is set to True, but there are servers listed in the IMAP server list, then all servers are processed regardless of the server list. If “process_all_traffic” is not set to True, only the IMAP servers in the server list are processed.

Shown below is an example policy with email attachments addressed in profile `profile2`.

```
show services advanced-anti-malware
...
policy policy1 {
```

```
    http {
        inspection-profile default_profile; # Global profile
        action permit;
    }
    imap {
        inspection-profile profile2; # Profile2 applies to IMAP email
        notification {
            log;
        }
    }
    verdict-threshold 8; # Globally, a score of 8 and above indicate possible malware
    fallback-options {
        action permit;
        notification {
            log;
        }
    }
    default-notification {
        log;
    }
    whitelist-notification {
        log;
    }
    blacklist-notification {
        log;
    }
    fallback-options {
        action permit; # default is permit and no log.
        notification log;
    }
}
...
```

In the above example, the email profile (profile2) looks like this:

```
show services advanced-anti-malware profile
Advanced anti-malware inspection profile:
Profile Name: profile2
version: 1443769434
  disabled_file_types:
  {
     application/x-pdfa: [pdfa],
```

```
    application/pdf: [pdfa],
    application/mbox: []
  },
  disabled_categories: [java, script, documents, code],
  category_thresholds: [
  {
    category: executable,
    min_size: 512,
    max_size: 1048576
  },
  {
    category: library,
    min_size: 4096,
    max_size: 1048576
  }]
```

The firewall policy is similar to before. The AAMW policy is place in trust to untrust zone. See the example below.

```
show security policies from-zone trust to-zone untrust {
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    advanced-anti-malware-policy policy1;
                    ssl-proxy {
                        profile-name ssl-proxy1;
                    }
                }
            }
        }
    }
}
```

Shown below is another example, using the `show services advanced-anti-malware policy` CLI command. In this example, emails are quarantined if their attachments are found to contain malware. A verdict score of 8 and above indicates malware.

```
show services advanced-anti-malware policy
Advanced-anti-malware configuration:
Policy Name: policy1
  Default-notification  : Log
  Whitelist-notification: No Log
  Blacklist-notification: No Log
  Fallback options:
    Action: permit
    Notification: Log
  Protocol: HTTP
  Verdict-threshold: recommended (7)
    Action: block
    Notification: No Log
    Inspection-profile: default
  Protocol: SMTP
  Verdict-threshold: recommended (7)
    Action: User-Defined-in-Cloud (permit)
    Notification: Log
    Inspection-profile: default
  Protocol: IMAP
  Verdict-threshold: recommended (7)
    Action: User-Defined-in-Cloud (permit)
    Notification: Log
    Inspection-profile: test
```

Optionally you can configure forward and reverse proxy for server and client protection, respectively. For example, if you are using IMAPS, you may want to configure reverse proxy. For more information on configuring reverse proxy, see "Configure Reverse Proxy on the SRX Series Firewall" on page 38.

```
# show services ssl
initiation { # for cloud connection
    profile srx_to_sky_tls_profile_name {
        trusted-ca sky-secintel-ca;
        client-certificate sky-srx-cert;
    }
}
```

```
proxy {
    profile ssl-client-protection { # for forward proxy
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-server-protection { # for reverse proxy
        server-certificate ssl-server-protection;
        actions {
            log {
                all;
            }
        }
    }
}
```

Use the `show services advanced-anti-malware statistics` CLI command to view statistical information about email management.

```
show services advanced-anti-malware statistics
Advanced-anti-malware session statistics:
 Session interested:    3291750
  Session ignored:       52173
  Session hit blacklist: 0
  Session hit whitelist: 0
                         Total      HTTP       HTTPS      SMTP       SMTPS   IMAP    IMAPS
  Session active:        52318      0          0          52318      0       0       0
  Session blocked:       0          0          0          0          0       0       0
  Session permitted:     1354706    0          0          1354706    0       0       0

Advanced-anti-malware file statistics:
                               Total      HTTP       HTTPS      SMTP       SMTPS   IMAP    IMAPS
  File submission success:     83134      0          0          83134      0       0       0
  File submission failure:     9679       0          0          9679       0       0       0
  File submission not needed:  86104      0          0          86104      0       0       0
  File verdict meets threshold: 65732     0          0          65732      0       0       0
  File verdict under threshold: 16223     0          0          16223      0       0       0
  File fallback blocked:       0          0          0          0          0       0       0
```

```
  File fallback permitted:      4512       0          0          4512       0        0      0
  File hit submission limit:    0          0          0          0          0        0      0

Advanced-anti-malware email statistics:
                           Total     SMTP       SMTPS   IMAP   IMAPS
  Email processed:         345794     345794     0       0      0
  Email permitted:         42722      42722      0       0      0
  Email tag-and-delivered: 0          0          0       0      0
  Email quarantined:       9830       9830       0       0      0
  Email fallback blocked:  0          0          0       0      0
  Email fallback permitted: 29580     29580      0       0      0
  Email hit whitelist:     0          0          0       0      0
  Email hit blacklist:     0          0          0       0      0
```

As before, use the `clear services advanced-anti-malware statistics` CLI command to clear the above statistics when you are troubleshooting.

Before configuring the IMAP threat prevention policy, make sure you have done the following:

- Define the action to take (block or deliver malicious messages) and the end-user email notification in the **Configure > Emails > IMAP** window.
- (Optional) Create a profile in the **Configure > Device Profiles** window to indicate which email attachment types to scan. Or, you can use the default profile.

The following steps show the minimum configuration. To configure the threat prevention policy for IMAP using the CLI:

1. Create the Juniper ATP Cloud policy.
   - In this example, the policy name is `imappolicy1`.

     ```
     set services advanced-anti-malware policy imappolicy1
     ```

   - Associate the policy with the IMAP profile. In this example, it is the `default_profile` profile.

     ```
     set services advanced-anti-malware policy imappolicy1 inspection-profile default_profile
     ```

- Configure your global threshold. If a verdict comes back equal to or higher than this threshold, then it is considered to be malware. In this example, the global threshold is set to 7.

```
set services advanced-anti-malware policy imappolicy1 verdict-threshold 7
```

- Apply the IMAP protocol and turn on notification.

```
set services advanced-anti-malware policy imappolicy1 imap notification log
```

- If the attachment has a verdict less than 7, create log entries.

```
set services advanced-anti-malware policy imappolicy1 default-notification log
```

- Send the email to the recipient and create a log entry for an error condition.

```
set services advanced-anti-malware policy imappolicy1 fallback-options action permit
set services advanced-anti-malware policy imappolicy1 fallback-options notification log
```

2. Configure the firewall policy to enable the advanced anti-malware (AAMW) application service.

```
[edit security zones]
set security policies from-zone untrust to-zone trust policy 1 then permit application-
services advanced-anti-malware imappolicy1
```

3. In this example, we will configure the reverse proxy.

   For reverse proxy:

   - Load the CA certificate.
   - Load the server certificates and their keys into the SRX Series Firewall certificate repository.

```
request security pki local-certificate load filename /cf0/cert1.pem key /cf0/key1.pem
certificate-id server1_cert_id
```

- Attach the server certificate ID to the SSL proxy profile.

```
set services ssl proxy profile server-protection-profile server-certificate server1_cert_id
```

RELATED DOCUMENTATION

- Blocked Attachments Overview
- Emails: Configure IMAP

Configure the SMTP Emails Policy on the SRX Series Firewall

Unlike file scanning policies where you define an action permit or action block statement, with SMTP email management the action to take is defined in the **Configure > Emails > SMTP** window. All other actions are defined with CLI commands as before.

Shown below is an example policy with email attachments addressed in profile `profile2`.

```
show services advanced-anti-malware
...
policy policy1 {
    http {
        inspection-profile default_profile; # Global profile
        action permit;
    }
    smtp {
        inspection-profile profile2; # Profile2 applies to SMTP email
        notification {
            log;
        }
    }
    verdict-threshold 8; # Globally, a score of 8 and above indicate possible malware
    fallback-options {
        action permit;
        notification {
            log;
        }
    }
    default-notification {
```

```
        log;
    }
    whitelist-notification {
        log;
    }
    blacklist-notification {
        log;
    }
    fallback-options {
        action permit; # default is permit and no log.
        notification log;
    }
}
...
```

In the above example, the email profile (profile2) looks like this:

```
show services advanced-anti-malware profile
Advanced anti-malware inspection profile:
Profile Name: profile2
version: 1443769434
  disabled_file_types:
  {
     application/x-pdfa: [pdfa],
     application/pdf: [pdfa],
     application/mbox: []
  },
  disabled_categories: [java, script, documents, code],
  category_thresholds: [
  {
    category: executable,
    min_size: 512,
    max_size: 1048576
  },
  {
    category: library,
    min_size: 4096,
    max_size: 1048576
  }]
```

The firewall policy is similar to before. The AAMW policy is place in trust to untrust zone. .See the example below.

```
show security policies from-zone trust to-zone untrust {
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    advanced-anti-malware-policy policy1;
                    ssl-proxy {
                        profile-name ssl-proxy1;
                    }
                }
            }
        }
    }
}
```

Shown below is another example, using the `show services advanced-anti-malware policy` CLI command. In this example, emails are quarantined if their attachments are found to contain malware. A verdict score of 8 and above indicates malware.

```
show services advanced-anti-malware policy policy1
Advanced-anti-malware configuration:
Policy Name: policy1
  Default-notification  : No Log
  Whitelist-notification: Log
  Blacklist-notification: Log
  Fallback options:
    Action: permit
    Notification: Log
  Inspection-profile: profile2
  Applications: HTTP
  Verdict-threshold: 8
  Action: block
  Notification: Log
```

```
  Protocol: SMTP
    Verdict-threshold: 8
    Action: User-Defined-in-Cloud (quarantine)
    Notification: Log
    Inspection-profile: profile2
```

Optionally you can configure forward and reverse proxy for server and client protection, respectively. For example, if you are using SMTPS, you may want to configure reverse proxy. For more information on configuring reverse proxy, see "Configure Reverse Proxy on the SRX Series Firewall" on page 38.

```
# show services ssl
initiation { # for cloud connection
    profile srx_to_sky_tls_profile_name {
        trusted-ca sky-secintel-ca;
        client-certificate sky-srx-cert;
    }
}
proxy {
    profile ssl-client-protection { # for forward proxy
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-server-protection { # for reverse proxy
        server-certificate ssl-server-protection;
        actions {
            log {
                all;
            }
        }
    }
}
```

Use the `show services advanced-anti-malware statistics` CLI command to view statistical information about email management.

```
show services advanced-anti-malware statistics
Advanced-anti-malware session statistics:
  Session interested:    3291750
  Session ignored:       52173
  Session hit blacklist: 0
  Session hit whitelist: 0
                         Total      HTTP       HTTPS      SMTP       SMTPS
  Session active:        52318      0          0          52318      0
  Session blocked:       0          0          0          0          0
  Session permitted:     1354706    0          0          1354706    0

Advanced-anti-malware file statistics:
                               Total      HTTP       HTTPS      SMTP       SMTPS
  File submission success:     83134      0          0          83134      0
  File submission failure:     9679       0          0          9679       0
  File submission not needed:  86104      0          0          86104      0
  File verdict meets threshold: 65732     0          0          65732      0
  File verdict under threshold: 16223     0          0          16223      0
  File fallback blocked:       0          0          0          0          0
  File fallback permitted:     4512       0          0          4512       0
  File hit submission limit:   0          0          0          0          0

Advanced-anti-malware email statistics:
                            Total     SMTP       SMTPS
  Email processed:          345794     345794     0
  Email permitted:          42722      42722      0
  Email tag-and-delivered:  0          0          0
  Email quarantined:        9830       9830       0
  Email fallback blocked:   0          0          0
  Email fallback permitted: 29580      29580      0
  Email hit whitelist:      0          0          0
  Email hit blacklist:      0          0          0
```

As before, use the `clear services advanced-anti-malware statistics` CLI command to clear the above statistics when you are troubleshooting.

Before configuring the SMTP threat prevention policy, make sure you have done the following:

- Define the action to take (quarantine or deliver malicious messages) and the end-user email notification in the **Configure > Emails > SMTP** window.
- (Optional) Create a profile in the **Configure > Device Profiles** window to indicate which email attachment types to scan. Or, you can use the default profile.

The following steps show the minimum configuration. To configure the threat prevention policy for SMTP using the CLI:

1. Create the Juniper ATP Cloud policy.
   - In this example, the policy name is `smtppolicy1`.

     ```
     set services advanced-anti-malware policy smtppolicy1
     ```

   - Associate the policy with the SMTP profile. In this example, it is the `default_profile` profile.

     ```
     set services advanced-anti-malware policy smtppolicy1 inspection-profile default_profile
     ```

   - Configure your global threshold. If a verdict comes back equal to or higher than this threshold, then it is considered to be malware. In this example, the global threshold is set to 7.

     ```
     set services advanced-anti-malware policy smtppolicy1 verdict-threshold 7
     ```

   - Apply the SMTP protocol and turn on notification.

     ```
     set services advanced-anti-malware policy smtppolicy1 smtp notification log
     ```

   - If the attachment has a verdict less than 7, create log entries.

     ```
     set services advanced-anti-malware policy smtppolicy1 default-notification log
     ```

   - Send the email to the recipient and create a log entry for an error condition.

     ```
     set services advanced-anti-malware policy smtppolicy1 fallback-options action permit
     set services advanced-anti-malware policy smtppolicy1 fallback-options notification log
     ```

2. Configure the firewall policy to enable the advanced anti-malware (AAMW) application service.

```
set security policies from-zone untrust to-zone trust policy 1 then permit application-
services advanced-anti-malware smtppolicy1
```

3. In this example, we will configure the reverse proxy.

   For reverse proxy:

   - Load the CA certificate.
   - Load the server certificates and their keys into the SRX Series Firewall certificate repository.

     ```
     request security pki local-certificate load filename /cf0/cert1.pem key /cf0/key1.pem
     certificate-id server1_cert_id
     ```

   - Attach the server certificate ID to the SSL proxy profile.

     ```
     set services ssl proxy profile server-protection-profile server-certificate server1_cert_id
     ```

RELATED DOCUMENTATION

Emails: Configure SMTP

2

PART

Configure

CHAPTER 5

Configure ATP Cloud Features on SRX Series Firewall

IN THIS CHAPTER

Encrypted Traffic Insights Overview

IN THIS SECTION

Encrypted traffic insights helps you to detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic.

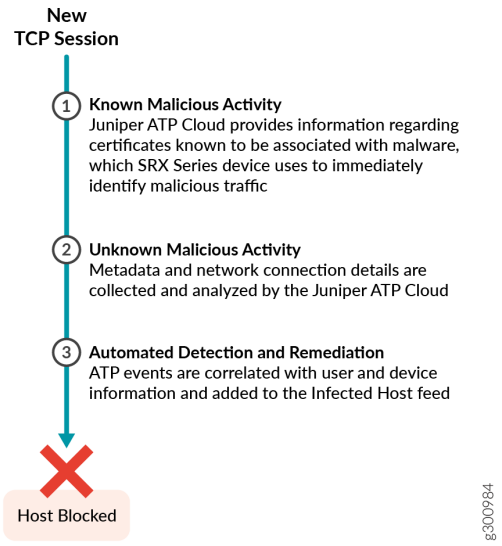
Benefits of Encrypted Traffic Insights

- Monitors network traffic for threats without breaking the encryption of the traffic, thereby adhering to data privacy laws.
- Erases the need for additional hardware or network changes to set up and manage the network:
  - The SRX Series Firewall provides the required metadata (such as known malicious certificates and connection details) and connection patterns to ATP Cloud.
  - The ATP Cloud provides behavior analysis and machine learning (ML) capabilities.
- Provides greater visibility and policy enforcement over encrypted traffic without requiring resource-intensive SSL decryption:
  - Based on the network behaviors analyzed by ATP Cloud, the network connections are classified as malicious or benign.
- Adds an additional layer of protection beyond traditional information security solutions to help organizations reduce and manage risk.
- Ensures no latency as we do not decrypt the traffic.

Encrypted Traffic Insights and Detection

The encrypted traffic insights combines rapid response and network analysis (both static and dynamic) to detect and remediate malicious activity hidden in encrypted sessions. Figure 5 on page 58 shows the staged approach for encrypted traffic insights.

Figure 5: Encrypted Traffic Insights and Detection



Workflow

This section provides the topology and workflow to perform encrypted traffic insights.

Figure 6 on page 59 shows the logical topology of encrypted traffic insights workflow.

Figure 6: Topology for encrypted traffic insights

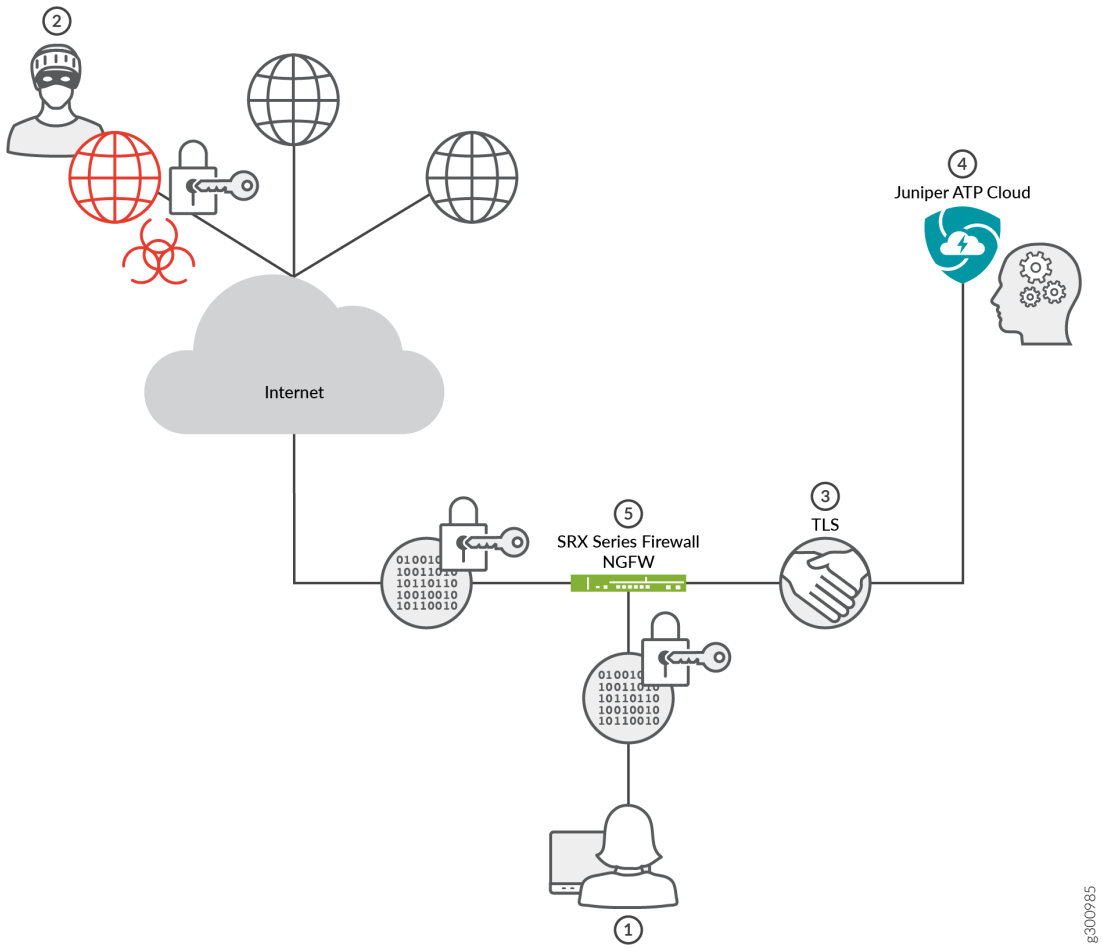


Table 8: Encrypted Traffic Insights Workflow

Step	Description
1	A client host, who is located behind an SRX Series Firewall requests a file to be downloaded from the Internet.
2	The SRX Series Firewall receives the response from the Internet. The SRX Series Firewall extracts the server certificate from the session and compares its signature with the blocklist certificate signatures. If a match occurs, then connection is blocked. **NOTE**: The Juniper Networks ATP Cloud feed keeps the SRX Series Firewall up to date with a feed of certificates associated with known malware sites.

Table 8: Encrypted Traffic Insights Workflow *(Continued)*

Step	Description
3	The SRX Series Firewall collects the metadata and connection statistics and sends it to the ATP Cloud for analysis.
4	The ATP Cloud performs behavioral analysis to classify the traffic as benign or malicious.
5	If a malicious connection is detected, the threat score of the host is recalculated. If the new score is above the threshold, then the client host is added to infected host list, The client host might be blocked based on policy configurations on SRX Series Firewalls.

Configure Encrypted Traffic Insights

Before You Begin

- Enroll the SRX Series Firewall to Juniper ATP Cloud. For more information, see Enroll an SRX Series Firewall Using the CLI.

To enable encrypted traffic insights on SRX Series Firewalls, include the following CLI configurations:

1. Configure the security-metadata-streaming policy.

```
set services security-metadata-streaming policy sms_policy http detections encryptedc2 action
permit
set services security-metadata-streaming policy sms_policy http detections encryptedc2
notification log
```

2. Attach the security-metadata-streaming policy to a security firewall policy.

```
set security policies from-zone trust to-zone untrust application-services security-metadata-
streaming-policy sms_policy
set security policies from-zone untrust to-zone trust application-services security-metadata-
streaming-policy sms_policy
```

3. Commit the configuration.

```
commit
```

Use the `show services security-metadata-streaming http statistics` command to view the statistics of security metadata streaming policy.

`show services security-metadata-streaming http statistics`

```
show services security-metadata-streaming http statistics
Security Metadata Streaming session statistics:
  Session inspected:    10
  Session whitelisted:   0
  Session detected:      6

Security Metadata Streaming submission statistics:
  Records submission success:         8
  Records submission failure:         2
```

To view the list of servers that are allowlisted for encrypted traffic insights, use the `show services security-metadata-streaming http whitelist` command.

`show services security-metadata-streaming http whitelist`

```
show services security-metadata-streaming http whitelist

No. IP-start IP-end Feed Address
1 192 0.5.0 192.0.5.1 eta_custom_whitelist ID-80001400
```

Adaptive Threat Profiling Overview

IN THIS SECTION

Juniper ATP Cloud Adaptive Threat Profiling allows SRX Series Firewalls to generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events.

This feature allows you to configure security or IDP policies that, when matched, inject the source IP address, destination IP address, source identity, or destination identity into a threat feed, which can be leveraged by other devices as a dynamic-address-group (DAG). While this feature is focused on tracking and mitigating threat actors within a network, you can also use it for non-threat related activities, such as device classification.

With adaptive threat profiling, the Juniper ATP Cloud service acts as a feed-aggregator and consolidates feeds from SRX Series Firewall across your enterprise and shares the deduplicated results back to all SRX Series Firewalls in the organization at regular intervals. SRX Series Firewalls can then use these feeds to perform further actions against the traffic.

NOTE: This feature requires a SecIntel License to function. Additional detection capabilities might require AppID, IDP, and Enhanced Web Filtering licenses to be added to your device if not already present. For more information, see Software Licenses for ATP Cloud.

Benefits of Adaptive Threat Profiling

- Enables new deployment architectures, whereby low cost SRX Series Firewalls can be deployed as sensors throughout the network on Tap ports, identifying and sharing intelligence to inline devices for real-time enforcement.
- Allows administrators near-infinite adaptability to changing threats and network conditions. Security policies can be staged with adaptive threat profiling feeds, which automatically populate with entries in the event of an intrusion or a malware outbreak.
- Provides the ability to perform endpoint classification. You can classify endpoints based on network behavior and/or deep packet inspection (DPI) results. For example, you can leverage AppID, Web-Filtering, or IDP to place hosts that communicate with Ubuntu's update servers into a dynamic-address-group that can be used to control Ubuntu-Server behavior on your network.

Configure and Deploy Adaptive Threat Profiling

An SRX Series Firewall that has already been enrolled with Juniper ATP Cloud should include all the necessary configuration to begin leveraging adaptive threat profiling.

To begin, validate that the device already contains a URL for security-intelligence (SecIntel).

1. Check the URL for the feed server.

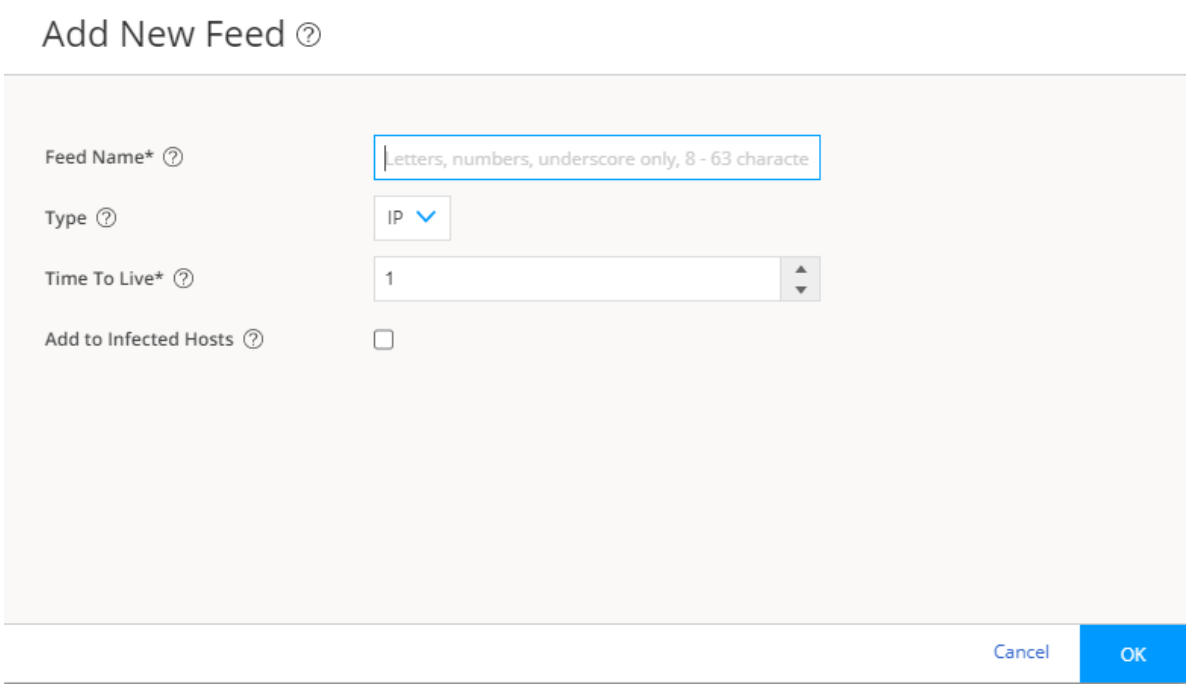
Your output should look similar to the following:

```
show services security-intelligence url
https://cloudfeeds.sky.junipersecurity.net/api/manifest.xml
```

NOTE: If the URL is not present in the configuration, try re-enrolling the device in Juniper ATP Cloud. See Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal.

2. Create an adaptive threat profiling feed in Juniper ATP Cloud. Log into Juniper ATP Cloud UI, select **Configure** > **Adaptive Threat Profiling**. The Adaptive Threat Profiling page appears as shown in Figure 7 on page 63. In this example, we will use the feed name **High_Risk_Users** with a time-to-live (TTL) of seven days.

Figure 7: Add New Feed



3. Click **OK** to save changes. For more information, see Create an Adaptive Threat Profiling Feed.

4. Ensure that the feed has been downloaded by your SRX Series Firewall. This is done automatically at regular intervals but can take a few seconds.

A manual download of the SecIntel database can speed up this process, if necessary.

```
> request services security-intelligence download

> request services security-intelligence download status |match High_Risk_Users

Feed High_Risk_Users (20200615.1) root-logical-system of category SecProfiling download
succeeded.
```

You can deploy adaptive threat profiling on the SRX Series Firewalls in the following ways:

- As a detection solution
- As an enforcement solution
- As both detection and enforcement solution

To use adaptive threat profiling to detect threats, you can define adaptive threat profiling actions in the following locations:

1. Within the security policy on deny, reject, and permit rules, where you can add the source and/or destination address of the flow to a feed of your choice.

```
[edit security policies global policy Threat_Profiling]
admin@vSRX# set then permit application-services security-intelligence ?
Possible completions:
> add-destination-identity-to-feed  Add Destination Identity to Feed
> add-destination-ip-to-feed  Add Destination IP to Feed
> add-source-identity-to-feed  Add Source Identity to Feed
> add-source-ip-to-feed  Add Source IP to Feed
```

2. Within an IDP Policy as an application-service that adds the origin of the exploit (the attacker) or the target of the exploit to a feed of your choice.

```
[edit security idp idp-policy Threat_Profiling rulebase-ips rule Scanners]
admin@vSRX# set then application-services security-intelligence ?
Possible completions:
  add-attacker-ip-to-feed  Specify the desired feed-name
  add-target-ip-to-feed  Specify the desired feed-name
```

To take effect, you must apply the IDP policy to a traditional policy or unified policy.

```
[edit security policies global policy Threat_Profiling]
admin@vSRX# set then permit application-services idp-policy Threat_?
Possible completions:
 <idp-policy>         Specify idp policy name
  Threat_Profiling     [security idp idp-policy]
```

Once the feed is created, it can then be referenced as a dynamic address group within a security policy as the source-address or destination-address match criteria.

In the following example, we have created a rule which allows authenticated users access to the Enterprise's **Crown Jewels**, but are excluding any source-addresses that are part of the **High_Risk_Users** dynamic address group (sourced from the threat feed of the same name).

```
[edit security policies global policy Access_To_Crown_Jewels]
admin@vSRX# show
match {
    source-address High_Risk_Users;
    destination-address Crown_Jewels;
    source-address-excluded;
    source-identity authenticated-user;
    dynamic-application any;
}
then {
    permit;
    log {
        session-close;
    }
}
```

Use the following command to view the feed summary and status:

```
show services security-intelligence sec-profiling-feed status
```

```
show services security-intelligence sec-profiling-feed status Category name    :SecProfiling
Feed name    :High_Risk_Users
Feed type        :IP
Last post time    :2020-02-06 10:54:10 PST Last post status code:200
Last post status    :succeeded
```

```
show security dynamic-address category-name SecProfiling
```

```
show security dynamic-address category-name SecProfiling
No.     IP-start          IP-end            Feed                Address
1       10.1.1.100        10.1.1.100        High_Risk_Users     High_Risk_Users
2       192.168.0.10      192.168.0.10      High_Risk_Users     High_Risk_Users
3       192.168.0.88      192.168.0.88      High_Risk_Users     High_Risk_Users
```

NOTE: Dynamic-address entries will only be displayed by this command if the feed name being referenced (High_Risk_Users in the example), has been used as a source or destination address in a security policy.

Feed contents can always be viewed in the Juniper ATP Cloud portal, regardless of their state on the SRX Series Firewalls.

Adaptive Threat Profiling Use Cases

SUMMARY

The following use cases demonstrate how adaptive threat profiling can automate threat detection, asset classification, and response across diverse network environments.

Threat Detection Use Case

In this example, we will continue with the definition of the `High_Risk_Users` use case, with the goal of identifying any unusual activity which might suggest an endpoint has been compromised.

1. Create a policy that detects the usage of The Onion Router (TOR), Peer-to-Peer (P2P), and Anonymizers / Proxies and add the their source IP addresses to the `High_Risk_Users` feed.

```
[edit security policies global policy Unwanted_Applications]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
```

```
    application junos-defaults;
    dynamic-application [ junos:p2p junos:web:proxy junos:TOR junos:TOR2WEB ];
}
then {
    deny {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    High_Risk_Users;
                }
            }
        }
    }
    log {
        session-close;
```

2. Create a second policy that looks for communication with known malicious sites and malware Command-and-Control (C&C) infrastructure as well as newly registered domains and adds it to High_Risk_Users feed.

```
[edit security policies global policy URL-C2-Detection]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
    application [ junos-http junos-https ];
    dynamic-application any;
    url-category [ Enhanced_Compromised_Websites Enhanced_Emerging_Exploits
Enhanced_Keyloggers Enhanced_Malicious_Embedded_Link Enhanced_Malicious_Embedded_iFrame
Enhanced_Malicious_Web_Sites Enhanced_Newly_Registered_Websites ];
}
then {
    deny {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    High_Risk_Users;
                }
            }
        }
    }
    log {
```

```
        session-close;
    }
}    }
}
```

3. Create an IDP policy that identifies unusual scanning activity and brute-force attempts.

```
[edit security idp idp-policy Threat_Profiling rulebase-ips rule Scanners]
admin@vSRX# show
match {
    attacks {
        predefined-attacks [ SCAN:NMAP:FINGERPRINT SCAN:METASPLOIT:SMB-ACTIVE
SCAN:METASPLOIT:LSASS SMB:AUDIT:BRUTE-LOGIN APP:RDP-BRUTE-FORCE FTP:PASSWORD:BRUTE-FORCE
LDAP:FAILED:BRUTE-FORCE SSH:BRUTE-LOGIN ];
    }
}
then {
    action {
        drop-connection;
    }
    notification {
        log-attacks;
        packet-log;
    }
    application-services {
        security-intelligence {
            add-attacker-ip-to-feed High_Risk_Users;
        }
    }
}
```

NOTE: This example shows a policy to deploy on a Tap-based SRX Series Firewall sensor. The example does not make sense to deploy on an inline device due to the permissive nature of the rule. In production, we recommend being more restrictive.

4. Apply the IDP rulebase to a security policy to take effect.

```
[edit security policies global policy IDP_Threat_Profiling]
admin@vSRX# show
```

```
match {
    source-address any;
    destination-address any;
    application any;
    dynamic-application any;
}
then {
    permit {
        application-services {
            idp-policy Threat_Profiling;
        }
    }
    log {
        session-close;
    }
}
```

5. Create a simple rule at the top of the rule base which drops any traffic from hosts within the `High_Risk_Users` threat feed.

```
[edit security policies global policy Drop_Risky_Users]
admin@vSRX# show
match {
    source-address High_Risk_Users;
    destination-address any;
    application any;
}
then {
    deny;
    log {
        session-close;
    }
}
```

Asset Classification Use Case

In this example, we will leverage AppID to identify Ubuntu and RedHat servers in an environment and add the servers to feed for use by other devices.

Many legacy devices lack the compute power for Deep-Packet Inspection (DPI). Adaptive threat profiling allows you to share DPI classification results between newer and older platforms.

Create a security policy that identifies Advanced Packaging Tool (APT) and Yellowdog Updater, Modified (YUM) communication with Ubuntu and RedHat Update servers:

```
[edit security policies global policy Linux_Servers]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
    application junos-defaults;
    dynamic-application [ junos:UBUNTU junos:REDHAT-UPDATE ];
}
then {
    permit {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    Linux_Servers;
                }
            }
        }
    }
}
```

Compromised Application Use Case

In this example, the user who is using a compromised application is added to the infected-hosts feed.

We will continue with the definition of the High_Risk_Users use case, with the goal of identifying any unusual activity which might suggest an endpoint has been compromised. We create a policy that detects the The Onion Router (TOR) usage and adds the source identity to the High_Risk_Users feed.

```
[edit security policies global policy Compromised_Applications]
admin@vSRX# show
match {
        source-address any;
        destination-address any;
        source-identity authenticated-user;
        dynamic-application junos:TOR;
      }
then {
      deny {
```

```
            application-services {
                                security-intelligence {
                                                add-source-identity-to-feed High_Risk_Users;
                                                }
                                }
             }
    }
```

Enable DNS SecIntel Detection

To enable DNS secintel detection:

1. Configure DNS profile. In this example, the profile name is `dns-profile`. For allowlisted feed `dns-feed-1`, the DNS request is logged and access is allowed. For custom DNS feed `custom-dns-feed-1`, the DNS request is configured for sinkholing.

```
set security-intelligence profile dns-profile category DNS
set security-intelligence profile dns-profile rule dns-rule-1 match feed-name dns-feed-1
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 1
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 2
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 3
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 4
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 5
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 6
set security-intelligence profile dns-profile rule dns-rule-1 match threat-level 7
set security-intelligence profile dns-profile rule dns-rule-1 then action permit
set security-intelligence profile dns-profile rule dns-rule-1 then log
set security-intelligence profile dns-profile rule dns-rule-2 match feed-name custom-dns-
feed-1
set security-intelligence profile dns-profile rule dns-rule-2 match threat-level 8
set security-intelligence profile dns-profile rule dns-rule-2 match threat-level 9
set security-intelligence profile dns-profile rule dns-rule-2 match threat-level 10
set security-intelligence profile dns-profile rule dns-rule-2 then action sinkhole
set security-intelligence profile dns-profile rule dns-rule-2 then log
```

Configure DNS sinkhole if the action is set as sinkhole. See "Configure DNS Sinkhole" on page 85.

2. Configure DNS policy.

```
set security-intelligence policy dns-policy category DNS security-intelligence-profile dns-
profile
```

3. Configure a security policy and assign the DNS policy to the security policy.

```
set policies from-zone trust to-zone untrust policy security-policy match source-address any
set policies from-zone trust to-zone untrust policy security-policy match destination-address
any
set policies from-zone trust to-zone untrust policy security-policy> match application any
set policies from-zone trust to-zone untrust policy security-policy then permit application-
services security-intelligence-policy dns-policy
```

To display DNS statistics for logical systems and tenant systems, use the following commands:

```
show services security-intelligence dns-statistics logical-system logical-system-name
```

```
show services security-intelligence dns-statistics tenant tenant-name
```

To display DNS profile statistics for logical systems and tenant systems, use the following commands:

```
show services security-intelligence dns-statistics profile p1 logical-system logical-system-name
```

```
show services security-intelligence dns-statistics profile p1 tenant tenant-name
```

To display all DNS statistics for logical systems and tenant systems, use the following commands:

```
show services security-intelligence dns-statistics logical-system all
```

```
show services security-intelligence dns-statistics tenant all
```

```
show services security-intelligence dns-statistics
```

To clear statistics for DNS filtering, use the following commands:

```
clear services security-intelligence dns-statistics logical-system logical-system-name
```

```
clear services security-intelligence dns-statistics logical-system all
```

```
clear services security-intelligence dns-statistics
```

NOTE: Domain Name System Security Extensions (DNSSEC) and Extension Mechanisms for DNS (EDNS) queries are not supported. By default, these queries are dropped.

DNS DGA Detection Overview

IN THIS SECTION

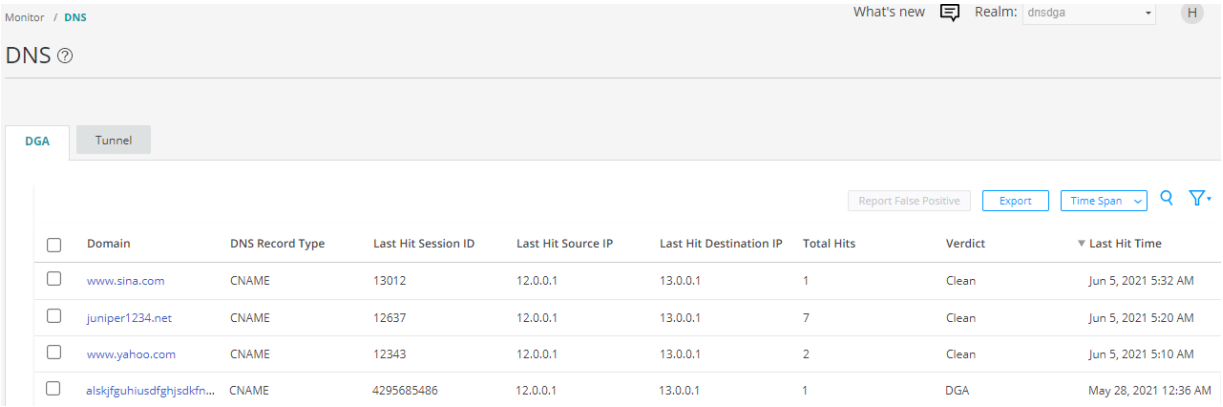
Domain Name System (DNS) Domain Generation Algorithm (DGA) generates seemingly random domain names that are used as rendezvous points with potential C&C servers. DNS DGA detection uses machine learning (ML) models as well as known pre-computed DGA domain names and provides domain verdicts, which helps inline blocking and sinkholing of DNS queries on SRX Series Firewalls.

Juniper ATP Cloud provides a machine learning-based DGA detection model. SRX Series Firewall acts as a collector of security metadata and streams the metadata to Juniper ATP Cloud for DGA analysis. We use both ATP Cloud service and security-metadata-streaming framework to conduct DGA Inspection in the cloud.

DNS DGA detection is available only with Juniper ATP Cloud license. For feature specific licensing information, see Software Licenses for ATP Cloud.

To view DNS DGA detections, log in to Juniper ATP Cloud Web portal and navigate to **Monitor > DNS**. The DGA detections are displayed as shown in Figure 8 on page 74.

Figure 8: DNS DGA Page



DGA Detection Procedure

The procedure for DNS DGA detection is as follows:

1. The Client generates a DNS request and forwards it to the corporate DNS server.
2. The Corporate DNS server checks its local cache and finds that it has no matching record. A cache-miss occurs and the corporate DNS server attempts to query a public DNS server.
3. The SRX Series device receives a DNS requests with record type A/AAAA/CNAME/MX, and so on.
4. Once SRX Series device receives the DNS query, it will consult its local DNS cache.
5. If the domain is not present in the cache (cache miss), SRX sends the domain to Juniper ATP Cloud for analysis.
6. Juniper ATP Cloud service runs rapid DGA machine learning model and responds to SRX Series device with the following verdicts.
   - Clean
   - DGA
   - Suspicious
7. If domain is present in the cache (cache hit), the SRX Series device consults the verdict.
   - If the domain is clean, the SRX Series device forwards the query and ignores the rest of the session.
   - If the domain is marked as DGA, the SRX Series device takes the action defined in the policy (permit/drop/sinkhole/log, and so on)
8. If the domain is not present in the cache, the SRX Series device

- Copies the domain and sends it to the Juniper ATP cloud for DGA analysis.
- Forwards the query to its original destination and requests the appropriate context (query type) from the pending response packet.

> **NOTE**: Only SecIntel has the ability to check its allowlist, blocklist, and C&C. The security-metadata-streaming CLI configuration does not perform matching against this list. Both features must be enabled on the policy to detect C&C and DGA/Tunnels.

Enable DNS DGA Detection

To enable DNS DGA detections on SRX Series Firewalls:

1. Configure the security-metadata-streaming policy.

```
set services security-metadata-streaming policy dns_policy dns cache ttl benign <ttl value >
set services security-metadata-streaming policy dns_policy dns cache ttl c2 <ttl value>
set services security-metadata-streaming policy dns_policy dns detections dga action <deny|
sinkhole|permit>
set services security-metadata-streaming policy dns_policy dns detections dga verdict-timeout
<value>
set services security-metadata-streaming policy dns_policy dns detections dga notification log
set services security-metadata-streaming policy dns_policy dns detections dga fallback-
options notification log
set services security-metadata-streaming policy dns_policy dns detections all action <permit
| deny | sinkhole>
set services security-metadata-streaming policy dns_policy dns detections all notification log
set services security-metadata-streaming policy dns_policy dns detections all fallback-
options notification log
```

   Configure DNS sinkhole if the action is set as sinkhole. See "Configure DNS Sinkhole" on page 85.

2. Configure `dga` option at `[edit services security-metadata-streaming policy` *`dns_policy`* `dns detections]` hierarchy level.

```
security-metadata-streaming {
    policy dns_policy {
        dns {
            detections {
```

```
                dga {
                    action [deny | permit | sinkhole];
                    fallback-options {
                        notification {
                            log;
                        }
                    }
                    verdict-timeout value;
                    notification [log | log-detections];
                }
              }
            }
          }
        }
```

3. Attach the security-metadata-streaming policy to a security firewall policy at zone-level.

   ```
   set security policies from-zone zone-name to-zone zone-name application-services security-metadata-streaming-policy dns_policy
   ```

4. Commit the configuration.

   ```
   commit
   ```

Use the `show services security-metadata-streaming dns statistics` command to view the DNS statistics of security metadata streaming policy.

```
show services security-metadata-streaming dns statistics
Logical system: root-logical-system
DNS session statistics:
  Cache Hits:               0
  Cache Misses:             116
  C2 Sessions Permitted:    0
  C2 Sessions Dropped:      0
  C2 Sessions Sinkholed:    12

DNS submission statistics:
  Domain Submission Success:   43
  Domain Submission Failures:  0
  Safe Verdicts Received:      8
  C2 Verdicts Received:        12
```

```
  DNS Tunnels Detected:        0
  Latency Fallback Triggered:  0

ATP latency statistics:
  Average Latency:             63ms
  Maximum Latency:             119ms
  Minimum Latency:             39ms
  sub-50ms response:           52 (6%)
  sub-100ms response:          4000 (88%)
  sub-250ms response:          30 (4%)
  sub-500ms response:          2 (2%)
```

Use the `show services dns-filtering cache` command to view the details within the DNS cache.

```
show services dns-filtering cache
Logical System:root-logical-system
DNS Cache Refresh Rate:5 Minutes on FPC0 PIC0
Domain-Name, TTL, Prevalence , Verdict, Hitcount
a0.com, 480, 1, C2, 1

Logical System:root-logical-system
DNS Cache Refresh Rate:5 Minutes on FPC0 PIC1
Domain-Name, TTL, Prevalence , Verdict, Hitcount
a10.com, 480, 1, C2, 1
```

NOTE: DNS DGA detection is supported on Junos OS 21.2R1 and later releases.

DNS Tunnel Detection Overview

IN THIS SECTION

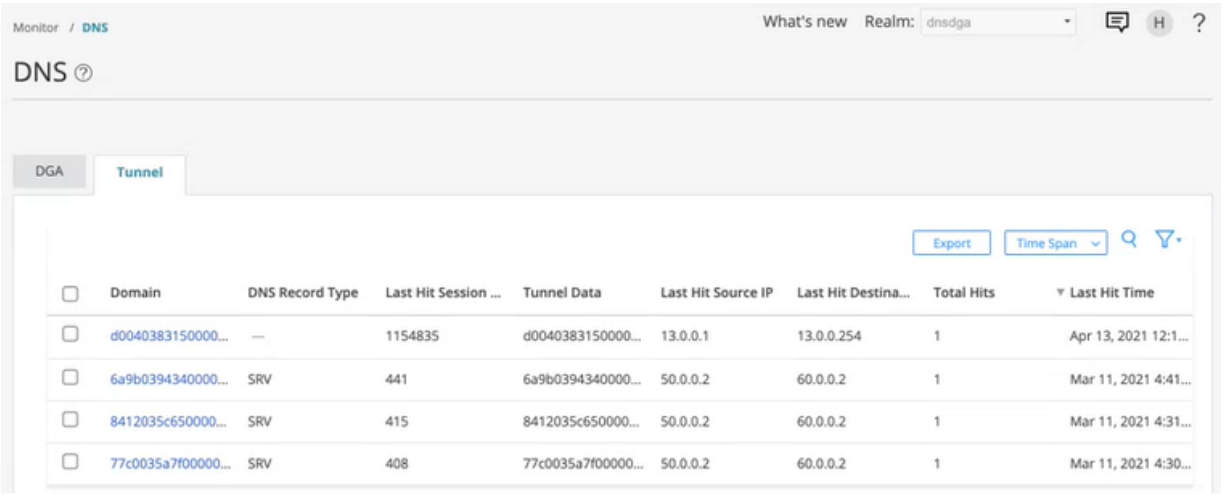
DNS Tunneling is a cyber-attack method that encodes the data of other programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beaconing.

When a DNS packet is detected as tunneled, the SRX Series Firewall can take permit, deny or sinkhole action.

DNS Tunneling detection is available only with Juniper ATP Cloud license. For feature specific licensing information, see Software Licenses for ATP Cloud.

SRX Series Firewall exports the tunneling metadata to Juniper ATP Cloud. To view the DNS tunneling detections, log in to Juniper ATP Cloud Web portal and navigate to **Monitor > DNS**. Click on the **Tunnel** tab to view the DNS tunnel detections as shown inFigure 9 on page 78 . You can click on a domain name to view more details of the hosts that have contacted the domain.

Figure 9: DNS Tunnel Page



DNS Tunneling Procedure

Here's how DNS tunneling works:

1. A cyber attacker registers a malicious domain, for example, “badsite.com”.
2. The domain’s name server points to the attacker’s server, where DNS Tunneling malware program is running.
3. DNS Tunnel client program running on the infected host generates DNS requests to the malicious domain.

4. DNS resolver routes the query to the attacker's command-and-control server.
5. Connection is established between victim and attacker through DNS resolver.
6. This tunnel can be used to exfiltrate data or for other malicious purposes.

Enable DNS Tunnel Detection

To enable DNS tunnel detections on SRX Series Firewalls:

1. Configure the security-metadata-streaming policy.

```
set services security-metadata-streaming policy dns_policy dns detections tunneling action
<deny| sinkhole|permit>
set services security-metadata-streaming policy dns_policy dns detections tunneling
notification log
set services security-metadata-streaming policy dns_policy dns detections tunneling
inspection-depth <value>
set services security-metadata-streaming policy dns_policy dns detections tunneling fallback-
options notification log
set services security-metadata-streaming policy dns_policy dns detections all action <permit
| deny | sinkhole>
set services security-metadata-streaming policy dns_policy dns detections all notification log
set services security-metadata-streaming policy dns_policy dns detections all fallback-
options notification log
```

   Configure DNS sinkhole if the action is set as sinkhole. See "Configure DNS Sinkhole" on page 85.

2. Configure `tunneling` option at `[edit services security-metadata-streaming policy` *`dns_policy`* `dns detections]` hierarchy level.

```
security-metadata-streaming {
    policy dns_policy {
        dns {
            detections {
                tunneling {
                    action [deny | permit | sinkhole];
                    fallback-options {
                        notification {
                            log;
                        }
```

```
                    }
                    inspection-depth value;
                    notification [log | log-detections];
                }
            }
        }
    }
}
```

3. Attach the security-metadata-streaming policy to a security firewall policy at zone-level.

```
set security policies from-zone zone-name to-zone zone-name application-services security-
metadata-streaming-policy dns_policy
```

4. Commit the configuration.

```
commit
```

Use the `show services security-metadata-streaming dns statistics` command to view the DNS statistics of security metadata streaming policy.

```
show services security-metadata-streaming dns statistics
Logical system: root-logical-system
DNS session statistics:
  Cache Hits:                0
  Cache Misses:              116
  C2 Sessions Permitted:     0
  C2 Sessions Dropped:       0
  C2 Sessions Sinkholed:     12

DNS submission statistics:
  Domain Submission Success:   43
  Domain Submission Failures:  0
  Safe Verdicts Received:      8
  C2 Verdicts Received:        12
  DNS Tunnels Detected:        0
  Latency Fallback Triggered:  0

ATP latency statistics:
  Average Latency:             63ms
```

```
  Maximum Latency:            119ms
  Minimum Latency:            39ms
  sub-50ms response:          52 (6%)
  sub-100ms response:         4000 (88%)
  sub-250ms response:         30 (4%)
  sub-500ms response:         2 (2%)
```

Use the `show services dns-filtering cache` command to view the details within the DNS cache.

```
show services dns-filtering cache
Logical System:root-logical-system
DNS Cache Refresh Rate:5 Minutes on FPC0 PIC0
Domain-Name, TTL, Prevalence , Verdict, Hitcount
a0.com, 480, 1, C2, 1

Logical System:root-logical-system
DNS Cache Refresh Rate:5 Minutes on FPC0 PIC1
Domain-Name, TTL, Prevalence , Verdict, Hitcount
a10.com, 480, 1, C2, 1
```

NOTE: DNS tunnel detection is supported on Junos OS 21.2R1 and later releases.

DNS Sinkhole Overview

IN THIS SECTION

The DNS Sinkhole feature enables you to block DNS requests for the disallowed domains by resolving the domains to a sinkhole server or by rejecting the DNS requests.

You can configure DNS filtering on SRX Series Firewalls to identify and block DNS requests for disallowed domains.

NOTE: Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if the feature is supported on your platform.

After identifying the DNS requests for disallowed domains, you can perform any of the following actions:

- Block access to the disallowed domain— Configure your SRX Series Firewall to send a DNS response that directs traffic to a sinkhole server. This server will have an IP address or a fully qualified domain name (FQDN) that you specify. When a client tries to access the disallowed domain, their traffic will be redirected to the sinkhole server instead of reaching its intended destination.
- Log the DNS request and reject access—The DNS request for the known malicious domains is handled as per the query type (QTYPE). The DNS queries of types A, AAAA, MX, CNAME, TXT, SRV and ANY will result in sinkhole action. These queries are individually counted and reported. The DNS queries of other types will only be logged when the queries match a malicious domain. These queries are allowed to proceed and collectively reported under the type miscellaneous.

The sinkhole server can block further access to a disallowed domain from unauthorized users or take other actions while allowing access. The actions of the sinkhole server are independent of the DNS filtering feature. You must configure the sinkhole server actions separately.

DNS Sinkhole Deployment Models

The SRX Series Firewall offers following ways to implement DNS sinkhole functionality:

- Transparent DNS inspection—SRX Series Firewall is positioned inline between clients and the DNS server. Clients are configured to use the DNS server, and the SRX Series Firewall inspects DNS traffic passing through it. When a malicious domain is detected, the SRX Series Firewall intercepts the response and substitutes the sinkhole IP address.
- DNS proxy—The clients are configured to use the SRX Series Firewall as their DNS server. The SRX Series Firewall forwards DNS queries to the DNS server and inspects the responses. For malicious domains, the SRX Series Firewall responds with the sinkhole IP address instead of the actual IP address.

Benefits

- Redirects DNS requests for disallowed domains to sinkhole servers and prevents anyone operating the system from accessing these domains.
- Provides inline blocking for disallowed domains through SecIntel feeds.

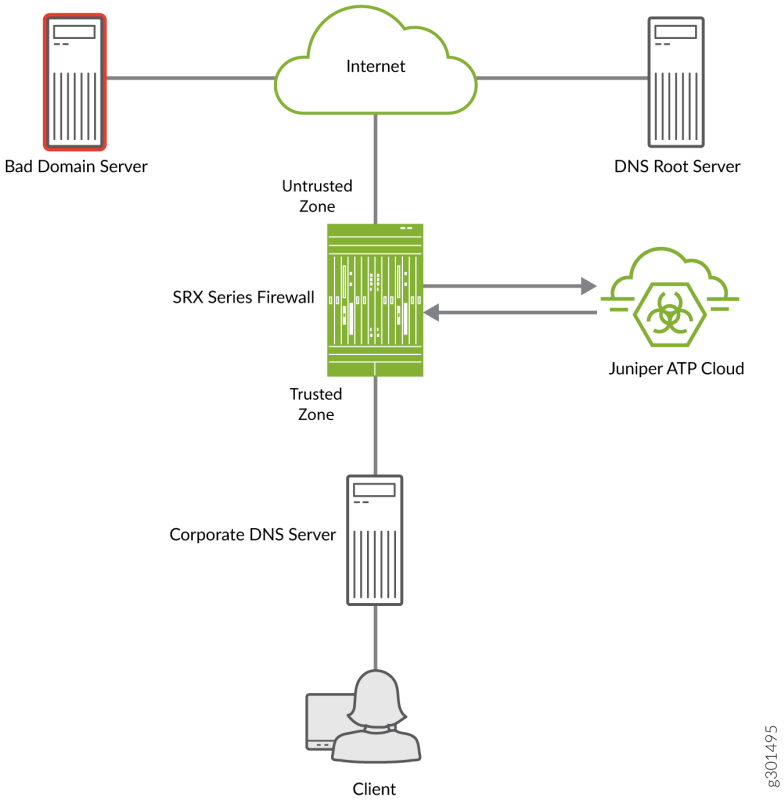
- Helps to identify the infected host in your network.

Workflow to Identify an Infected Host Using DNS Sinkhole

The logical topology for DNS Sinkhole is shown in Figure 10 on page 83.

Figure 10 on page 83 shows a deployment where the SRX Series Firewall is placed between the clients and the corporate DNS server, providing transparent DNS inspection. In this configuration, the sinkhole IP address is assigned directly to an interface on the SRX Series Firewall rather than a separate physical server. This configuration allows the SRX Series Firewall to intercept and analyze DNS queries, and then redirect malicious requests to the sinkhole IP address to prevent harm.

Figure 10: DNS Sinkhole



A high-level workflow to identify an infected host in a network using DNS Sinkhole feature is as follows:

Table 9: Identifying Infected Host using DNS Sinkhole

Step	Description
1	Client sends a DNS request for Bad Domain Server.
2	The SRX Series Firewall first queries the DNS server for the domain.
3	The SRX Series Firewall, configured with Juniper ATP Cloud policy, intercepts the traffic based on the DNS security profile. The SRX Series Firewall then streams the unknown DNS query from the DNS server to the Juniper ATP Cloud for inspection.
4	Juniper ATP Cloud provides per tenant (Logical System (LSYS)/Tenant System (TSYS)) domain feeds such as allowlist DNS feeds, custom DNS feeds and global DNS feeds to the SRX Series Firewall. Juniper ATP Cloud collects the FQDN information from third party source, and Juniper threat lab for its global DNS feeds. You can post your own customized DNS feed through OpenAPI.
5	The SRX Series Firewall downloads the DNS domain feeds from ATP Cloud and applies actions such as sinkhole, block (drop/close), permit, or recommended for the matched domains. • For allowlisted feeds, the DNS request is logged and access is allowed. • For custom DNS feeds, `sinkhole`, `block` with drop or close, `permit`, and `recommended` actions are allowed based on threat-level for the matched domains. **NOTE**: By default, the SRX Series Firewall responds to the DNS queries for the disallowed domain with the default sinkhole server.
6	In this example, the SRX Series Firewall is configured with the sinkhole action. After Juniper ATP Cloud has identified bad domain server as a malicious domain the SRX Series Firewall responds to queries for bad domain server with its own sinkhole IP address.
7	When the client attempts to communicate with bad domain server, the client traffic is redirected to the sinkhole IP address that is configured on the SRX Series Firewall. The SRX Series Firewall then performs security actions such as logging the connection attempt or applying specific security policies to the traffic.
8	The infected client connecting to the sinkhole IP address is identified, added to the infected-hosts feed, and quarantined. The system administrator can identify all clients trying to communicate with the sinkhole IP address by searching for the sinkhole IP address in the threat and traffic logs.

DNS sinkhole feature is available only with a Juniper ATP Cloud license. For feature-specific licensing information, see Software Licenses for ATP Cloud.

Configure DNS Sinkhole

To configure DNS sinkhole for disallowed domains:

1. Configure DNS sinkhole server. We will set the domain name for the DNS sinkhole server as `sinkhole.junipernetworks.com`.

```
set services dns-filtering sinkhole ipv4-address <ipv4-address>
set services dns-filtering sinkhole ipv6-address <ipv6-address>
set services dns-filtering sinkhole fqdn sinkhole.junipernetworks.com
```

NOTE:

- DNS sinkhole configuration is mandatory if the action is set as sinkhole. See "Enable DNS SecIntel Detection" on page 71, "Enable DNS DGA Detection" on page 75 and "Enable DNS Tunnel Detection" on page 79.
- The FQDN value `sinkhole.junipernetworks.com` is provided as an example, do not use it in actual configuration.
- If you do not configure the DNS sinkhole server, then by default, the sinkhole IP address that is hosted on the SRX Series Firewall acts as the sinkhole server.

DNS Security Logs

Logging provides insights on the action taken and the workflow followed to enable features.
To stream DNS logs from the security policies, use the following command:

```
set log stream <dnsf-stream-name> category dnsf
```

To enable logging for the security-metadata-streaming feature that is enabled, use the following command:

```
set services security-metadata-streaming policy p1 dns detections all notification log
```

Geolocation IPs and Juniper ATP Cloud

IP-based Geolocation (GeoIP) is a mapping of an IP address to the geographic location of an Internet connected to a computing device. Juniper ATP Cloud supports GeoIP, giving you the ability to filter traffic to and from specific geographies in the world.

NOTE: Currently you configure GeoIP through CLI commands and not through the Web interface.

GeoIP uses a Dynamic Address Entry (DAE) infrastructure. A DAE is a group of IP addresses, not just a single IP prefix, that can be imported into Juniper ATP Cloud from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. The administrator can then configure security policies to use the DAE within a security policy. When the DAE is updated, the changes automatically become part of the security policy. There is no need to update the policy manually.

The cloud feed URL is set up automatically for you when you run the op script to configure your SRX Series Firewall.

Currently, configuring GeoIP and security policies is done completely on the SRX Series Firewall using CLI commands.

Configure Juniper ATP Cloud with Geolocation IP

To configure Juniper ATP Cloud with GeoIP, create the GeoIP DAE and specify the interested countries. Then, create a security firewall policy on the SRX Series Firewall to reference the DAE and define whether to allow or block access.

To create the GeoIP DAE and security firewall policy:

1. Create the DAE using the `set security dynamic-address` CLI command. Set the category to `GeoIP` and property to `country` (all lowercase). When specifying the countries, use the two-letter ISO 3166 country code in capital ASCII letters; for example, US or DE. For a complete list of country codes, see

ISO 3166-1 alpha-2. Table 10 on page 87 lists the additional codes that are not part of ISO 3166-1 alpha-2.

Table 10: Additional Codes

Code	Country	Additional Information
A1	Anonymous Proxy	This country code identifies a set of IP addresses used by specific anonymous proxies or VPN services. These types of services may be used to bypass GeoIP restrictions. **NOTE**: This country code does not provide complete coverage of all proxy traffic. It identifies the traffic for specific legal anonymous proxies.
A2	Satellite Provider	This country code identifies a set of IP addresses used by Satellite ISPs to provide Internet service to multiple countries. Examples: Nigeria and Ghana.
AP	Asia/Pacific Region	This country code identifies a set of IP addresses that are spread out through the Asia/Pacific region. The country of origin for this set of IP addresses is unknown. **NOTE**: This country code consists of a small subset of IP addresses in the Asia/Pacific region.
EU	Europe	This country code identifies a set of IP addresses that are spread out through Europe. The country of origin for this set of IP addresses is unknown. **NOTE**: This country code does not cover all IP addresses in Europe.
VA	Vatican City State	
AS	Asia	

Table 10: Additional Codes *(Continued)*

Code	Country	Additional Information
OC	Oceania	

In the following example, the DAE name is `my-geoip` and the interested countries are the United States (US) and Great Britain (GB).

```
set security dynamic-address address-name my-geoip profile category GeoIP property country
string US
set security dynamic-address address-name my-geoip profile category GeoIP property country
string GB
```

2. Use the `show security dynamic-address` CLI command to verify your settings. Your output should look similar to the following:

```
show security dynamic-address
address-name my-geoip {
    profile {
        category GeoIP {
            property country {
                string US;
                string GB;
            }
        }
    }
}
```

3. Create the security firewall policy using the `set security policies` CLI command.

   In the following example, the policy is from the untrust to trust zone, the policy name is `my-geoip-policy`, the source address is `my-geoip` created in Step 1, and the action is to deny access from the countries listed in `my-geoip`.

```
set security policies from-zone untrust to-zone trust policy my-geoip-policy match source-
address my-geoip destination-address any application any
set security policies from-zone untrust to-zone trust policy my-geoip-policy then deny
```

4. Use the `show security policies` CLI command to verify your settings. Your output should look similar to the following:

```
show security policies
...
from-zone untrust to-zone trust {
    policy my-geoip-policy {
        match {
            source-address my-geoip;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}

...
```

5. Import the category feeds to the dynamic address using the `set dynamic address` CLI command.

   In the following example, the source address is `my-geoip` created in Step 1 and the action is to import feeds under the GeoIP category to the dynamic address.

```
set security dynamic-address address-name my-geoip profile category GeoIP feed fd property
country string US
```

6. Use the `show security dynamic-address` CLI command to verify your settings. Your output should look similar to the following:

```
show security dynamic-address
...
address-name my-geoip {
    profile {
        category GeoIP {
            property country {
                string US;
            }
        }
    }
}
```

```
address-name my-geoip {
    profile {
        category GeoIP {
            feed fd;
            property country {
                string US;
            }
        }
    }
}
```

Deleting GeoIP-based Dynamic Addresses for a Single Country Code

You can delete GeoIP-based dynamic addresses for a single country code using the following step:

```
delete security dynamic-address address-name address-name profile category GeoIP property
country string CA
```

In the following example, the DAE name is `my-geoip` and the country codes you want to delete are—United States (US) and Great Britain (GB).

```
delete security dynamic-address address-name my-geoip profile category GeoIP property country
string US
delete security dynamic-address address-name my-geoip profile category GeoIP property country
string GB
```

Above step deletes country successfully from the profile without affecting the other country entries.

After you delete the country code, you can confirm the deletion using the `show security dynamic-address` command.

```
show security dynamic-address
```

```
node0:
--------------------------------------------------------------------------
Instance default Total number of matching entries: 0
No. IP-start IP-end Feed Address CountryCode
1 1.0.0.0 1.0.0.255 geoip_country my-geoip1 AU
2 1.0.0.0 1.0.0.255 geoip_country my-geoip2 CN
```

Juniper ATP Cloud with GeoIP provides improved consistency checks and logging from SRX Series Firewalls that are enrolled with Juniper ATP Cloud.

The session deny message includes the following fields:

- `source-country`—Displays the country code of the source address with reference to the policy dynamic address match.
- `destination-country`—Displays the country code of the destination address with reference to the policy dynamic address match.

The system log message displays the valid country code only if the matched policy includes a dynamic address configured with GeoIP. If the matched policy does not have GeoIP configured, then the `source-country` and `destination-country` fields display `N/A`. See System Log Explorer for more details.

RELATED DOCUMENTATION

Geolocation IPs and Juniper ATP Cloud | 86

Configure IPFilter Category

IP filters allow you to create rules to control traffic coming into your network.

To configure IPFilter category:

1. Configure the IPFilter profile.

   In this example, the profile name is `ipf_profile`. The rules are `ipf_rule`, `ipf_rule1` and `ipf_rule2`.

```
set services security-intelligence profile ipf_profile category IPFilter
set services security-intelligence profile ipf_profile rule ipf_rule match threat-level [8 9
10]
set services security-intelligence profile ipf_profile rule ipf_rule then action block
dropset services security-intelligence profile ipf_profile rule ipf_rule then log
set services security-intelligence profile ipf_profile rule ipf_rule1 match threat-level 4
set services security-intelligence profile ipf_profile rule ipf_rule1 then action block close
http message "SecIntel Redirect Message"
set services security-intelligence profile ipf_profile rule ipf_rule1 then logset services
security-intelligence profile ipf_profile rule ipf_rule2 match feed-name fd1
set services security-intelligence profile ipf_profile rule ipf_rule2 then action permit
set services security-intelligence profile ipf_profile rule ipf_rule then logset services
security-intelligence profile ipf_profile rule ipf_rule2 match threat-level 5set services
```

```
security-intelligence profile ipf_profile rule ipf_rule2 then action block close http file
secintel_redirect.txtset services security-intelligence profile ipf_profile rule ipf_rule2
match threat-level 6
set services security-intelligence profile ipf_profile rule ipf_rule2 then action block close
http redirect-url http://www.yahoo.com/redirect.html
set services security-intelligence profile ipf_profile rule ipf_rule2 then logset services
security-intelligence profile ipf_profile default-rule then action recommendedset services
security-intelligence profile ipf_profile default-rule then log
```

2. Use the `show services security-intelligence` CLI command to verify your profile. Your output should look similar to the following:

```
show services security-intelligence
...
}
profile ipf_profile {
    category IPFilter;
    rule ipf_rule {
        match {
            feed-name fd1;
            threat-level [ 8 9 10 ];
        }
        then {
            action {
                block {
                    drop;
                }
            }
            log;
        }
    }
    rule ipf_rule2 {
        match {
            feed-name fd1;
            threat-level [ 5 6 ];
        }
        then {
            action {
                block {
                    close {
                        http {
                            redirect-url http://www.yahoo.com/redirect.html;
```

```
                        }
                    }
                }
            }
            log;
        }
    }
    rule ipf_rule1 {
        match {
            threat-level 4;
        }
        then {
            action {
                block {
                    close {
                        http {
                            message "Secintel Redirect Message";
                        }
                    }
                }
            }
            log;
        }
    }
    default-rule {
        then {
            action {
                recommended;
            }
            log;
        }
    }
}
```

3. Configure your IPFilter policy to point to the profile created in Step 1. In this example, the IPFilter policy name is `ipf_policy`.

```
set services security-intelligence policy ipf_policy IPFilter ipf_profile
```

4. Use the `show services security-intelligence` CLI command to verify your policy. Your output should look similar to the following:

```
show services security-intelligence policy ipf_policy
IPFilter {
    ipf_profile;
}
```

5. Configure the firewall policy to include the IPFilter policy. This example sets the trust-to-untrust zone.

```
set security policies from-zone trust to-zone untrust policy p1 match source-address any
destination-address any application any
set security policies from-zone trust to-zone untrust policy p1 then permit application-
services security-intelligence-policy ipf_policy
```

6. Use the `show security policies` CLI command to verify your settings. Your output should look similar to the following:

```
show security policies
...
}
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application any;
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy ipf_policy;
                }
            }
        }
    }
}
from-zone untrust to-zone trust {
    policy p1 {
        match {
```

```
            source-address [ sda-1 any ];
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
default-policy {
    permit-all;
}
```

7. Commit your changes.

Configure Reverse Shell Detection

IN THIS SECTION

Configure Reverse Shell Detection on SRX Series Firewall

A reverse shell allows the attacker to bypass firewalls and other security mechanisms to open the ports to the target system. It takes advantage of the vulnerabilities in the target system to start a shell session and access the system remotely. Reverse shell detection helps you to detect shell attacks and prevent potential data thefts. For more information, see Juniper Advanced Threat Prevention Cloud User Guide.

To enable reverse shell detection on SRX Series Firewalls, include the following CLI configurations:

1. Configure the security intelligence (SecIntel) profile and policy.

```
services security-intelligence profile RevShellProfile category Reverse-Shell
services security-intelligence profile RevShellProfile rule RevShellRule1 match threat-level 7
services security-intelligence profile RevShellProfile rule RevShellRule1 match threat-level 8
services security-intelligence profile RevShellProfile rule RevShellRule1 match threat-level
9services security-intelligence profile RevShellProfile rule RevShellRule1 match threat-level
```

```
10
services security-intelligence profile RevShellProfile rule RevShellRule1 then action permit
services security-intelligence profile RevShellProfile rule RevShellRule1 then logservices
security-intelligence policy secintel_policy Reverse-Shell RevShellProfile
```

2. Assign the SecIntel policy to a security firewall policy.

```
set security policies from-zone trust to-zone untrust policy atp_policy then permit
application-services security-intelligence-policy secintel_policyset security policies from-
zone untrust to-zone trust policy atp_policy then permit application-services security-
intelligence-policy secintel_policy
```

Use the `show services security-intelligence statistics` command to view the SecIntel statistics.

```
show services security-intelligence statistics
Logical system: root-logical-system
Category Whitelist:
  Profile Whitelist:
    Total processed sessions:      1816
    Permit sessions:               0
    Reverse shell permit sessions: 0
Category Blacklist:
  Profile Blacklist:
    Total processed sessions:      1816
    Block drop sessions:           0
Category CC:
  Profile feed-cc-log-only:
    Total processed sessions:      0
    Permit sessions:               0
    Block drop sessions:           0
    Block close sessions:          0
    Close redirect sessions:       0
  Profile secintel_profile:
    Total processed sessions:      116
    Permit sessions:               0
    Block drop sessions:           0
    Block close sessions:          0
    Close redirect sessions:       0
Category Infected-Hosts:
  Profile ih_profile:
    Total processed sessions:      116
```

```
    Permit sessions:               0
    Block drop sessions:           0
    Block close sessions:          0
    Close redirect sessions:       0
Category Reverse-Shell:
  Profile RevShellProfile:
    Total processed sessions:      116
    Permit sessions:               0
    Block drop sessions:           0
    Block close sessions:          0
    Close redirect sessions:       0
```

Use the `show services security-intelligence category summary` command to view the summary of SecIntel category.

```
show services security-intelligence category summary
Category name     :Whitelist
  Status          :Enable
  Description     :Whitelist data
  Update interval :300s
  TTL             :3456000s
  Feed name       :whitelist_domain
    logical-system:root-logical-system
    Vrf name      :junos-default-vrf
    Version       :20230714.1
    Objects number:0
    Create time   :2023-07-14 10:05:33 PDT
    Update time   :2023-09-06 13:21:14 PDT
    Update status :N/A
    Expired       :Yes
    Status        :Active
    Options       :N/A
  Feed name       :whitelist_ip
    logical-system:root-logical-system
    Vrf name      :junos-default-vrf
    Version       :20230714.1
    Objects number:0
    Create time   :2023-07-14 10:05:31 PDT
    Update time   :2023-09-06 13:21:14 PDT
    Update status :N/A
    Expired       :Yes
    Status        :Active
```

```
    Options       :N/A
  Feed name       :whitelist_reverse_shell_domain
    logical-system:root-logical-system
    Vrf name      :junos-default-vrf
    Version       :20230629.2
    Objects number:1
    Create time   :2023-08-22 21:05:02 PDT
    Update time   :2023-09-06 13:21:14 PDT
    Update status :Store succeeded
    Expired       :No
    Status        :Active
    Options       :N/A
  Feed name       :whitelist_reverse_shell_ip
    logical-system:root-logical-system
    Vrf name      :junos-default-vrf
    Version       :20230823.2
    Objects number:1
    Create time   :2023-08-22 21:04:48 PDT
    Update time   :2023-09-06 13:21:14 PDT
    Update status :Store succeeded
    Expired       :No
    Status        :Active
    Options       :N/A
```

CHAPTER 6

Configure AI Predictive Threat Prevention on SRX Series Firewall

IN THIS CHAPTER

AI-Predictive Threat Prevention Overview

SUMMARY

AI-Predictive Threat Prevention uses artificial intelligence (AI) on packet snippets to predict and prevent both known and zero-day malware on the wire. By actively distinguishing and ignoring non-threatening activities, this system significantly reduces false positives. It enables human experts to concentrate on more critical security tasks and identify genuine, dangerous threats throughout the entire attack life cycle. This process continuously safeguards the network from initial and subsequent attacks.

IN THIS SECTION

Users today are increasingly on the move, requiring fast and secure network access from any location. This heightened mobility raises malware vulnerability, as network security administrators often have limited control over the networks users connect to for accessing corporate resources. Therefore, it is crucial to implement a network security solution that is innovative, swift, and adept at detecting and preventing malware. This topic explores how Juniper Networks' AI-Predictive Threat Prevention, a security solution powered by AI and machine learning (ML), functions.

Juniper Networks' AI-Predictive Threat Prevention is an advanced malware detection and prevention solution designed to safeguard your network against threats arising from users accessing corporate resources from various locations and browsing the Internet to many destinations. Powered by AI and ML, this intelligent security solution enhances the ability to predict and identify genuine threats more swiftly, allowing human experts to concentrate on strategic security initiatives.

AI-Predictive Threat Prevention includes the following features:

- Anti-malware prevention—AI-Predictive Threat Prevention offers effective anti-malware capabilities, scanning vast amounts of data across the network. Traditional solutions require a complete file to determine whether it is malicious. Additionally, the traditional detection process often necessitates enabling a TCP proxy, which can slow down firewall throughput performance. Juniper Networks' organically built anti-malware solution employs a proxy-less architecture with AI to detect threats efficiently.
- AI-generated custom signatures—Organizations can leverage AI-Predictive Threat Prevention with an advanced anti-malware solution to generate custom signatures tailored to their specific environment. Unlike other technologies, AI-Predictive Threat Prevention ensures that these signatures remain active throughout the attack life cycle. This AI-driven anti-malware solution continuously updates threat signatures, detects abnormal behavior patterns, and offers robust protection against subsequent attacks. As a result, security teams can identify potential threats more quickly and efficiently.

Use Feature Explorer to confirm platform and release support for specific features.

For information about licenses for your supported platforms, see Software Licenses for SRX Series Firewalls.

Benefits

- Active threat detection for known and unknown threats
- Improved throughput
- Reduced false positives by filtering out non-threatening activities
- Analysis based on AI and ML in addition to autogenerated signatures

Solution

Flow-based Antivirus Scanning

Starting in Junos OS Release 23.4R1, you can use the flow-based antivirus solution to scan your network traffic and prevent threats in real time using a unified pattern-matching engine.

The flow-based antivirus scanning is an organically built solution that operates at line rate, providing superior efficacy and rapid response to ongoing attacks without compromising performance. Utilizing a proxy-less architecture, it intelligently detects malware by scanning packets as they stream in, without requiring full file downloads. It comprises Juniper Networks curated signatures, which are continuously updated from Juniper ATP Cloud and distributed through Juniper Networks' content delivery network (CDN).

With the flow-based antivirus solution, you can enable inline blocking capabilities that are based on threat intelligence and recent threat detection events across all Juniper's ATP Cloud customer base.

To enforce a flow-based antivirus solution, you must install the Juniper Antivirus license, *Juniper AV* and enable the antivirus policy. For more information, see "Configure Flow-Based Antivirus Policy" on page 107.

Machine-Learning-based Threat Detection

Starting in Junos OS Release 24.2R1, you can configure ML-based threat detection for zero-day threats.

The ML-based threat detection scans files inline on your firewall and blocks infected files before they are downloaded. This threat detection process occurs without Internet access, and requires only a small section of the file to return a verdict.

ML-based threat detection is enabled on your firewall when the scan engine binary file is automatically downloaded from the Juniper Networks CDN server to your firewall. By default, an ML model binary file is automatically downloaded from the CDN server to your firewall device, generally once a week.

To implement machine-learning-based threat detection, you must install the Juniper Antivirus license, *Juniper AV* and enable machine learning. For more information, see "Configure Machine Learning-Based Threat Detection" on page 113.

Workflow

Here is a high-level workflow for AI-Predictive Threat Prevention:

Figure 11: AI-Predictive Threat Prevention

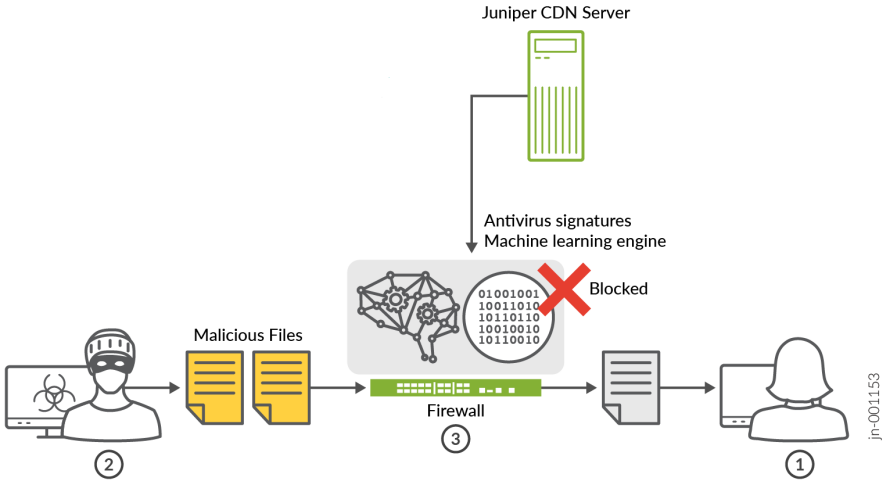


Table 11: AI-Predictive Threat Prevention Workflow

Step	Description
1	The client configures the antivirus policy and CDN server URL on SRX Series Firewall to receive the latest antivirus signatures and ML scan engine updates from the CDN server.
2	The client requests a file to be downloaded from the Internet.
3	As the file passes through the SRX Series Firewall, some portions of the file are matched against the latest antivirus signatures that are received from the CDN server. If a matching signature is found, the file can be blocked and not allowed to be downloaded, depending on the policy action. For .exe and .dll file types, if no matching antivirus signature is found, the ML scan engine analyzes the file inline on the SRX Series Firewall and immediately provides a verdict. Based on this verdict, the SRX Series Firewall can block any infected files before they are downloaded, depending on the policy action.

NOTE:

- If the SRX Series Firewall is enrolled to Juniper ATP Cloud, then in addition to flow-based antivirus scanning and ML-based threat detection, the file is also submitted to Juniper ATP Cloud for analysis.
- You can configure AI-Predictive Threat Prevention on the SRX Series Firewall without enrolling to Juniper ATP Cloud.

Personas

Table 12: Personas and benefits

Personas	Benefits
Chief information security officer (CISO)	• Significantly reduced risk of a successful attack or breach— The AI-powered solution identifies and averts potential threats. • Minimal impact on user experience— Active threat detection at line rate ensures user experience is not impacted by proxying, threat sandboxing, and so on. • Improve resource efficiency— Prioritizing threats based on AI insights allows for a more efficient allocation of security resources.
InfoSec director	• More time for strategic initiatives— Proactive threat identification and mitigation reduces risk, improves overall security, and frees up resources. • Enhanced credibility and visibility— You can spend more time on achieving strategic quantifiable business outcomes that senior leadership recognizes. • Stronger team performance— Automation and AI-driven efficiency enables personnel to focus on more complex tasks.

Table 12: Personas and benefits *(Continued)*

Personas	Benefits
InfoSec architect	• Reduced stress— AI-powered threat prevention can alleviate the pressure of staying ahead of emerging threats. • Enhanced detection accuracy— Industry-leading efficacy means less time wasted pursuing false positives. • Faster/real-time response— The ability to detect and block zero-day threats in real time minimizes downtime and fire-drills.
Network architect	• Faster real-time response—The ability to detect and block zero-day threats in real time minimizes downtime and fire drills. • Less time spent following up with infosec teams—Fewer threats reduce efforts of infosec experts.

Use Cases

AI-Predictive Threat Prevention is ideal for customers who need to protect their business assets from today's advanced cyberthreat, especially in the following use cases:

- Campus
- Enterprise
- Data center
- Public, private, and hybrid cloud
- Service provider

Solution Comparison Matrix

Here's a comparison table that outlines key features and differences between Juniper ATP Cloud, flow-based antivirus solution, and machine learning-based security solution.

Table 13: Solution Comparison Matrix

Requirements	Juniper ATP Cloud	Flow-Based Antivirus	ML-Based Threat Detection
Services	Advanced anti-malware	Static antivirus engine with frequent signature updates	Static antivirus engine with frequent signature updates + ML scan engine
File submission	Cloud	Block mode, no submission to cloud	Block mode, no submission to cloud
Internet access	Access required for feature to function	Required to download antivirus database from Juniper CDN server.	Required to download ML models from Juniper CDN server.
AAMW role	Works with cloud to download AI-generated signatures.	Works offline after database download	Works offline after ML engine download
CLI configuration	`set services advanced-anti-malware`	`set services anti-virus`	`set services anti-virus policy <policy name> machine-learning-scan`
Supported protocols	HTTP and HTTPS IMAP and IMAPS SMTP and SMTPS SMB	HTTP and HTTPS IMAP and IMAPS SMTP and SMTPS SMB	HTTP and HTTPS IMAP and IMAPS SMTP and SMTPS SMB
Supported release	See Feature Explorer	See Feature Explorer	See Feature Explorer
Juniper ATP Cloud enrollment	Yes	Not required	Not required

Table 13: Solution Comparison Matrix *(Continued)*

Requirements	Juniper ATP Cloud	Flow-Based Antivirus	ML-Based Threat Detection
Summary	Leverages cloud infrastructure for scalability and quick response times. Offers a combination of signature-based and behavior analysis for detecting threats.	Primarily relies on signature-based detection and flow inspection. Easier to deploy; performs frequent signature updates.	Uses advanced algorithms for anomaly detection and pattern recognition, offering robust protection against both known and unknown threats. Provides real-time analysis and adapts over time to new threats.

Juniper ATP Cloud and AI-Predictive Threat Prevention are licensed as separate products. Flow-based antivirus and ML-based threat detection are components of AI-Predictive Threat Prevention. These components can be used independently and do not require enrollment in Juniper ATP Cloud. For licensing information about AI-Predictive Threat Prevention, see Software Licenses for SRX Series Firewalls.

You can choose a solution that aligns with the specific needs, infrastructure, and resources of your organization, or you can layer these solutions for more effective enforcement. Apply all of these solutions in a security policy.

What's Next?

In the next section, you'll learn how to configure flow-based antivirus and ML-based threat detection on your firewall. You can also update the flow-based antivirus policy and ML-based threat detection on your SRX Series Firewall in offline mode.

RELATED DOCUMENTATION

- Configure Flow-Based Antivirus Policy | **107**
- Configure Machine Learning-Based Threat Detection | **113**
- Update Flow-Based AV and ML-Based Threat Detection in Offline Mode | **118**

Configure Flow-Based Antivirus Policy

IN THIS SECTION

Overview

Let's take a look at a typical enterprise network. An end user unknowingly visits a compromised website and downloads a malicious content. This action results in compromise of the endpoint. The harmful content on the endpoint also becomes a threat to other hosts within the network. It is important to prevent the download of the malicious content.

You can use an SRX Series Firewall with flow-based antivirus to protect users from virus attacks and to prevent the spread of malware in your network. The flow-based antivirus scans network traffic for viruses, Trojans, rootkits, and other types of malicious code and blocks the malicious content immediately when detected.

The following configuration creates a flow-based antivirus policy with the following properties:

- Firewall policy name is firewall-av-policy.
- Flow antivirus policy is av-policy.
- Block any file if its returned verdict is greater than or equal to 7 and create a log entry.
- When there is an error condition, allow files to be downloaded and create a log entry.

Requirements

Before you begin

- Configure security zones and security policies. For more information, see Example: Creating Security Zones in Security Policies User Guide for Security Devices.
- Verify that you have a valid Juniper license. For licensing information about AI-Predictive Threat Prevention, see Software Licenses for SRX Series Firewalls.

- The CDN server must be reachable from the SRX Series Firewall. For releases before Junos OS 24.2R1, the Juniper content delivery network (CDN) server must be https://signatures.juniper.net/phase. From Junos OS Release 24.2R1 onwards, the CDN server is https://signatures.juniper.net.
- SRX Series Firewall with Junos OS Release 23.4R1 or later

Configuration

IN THIS SECTION

Step-By-Step Procedure

The following configuration requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the Junos OS CLI User Guide.

1. Create the antivirus policy and block any file if its returned verdict is greater than or equal to 7.

```
set services anti-virus policy av-policy action block
set services anti-virus policy av-policy default-notification log
set services anti-virus policy av-policy fallback-options notification log
set services anti-virus policy av-policy http-client-notify message "test message for anti-
virus flow"
set services anti-virus policy av-policy notification log
set services anti-virus policy av-policy verdict-threshold 7
```

2. By default, the latest antivirus signature pack is automatically downloaded from the Juniper Networks content delivery network (CDN) server to your firewall device every five minutes. You can manually update the virus signature database by specifying the URL of the CDN server.

```
set services anti-virus update url https://signatures.juniper.net/
```

You can also customize the setting by using the `set services anti-virus update automatic interval <5...60>` command.

NOTE: Use the proxy profile to the antivirus pattern update process.

```
set services anti-virus update proxy-profile proxy-name
```

Use this option in case your internal network device do not have direct access to the Internet and the device can reach the Internet only through a proxy server.

3. Configure the firewall policy and apply the antivirus policy.

```
set security policies from-zone trust to-zone untrust policy fw-av-policy match source-
address any
set security policies from-zone trust to-zone untrust policy fw-av-policy match destination-
address any
set security policies from-zone trust to-zone untrust policy fw-av-policy match application
any
set security policies from-zone trust to-zone untrust policy fw-av-policy match dynamic-
application any
set security policies from-zone trust to-zone untrust policy fw-av-policy then permit
application-services anti-virus-policy av-policy
```

4. Commit the configuration.

```
commit
```

You can use the AI-PTP tab in the Allowlists page to add, replace, merge, or delete AI-PTP signatures in the allowlists. You can add the file signatures that are identified as false positives to the allowlists. This process excludes the specified signatures from malware inspection performed by the SRX Series Firewalls. For more information, see Create Allowlists and Blocklists.

To view the list of anti-virus signatures added to the allowlists on SRX Series Firewalls, use the CLI command `show services anti-virus signature-exempt-list`.

```
Anti-virus Signature Exempt List:
  C1994069136041805794
  J5381964424818232941
  J12111449344962437113
  J4660909146742838820
Total exempt signatures: 4
```

To clear the file signature allowlists on the SRX Series Firewalls, use CLI command `clear services anti-virus signature-exempt-list`.

You can also run the following CLI commands on your SRX Series Firewalls to add, delete, export, and import file signatures:

- `request services anti-virus signature-exempt-list add <signature-id>`—add file signature IDs on your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list add J4660909146742838820`.
- `request services anti-virus signature-exempt-list delete <signature-id>`—delete file signature IDs on your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list delete J4660909146742838820`.
- `request services anti-virus signature-exempt-list import <txt-file-with-signature-ids>`—import TXT file that contains signature IDs on your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list import /var/tmp/av-exempt-list.txt`.
- `request services anti-virus signature-exempt-list export <txt-file-with-signature-ids>`—export TXT file that contain signature IDs from your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list export /var/tmp/av-exempt-list.txt`.

Results

From configuration mode, confirm your configuration by entering the `show services anti-virus policy av-policy` and `show configuration |display set` commands. If the output does not display the intended configuration, repeat the configuration instructions to correct it.

Check the results of the configuration:

```
show services anti-virus
update {
    url https://signatures.juniper.net/;
}
policy av-policy {
    action block;
    default-notification {
        log;
    }
    fallback-options {
        notification {
            log;
        }
    }
    http-client-notify {
```

```
        message "test message for anti-virus flow";
    }
    notification {
        log;
    }
    verdict-threshold 7;
}
```

```
show security policies from-zone trust to-zone untrust
policy fw-av-policy {
    match {
        source-address any;
        destination-address any;
        application any;
        dynamic-application any;
    }
    then {
        permit {
            application-services {
                anti-virus-policy av-policy;
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Obtaining Information About the Current Antivirus Statistics | 112

To verify the configuration is working properly, use the following steps:

Obtaining Information About the Current Antivirus Statistics

Purpose

After some traffic has passed through your SRX Series Firewall, check the statistics to see how many sessions were permitted, blocked, and so on according to your profile and policy settings.

Action

From operational mode, enter the `show services anti-virus statistics` command.

Sample Output

`show services anti-virus statistics`

```
show services anti-virus statistics
Anti-virus scan statistics:
  Virus DB type: anti-virus
  Total signatures: 11
  Anti-virus DB version: 1654594666
  Anti-virus DB update time: 2022-08-25 13:03:58 PDT
                    Total      HTTP       HTTPS      SMTP       SMTPS      IMAP       IMAPS
SMB
  File scanned:     419382     81947      177549     16067      31591      15994      31925
64309
  Virus found:      290713     1613       161485     15940      31591      15994      31925
32165
  Virus blocked:    290713     1613       161485     15940      31591      15994      31925
32165
  Virus permitted:  0          0          0          0          0          0          0
0
```

Meaning

Shows statistics on viruses scanned, identified and blocked or permitted.

RELATED DOCUMENTATION

anti-virus

show services anti-virus statistics

AI-Predictive Threat Prevention Overview

Create Allowlists and Blocklists

Configure Machine Learning-Based Threat Detection

IN THIS SECTION

Let's take a look at a typical enterprise network. An end user unknowingly visits a compromised website and downloads a malicious content. This action results in compromise of the endpoint. The harmful content on the endpoint also becomes a threat to other hosts within the network. It is important to prevent the download of the malicious content.

You can use an SRX Series Firewall with flow-based antivirus and ML-based threat detection to protect users from malware attacks and to prevent the spread of malware in your network.

The following configuration creates an ML-based antivirus policy with the following properties:

- Firewall policy name is fw-ml-policy.
- ML policy name is ml-policy.
- Block any file if its returned verdict is greater than or equal to 7 and create a log entry.
- When there is an error condition, allow files to be downloaded and create a log entry.

Requirements

Before you begin

- Configure security zones and security policies. For more information, see Example: Creating Security Zones in Security Policies User Guide for Security Devices.
- Verify that you have a valid Juniper license. For licensing information about AI-Predictive Threat Prevention, see Software Licenses for SRX Series Firewalls.

- SRX Series Firewall with Junos OS Release 24.2R1 or later

NOTE:

- ML-based zero-day threat detection supports IMAPS, SMTPS, HTTPS, and SMB protocols.
- The detection supports following file types:
  - Portable Executable (PE) files, such as Windows.exe or .dll
  - Executable and Linkable Format (ELF) files, such as Linux binaries

Configuration

IN THIS SECTION

Step-By-Step Procedure

The following configuration requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the Junos OS CLI User Guide.

1. Create the antivirus policy and block any file if its returned verdict is greater than or equal to 7.

```
set services anti-virus policy ml-policy action block
set services anti-virus policy ml-policy default-notification log
set services anti-virus policy ml-policy fallback-options notification log
set services anti-virus policy ml-policy http-client-notify message "test message for machine-
learning flow"
set services anti-virus policy ml-policy notification log
set services anti-virus policy ml-policy verdict-threshold 7
set services anti-virus policy ml-policy machine-learning-scan action block
set services anti-virus policy ml-policy machine-learning-scan notification log
```

2. By default, your firewall downloads the signatures from the CDN server every week.

You can manually update the virus signature database by specifying the URL of the database server.

```
set services anti-virus update url https://signatures.juniper.net
```

3. Configure the firewall policy and apply the antivirus policy.

```
set security policies from-zone trust to-zone untrust policy fw-ml-policy match source-
address any
set security policies from-zone trust to-zone untrust policy fw-ml-policy match destination-
address any
set security policies from-zone trust to-zone untrust policy fw-ml-policy match application
any
set security policies from-zone trust to-zone untrust policy fw-ml-policy match dynamic-
application any
set security policies from-zone trust to-zone untrust policy fw-ml-policy then permit
application-services anti-virus-policy ml-policy
```

4. Commit the configuration.

```
commit
```

Here are the possible completions for the ML scan:

```
set services anti-virus policy ml-policy machine-learning-scan ?
Possible completions:
  action               Action when malware is found by machine learning scan
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> default-notification  Notification action taken for action
> notification         Notification when malware is found by machine learning scan
```

```
set services anti-virus machine-learning-scan ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  max-concurrent       Max files concurrent scanned by machine learning scan
```

Results

From configuration mode, confirm your configuration by entering the `show services anti-virus policy ml-policy` and `show configuration | display set` commands. If the output does not display the intended configuration, repeat the configuration instructions to correct it.

Check the results of the configuration:

```
show services anti-virus
update {
    url https://signatures.juniper.net;
}
policy ml-policy {
    action block;
    default-notification {
        log;
    }
    fallback-options {
        notification {
            log;
        }
    }
    http-client-notify {
        message "test message for machine-learning flow";
    }
    notification {
        log;
    }
    machine-learning-scan {
        action block;
        notification {
            log;
        }
    }
    verdict-threshold 7;
}
```

```
show security policies from-zone trust to-zone untrust
policy fw-ml-policy {
    match {
        source-address any;
```

```
        destination-address any;
        application any;
        dynamic-application any;
    }
    then {
        permit {
            application-services {
                anti-virus-policy ml-policy;
            }
        }
    }
}
```

Verification

IN THIS SECTION

To verify the configuration is working properly, use the following steps:

Obtaining Information About ML Statistics

Purpose

After some traffic has passed through your SRX Series Firewall, check the statistics to see how many sessions were permitted, blocked, and so on according to your profile and policy settings.

Action

From operational mode, enter the `show services anti-virus machine-learning-scan-statistics` command.

Sample Output

`show services anti-virus machine-learning-scan-statistics`

```
show services anti-virus machine-learning-scan-statistics
Anti-virus machine learning scan statistics:
```

```
  Machine learning scan engine version: 1696526121
  Machine learning scan engine update time: 2023-10-05 22:48:50 UTC
                    Total      HTTP       HTTPS      SMTP       SMTPS      IMAP       IMAPS
SMB
  File scanned:     359382     68947      154549     14367      24591      12494      20025
52309
  Virus found:      187713     1417       146795     13840      24591      12494      20025
25165
  Virus blocked:    187713     1417       146795     13840      24591      12494      20025
25165
  Virus permitted:  0          0          0          0          0          0          0
0
```

Meaning

Shows statistics on viruses scanned, identified and blocked or permitted.

RELATED DOCUMENTATION

- anti-virus
- show services anti-virus statistics
- AI-Predictive Threat Prevention Overview

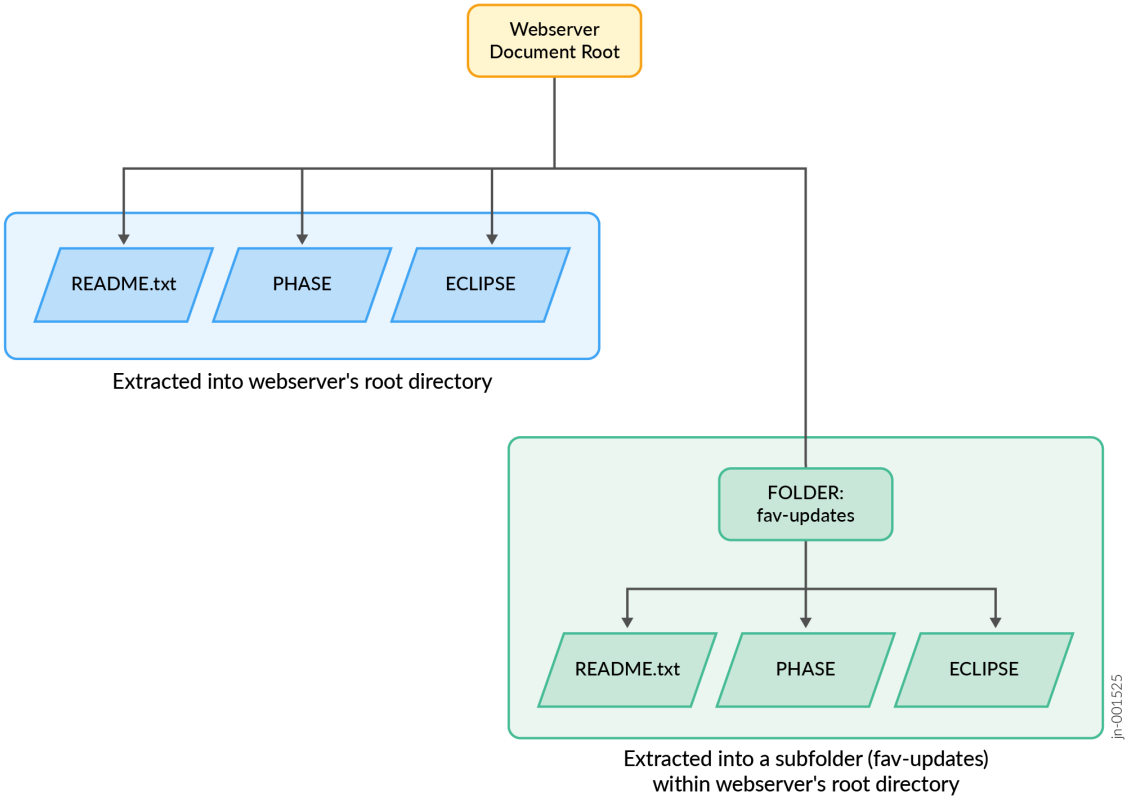
Update Flow-Based AV and ML-Based Threat Detection in Offline Mode

You can update the flow-based antivirus (AV) policy and machine learning (ML)-based threat detection on your SRX Series Firewall in offline mode. Download the signature bundle and store it in your local server that is not connected to the Internet.

To perform offline updates:

1. Download the offline update package from https://signatures.juniper.net/phase/offline.zip to a local server.
2. Unzip offline.zip on the server to extract phase, eclipse, and README.txt. Make sure your SRX Series Firewall can access these files on your local server. You can extract the zip contents directly into the webserver's document root directory, or into a subfolder within the document root directory as shown in Figure 12 on page 119.

Figure 12: Webserver Directory Structure



3. Configure the update URL and antivirus policy using the following commands:

```
set services anti-virus update url https://<webserver-ip-address>/fav-updates/>
set services anti-virus policy p1 action block/permit
set services anti-virus policy p1 default-notification log
set services anti-virus policy p1 fallback-options notification log
set services anti-virus policy p1 http-client-notify message "Blocked by Juniper AV"
set services anti-virus policy p1 notification log
set services anti-virus policy p1 machine-learning-scan action block/premit
set services anti-virus policy p1 verdict-threshold 7
set security policies from-zone trust to-zone untrust policy 1 then permit application-
services anti-virus-policy p1
```

Juniper offline update bundle is valid for up to 24 hours after downloading. The update must be processed by the SRX Series Firewall before the expiration time specified in the README.txt file. For security reasons, the certificate revocation list (CRL) is updated daily and cannot be used after the expiration time.

4. Commit the configuration.

```
commit
```

5. To verify that the configuration is updated, enter the following commands in operational mode:

   - `show services anti-virus statistics`

```
show services anti-virus statistics
Anti-virus scan statistics:
  Virus DB type: anti-virus
  Total signatures: 26139
  Anti-virus DB version: 1759855921
  Anti-virus DB update time: 2025-10-07 09:55:30 PDT
                    Total      HTTP       HTTPS      HTTP2      SMTP       SMTPS
IMAP      IMAPS     SMB
  File scanned:      0          0          0          0          0          0
0         0         0
  Virus found:       0          0          0          0          0          0
0         0         0
  Virus blocked:     0          0          0          0          0          0
0         0         0
  Virus permitted:   0          0          0          0          0          0
0         0         0


Anti-virus block cache (URI-Client IP) statistics:
  Block cache hit count:         0
  Block cache current entries:   0
  Block cache timed out entries: 0
```

   - `show services anti-virus machine-learning-scan-statistics`

```
show services anti-virus machine-learning-scan-statistics
Anti-virus machine learning scan statistics:
  Machine learning scan engine version: 1759752211
  Machine learning scan engine update time: 2025-10-06 05:03:31
                    Total      HTTP       HTTPS      HTTP2      SMTP       SMTPS
IMAP       IMAPS     SMB
  File scanned:      0          0          0          0          0          0
0          0         0
```

```
  Virus found:       0          0          0          0          0          0
0          0         0
  Virus blocked:     0          0          0          0          0          0
0          0         0
  Virus permitted:   0          0          0          0          0          0
0          0         0
```

You can ensure that the flow-based antivirus policy and ML-based threat detection are up-to-date, even without an Internet connection

If you want to install a new package, delete the existing phase and eclipse directories from your server and repeat the steps.

3

PART

Configuration Statements and Operational Commands

CHAPTER 7

SRX Series Firewall Commands to Configure Juniper ATP Cloud

IN THIS CHAPTER

SRX Series Firewall Commands to Configure Juniper ATP Cloud

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

Use the below configuration statements and operational commands to configure, monitor, and manage Juniper ATP Cloud features in SRX Series Firewalls and vSRX Virtual Firewall instances.

Table 14: Configuration Statements

Statement	Description
advanced-anti-malware connection	Check and verify the status of connection to the cloud server from the SRX Series Firewall.
advanced-anti-malware policy	Configure the Juniper ATP Cloud policy.
advanced-anti-malware traceoptions	Trace the Juniper ATP Cloud configuration for troubleshooting.
application-services (security-metadata-streaming)	Enable security metadata streaming-policy on SRX Series Firewall.

Table 14: Configuration Statements *(Continued)*

Statement	Description
anti-virus	Configure flow-based antivirus policy.
category (Security Logging)	Set the category of logging.
dns-filtering	Configure DNS filtering to identify DNS requests for disallowed domains
dynamic-filter	Configure dynamic filtering options for security metadata streaming policy on SRX Series Firewalls.
security-intelligence(services)	Configure SecIntel profiles and policies to work with SecIntel feeds, such as infected hosts and C&C.
security-intelligence	Add source and destination addresses to the SecIntel profiles.
security-metadata-streaming	Configure security metadata streaming policy on SRX Series Firewalls.

Table 15: Operational Commands

Command	Description
clear services advanced-anti-malware statistics	Set the AAMW statistics to 0.
clear services dns-filtering cache	Clear all entries in the DNS cache.
clear services security-metadata-streaming	Set the DNS and HTTP security-metadata-streaming statistics to 0.
clear services security-intelligence dns-statistics	Set DNS statistics to 0.

Table 15: Operational Commands *(Continued)*

Command	Description
request services advanced-anti-malware data-connection	Test the connection between the SRX Series Firewall and the Juniper ATP Cloud by initiating a web socket connection and then sending data payloads of a given size.
request services advanced-anti-malware diagnostic	Verify your Internet connection to the cloud before enrolling your SRX Series Firewall with Juniper ATP Cloud.
request services advanced-anti-malware redirect-file	Add a customized file for users to be directed to.
request services anti-virus update	Trigger antivirus database update immediately.
show services advanced-anti-malware policy	Verify the policy on the SRX Series Firewall for debugging purposes
show services advanced-anti-malware profile	Verify you are sending the correct files to the cloud during troubleshooting.
show services advanced-anti-malware statistics	Displays the Juniper ATP Cloud statistics, such as total number of sessions processed and number of sessions blocked.
show services advanced-anti-malware status	Displays the connection status between the Juniper ATP Cloud service and the SRX Series Firewall.
show services advanced-anti-malware dynamic-filter status	Displays the connection status between the Juniper ATP Cloud service and the SRX Series Firewall.
show services anti-virus statistics	Displays the statistics of antivirus database.
show services dns-filtering cache	Show all entries within the DNS cache.

Table 15: Operational Commands *(Continued)*

Command	Description
show security dynamic-address	Displays information about dynamic addresses.
show services security-metadata-streaming	Displays the statistics of security metadata streaming sessions for HTTP and DNS protocols, and allowlist servers that are configured by the users for HTTP protocol.
show security flow session advanced-anti-malware	Display information about all currently active AAMW sessions on the device
show services security-intelligence dns-statistics	Displays the DNS profile statistics.
show services security-intelligence update status	Display the status of the connection with Policy Enforcer.
show services security-intelligence category summary	Displays the status of security profiling feeds.
show services security-intelligence	Display summary for the specified SecIntel category.

4

PART

Use Cases

CHAPTER 8

SecIntel Feeds for MX Series Routers

IN THIS CHAPTER

Configure SecIntel Feeds for MX Series Routers

IN THIS SECTION

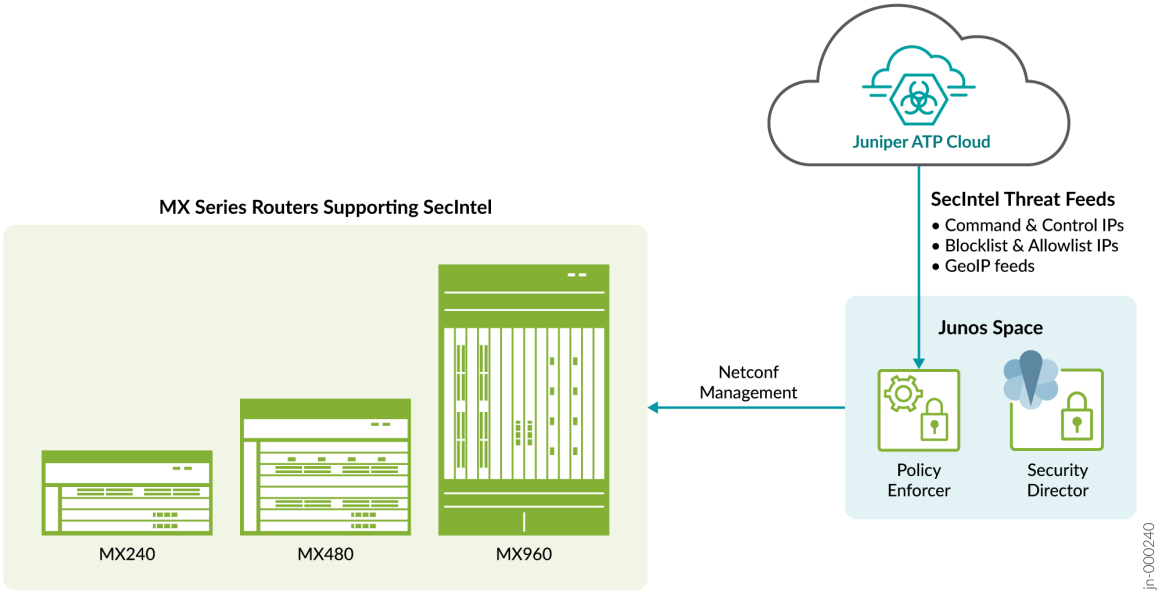
Overview

SecIntel provides carefully curated, verified threat intelligence from Juniper ATP Cloud to MX Series routing platforms, blocking command-and-control (C&C) communications to and from malicious IPs at unparalleled line rate.

With SecIntel and MX Series router integration, you can:

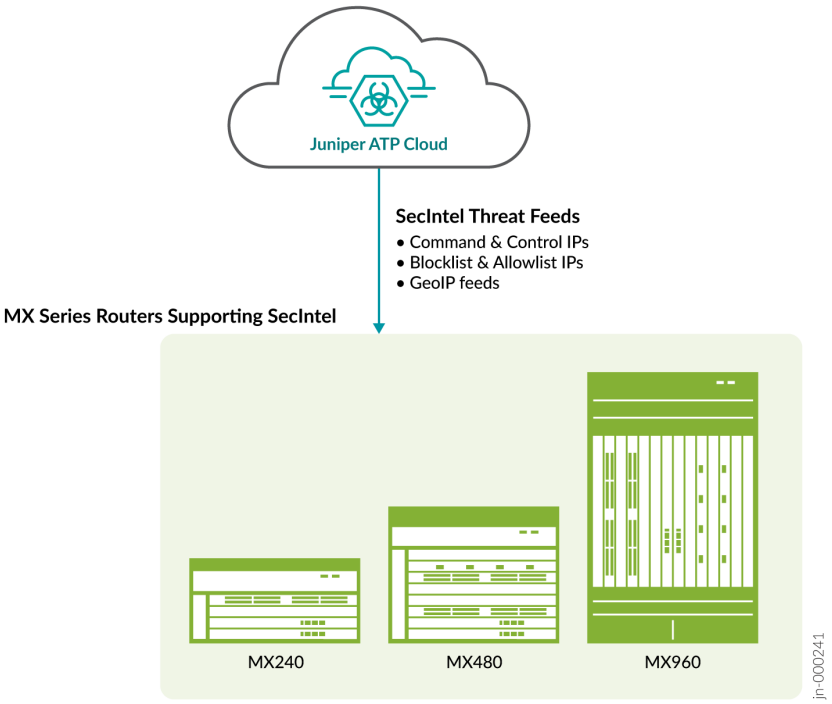
- Detect and block known malicious IPs, infected C&C hosts, and DDoS attacks.
- Sinkhole malicious DNS requests.
- Enable customer IP threat feeds.

Starting in Junos OS 19.3R1 and later releases, SecIntel feeds are supported on MX240, MX480, and MX960 routers with the use of Policy Enforcer.



Starting in Junos OS 22.1R1 and later releases, SecIntel feed on the MX devices include GeoIP filtering as well as direct enrollment option to Juniper ATP Cloud.

Direct Enrollment to Juniper ATP Cloud is supported on MX240, MX480, and MX960 routers.



For more information, see Juniper SecIntel on MX.

Benefits

With SecIntel and MX Series router integration, you can:

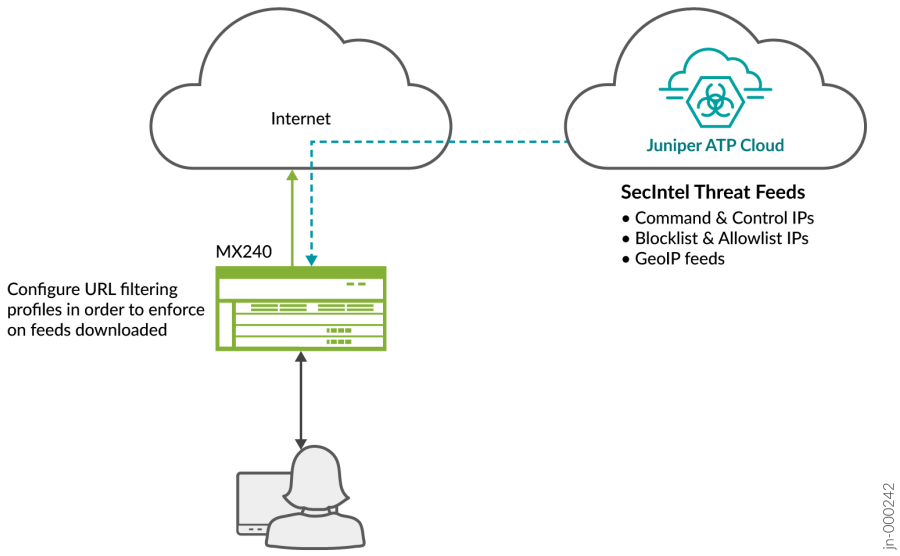
- Shut down attacks before they start.
- Protect users, applications, and infrastructure from compromise—including subscribers.
- Turn connectivity layers into security layers without additional infrastructure.

Use Case 1: Direct Enrollment to Juniper ATP Cloud

In earlier releases, MX Series routers downloaded SecIntel feeds through Junos Space Security Director/ Policy Enforcer. Starting in Junos OS Release 22.1R1, MX Series routers can download global SecIntel feeds directly from Cloud Feeds without enrolling to Juniper ATP Cloud.

In this use case, we'll see how to enroll an MX Series router to Juniper ATP Cloud without connecting to Junos Space Security Director or Policy Enforcer.

Topology



Prerequisites

- Juniper SecIntel for MX Series Universal Router license (-S-MXxxx-CSECINTELx).

Workflow

1. Get a SecIntel license from Juniper for your MX Series Universal Router. For MX Series Universal Router licenses, see Software Licenses for MX Series Routers and MPC Service Cards. You will need the Software Serial Number (SSRN).

2. Enroll the MX Series router to Juniper ATP Cloud.

3. Verify the feeds from Juniper ATP Cloud.

4. Implement filtering configuration to enforce the downloaded feeds.

Configurations required on MX Series router

- Enrollment script
- Filter configuration

You can only configure US region cloud feed endpoint. All the MX cloud feed request are served only from US region CF.

Software Support Reference Number (SSRN) is a software serial number provided on the fulfillment document which ships electronically following the purchase of your Juniper software license.

If the license has already been installed for your software, the Software Support Reference Number (SSRN) might be obtained by running the `show system license` command. The SSRN is included as the first 12 numerical digits of the 'Software Serial Number' listed in JUNOS.

Some products will report their SSRN in the below format, which creates a unique identifier for each software instance purchased. In this scenario, remove the suffix letters, which will leave the actual numeric SSRN to be used for support entitlement purposes.

```
> show system license
Software Serial Number: XXXXXXXXXXXX-abcdef
Support Reference Number:  XXXXXXXXXXX
```

To receive feeds from Cloud feeds, first enroll the MX Series router with Juniper ATP Cloud. Sample command to enroll is:

```
rootuser> op url https://amer.sky.junipersecurity.net/v2/skyatp/ui_api/bootstrap/enroll/
secintel/mx/mx-secintel.slax
version 21.3XYZ is valid for bootstrapping.
Please provide the Juniper SecIntel license SSRN or press 0 to cancel
Secintel license SSRN: XXXXXXXXXXXXXXX
```

To remove the SecIntel configuration from MX Series router, you must dis-enroll the device. Sample command to dis-enroll is:

```
rootuser> op url https://amer.sky.junipersecurity.net/v2/skyatp/ui_api/bootstrap/disenroll/
secintel/mx/mx-secintel.slaxversion 21.3XYZ is valid for bootstrapping.
```

```
Please provide the activation code or press 0 to cancel
SSRN: XXXXXXXXXXXXXXX
```

The following global SecIntel feeds are available for MX series routers:

- cc_ip_data
- cc_ipv6_data
- cc_ip_blocklist
- geoip_country
- geoip_country_ipv6

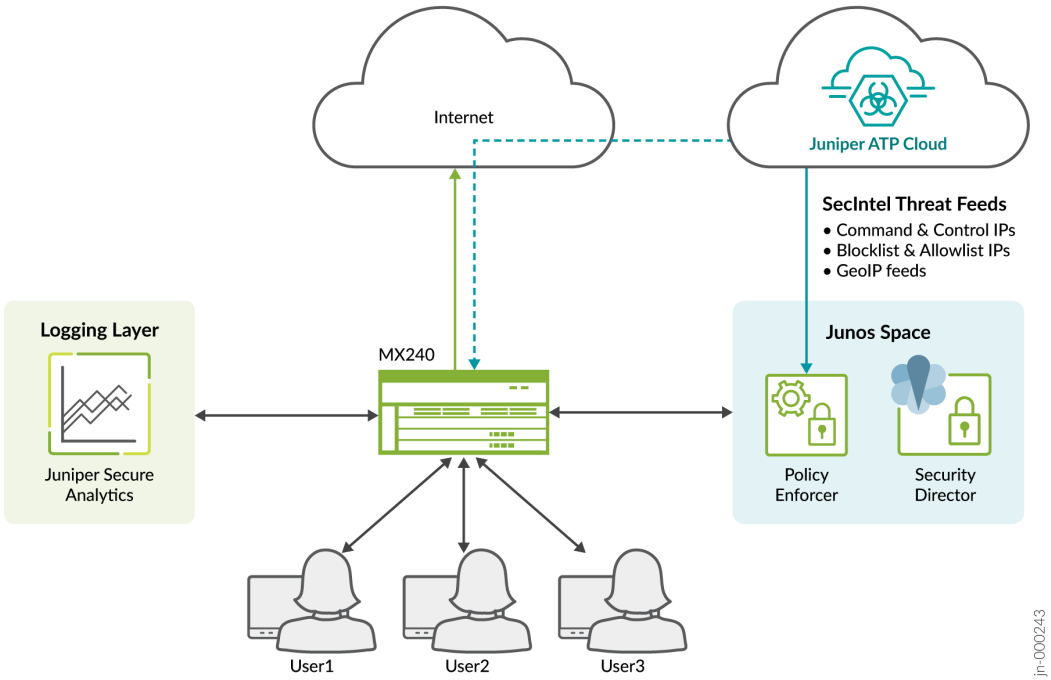
Benefits

- No complex setup using Junos Space SD or PE.
- Simple configuration to enforce downloaded feeds.

Use Case 2: Enrollment to Juniper ATP Cloud Using Junos Space Security Director and Policy Enforcer.

In this use case, we'll see how to enroll an MX Series router to Juniper ATP Cloud using Junos Space Security Director and Policy Enforcer.

Topology



Workflow

- Configuration of Junos Space Security Director and Policy Enforcer.
- Discovery of MX Series router in Junos Space added as a device in Threat Protection Fabric (This is enrollment process for MX Series router to Policy Enforcer).
- License requirements (Reach out to Juniper Sales / Account Team).

Configuration required on MX Series router and SD/PE

- Custom feed configuration in SD.
- Understanding how feeds are applied on MX Series router.
- Filter configuration on MX Series router.

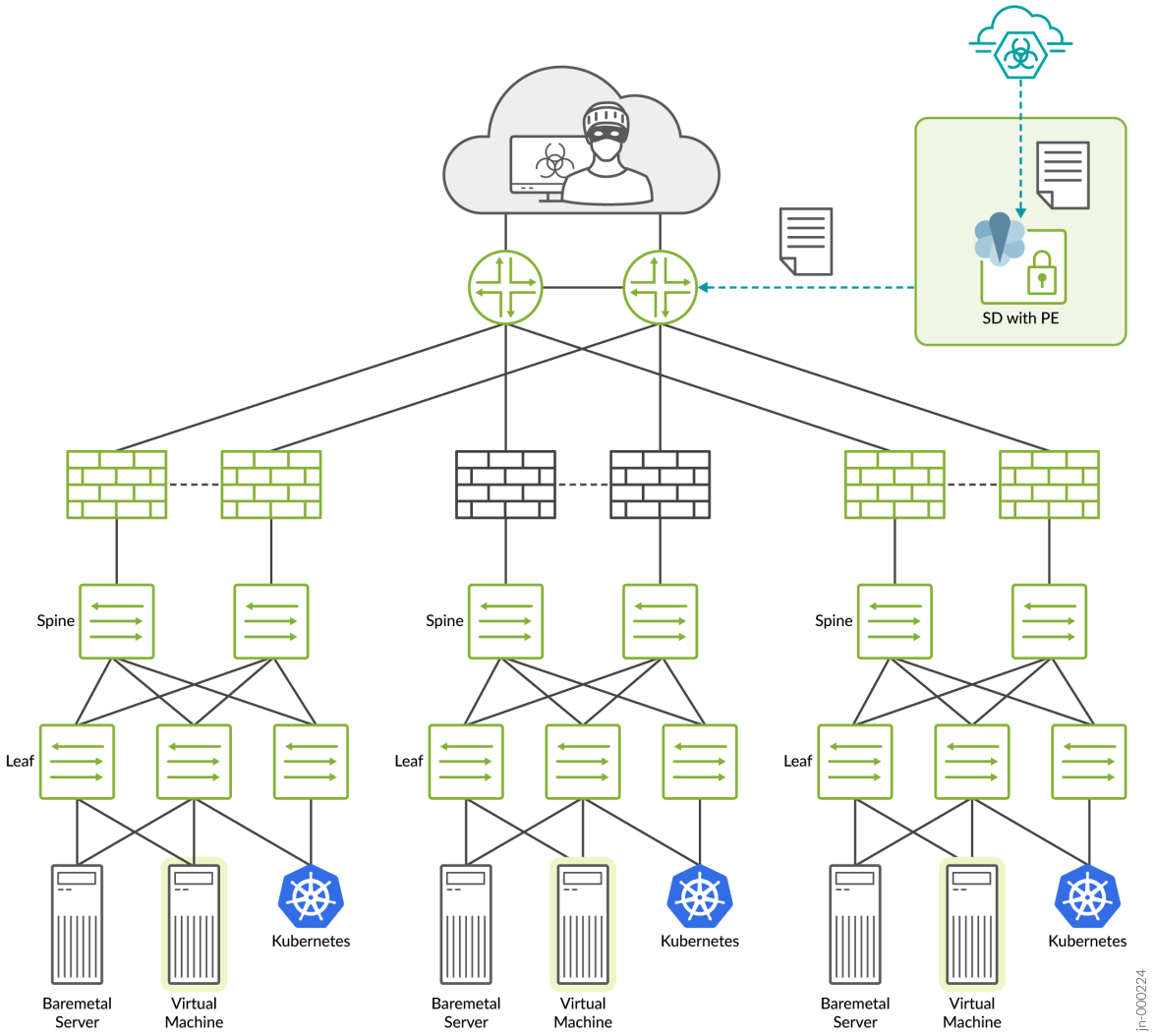
Benefits

- Feeds can be customized for each customer's serviced by a VRF on the service providers router.
- All threat mitigation are processed at line rate improving performance.

Use Case 3: Identify and Block Command-and-Control Traffic on MX Series Router

In this use case, we'll see how to block C&C traffic at the network edge in a connected security setup. Here, the client is trying to reach a C&C server and the MX router is used to block the traffic.

Topology



Configurations required on MX Series router and SD/PE

- Juniper ATP Cloud C&C feed and Security Director with Policy Enforcer.
- Juniper MX Series router

Workflow

1. Policy Enforcer downloads C&C feed from Juniper ATP Cloud.
2. Juniper MX Series router downloads C&C feed from Policy Enforcer.
3. Juniper MX Series router adds IP data to Ephemeral DB filter.

4. Juniper MX Series router drops traffic to/from C&C servers listed in C&C feed, protecting against Botnets & Malware.
5. Juniper MX Series router offloads C&C protection from firewalls that are under load or cannot support C&C feeds.

For configuration details, see SecIntel on MX Demo.

CHAPTER 9

Amazon Web Services GuardDuty with vSRX Virtual Firewall

IN THIS CHAPTER

Integrate AWS GuardDuty with vSRX Virtual Firewall

IN THIS SECTION

Solution Overview

AWS GuardDuty is a continuous security monitoring service that identifies unexpected, potentially unauthorized, and malicious activity within your AWS environment. The threats detected by AWS GuardDuty are sent as security feeds to the vSRX in the your AWS environment. The vSRX can access the feeds in two ways:

- Directly downloading the feeds from the AWS S3 bucket
- The feeds are pushed to the firewall device along with the ATP Cloud security intelligence (SecIntel) feeds, if the firewall device is enrolled with Juniper ATP Cloud.

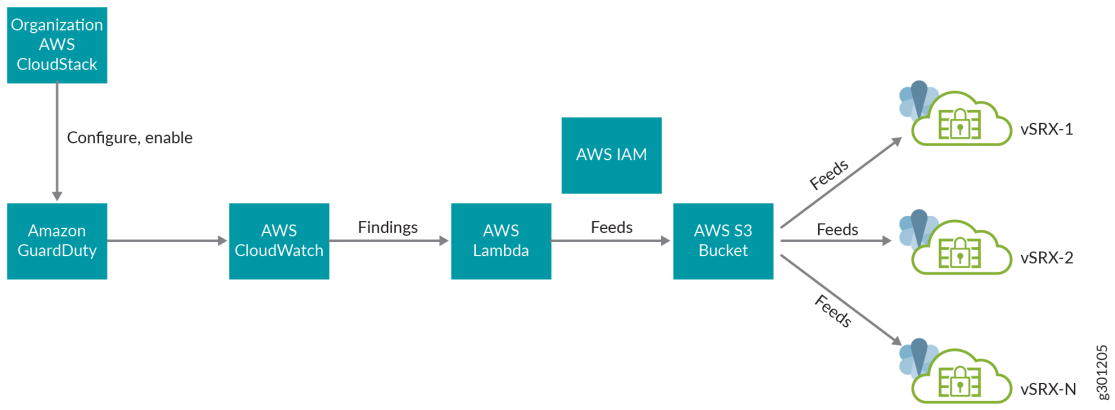
In turn, the vSRX enables you to take actions on the feed and block or log connections to the threat sources identified in the feed. For more information about AWS components, see AWS Documentation.

The deployment scenarios that are supported in this solution are:

- Direct Integration of AWS GuardDuty with vSRX

You don't need a Juniper ATP Cloud license for this deployment. The threat feeds from AWS GuardDuty are processed through the AWS Lambda function and then stored in the AWS S3 bucket. You must configure, and deploy the AWS Lambda function. Once deployed, the Lambda function translates the data from AWS GuardDuty findings into a list of malicious IP addresses and URLs. The resultant list is stored in a configured AWS S3 bucket in the format that can be ingested by the vSRX. You must configure vSRX to periodically download the threat feeds from the AWS S3 bucket. You must also ensure that IDP signature package is already available on your firewall device for the traffic to hit SecIntel policy.

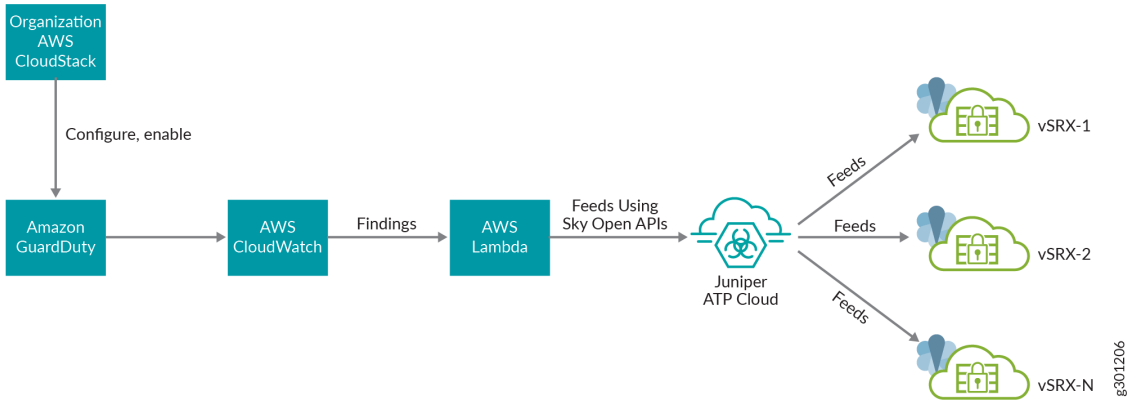
Figure 13: Direct Ingestion of threat feeds by vSRX Virtual Firewall



- Integration of AWS GuardDuty with vSRX using ATP Cloud

  You must install a Juniper ATP Cloud license on your SRX Series Firewalls and vSRX for this deployment. For more information, see Software Licenses for ATP Cloud. The threat feeds from AWS GuardDuty are processed through the AWS Lambda function. You must configure and deploy the Lambda function and enable ATP Cloud on your vSRX. The AWS Lambda function sends the threat feed to ATP Cloud (upload feeds to C&C category) using OpenAPIs. The threat feeds are pushed to all enrolled vSRX along with the ATP Cloud SecIntel feeds.

Figure 14: Ingestion of threat feeds through ATP Cloud



Workflow to Integrate AWS GuardDuty with vSRX Virtual Firewall

IN THIS SECTION

Retrieve Necessary Files from GitHub Repository

To retrieve necessary files:

1. Navigate to GitHub repository https://github.com/Juniper/vSRX-AWS.
2. Click the **Code** drop-down list.
3. Click **Download ZIP**.

   The vSRX-AWS-master.zip file is downloaded onto your system. You will need the manifest.xml and cc_schema files found within the SRX-GD-Threatfeed folder.

Configure S3 Bucket

This step is required only if the threat feeds are directly ingested by vSRX Virtual Firewall. You need not configure S3 bucket if the ingestion of threat feeds is through ATP Cloud.

1. Log in to your AWS Management console, navigate to the **Create Bucket** page.
2. Assign a name and a region to the S3 Bucket.
3. Uncheck the **Block all public access** option.
4. Leave the remaining options in the default states and click **Create bucket**.

   The green alert at the top confirms our new bucket.
5. Click the newly created bucket to view more options.
6. Under the **Objects** tab, we'll upload the two files we retrieved earlier by clicking **Upload** and then **Add Files**.
7. Navigate to the cc_schema and manifest files and then click **Upload**.
8. Select the two files, now listed on the Objects tab, and then click the **Actions** drop-down list.
9. Choose **Make Public**.

   This action enables anyone to access and read the files.
10. Click **Make Public**.

BEST PRACTICE:

- Make a note of the S3 bucket name for future references.
- The S3 bucket access must always be public so that the SRX Series Firewall can download the files and feed from the S3 bucket.
- Configure the S3 bucket such that download or read operation does not require any API keys.
- Write access on S3 bucket is only available with the Lambda function.
- For S3 configuration details, see Setting up Amazon S3.

Configure GuardDuty

GuardDuty findings can be exported to either S3 bucket or CloudWatch events. In this solution we export the findings to CloudWatch events. Eventually CloudWatch events rule will trigger Lambda Function to convert findings into a compatible format with vSRX Virtual Firewall and push to AWS S3 bucket.

To configure AWS guardduty:

1. Log in to your AWS account.

2. Click **Services** tab and search for **GuardDuty**.
3. Select **GuardDuty** service.

   The GuardDuty Findings page appears displaying the list of events that are generated by GuardDuty.
4. Click **Settings** in the left pane.

   The About GuardDuty page appears.
5. In **Finding export options** section, select the frequency for updated findings. The available options are:

   - Update CWE and S3 every 6 hours (default)
   - Update CWE and S3 every 1 hour
   - Update CWE and S3 every 15 minutes
6. Choose an option and click **Save**.

   Based on the frequency that you have selected, the GuardDuty service generates events at regular intervals and share the events with Cloud Watch Events (CWE) Service.

Configure Lambda Function

AWS Lambda function uploads GuardDuty findings to ATP Cloud using the ATP Cloud OpenAPI. Lambda function updates the AWS S3 bucket with feed information in the standard SRX manifest file format. Lambda must be configured with the application token generated per organization in the ATP Cloud Web Portal. The threat feed is available under the C&C category.

To create Lambda function:

1. Navigate to **Services > Lambda**.
2. Click **Create Function.**
3. Assign a name to the Lambda function.
4. Choose the Runtime language the function will be written in. for example, **Runtime python 3.6**.
5. In the Execution role section, choose **Use an existing role**.
6. In the Existing role drop-down list, select the **guardduty-lambdarole-test** option.

   Open the link that now appears below the drop-down list to review the role details.

   NOTE: You must provide an appropriate Identity and Access Management (IAM) role. Create a new IAM role and assign the role to the Lambda function. This enables Lambda function to upload or write/read objects to/from the S3 bucket. For more information, see Create an IAM user
7. With the role details in order, return to the Lambda page and click **Create Function**.
8. To upload a Lambda file.

a. Log in to GitHub repository https://github.com/Juniper/vSRX-AWS, navigate to **SRX-GD-ThreatFeed** folder, and download the **SRX-GD-ThreatFeed.zip** lambda file.

b. Navigate to **Lambda > Functions > your_lambda_function_name**.

c. Click **Actions > Upload a .zip file**. Upload **SRX-GD-ThreatFeed.zip** file from Function code section.

d. Click **OK**.

The Lambda configurations are displayed in the Environment variables section. Follow the guidelines in Table 16 on page 141 to configure Lambda.

9. Configure Lambda function.

a. Navigate to **Lambda > Functions > *your_lambda_function_name* > Edit Environment variables**.

b. Complete the configurations according to guidelines provided in Table 16 on page 141.

Table 16: AWS Lambda Configurations

Parameters	Description
MAX_ENTRIES	Defines the maximum number of entries that will be retained in the corresponding data file. Older entries will expire once this limit is reached. Default value: 10000 Range:1000-100000 Example: 1000
IP_FEED_NAME	Defines the CC IP feed name, which is also the key name for S3 data file. If there is a False Alarm entry that needs to be removed; you must manually delete it from the corresponding key derived from IP_FEED_NAME parameter. Example: custom_cc_(content_type)_data
DNS_FEED	Defines the CC DNS feed name, which is also the key name for S3 data file. If there is a False Alarm entry that needs to be removed; you must manually delete it from the corresponding key derived from DNS_FEED parameter. Example: custom_cc_dns_(content_type)_data

Table 16: AWS Lambda Configurations *(Continued)*

Parameters	Description
S3_BUCKET	Name of S3 Bucket. The bucket name is used in S3 URL name as well. Example: guardduty-integration-test
SEVERITY_LEVEL	Level beyond which AWS Guardduty event IPs/URLs are added to the feed file. **NOTE**: Severity Level maps one-to-one with ATP Cloud Threat Levels. Default value: 8 Range: 1-10 Example: 4
SKY_APPLICATION_TOKEN	Used to upload entries into the ATP Cloud OpenAPI. You must log in to Juniper ATP Cloud Web Portal and generate the application token. You must have at least one device configured with premium license to generate the application token. For more information, see Software Licenses for ATP Cloud. Example: TOKEN_VALUE
SKY_OPENAPI_BASE_PATH	Base path for the Sky Open APIs, which are used to upload feeds from Lambda function to ATP Cloud. Example: https://threat-api.sky.junipersecurity.net/v1/cloudfeeds
FEED_TTL	Use the Time to Live (TTL) to specify the number of days for the feed to be active. The feed entries will expire on SRX Series Firewall if it is not updated within the TTL. Default value: 3456000 Range: 86400-31556952
FEED_UPDATE_INTERVAL	Update interval for the feeds. Default value: 300 Range: 300-86400

NOTE:

- In case of **Direct Ingestion of threat feeds by vSRX firewalls**, you need not define SKY_APPLICATION_TOKEN and SKY_OPENAPI_BASE_PATH parameters. If these parameters are not configured, the feeds are directly uploaded to AWS S3 bucket.
- In case of **Ingestion of threat feeds through ATP Cloud**, you must define SKY_APPLICATION_TOKEN and SKY_OPENAPI_BASE_PATH parameters. These parameters must be configured to upload the feeds from AWS Lambda to ATP Cloud. You need not define S3_BUCKET parameter.

10. Configure time-out settings. Navigate to **Lambda > Functions > your_lambda_function_name > Basic settings** and update **Timeout** to 10sec.
11. Click **Save**.

Configure CloudWatch

Create rules and specify the event source (GuardDuty) and event target (Lambda function).

To create rules:

1. Select **Events > Rules**.

   The Rules page appears.
2. Click **Create Rule**.
3. Under Event Source section, select the service name as **GuardDuty** and event type as **GuardDuty Finding**.
4. In the Targets section, click **Add Targets** and ensure the Lambda function is selected.

   By specifying GuardDuty and the Lambda function as the event source and target, the CloudWatch Logs Insights will allow you to search and analyze your logs.
5. Click **Configure Details**.
6. On the Rule Definition page, specify a name for the rule.
7. Click **Create Rule**.

Configure Direct Integration of vSRX Virtual Firewall with AWS GuardDuty

The following section lists the CLI configurations that are required on vSRX Virtual Firewall.

This example configures a profile name, a profile rule and the threat level scores. Anything that matches these threat level scores is considered malware or an infected host. The ATP Cloud threat level maps one-to-one with the Severity Level in AWS GuardDuty.

NOTE: You can change the severity level in AWS GuardDuty anytime, but the severity level must always match the threat level that you configure on your vSRX Virtual Firewall.

To configure vSRX Virtual Firewall with AWS GuardDuty (without using ATP Cloud):

1. Open a console window and log in to the vSRX Virtual Firewall.

   login as: root@user-vsrx

   % cli

2. Issue the show configuration command to view the existing SecIntel details.

   root@user-vsrx> show configuration | display set | match security-intel

3. Ensure that the IDP security package is downloaded to your vSRX Virtual Firewall. To manually download and install the IDP security package from the Juniper Security Engineering portal, use the following command

   root@user-vsrx> request security idp security-package download

```
Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3383(Tue May 18 14:38:22 2021 UTC, Detector=12.6.180210326)
```

   root@user-vsrx> request security idp security-package download status

```
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:2014(Thu Oct 20 12:07:01 2011, Detector=11.6.140110920)
```

   root@user-vsrx> request security idp security-package install

```
Done;Attack DB update : successful - [UpdateNumber=3383,ExportDate=Tue May 18
14:38:22 2021 UTC,Detector=12.6.180210326]
Updating control-plane with new detector : successful
Updating data-plane with new attack or detector : not performed due to no
active policy configured.
```

   root@user-vsrx> request security idp security-package install status

```
Done; policy-template has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xsl)!
```

4. Enter configuration mode.

   ```
   root@user-vsrx> configure
   ```

5. Configure security intelligence URL.

   root@user-vsrx# set services security-intelligence url https://guardduty-integration-test.s3-us-west-2.amazonaws.com/manifest.xml

6. Configure security intelligence profile and policy. In this example the profile name is `secintel_profile` and threat levels 8 and above are blocked.

   ```
   root@user-vsrx# set services security-intelligence profile secintel_profile category CC
   root@user-vsrx# set services security-intelligence profile secintel_profile rule
   secintel_rule match threat-level 8
   root@user-vsrx# set services security-intelligence profile secintel_profile rule
   secintel_rule match threat-level 9
   root@user-vsrx# set services security-intelligence profile secintel_profile rule
   secintel_rule match threat-level 10
   root@user-vsrx# set services security-intelligence profile secintel_profile rule
   secintel_rule then action block drop
   root@user-vsrx# set services security-intelligence profile secintel_profile rule
   secintel_rule then log
   root@user-vsrx# set services security-intelligence policy secintel_policy CC
   secintel_profile
   ```

7. Configure a security policy and assign the security intelligence policy to the security policy.

   root@user-vsrx# set security policies from-zone trust to-zone untrust policy 1 match source-address any

   root@user-vsrx# set security policies from-zone trust to-zone untrust policy 1 match destination-address any

   root@user-vsrx# set security policies from-zone trust to-zone untrust policy 1 match application any

   root@user-vsrx# set security policies from-zone trust to-zone untrust policy 1 then permit application-services security-intelligence-policy secintel_policy

8. Run the **request services security-intelligence download status** command to check the SecIntel feed download status.

   root@user-vsrx# request services security-intelligence download status

   ```
   Security intelligence feed download status:
   Start time:Thu Feb 4 20:46:13 2021
   Start downloading the latest manifest.
   ```

```
Start parsing manifest file.
Parse manifest succeeded, version: fd36ca761080aa10910763a8ee0d6104.
Start handling new category: CC.
Start downloading schema of category CC.
Start parsing schema of category CC.
...
End time:Thu Feb 4 20:46:14 2021
```

The vSRX Virtual Firewall has started checking for both DNS and IP Feeds for the CC category, which we configured earlier with the Lambda function.

9. Run the following command to display the details for the SecIntel category.

   root@user-vsrx# show services security-intelligence category detail category-name CC feed-name cc_guardduty_ip count 10 start 0 all-logical-systems-tenants

```
Category name :CC
  Feed name   :cc_guardduty_ip
  Version     :N/A
  Objects number:320
  Create time :02-04 20:26:08 PST
  Update time :02-04 20:46:14 PST
  Update status :Store succeeded
  Expired     :No
  Options     :N/A
```

10. Issue the **run show security dynamic-address category-name CC** command to view the matching entries.

```
No.   IP-start         IP-end              Feed     Address
1     10.0.210.98      10.0.210.98          CC/1     ID-fffc081a
2     10.1.238.97      10.1.238.97          CC/1     ID-fffc081a
3     10.53.88.149     10.53.88.149         CC/1     ID-fffc081a
4     10.54.200.84     10.54.200.84         CC/1     ID-fffc081a
5     10.55.105.189    10.55.105.189        CC/1     ID-Iffc081a
6     10.80.62.249     10.80.62.249         CC/1     ID-fffc081a
7     10.87.149.74     10.87.149.74         CC/1     ID-fffeesia
8     10.171.46.235    10.171.46.235       CC/1     ID-fffc081a
9     10.177.144.242   10.177.144.242      CC/1     ID-fffc081a
...
Instance default Total number of matching entries: 65
```

We can see from the IP addresses that the vSRX Virtual Firewall is receiving the feeds and has been directly integrated with AWS GuardDuty.

To check the security intelligence statistics, use the **show services security-intelligence statistics** command.

```
> show services security-intelligence statistics
Logical system: root-logical-system
Category CC:
  Profile secintel_profile:
    Total processed sessions: 0
    Permit sessions:          0
    Block drop sessions:      0
    Block close sessions:     0
    Close redirect sessions:  0
```

Configure vSRX Virtual Firewall with AWS GuardDuty using ATP Cloud

To configure vSRX Virtual Firewall with AWS GuardDuty using ATP Cloud:

1. Install ATP Cloud license.
2. Enroll vSRX Virtual Firewall to ATP Cloud. See Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal.

   root@user-vsrx# request services advanced-anti-malware enroll https://amer.sky.junipersecurity.net/v2/skyatp/ui_api/bootstrap/enroll/HASH/HASH.slax

   The enrollment script will generate the aamw-ssl tls profile, which will be used in the Step 3.
3. Configure security intelligence URL.

   set services security-intelligence url https://cloudfeeds.argonqa.junipersecurity.net/api/manifest.xmlset services security-intelligence authentication tls-profile aamw-ssl
4. Configure security intelligence profiles and policies. In this example the profile name is `secintel_profile` and threat level 8 and above are blocked.

   set services security-intelligence profile secintel_profile category CC

   set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 8

   set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 9

   set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 10
   set services security-intelligence profile secintel_profile rule secintel_rule then action block drop

   set services security-intelligence profile secintel_profile rule secintel_rule then log

set services security-intelligence profile ih_profile category Infected-Hosts

set services security-intelligence profile ih_profile rule ih_rule match threat-level 8

set services security-intelligence profile ih_profile rule ih_rule match threat-level 9

set services security-intelligence profile ih_profile rule ih_rule match threat-level 10

set services security-intelligence profile ih_profile rule ih_rule then action block drop

set services security-intelligence profile ih_profile rule ih_rule then log

set services security-intelligence policy secintel_policy Infected-Hosts ih_profile

set services security-intelligence policy secintel_policy CC secintel_profile

5. Configure a security policy and assign the security intelligence policy to the security policy.

   set security policies from-zone trust to-zone untrust policy 1 then permit application-services security-intelligence-policy secintel_policy

   commit

To check the security-intelligence status, use the `show services security-intelligence update status` command.

```
show services security-intelligence update status
Current action :Downloading feed cc_ip_data (20200330.35) in category CC.
Last update status :Feed cc_ip_data (20200330.4) of category CC not changed
Last connection status:succeeded
Last update time :2020-03-30 14:42:05 PDT
```

To check the security intelligence statistics, use the `show services security-intelligence statistics` command.

```
> show services security-intelligence statistics
Logical system: root-logical-system
Category Whitelist:
Profile Whitelist:
Total processed sessions: 337
Permit sessions: 0
Category Blacklist:
Profile Blacklist:
Total processed sessions: 337
Block drop sessions: 0
Category CC:
```

```
Profile secintel_profile:
Total processed sessions: 337
Permit sessions: 0
Block drop sessions: 337
Block close sessions: 0
Close redirect sessions: 0
Category Infected-Hosts:
Profile ih_profile:
Total processed sessions: 0
Permit sessions: 0
Block drop sessions: 0
Block close sessions: 0
Close redirect sessions: 0
```

No additional configuration is required in ATP Cloud Web portal when the vSRX Virtual Firewall is integrated with ATP Cloud. All settings, including the SecIntel configuration, is automatically created while enrolling the vSRX Virtual Firewall with ATP Cloud.

Use case for AWS GuardDuty

In this example, let us configure the vSRX Virtual Firewall to download the threat feeds.

1. Log in to the vSRX Virtual Firewall.

   login as: root@user-vsrx

   % cli
2. Issue the show configuration command to view the existing SecIntel details.

   root@user-vsrx> show configuration | display set | match security-intel
3. Enter configuration mode.

   root@user-vsrx> configure
4. Configure the SecIntel URL on the SRX Series Firewall:

   root@user-vsrx> set services security-intelligence url *guardduty-url*
5. Commit the configuration.

   root@user-vsrx> commit
6. Run the **cat /var/db/secinteld/tmp/manifest.xml** from shell and verify if the manifest file is downloaded successfully.
7. If it is not then run the following command

   root@user-vsrx> request services security-intelligence download
8. Verify if the manifest file is downloaded successfully.
9. Once the manifest file is downloaded, run the following commands.

root@user-vsrx> show services security-intelligence category detail category-name CC feed-name *feed_name_gd*

```
Category name   :CC
  Feed name     :cc_guardduty_ip
  Version       :20210518.142
  Objects number:974
  Create time   :2021-05-18 10:01:06 PDT
  Update time   :2021-05-18 10:33:23 PDT
  Update status :Store succeeded
  Expired       :No
  Options       :N/A
```

10. Run the following command from CLI to check if the feed is present under the dynamic address:

    root@user-vsrx> show security dynamic-address category-name CC

```
No.     IP-start            IP-end              Feed          Address
1       1.0.210.98          1.0.210.98          CC/1          ID-
fffc081a
2       1.1.153.43          1.1.153.43          CC/1          ID-
fffc081a
3       1.1.201.151         1.1.201.151         CC/1          ID-
fffc081a
4       1.1.238.97          1.1.238.97          CC/1          ID-
fffc081a
5       1.4.157.88          1.4.157.88          CC/1          ID-
fffc081a
6       1.4.205.9           1.4.205.9           CC/1          ID-fffc081a
```

11. Pick any IP address from the list, for example, 1.0.210.98 and run a ping test from the client and verify that the secintel CC block drop counters are incrementing.

    You should be able to get a response for the ping. Make sure you verify the traffic passing from the client is hitting the SecIntel policy on the SRX Series Firewall.

NOTE: IDP signature package is required for the traffic to hit SecIntel policy, please run the **request security idp security-package download** command if you do not have the signature package already.

Run the **root@user-vsrx> show security flow session source-prefix *Client_IP*** command.

```
show services security-intelligence statistics

Logical system: root-logical-system
Category Whitelist:
  Profile Whitelist:
    Total processed sessions: 38
    Permit sessions:          0
Category Blacklist:
  Profile Blacklist:
    Total processed sessions: 38
    Block drop sessions:      0
Category CC:
  Profile secintel_profile:
    Total processed sessions: 38
    Permit sessions:          0
    Block drop sessions:      18
    Block close sessions:     0
    Close redirect sessions:  0
```

CHAPTER 10

Juniper ATP Cloud with Policy Enforcer

IN THIS CHAPTER

How to Enroll Your SRX Series Firewalls in Juniper ATP Cloud Using Policy Enforcer

SUMMARY

This section provides step-by-step instructions to enroll SRX Series Firewalls in Juniper ATP Cloud using the Guided Setup wizard in Policy Enforcer.

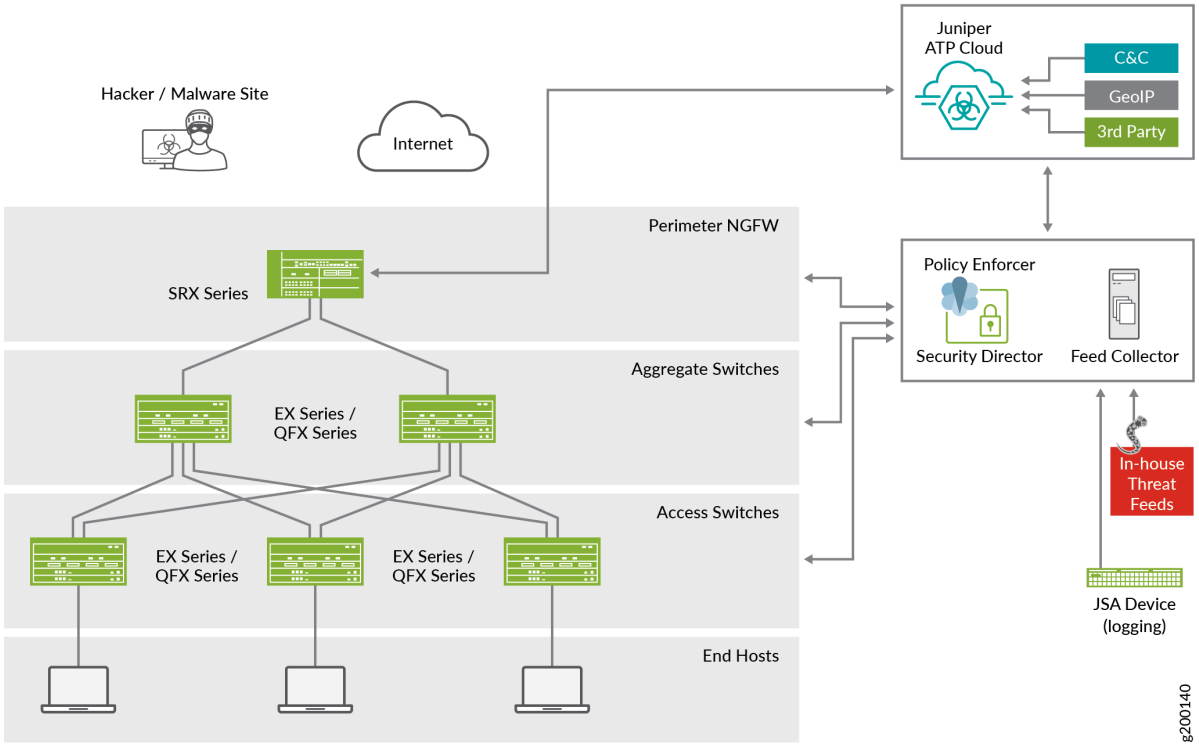
IN THIS SECTION

Solution Overview

IN THIS SECTION

Figure 15 on page 153 shows a high-level workflow of how Policy Enforcer, Security Director, Juniper ATP Cloud, and Junos OS devices interact to provide a secure network deployment with Juniper Connected Security.

Figure 15: Juniper Connected Security Solution Components



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

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

SRX Series Firewalls provide security enforcement and deep inspection across all network layers and applications. In the context of the Juniper Connected Security solution, SRX Series Firewalls 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 automatically updates policies and deploys 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 addresses, allowing tracking and continued blocking of the host even if it moves to another switch or access point (AP) on the network.

When these components works 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.

Benefits

The Guided Setup wizard in Policy Enforcer is a one-stop shop to get your Juniper Connected Security solution up and running in one go. It is also the most efficient way to complete your Juniper ATP Cloud configurations with Juniper Connected Security because it simplifies security policy creation, threat detection, and security policy enforcement across your network.

Before You Begin

- Install and configure Security Director. See Security Director Installation and Upgrade Guide.
- Install and configure SRX Series Firewalls. See Software Installation and Upgrade Guide.
- Download, deploy, and configure the Policy Enforcer virtual machine (VM). See Policy Enforcer Documentation.
- Connect Policy Enforcer to Security Director. See Policy Enforcer Documentation.
- Obtain a Juniper ATP Cloud license and create an ATP Cloud portal account. An ATP Cloud license and account are needed for all ATP Cloud Configuration Types (ATP Cloud with Juniper Connected Security, ATP Cloud, and Cloud Feeds only). If you don't have an ATP Cloud license, contact your nearest Juniper Networks sales office or Juniper Networks partner. If you don't have an ATP Cloud account, you are redirected to the ATP Cloud server to create one.
- Ensure that the SRX Series Firewall that you want to set up threat prevention for is already discovered and available on Junos Space. See Overview of Device Discovery in Security Director.

Enroll SRX Series Firewalls in Juniper ATP Cloud Using Guided Setup in Policy Enforcer

IN THIS SECTION

Step 1: Configure Policy Enforcer Settings

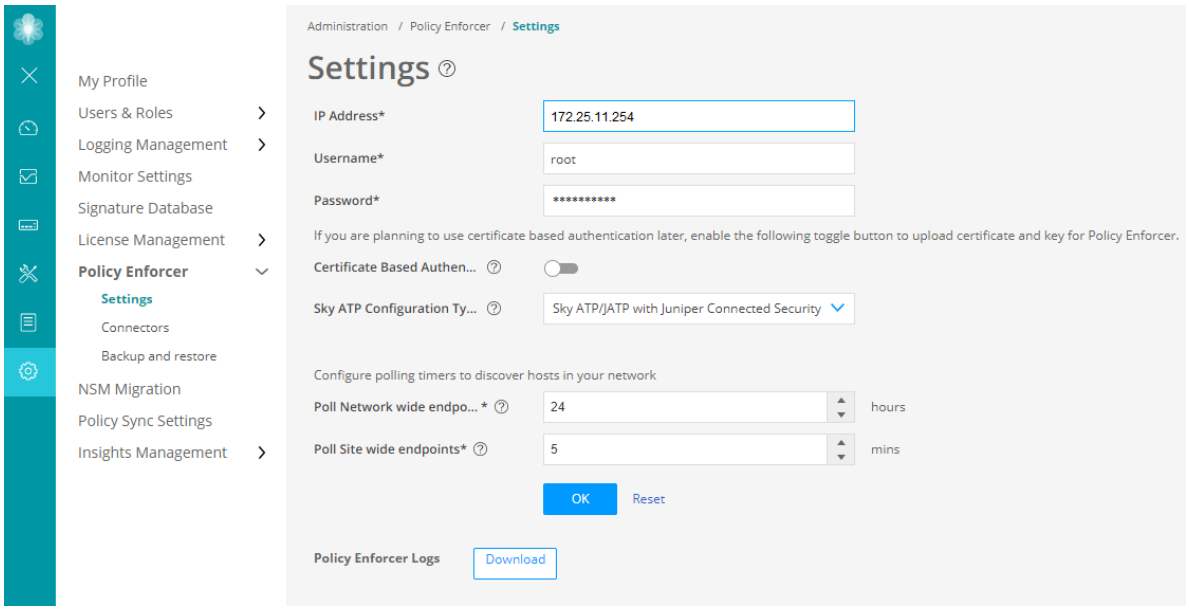
The Juniper ATP Cloud Configuration Type you select on the Policy Enforcer Settings page determines the guided setup process. Guided Setup provides all the configuration items you need for your chosen configuration type. See ATP Cloud Configuration Type Overview for details of each configuration type.

NOTE: We will be configuring only the mandatory parameters that are required for the use case. You can choose to change the default values as per your network requirement.

To configure Policy Enforcer settings:

1. Select **Administration** > **Policy Enforcer** > **Settings**.
   The Settings page appears as shown in Figure 16 on page 155.

Figure 16: Policy Enforcer Settings



2. Enter the IP address, username, and password for the Policy Enforcer VM. Use the instructions provided in Policy Enforcer Settings.
3. Select the ATP Cloud Configuration Type as **Sky ATP/JATP with Juniper Connected Security**.

4. Click **OK**.

   The status of the Policy Enforcer configuration appears.

```
Policy Enforcer is now successfully configured. Would you like to setup your Threat Policies
in Guided Setup?
```

5. Click **OK** to proceed to the Guided Setup wizard.

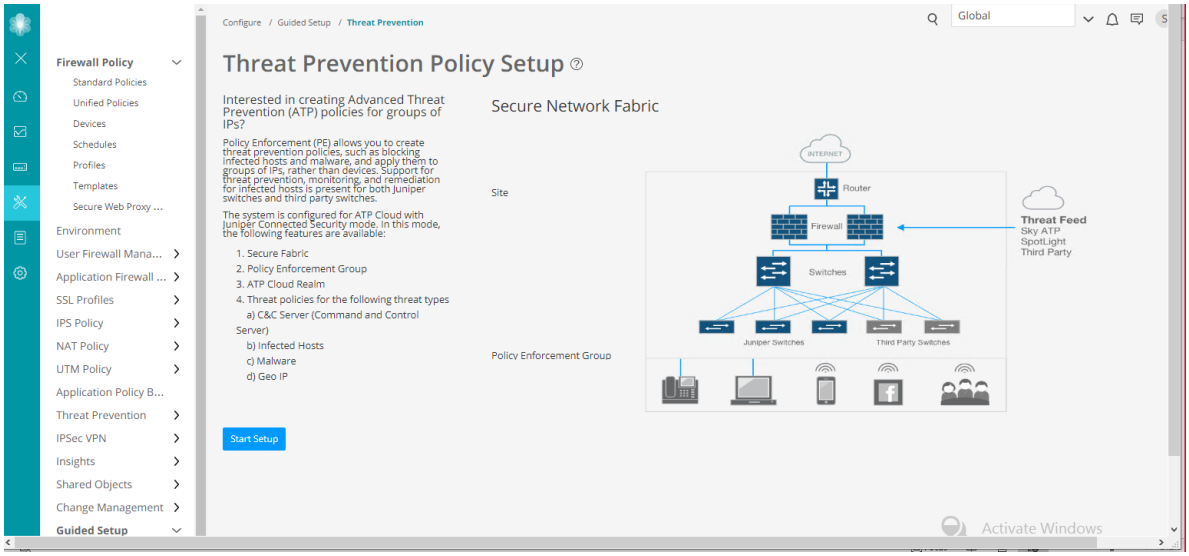
Step 2: Access the Guided Setup Wizard

Perform the steps in this section and the subsequent sections for configuring Juniper Connected Security with Juniper ATP Cloud.

1. Select **Configure** > **Guided Setup** > **Threat Prevention**.

   The Threat Prevention Policy Setup page appears as shown in Figure 17 on page 156.

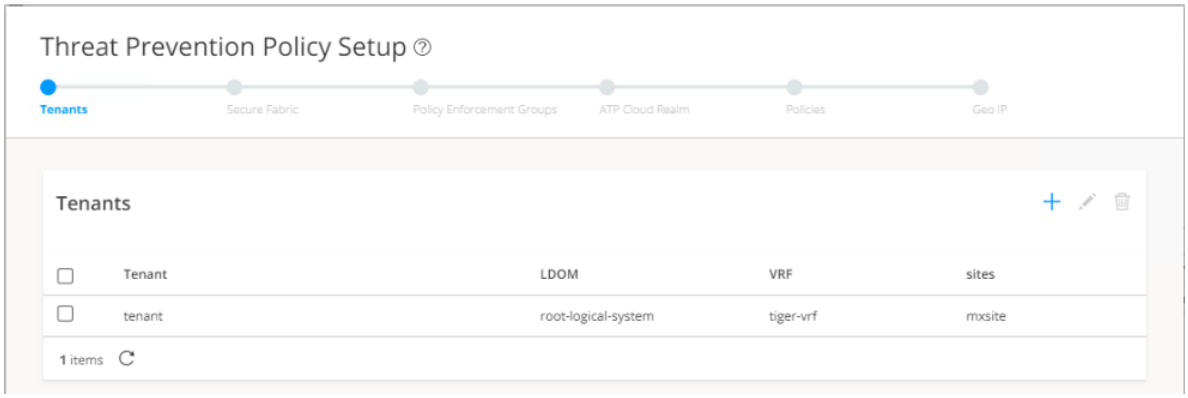
Figure 17: Threat Prevention Policy Setup



2. Click **Start Setup** to begin the guided setup.

   The Tenants page appears as shown in Figure 18 on page 157.

Figure 18: Tenant Configuration



Tenant configuration is not applicable for SRX Series Firewalls. You must configure tenants only for MX Series Universal Routers. You can skip this step.

3. Click **Next**.

   The Secure Fabric page appears.

Step 3: Create a Secure Fabric

Secure fabric is a collection of sites that contain network devices (switches, routers, firewalls, and other security devices), to which users or user groups can apply aggregated threat prevention policies using the policy enforcement groups.

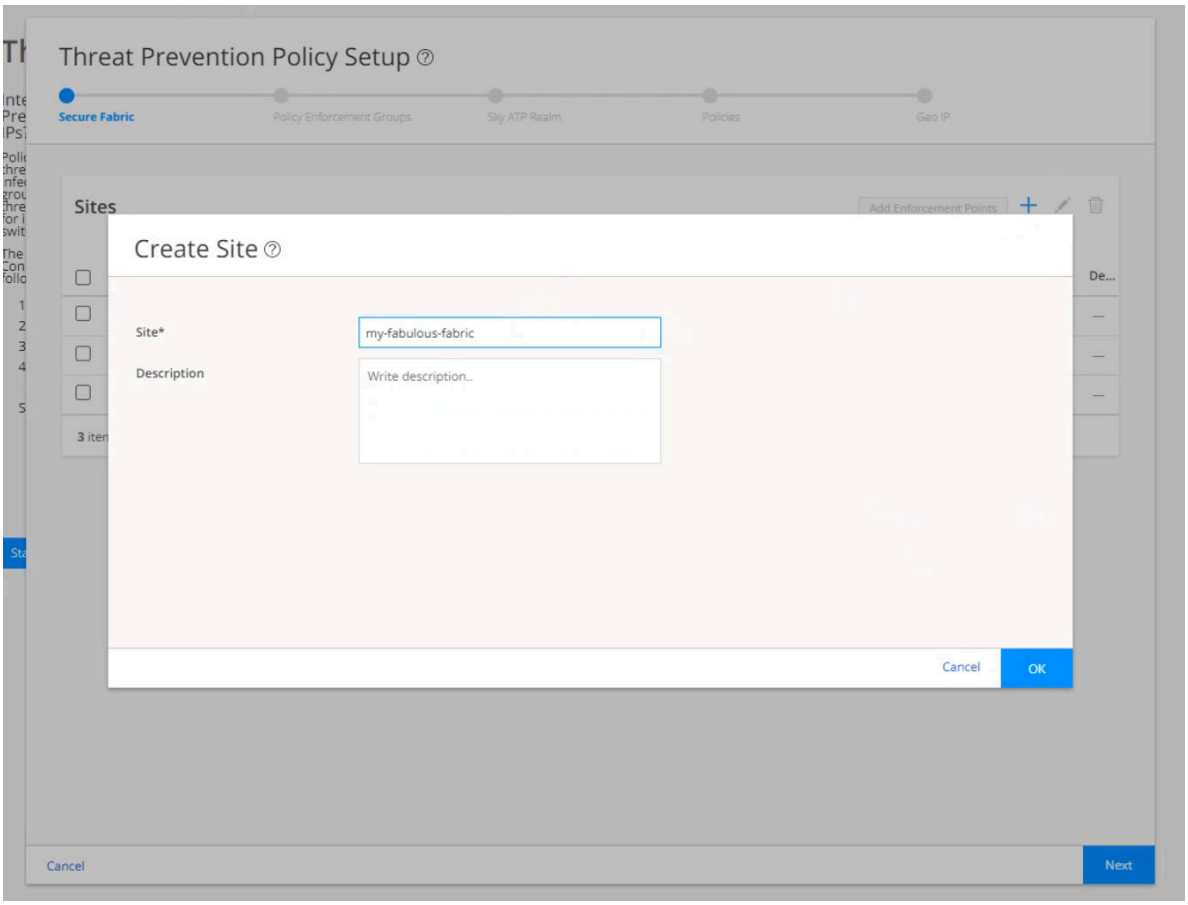
When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. This is how threat prevention is aggregated across your secure fabric. When you create a site, you must identify the perimeter firewalls so you can enroll them with Juniper ATP Cloud.

To create a secure fabric:

1. Click the **+** on the top-right corner of the Sites page.

   The Create Site page appears as shown in Figure 19 on page 158.

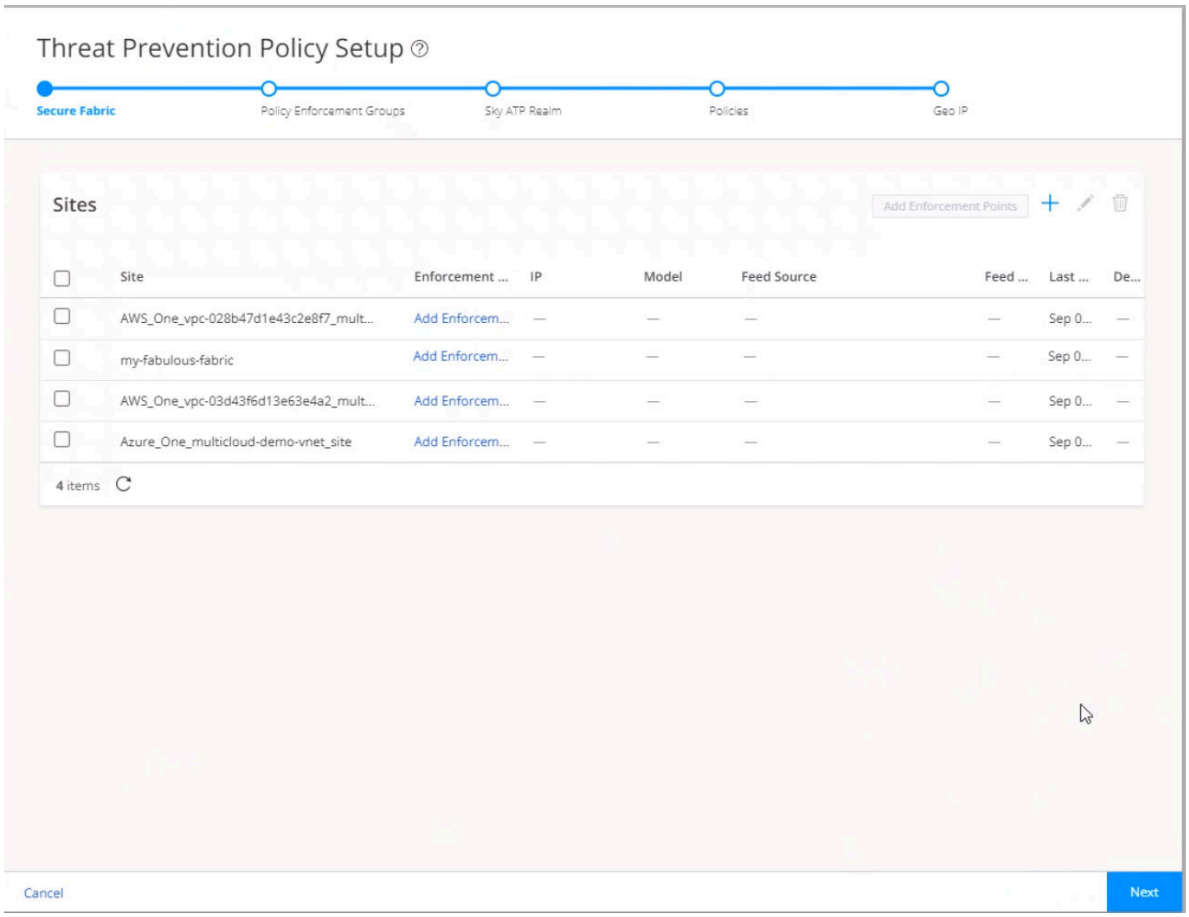
Figure 19: Create Site



2. Enter the site name and site description. Use the instructions provided in Creating Secure Fabric and Sites.
3. Click **OK**.

   The newly created site is displayed in the Sites page as shown in Figure 20 on page 159.

Figure 20: Sites

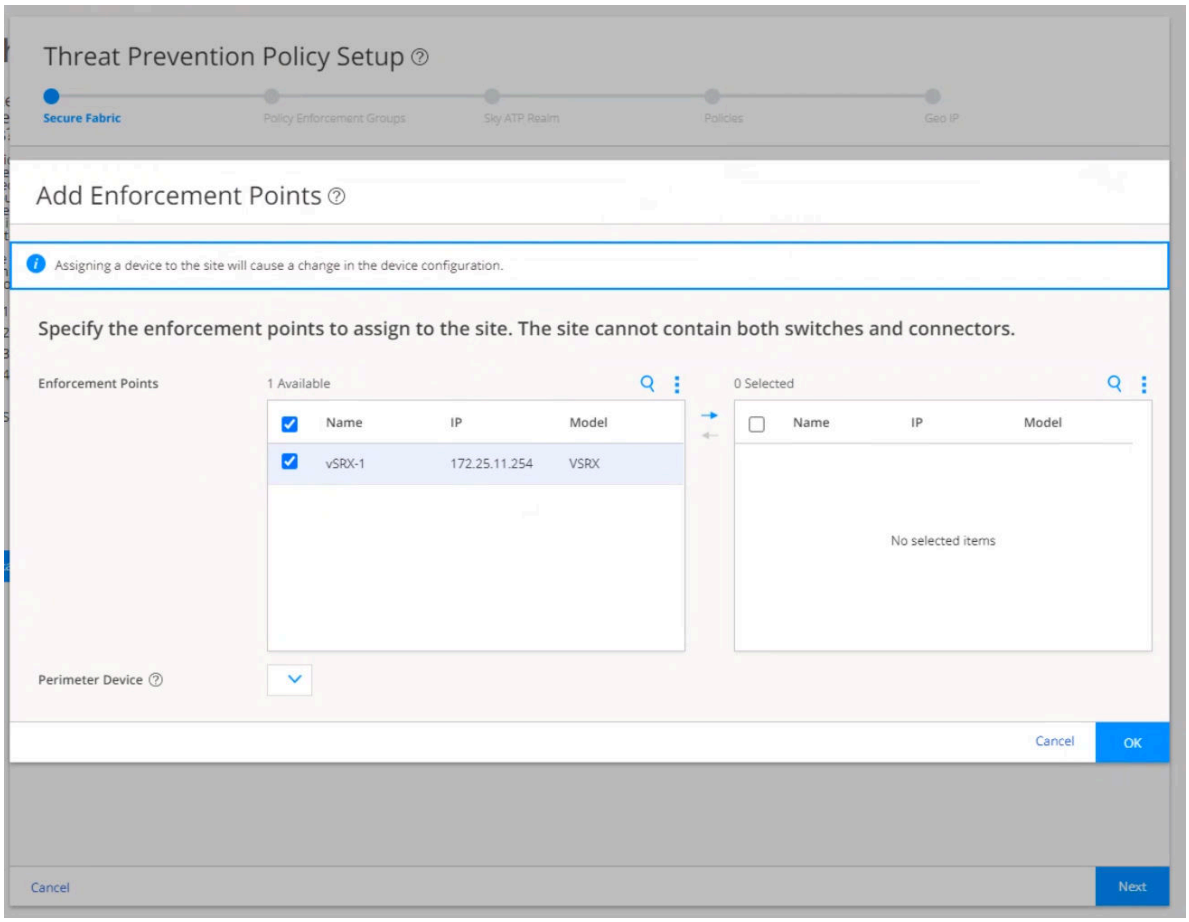


You must now add the devices for which you want to apply a common security policy to the site.

4. Click **Add Enforcement Points** in the Enforcement Points column of a device or select a device and click **Add Enforcement Points** on the top-right corner of the page.

   The Add Enforcement Point page appears as shown in Figure 21 on page 160.

Figure 21: Add Enforcement Point

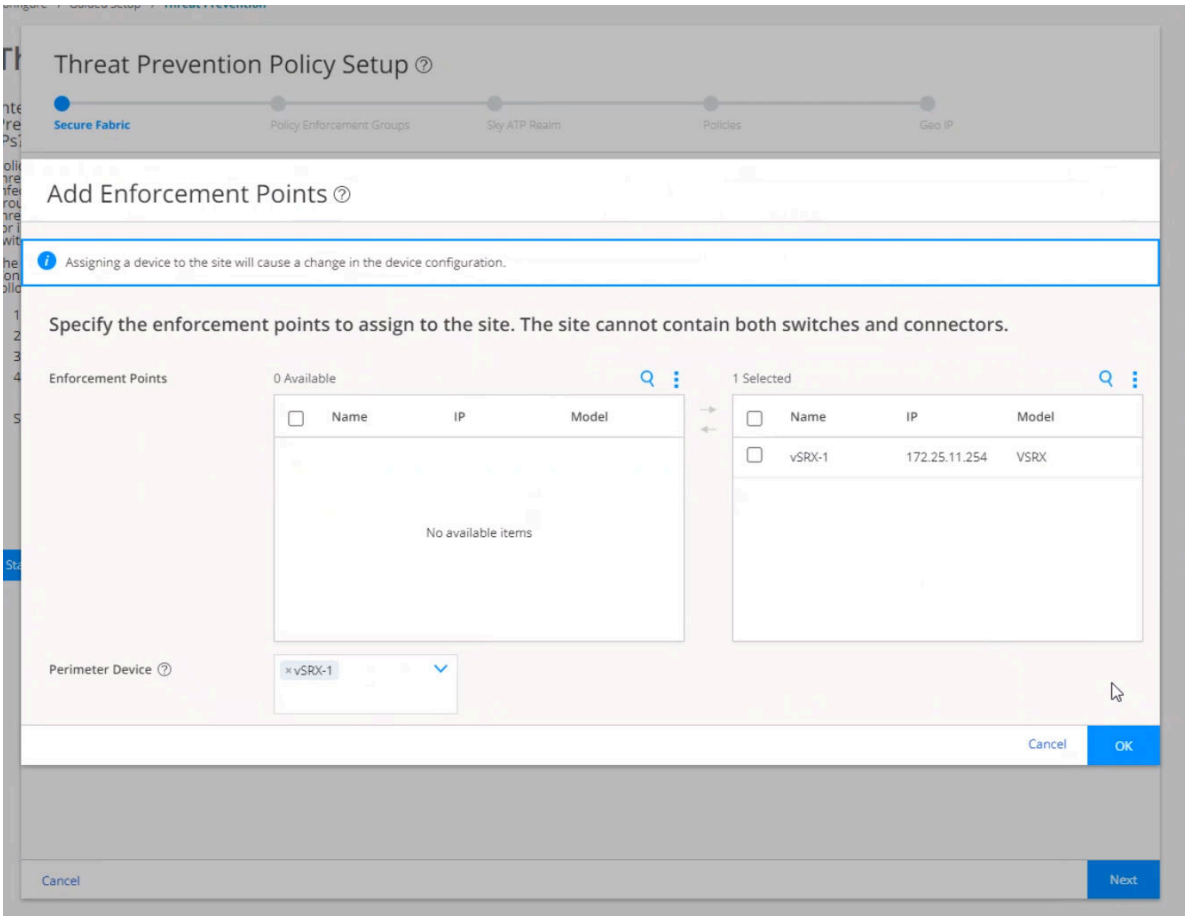


NOTE:

- A device can belong to only one site and you must remove it from any other site where it is used. To remove devices from a site, you must move the devices from the Selected column back to the Available column in the Enforcement Points section. For more information, see Adding Enforcement Points.
- Firewall devices are automatically enrolled with ATP Cloud as part of this step. No manual enrollment is required.
- Before adding an enforcement point for SRX Series Firewalls in Chassis Cluster mode, ensure that both the nodes are discovered in Security Director.

5. To include a device, select the check box beside the device in the Available list and click the **>** icon to move them to the Selected list. The devices in the Selected list will be included in the site as shown in Figure 22 on page 161.

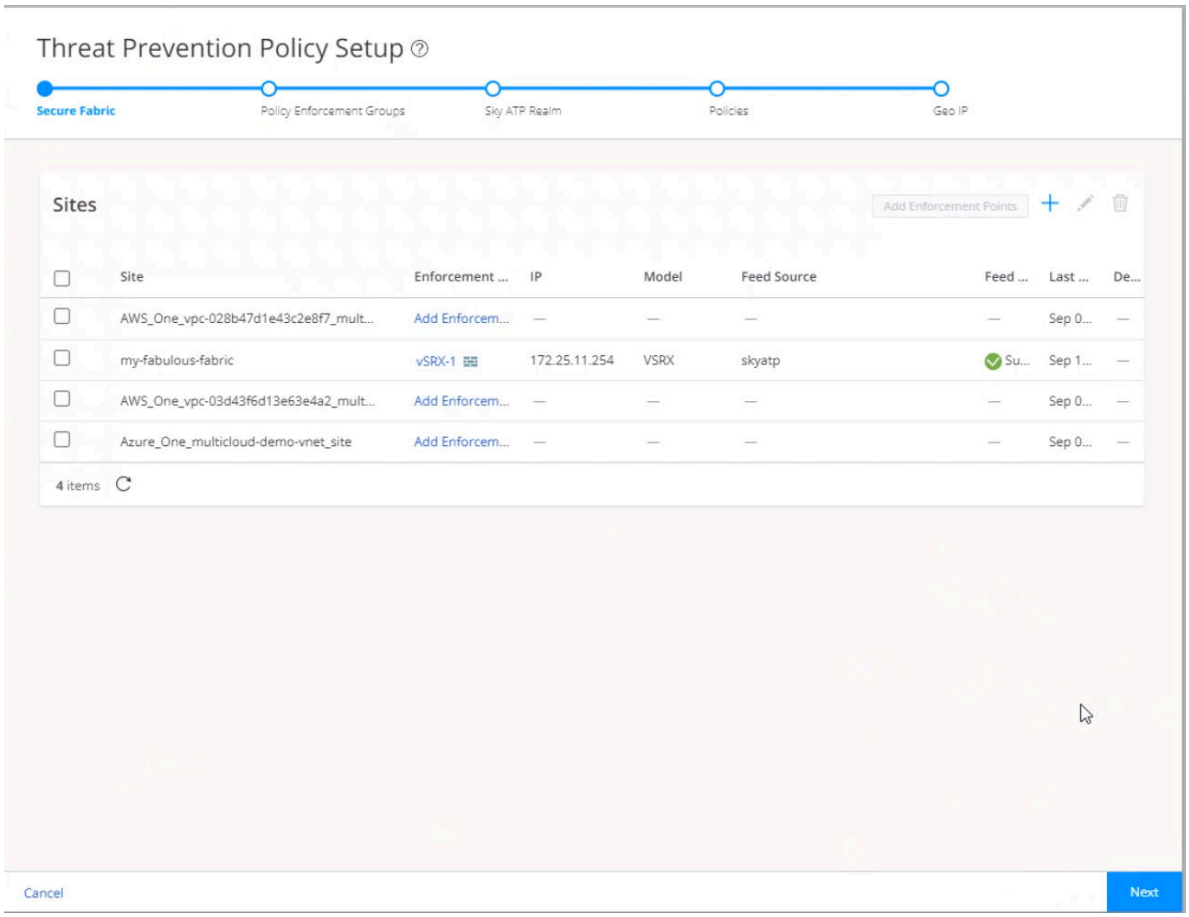
Figure 22: Assign Device to Site



6. Click **OK**.

   You can view the Secure Fabric that you created on the Sites page as shown in Figure 23 on page 162.

Figure 23: Site with Enforcement Point



7. Click **Next**.

   The Policy Enforcement Group page appears.

Step 4: Create a Policy Enforcement Group

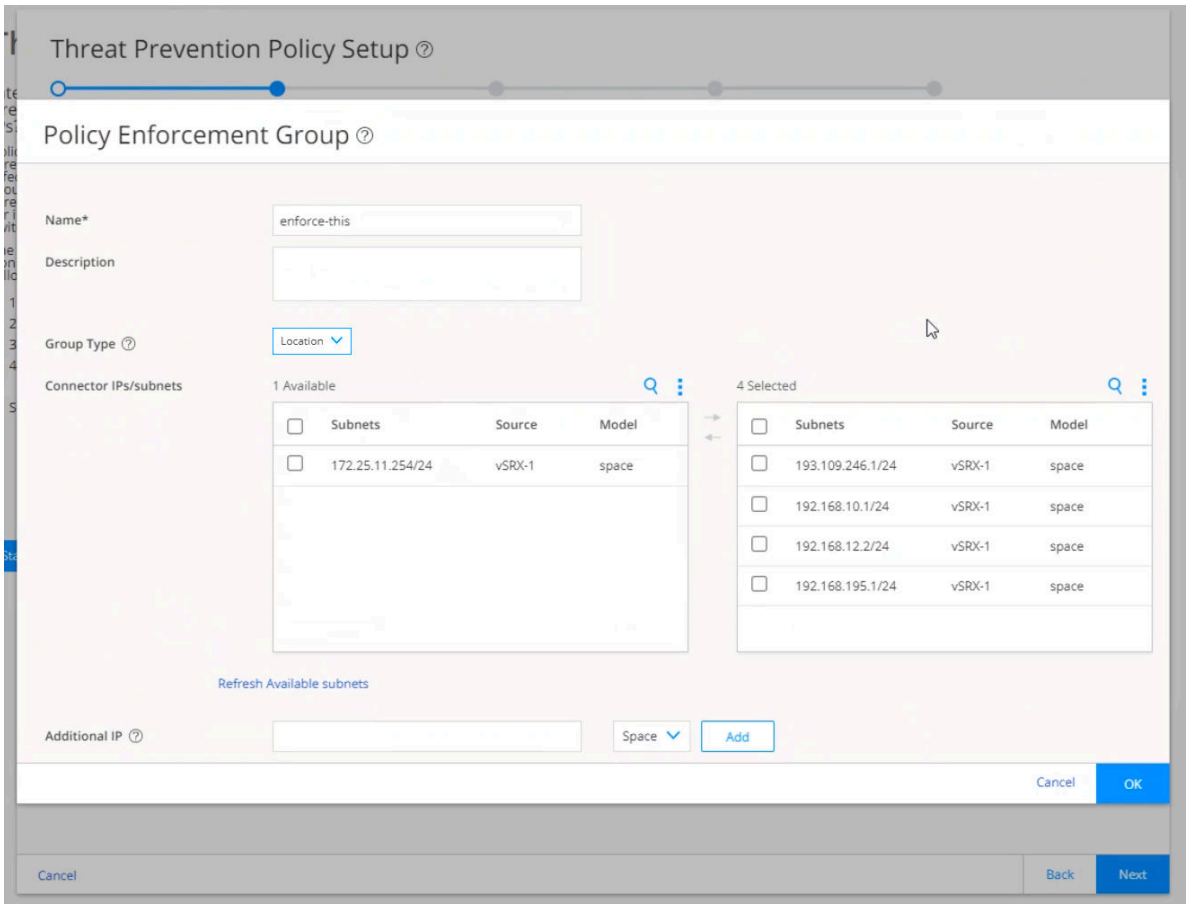
A policy enforcement group is a grouping of endpoints to which you can apply advanced threat prevention policies. Create a policy enforcement group by adding endpoints (firewalls, switches, subnets, set of end users) under one common group name and later applying a threat prevention policy to that group. Determine what endpoints you will add to the group based on how you will configure threat prevention, either according to location, users and applications, or threat risk. Endpoints cannot belong to multiple policy enforcement groups.

To create a policy enforcement group:

1. Click the **+** on the top-right corner of the Policy Enforcement Groups page.

   The Policy Enforcement Group page appears as shown in Figure 24 on page 163.

Figure 24: Policy Enforcement Group



2. Enter the policy enforcement group name and description. Sites with the threat remediation enabled instances are only listed, if the Group Type is Location. Select the check box beside the sites in the Available list and click the > icon to move them to the Selected list. Use the instructions provided in Creating Policy Enforcement Groups to create a policy enforcement group.

   You can view the new policy enforcement group in the Policy Enforcement Group page.

3. Click **Next**.

   The ATP Cloud Organization page appears.

Step 5: Enroll Juniper ATP Cloud

An organization is a unique entity or identifier to manage and restrict access to Web applications. You must create at least one organization to log in to Juniper ATP Cloud. Once you create an organization, you can enroll SRX Series Firewalls into the organization. You can also give more users (administrators) permission to access the organization. If you have multiple organizations, note that each SRX Series Firewall can be bound to only one organization, and users cannot switch between organizations.

Before you begin:

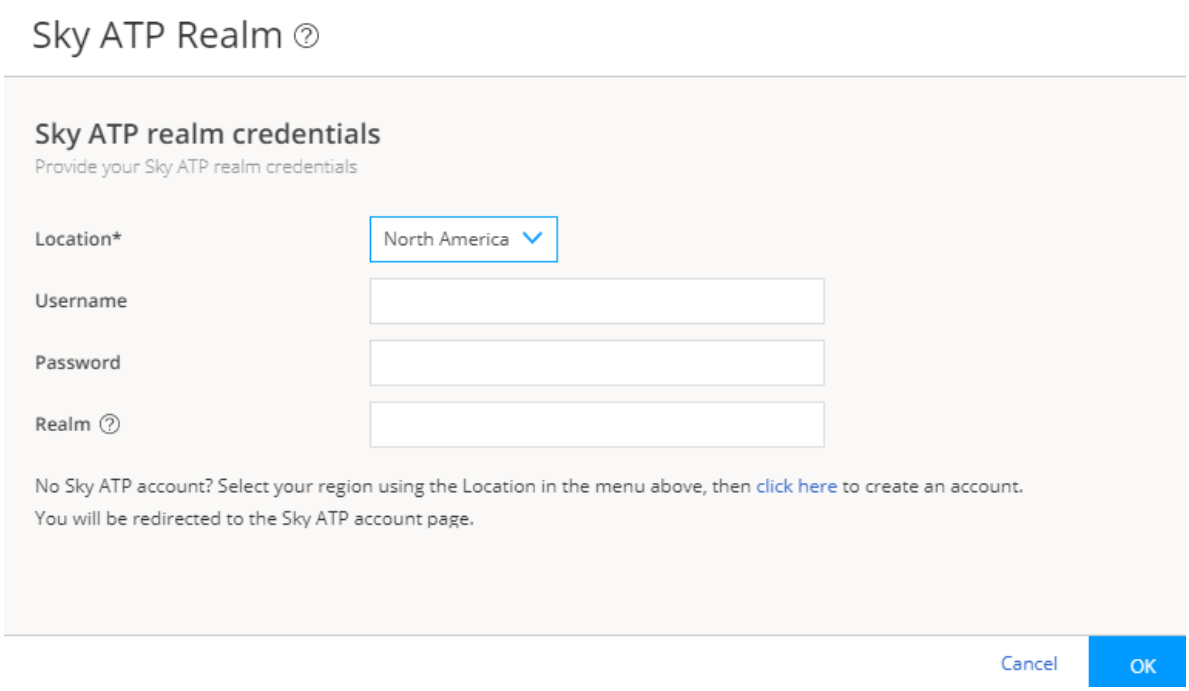
- Ensure that your ATP Cloud account is associated with a license. For more information, see Software Licenses for ATP Cloud.
- Know which region will be covered by the organization that you create. You must a select a region when you configure an organization.

To create an organization from your ATP Cloud account:

1. Click the **+** sign on the top-right corner of the ATP Cloud Organization page.

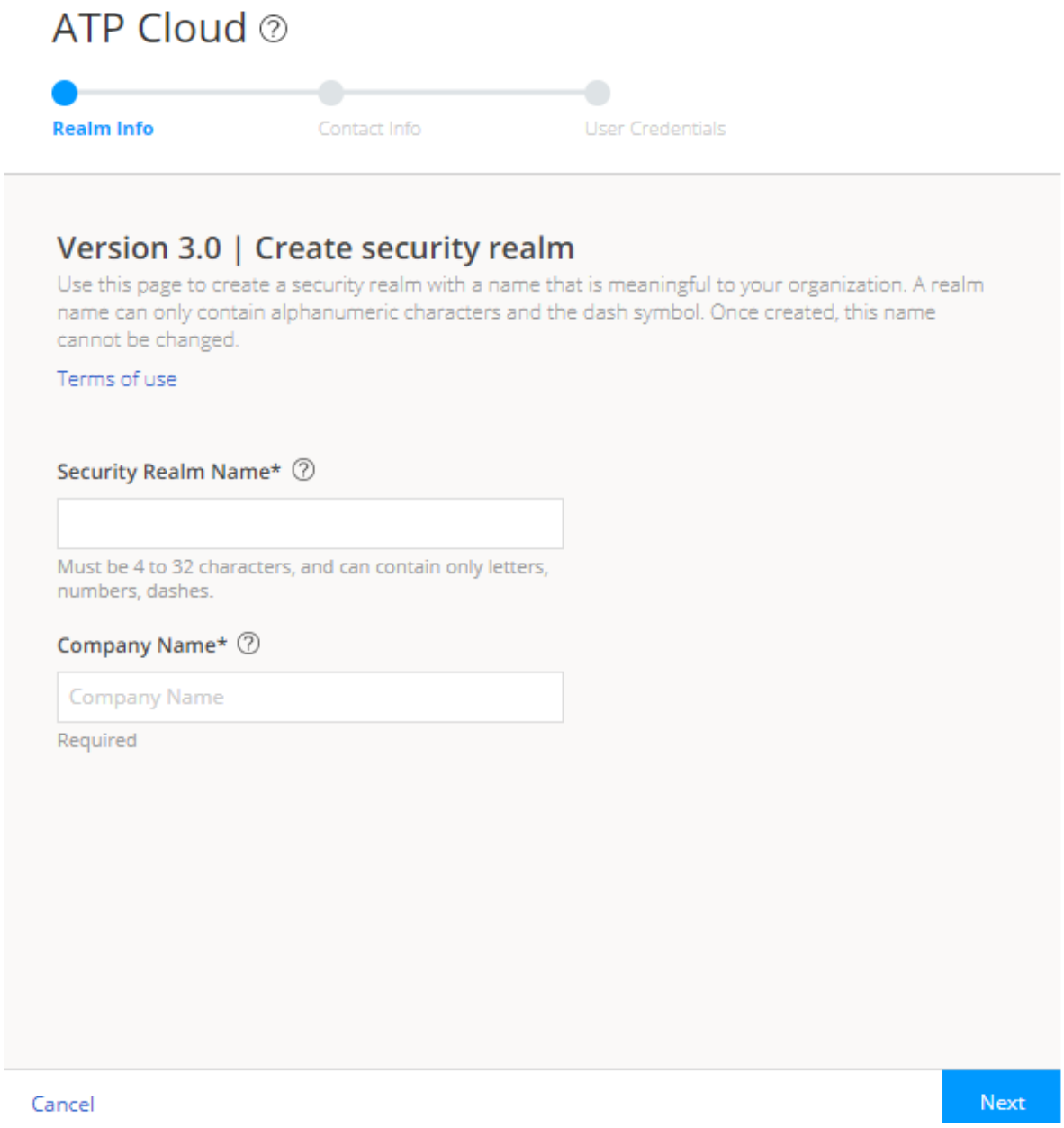
   The ATP Cloud organization credentials page appears as shown in Figure 25 on page 164.

   Figure 25: ATP Cloud Organization



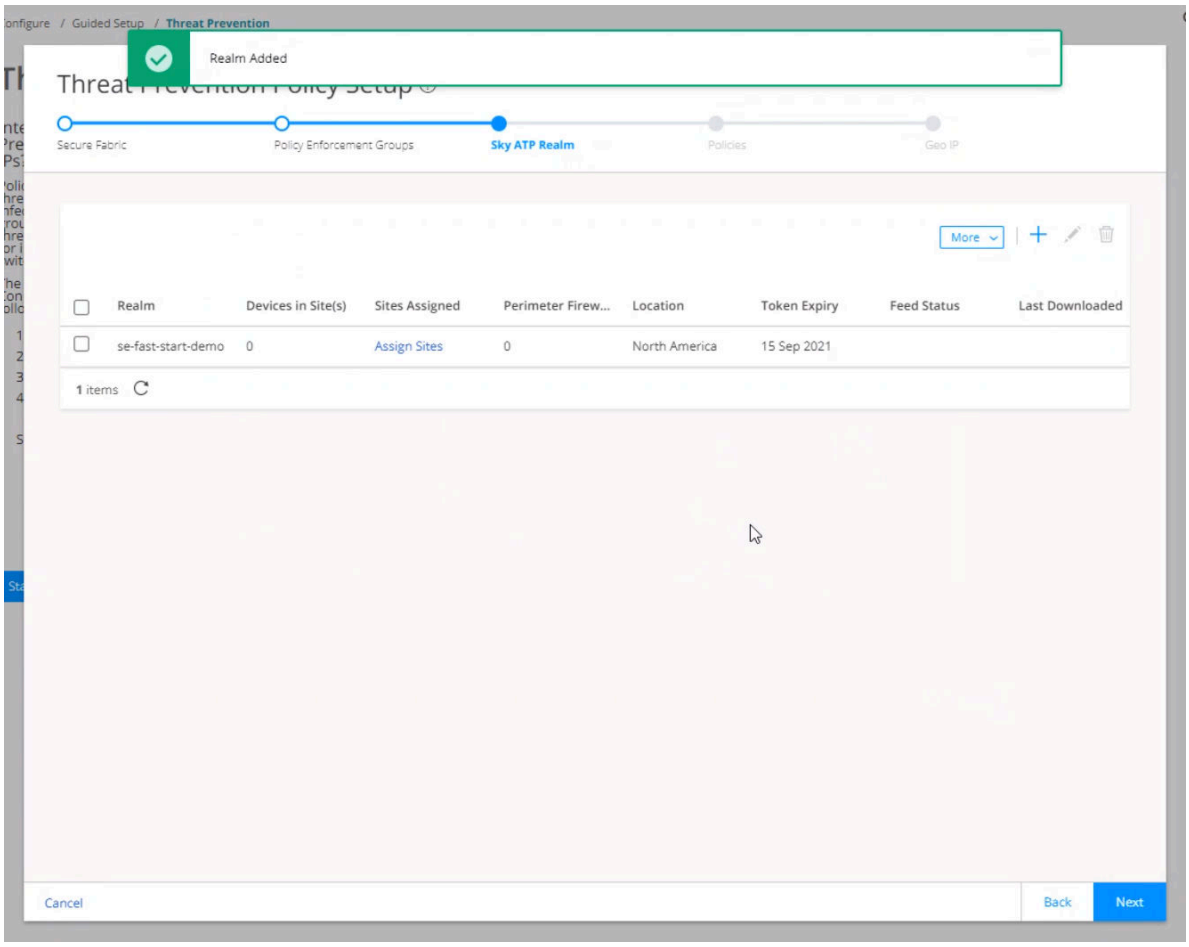
2. Select the location. Enter the username, password and organization details. See Juniper ATP Cloud User Name to create and register an organization, and then enroll your SRX Series Firewalls into the organization.

Figure 26: Create Security Organization



If an organization is already created with a site assigned, all devices in a site are listed under the Devices in Site(s) column that includes EX Series Switches, SRX Series, all enforcement points, and devices that are originally from an organization. Devices that are marked as perimeter firewall devices are listed under the Perimeter Firewall column.

Figure 27: New Organization Without Sites

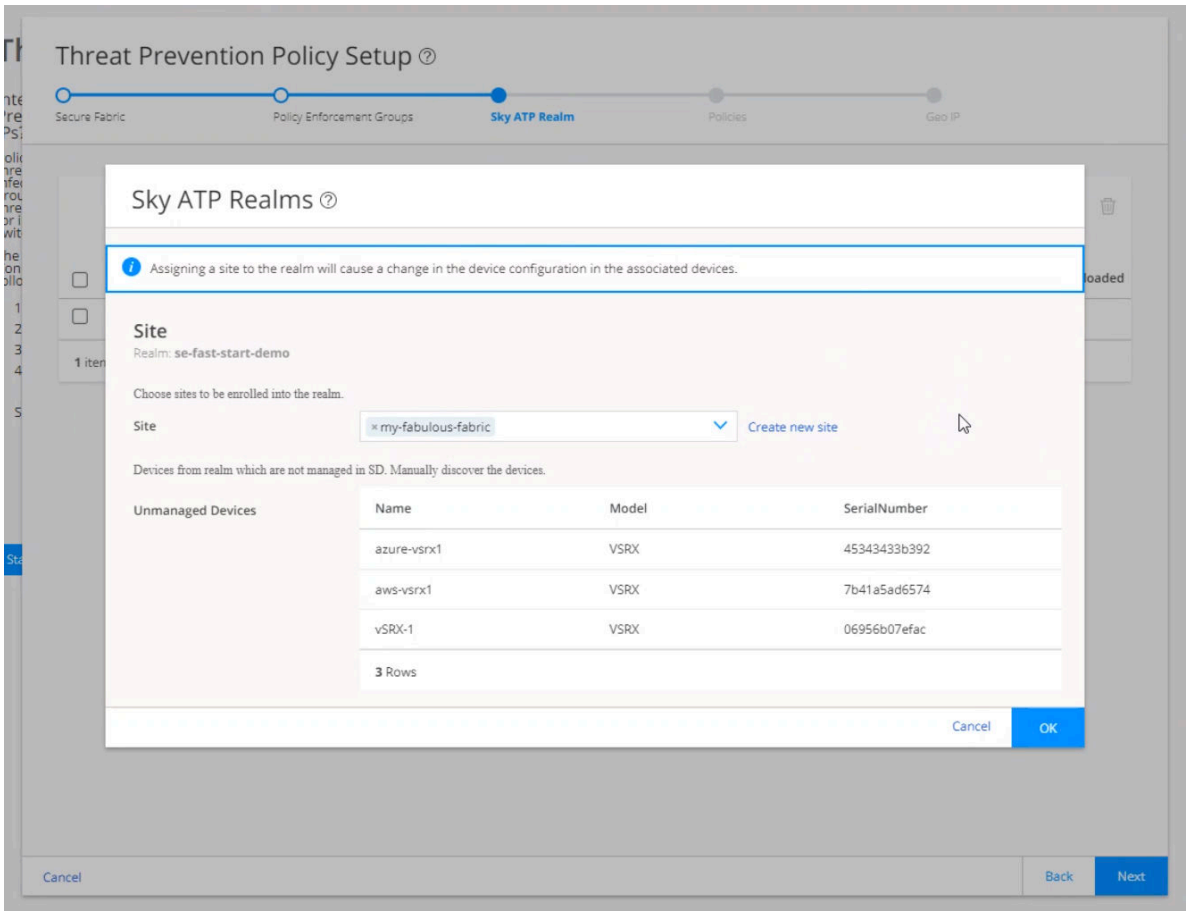


NOTE: If the organization addition is not successful, it means there is a network issue and Security Director is unable to reach Internet. Ensure that all devices and components can reach the Internet and each other.

If an organization does not have any site assigned, click **Assign Sites**.

The Sites page appears as shown in Figure 28 on page 167.

Figure 28: Assign Site to a Organization



Select one or more sites to enroll into the organization. If there are no sites associated with the organization, click **Create new site**. To know more about creating a site, see Creating Secure Fabric and Sites.

3. Click **OK**.

   The ATP Cloud Organizations page appears with sites enrolled to the organization.

4. Click **Next**.

   The Policies page appears.

Step 6: Create a Threat Prevention Policy

Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, infected hosts, and malware. Using feeds from Juniper ATP Cloud and custom feeds you configure, ingress and egress traffic is monitored for suspicious content and behavior. Based on a threat score, detected threats are evaluated and action might be taken once a verdict is reached. Once you have a Threat Prevention Policy, you assign one or more policy enforcement groups to it.

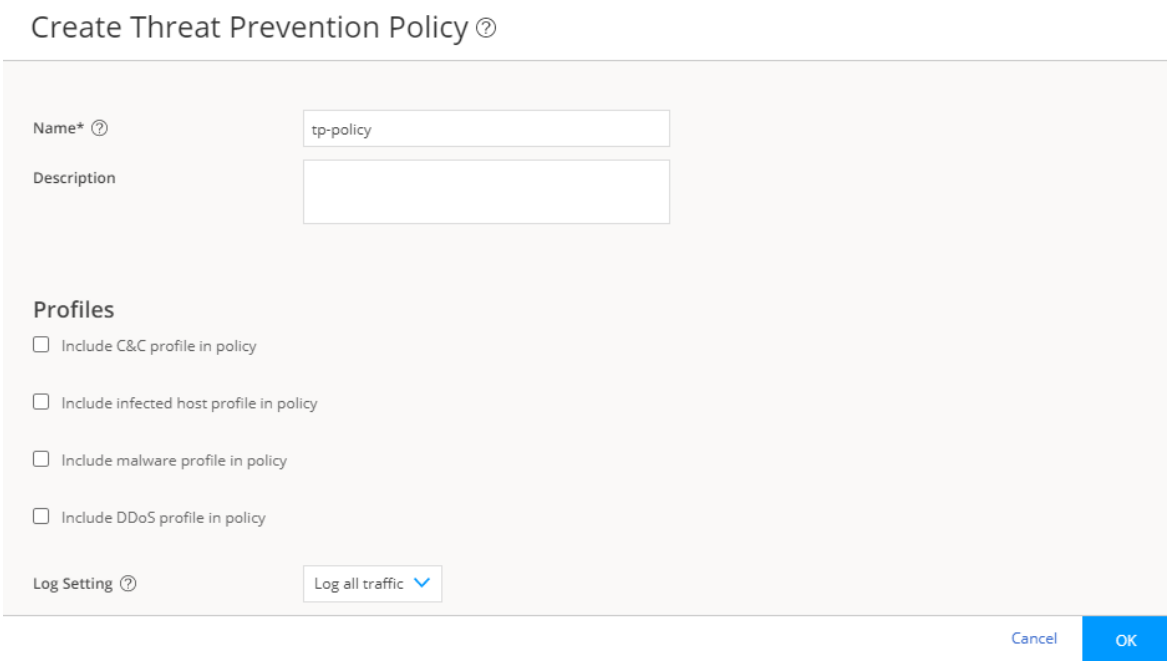
Before you begin:

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

To create a threat prevention policy:

1. Click **+** on the top-right corner of the Policies page.
   The Create Threat Prevention Policy page appears as shown in Figure 29 on page 168.

Figure 29: Create Threat Prevention Policy 1



2. Configure the profile parameters as shown in Figure 30 on page 169 and Figure 31 on page 170. Use the instructions provided in Creating Threat Prevention Policies.

Figure 30: Create Threat Prevention Policy 2

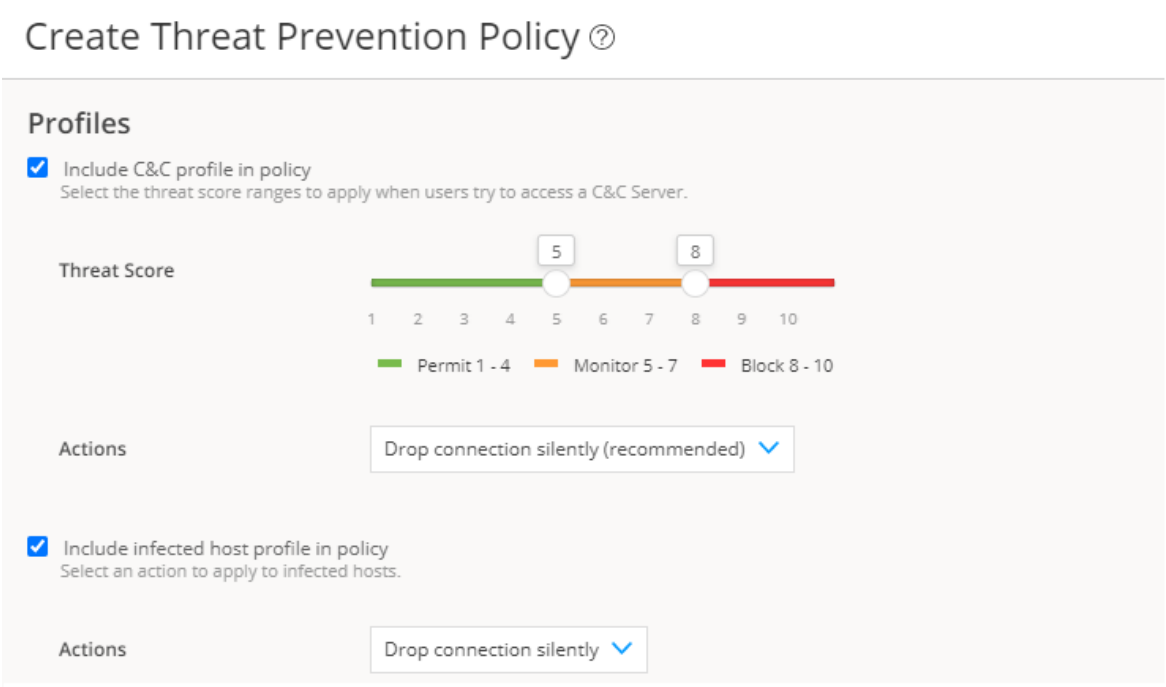
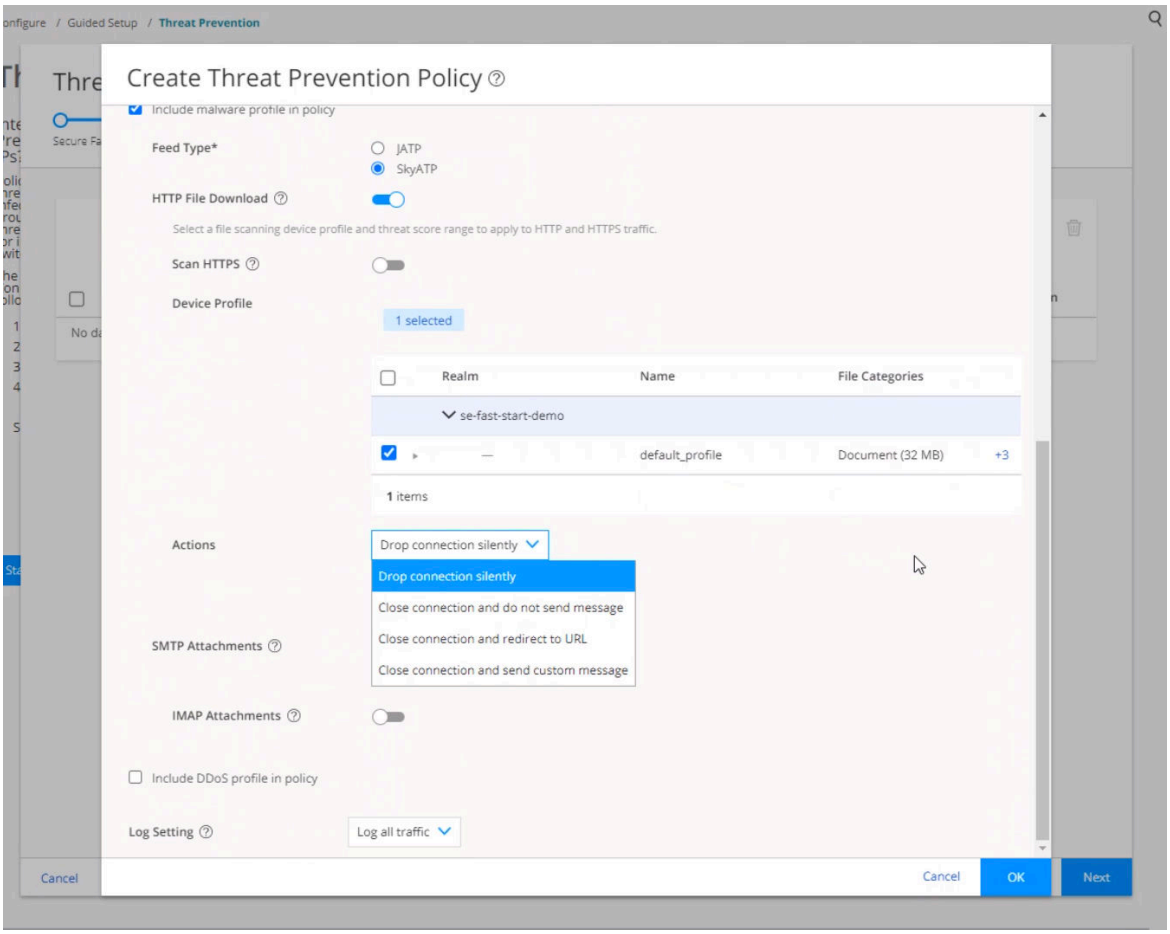


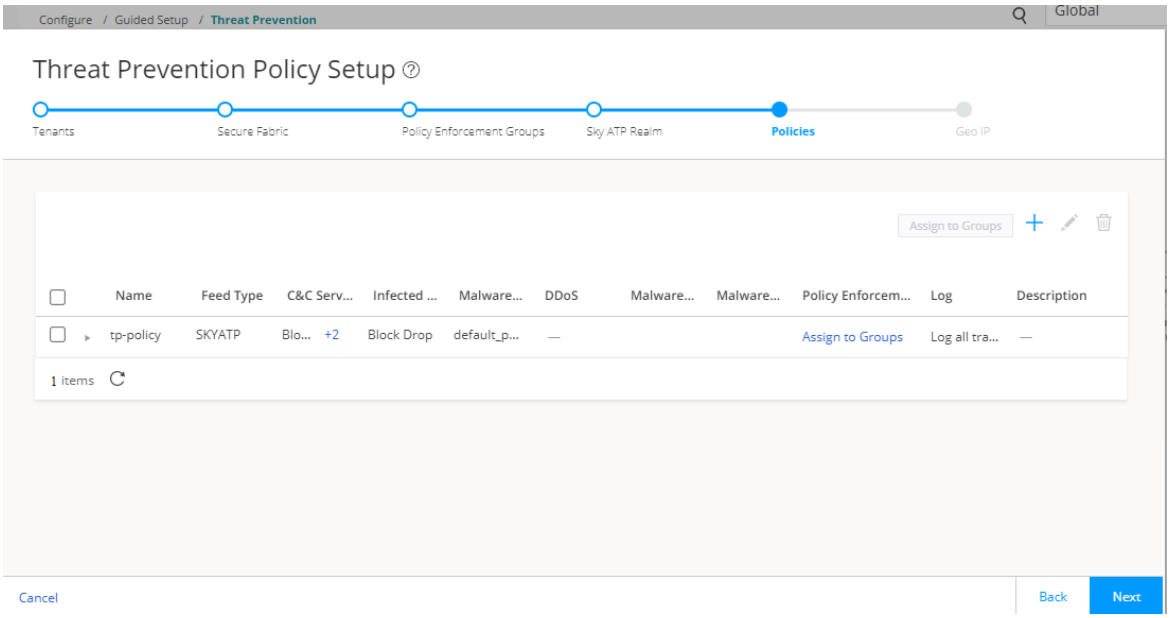
Figure 31: Create Threat Prevention Policy 3



3. Click **OK**.

The new policy appears in the Policies page as shown in Figure 32 on page 171.

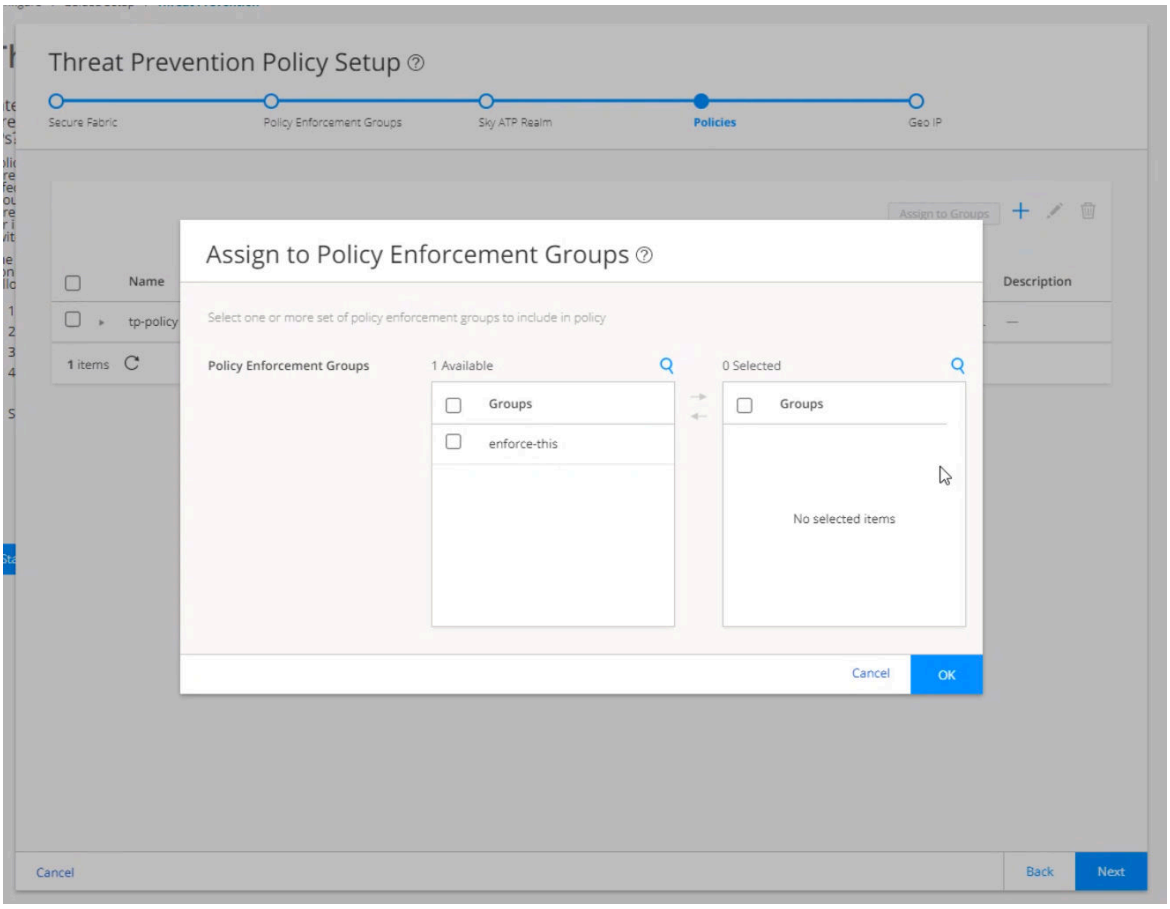
Figure 32: Policies



4. Click **Assign to Groups** to assign the threat prevention policy to the desired policy enforcement group.

   The Assign to Policy Enforcement Groups page appears as shown in Figure 33 on page 172.

Figure 33: Assign to Policy Enforcement Groups

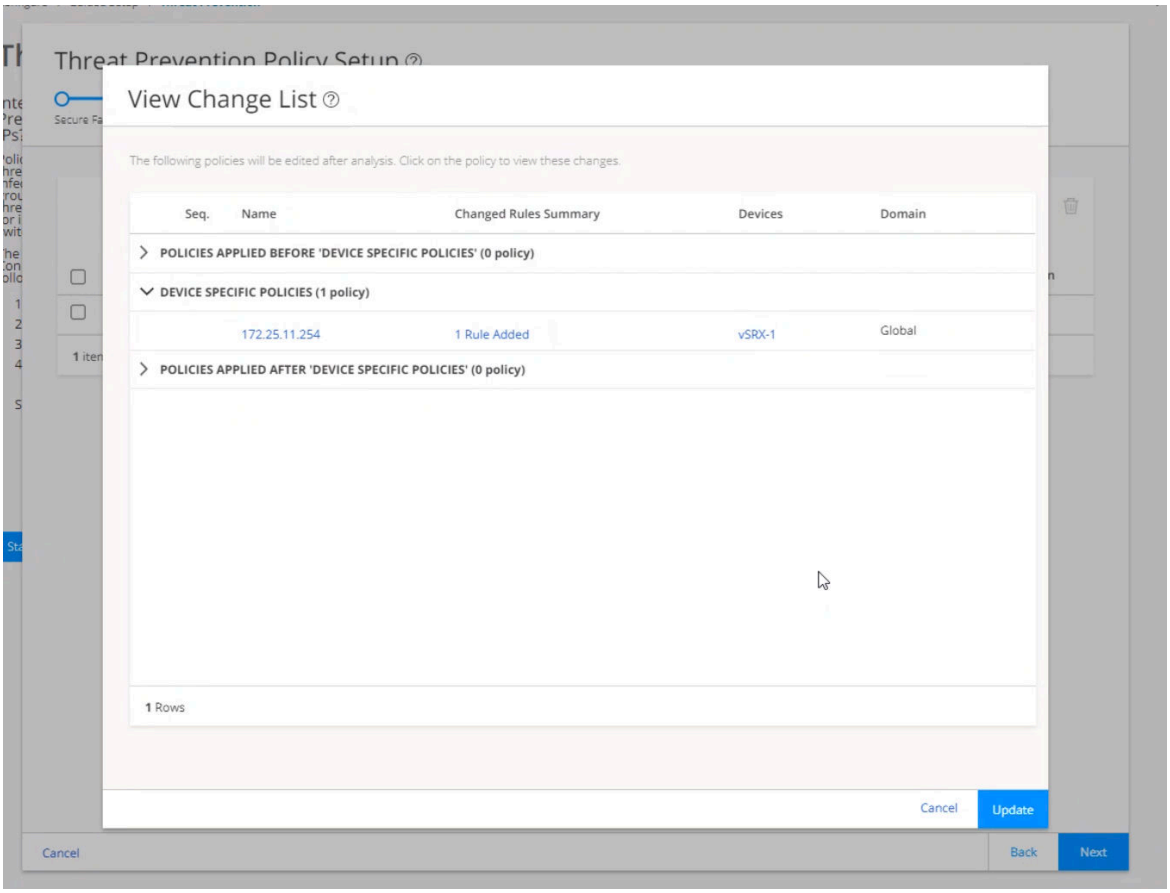


5. Select one or more policy enforcement groups from the Available column and move it to the Selected column to include in the policy. Click **OK**.

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

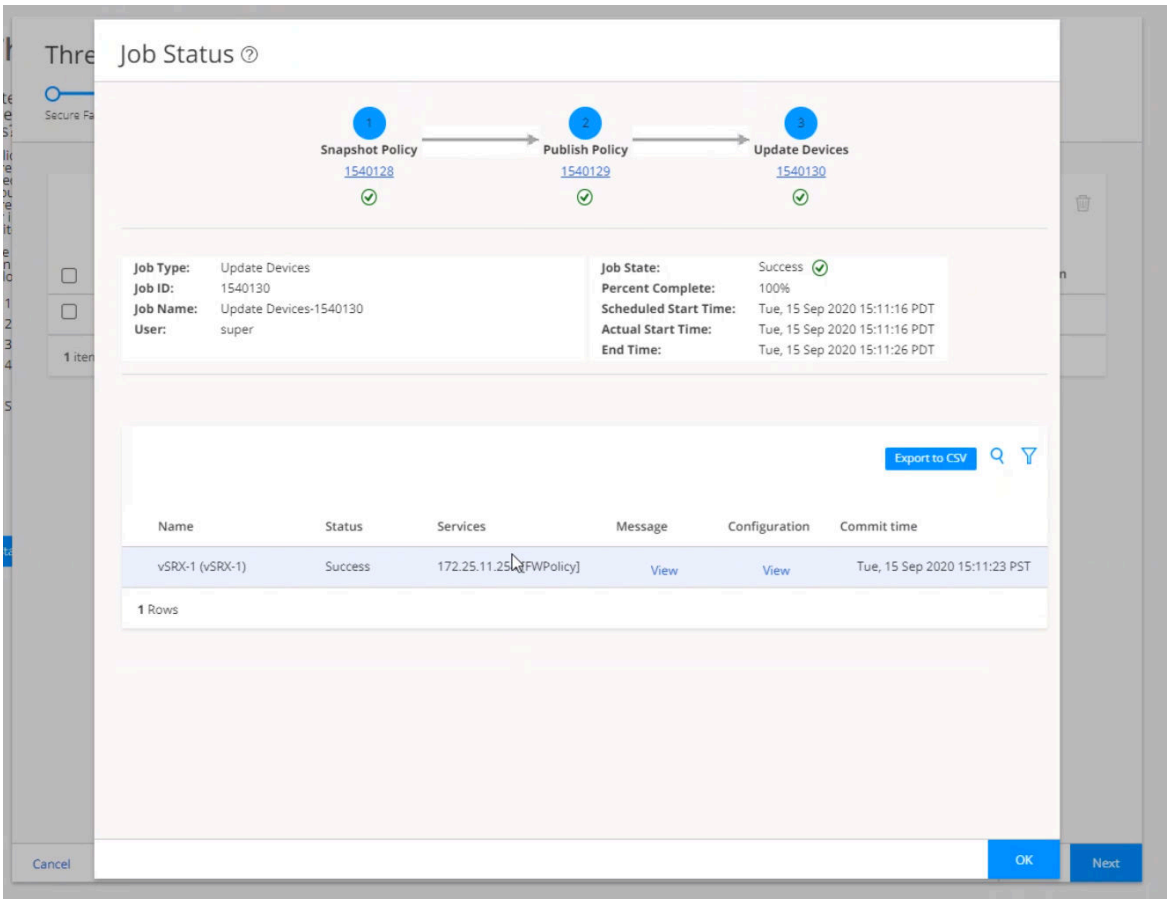
   The View Change List page appears as shown in Figure 34 on page 173.

Figure 34: View Change List



6. Click **Update** to instruct the system to push the newly created policy to the SRX Series Firewall. The Job Status page appears as shown in Figure 35 on page 174.

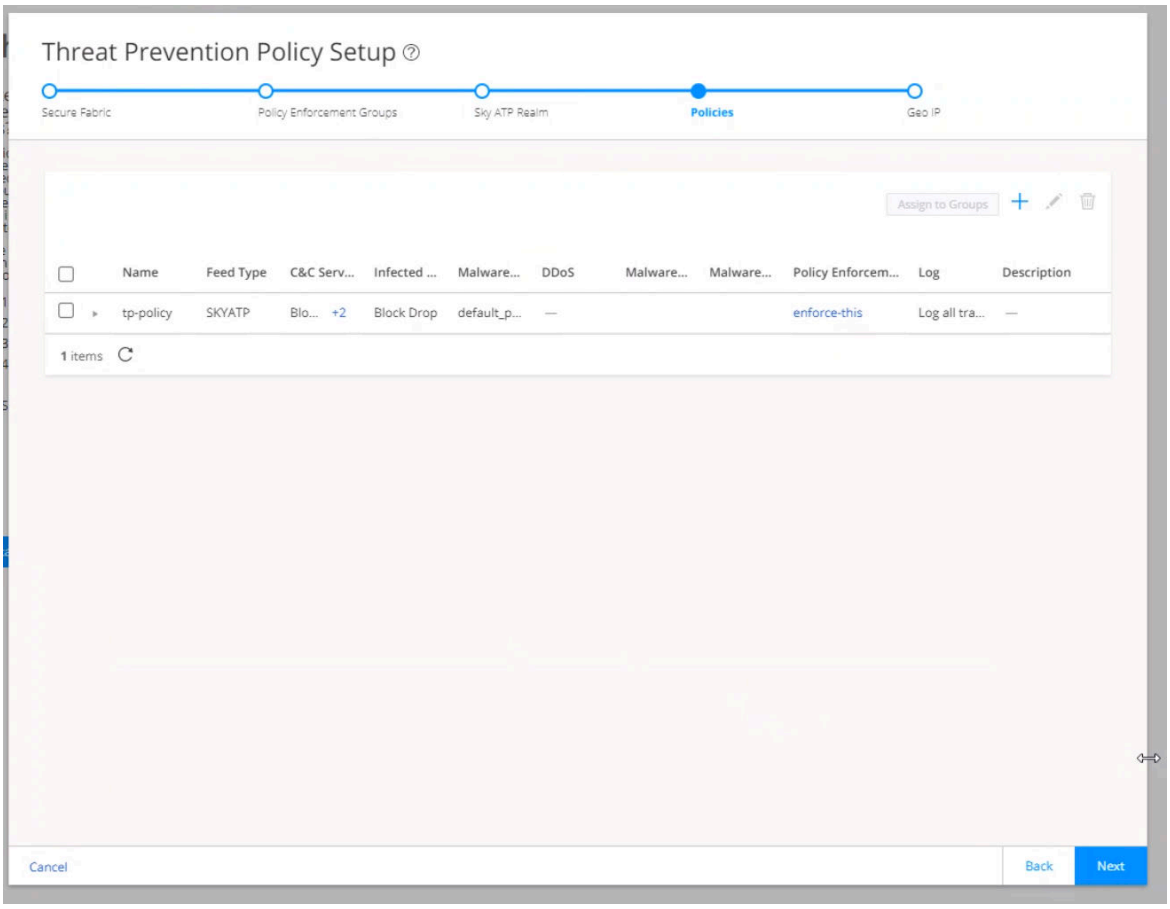
Figure 35: Job Status



7. Click the job status ID (Snapshot Policy, Publish Policy, and Update Devices) to view the job details. To exit, click **OK**.

   The new threat prevention policy appears in the Policies page.

Figure 36: Policy Assigned to Policy Enforcement Group



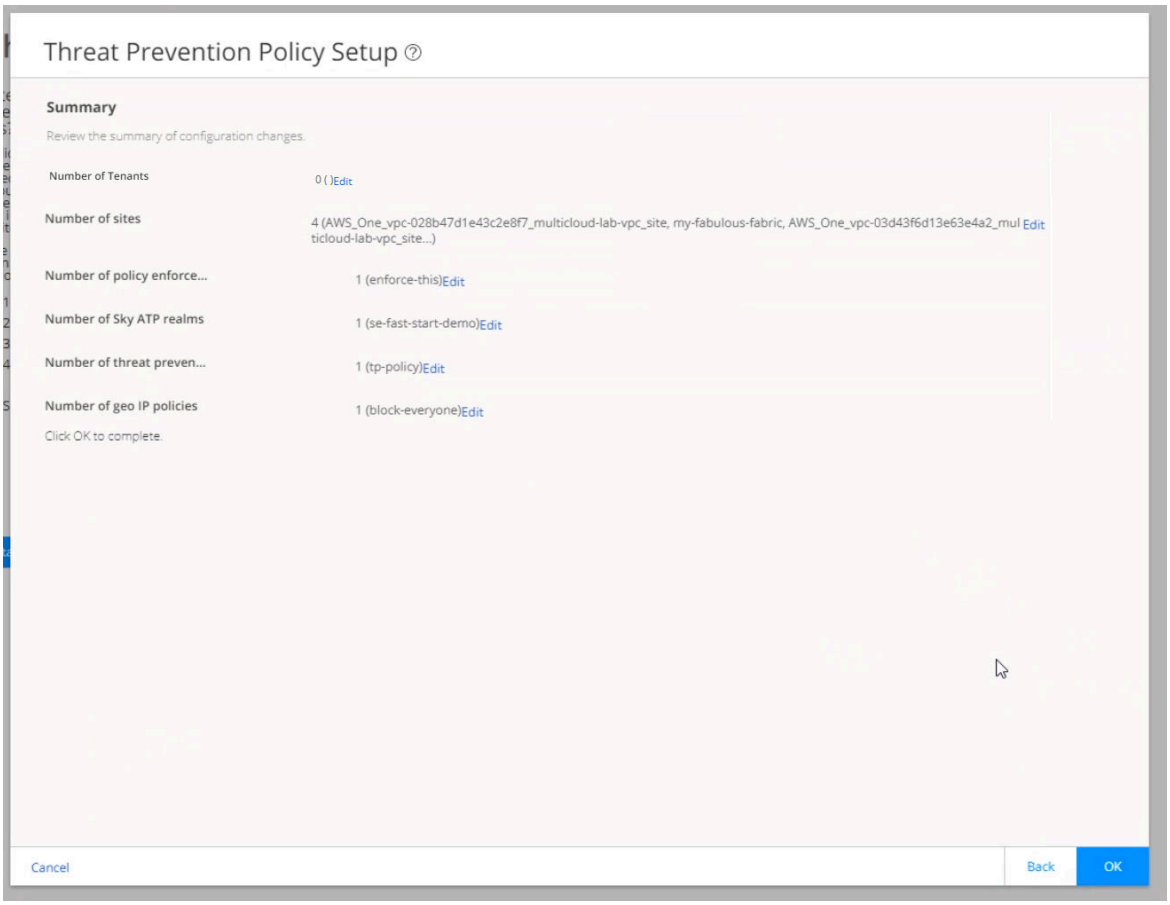
8. Click **Next**.

   The GeoIP page appears.

9. To configure GeoIP, see "Step 7: (Optional) Configure GeoIP" on page 176, else click **Finish** to go to the Summary page.

   The Summary page lists all the parameters that you have configured using the Guided Setup wizard.

Figure 37: Summary



10. Click **Edit** to further edit any parameters or click **OK**.

    The Threat Prevention Policy page appears with the newly created policy.

Step 7: (Optional) Configure GeoIP

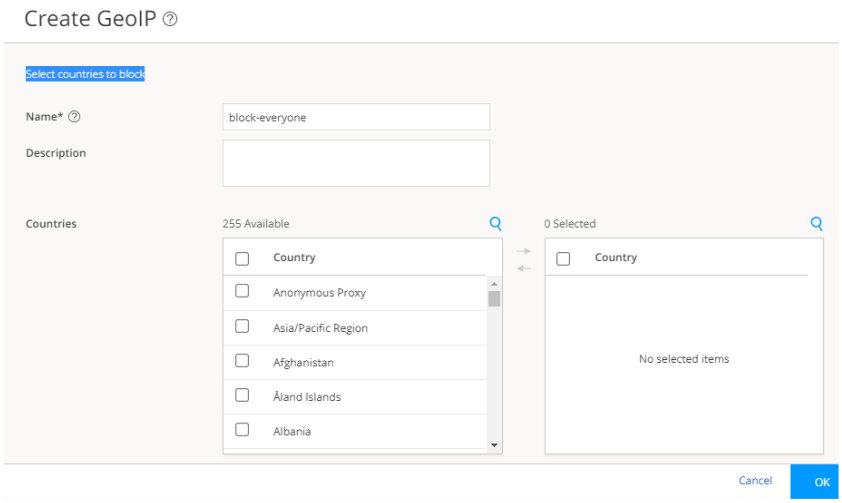
GeoIP is the method of finding a computer terminal's geographic location by identifying that terminal's IP address. A GeoIP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping IP addresses to the sources of attack traffic, you can determine the geographic regions of origin and filter traffic to and from specific locations in the world.

To create a GeoIP:

1. Click **+** on the top-right corner of the GeoIP page.

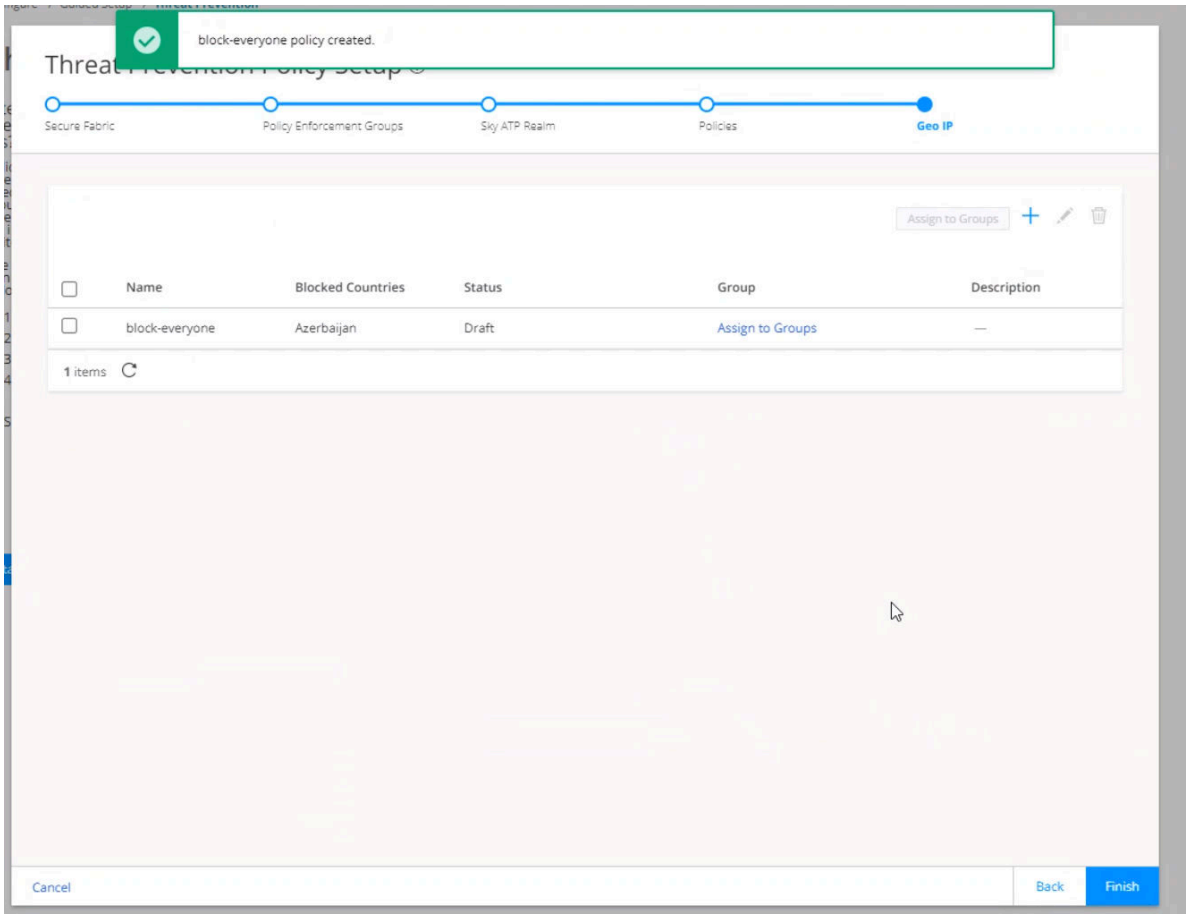
   The Create Geo IP page appears as shown in Figure 38 on page 177.

Figure 38: Create Geo IP



2. Use the instructions provided in Creating Geo IP Policies to create a GeoIP.

Figure 39: New GeoIP



3. Click **Assign to Groups** to assign one or more policy enforcement groups to include in the policy.

   The Assign to Policy Enforcement Groups page appears.
4. Select one or more policy enforcement groups to include in the policy. Click **OK**.

   The View Change List page appears.
5. Click **Update**.

   The Job Status page appears.
6. Click **Finish** to move to the Summary page as shown in Figure 37 on page 176.

   The Summary page lists all the parameters that you have configured using the Guided Setup wizard.
7. Click **Edit** to further edit any parameters or click **OK**.

   The Threat Prevention Policy page appears with the newly created policy.

What's Next?

Now that you have successfully created the threat prevention policy, you must assign the threat prevention policy to a security firewall policy before it can take affect. For more information, see Firewall Policies Overview and Creating Firewall Policy Rules.

Verify the Enrollment of the SRX Series Firewall in Juniper ATP Cloud

IN THIS SECTION

Purpose

Verify that the SRX Series Firewall is enrolled in ATP Cloud.

Action

Log in to Security Director Web portal and perform the following tasks:

Table 17: Security Director Web Portal

Action	Meaning
Select **Devices** > **Secure Fabric** > **Sites**.	The Feed Source Status column displays the status (Success/Failed) of SRX Series Firewall enrollment in ATP Cloud.
Select **Devices** > **Secure Devices**.	The ATP Cloud organization name displayed under the Feed Source Status column confirms the enrollment of the device in ATP Cloud organization.
Select **Configure** > **Threat Prevention** > **Feed Sources** > **Sky ATP**.	The Enrollment Status column displays the status (Success/Failed) of the Policy Enforcer in ATP Cloud organization.

5
PART

Troubleshoot

Juniper ATP Cloud Troubleshooting Overview

This topic provides a general guide to troubleshooting some typical problems you might encounter on Juniper ATP Cloud.

Table 18 on page 181 provides a summary of the symptom or problem and recommended actions with links to the troubleshooting documentation.

Table 18: Troubleshooting Juniper ATP Cloud

Symptom or Problem	Recommended Action
SRX Series Firewall can't communicate with cloud	See "Troubleshooting Juniper ATP Cloud: Checking DNS and Routing Configurations" on page 182 See "Troubleshooting Juniper ATP Cloud: Checking Certificates" on page 184 See "Troubleshooting Juniper ATP Cloud: Checking the Routing Engine Status" on page 186 See request services advanced-anti-malware data-connection See request services advanced-anti-malware diagnostic
Files not being sent to cloud	See "Troubleshooting Juniper ATP Cloud: Checking DNS and Routing Configurations" on page 182 See "Troubleshooting Juniper ATP Cloud: Checking Certificates" on page 184 See "Troubleshooting Juniper ATP Cloud: Checking the Routing Engine Status" on page 186 See Troubleshooting Juniper Advanced Threat Prevention Cloud: Checking the application-identification License
Viewing system log messages	See "Viewing Juniper ATP Cloud System Log Messages" on page 188
Setting traceoptions	See "Configure Traceoptions " on page 189 See "View the Traceoptions Log File" on page 192 See "Turning Off Traceoptions" on page 192

Table 18: Troubleshooting Juniper ATP Cloud *(Continued)*

Symptom or Problem	Recommended Action
Dashboard reports not displaying any data	See "Juniper ATP Cloud Dashboard Reports Not Displaying" on page 193

Troubleshooting Juniper ATP Cloud: Checking DNS and Routing Configurations

Domain name system (DNS) servers are used for resolving hostnames to IP addresses.

For redundancy, it is a best practice to configure access to multiple DNS servers. You can configure a maximum of three DNS servers. The approach is similar to the way Web browsers resolve the names of a Web site to its network address. Additionally, Junos OS enables you configure one or more domain names, which it uses to resolve hostnames that are not fully qualified (in other words, the domain name is missing). This is convenient because you can use a hostname in configuring and operating Junos OS without the need to reference the full domain name. After adding DNS server addresses and domain names to your Junos OS configuration, you can use DNS resolvable hostnames in your configuration and commands instead of IP addresses.

DNS servers are site-specific. The following presents examples of how to check your settings. Your results will be different than those shown here.

First, check the IP addresses of your DNS servers.

```
show groups global system name-server
xxx.xxx.x.68;
xxx.xxx.xx.131;
```

If you set up next-hop, make sure it points to the correct router.

```
show routing-options
static {
    route 0.0.0.0/0 next-hop xx.xxx.xxx.1;
```

```
show groups global routing-options
static {
    route xxx.xx.0.0/12 {
        next-hop xx.xxx.xx.1;
        retain;
        no-readvertise;
    }
}
```

Use ping to verify the SRX Series Firewall can communication with the cloud server. First use the `show services advanced-anti-malware status` CLI command to get the cloud server hostname.

```
show service advanced-anti-malware status
Server connection status:
  Server hostname: xxx.xxx.xxx.com
  Server port: 443
    Control Plane:
      Connection Time: 2015-12-14 00:08:10 UTC
      Connection Status: Connected
    Service Plane:
      fpc0
        Connection Active Number: 0
        Connection Failures: 0
```

Now ping the server. Note that the cloud server will not respond to ping, but you can use this command to check that the hostname can be resolved to the IP address.

```
ping xxx.xxx.xxx.com
```

If you do not get a `ping: cannot resolve` *`hostname`*`: Unknown host` message, then the hostname can be resolved.

You can also use telnet to verify the SRX Series Firewall can communicate to the cloud server. First, check the routing table to find the external route interface. In the following example, it is `ge-0/0/3.0`.

```
show route
inet.0: 23 destinations, 23 routes (22 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 2d 17:42:53
                    > to xx.xxx.xxx.1 via ge-0/0/3.0
```

Now telnet to the cloud using port 443.

```
telnet xxx.xxx.xxx.xxx.com port 443 interface ge-0/0/3.0
Trying xx.xxx.xxx.119...
Connected to xxx.xxx.xxx.xxx.com
Escape character is '^]'
```

If telnet is successful, then your SRX Series Firewall can communicate with the cloud server.

Troubleshooting Juniper ATP Cloud: Checking Certificates

Use the `show security pki local-certificate` CLI command to check your local certificates. Ensure that you are within the certificate's valid dates. The `ssl-inspect-ca` certificate is used for SSL proxy. Shown below are some examples. Your output might look different as these are dependent on your setup and location.

```
show security pki local-certificate
Certificate identifier: ssl-inspect-ca
  Issued to: www.juniper_self.net, Issued by: CN = www.juniper_self.net, OU = IT
, O = Juniper Networks, L = xxxxx, ST = xxxxx, C = IN
  Validity:
    Not before: 11-24-2015 22:33 UTC
    Not after: 11-22-2020 22:33 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: argon-srx-cert
  Issued to: xxxx-xxxx_xxx, Issued by: C = US, O = Juniper Ne
```

```
tworks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.net) subCA for SRX dev
ices, emailAddress = xxx@juniper.net
  Validity:
    Not before: 10-30-2015 21:56 UTC
    Not after: 01-18-2038 15:00 UTC
  Public key algorithm: rsaEncryption(2048 bits)
```

Use the `show security pki ca-certificate` command to check your CA certificates. The `argon-ca` certificate is the client certificate's CA while the `argon-secintel-ca` is the server certificate's CA. Ensure that you are within the certificate's valid dates.

```
root@host> show security pki ca-certificate
Certificate identifier: argon-ca
  Issued to: SecIntel (junipersecurity.net) subCA for SRX devices, Issued by: C
= US, O = Juniper Networks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.ne
t) CA, emailAddress = xxx@juniper.net
  Validity:
    Not before: 05-19-2015 22:12 UTC
    Not after: 05- 1-2045 15:00 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: argon-secintel-ca
  Issued to: SecIntel (junipersecurity.net) CA, Issued by: C = US, O = Juniper N
etworks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.net) CA, emailAddress
 = xxx@juniper.net
  Validity:
    Not before: 05-19-2015 03:22 UTC
    Not after: 05-16-2045 03:22 UTC
  Public key algorithm: rsaEncryption(2048 bits)
```

When you enroll an SRX Series Firewall, the ops script installs two CA certificates: one for the client and one for the server. Client-side CA certificates are associated with serial numbers. Use the `show security pki local-certificate detail` CLI command to get your device's certificate details and serial number.

```
show security pki local-certificate detail
Certificate identifier: aamw-srx-cert
  Certificate version: 3
  Serial number: xxxxxxxxxx
  Issuer:
    Organization: Juniper Networks Inc, Organizational unit: SecIntel, Country: US,
    Common name: SecIntel (junipersecurity.net) subCA for SRX devices
```

```
  Subject:
    Organization: xxxxxxxxxx, Organizational unit: SRX, Country: US,
    Common name: xxxxxxxxxx
  Subject string:
    C=US, O=xxxxxxxx, OU=SRX, CN=xxxxxxxx, emailAddress=secintel-ca@juniper.net
  Alternate subject: secintel-ca@juniper.net, fqdn empty, ip empty
  Validity:
    Not before: 11-23-2015 23:08 UTC
    Not after: 01-18-2038 15:00 UTC
```

Then use the `show security pki crl detail` CLI command to make sure your serial number is not in the Certificate Revocation List (CRL). If your serial number is listed in the CRL then that SRX Series Firewall cannot connect to the cloud server.

```
show security pki crl detail
CA profile: aamw-ca
  CRL version: V00000001
  CRL issuer: C = US, O = Juniper Networks Inc, OU = SecIntel, CN = SecIntel
(junipersecurity.net) subCA for SRX devices, emailAddress = secintel-ca@juniper.net
  Effective date: 11-23-2015 23:16 UTC
  Next update: 11-24-2015 23:16 UTC
  Revocation List:
    Serial number              Revocation date
    xxxxxxxxxxxxxxxx                10-26-2015 17:43 UTC
    xxxxxxxxxxxxxxxx                11- 3-2015 19:07 UTC
    ...
```

Troubleshooting Juniper ATP Cloud: Checking the Routing Engine Status

Use the `show services advanced-anti-malware status` CLI command to show the connection status from the control plane or routing engine.

```
show services advanced-anti-malware status
Server connection status:
  Server hostname: xxx.xxx.xxx.xxx.com
  Server port: 443
```

```
    Control Plane:
      Connection Time: 2015-12-01 08:58:02 UTC
      Connection Status: Connected
    Service Plane:
      fpc0
        Connection Active Number: 0
        Connection Failures: 0
```

If the connection fails, the CLI command will display the reason in the Connection Status field. Valid options are:

- Not connected
- Initializing
- Connecting
- Connected
- Disconnected
- Connect failed
- Client certificate not configured
- Request client certificate failed
- Request server certificate validation failed
- Server certificate validation succeeded
- Server certificate validation failed
- Server hostname lookup failed

Troubleshooting Juniper ATP Cloud: Checking the Application-Identification License

You must have a valid application-identification (AppID) license installed for the supported platforms. For the complete list of supported features and platforms, see Application Identification in Feature

Explorer. Use the `show services application-identification version` CLI command to verify the applications packages have been installed. You must have version 2540 or later installed. For example:

```
show services application-identification version
Application package version: 2540
```

If you do not see the package or the package version is incorrect, use the `request services application-identification download` CLI command to download the latest application package for Junos OS AppID. For example:

```
request services application-identification download
Please use command "request services application-identification download status"  to check status
```

Then use the `request services application-identification install` CLI command to install the downloaded application signature package.

```
request services application-identification install
Please use command "request services application-identification install status"  to check status
```

Use the `show services application-identification application version` CLI command again to verify the applications packages is installed.

Viewing Juniper ATP Cloud System Log Messages

The Junos OS generates system log messages (also called syslog messages) to record events that occur on the SRX Series Firewall. Each system log message identifies the process that generated the message and briefly describes the operation or error that occurred. Juniper ATP Cloud logs are identified with a `SRX_AAWM_ACTION_LOG` or `SRX AAMWD` entry.

The following example configures basic syslog settings.

```
set groups global system syslog user * any emergency
set groups global system syslog host log kernel info
set groups global system syslog host log any notice
set groups global system syslog host log pfe info
set groups global system syslog host log interactive-commands any
set groups global system syslog file messages kernel info
```

```
set groups global system syslog file messages any any
set groups global system syslog file messages authorization info
set groups global system syslog file messages pfe info
set groups global system syslog file messages archive world-readable
```

To view events in the CLI, enter the following command:

```
show log
```

Example Log Message

```
<14> 1 2013-12-14T16:06:59.134Z pinarello RT_AAMW - SRX_AAMW_ACTION_LOG [junos@xxx.x.x.x.x.28
http-host="www.mytest.com" file-category="executable" action="BLOCK" verdict-number="8" verdict-
source=”cloud/blacklist/whitelist” source-address="x.x.x.1" source-port="57116" destination-
address="x.x.x.1" destination-port="80" protocol-id="6" application="UNKNOWN" nested-
application="UNKNOWN" policy-name="argon_policy" username="user1" session-id-32="50000002"
source-zone-name="untrust" destination-zone-name="trust"]

http-host=www.mytest.com file-category=executable action=BLOCK verdict-number=8 verdict-
source=cloud source-address=x.x.x.1 source-port=57116 destination-address=x.x.x.1 destination-
port=80 protocol-id=6 application=UNKNOWN nested-application=UNKNOWN policy-name=argon_policy
username=user1 session-id-32=50000002 source-zone-name=untrust destination-zone-name=trust
```

Configure Traceoptions

In most cases, policy logging of the traffic being permitted and denied is sufficient to verify what Juniper ATP Cloud is doing with the SRX Series Firewall data. However, in some cases you might need more information. In these instances, you can use traceoptions to monitor traffic flow into and out of the SRX Series Firewall.

Using trace options are the equivalent of debugging tools. To debug packets as they pass through the SRX Series Firewall, you need to configure `traceoptions` and flag `basic-datapath`. This configuration will trace packets as they enter the SRX Series Firewall until they exit, giving you details of the different actions the SRX Series Firewall is taking along the way. See Debugging the Data Path in the SRX Series documentation for details.

A minimum `traceoptions` configuration must include both a target `file` and a `flag`. The target `file` determines where the trace output is recorded. The `flag` defines what type of data is collected. For more information about using `traceoptions`, see the documentation for your SRX Series Firewall.

To set the trace output file, use the `file filename` option. The following example defines the trace output file as `srx_aamw.log`:

```
edit services advanced-anti-malware traceoptions
[edit services advanced-anti-malware traceoptions]
set file srx_aamw.log
```

where `flag` defines what data to collect and can be one of the following values:

- `all`—Trace everything.
- `connection`—Trace connections to the server.
- `content`—Trace the content buffer management.
- `daemon`—Trace the Juniper ATP Cloud daemon.
- `identification`—Trace file identification.
- `parser`—Trace the protocol context parser.
- `plugin`—Trace the advanced anti-malware (AAMW) plug-in.
- `policy`—Trace the AAMW policy.

The following example traces connections to the SRX Series Firewall and the AAMW policy:

```
edit services advanced-anti-malware traceoptions
[edit services advanced-anti-malware traceoptions]set services advanced-anti-malware
traceoptions file skyatp.logset services advanced-anti-malware traceoptions file size 100M
set services advanced-anti-malware traceoptions level allset services advanced-anti-malware
traceoptions flag all
```

Before committing your `traceoption` configuration, use the `show services advanced-anti-malware` command to review your settings.

```
# show services advanced-anti-malware
url https://xxx.xxx.xxx.com;
authentication {
    tls-profile
        ...
}
traceoptions {
```

```
    file skyatp.log;
    flag all;
    ...
}

...
```

You can also configure public key infrastructure (PKI) trace options. For example:

```
set security pki traceoptions file pki.log
set security pki traceoptions flag all
```

Debug tracing on both the Routing Engine and the Packet Forwarding Engine can be enabled for SSL proxy by setting the following configuration:

```
set services ssl traceoptions file ssl.log
set services ssl traceoptions file size 100m
set services ssl traceoptions flag all
```

You can enable logs in the SSL proxy profile to get to the root cause for the drop. The following errors are some of the most common:

- Server certification validation error
- The trusted CA configuration does not match your configuration.
- System failures such as memory allocation failures
- Ciphers do not match.
- SSL versions do not match.
- SSL options are not supported.
- Root CA has expired. You need to load a new root CA.

Set flow trace options to troubleshoot traffic flowing through your SRX Series Firewall:

```
set security flow traceoptions flag all
set security flow traceoptions file flow.log size 100M
```

RELATED DOCUMENTATION

- SSL Proxy
- traceoptions (Security PKI)

View the Traceoptions Log File

Once you commit the configuration, `traceoptions` starts populating the log file with data. Use the `show log` CLI command to view the log file. For example:

```
show log srx_aamw.log
```

Use `match`, `last` and `trim` commands to make the output more readable. For more information about using these commands, see Configuring Traceoptions for Debugging and Trimming Output.

Turning Off Traceoptions

`traceoptions` is very resource-intensive. We recommend you turn off `traceoptions` when you are finished to avoid any performance impact. There are two ways to turn off `traceoptions`.

The first way is to use the `deactivate` command. This is a good option if you need to activate the trace in the future. Use the `activate` command to start capturing again.

```
deactive services advanced-anti-malware traceoptionscommit
```

The second way is to remove `traceoptions` from the configuration file using the `delete` command.

```
delete services advanced-anti-malware traceoptions
commit
```

You can remove the `traceoptions` log file with the `file delete` *`filename`* CLI command or clear the contents of the file with the `clear log` *`filename`* CLI command.

Juniper ATP Cloud Dashboard Reports Not Displaying

Juniper ATP Cloud dashboard reports require the Juniper ATP Cloud premium license for the C&C Server & Malware report. If you do not see any data in this dashboard report, make sure that you have purchased a premium license. For more information, see Software Licenses for ATP Cloud.

NOTE: Juniper ATP Cloud does not require you to install a license key onto your SRX Series Firewall. Instead, your entitlement for a specific serial number is automatically transferred to the cloud server. It might take up to 24 hours for your activation to be updated in the Juniper Advanced Threat Cloud server. For more information, see Manage the Juniper Advanced Threat Prevention Cloud License.

All reports are specific to your organization; no report currently covers trends derived from the Juniper ATP Cloud worldwide database. Data reported from files uploaded from your SRX Series Firewalls and other features make up the reports shown in your dashboard.

If you did purchase a premium license and followed the configuration steps (Quick Start) and are still not seeing data in the dashboard reports, contact Juniper Networks Technical Support.

Juniper ATP Cloud RMA Process

On occasion, because of hardware failure, a device needs to be returned for repair or replacement. For these cases, contact Juniper Networks, Inc. to obtain a Return Material Authorization (RMA) number and follow the RMA Procedure.

Once you transfer your license keys to the new device, it might take up to 24 hours for the new serial number to be registered with the Juniper ATP Cloud cloud service.

WARNING: After any serial number change on the SRX Series Firewall, a new RMA serial number needs to be re-enrolled with Juniper ATP Cloud cloud. This means that you must enroll your replacement unit as a new device. See Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal. Juniper ATP Cloud does not have an “RMA state”, and does not see these as replacement devices from a configuration or registration point of view. Data is not automatically transferred to the replacement SRX Series Firewall from the old device.

PART 6

More Documentation

CHAPTER 11

Additional Documentation on Juniper.net

IN THIS CHAPTER

Links to Documentation on Juniper.net

- For more information, visit the Juniper Advanced Threat Prevention Cloud Documentation page in the Juniper Networks TechLibrary.
- For information about configuring the SRX Series with ATP Cloud using the available CLI commands, see Junos CLI Reference Guide.
- For troubleshooting information, see Juniper ATP Cloud Troubleshooting Overview.
- For Internet of Things (IoT) device discovery and classification on your security device, see Security IoT User Guide.
- For information about Juniper Security Director, Juniper Security Director Cloud and Juniper Secure Edge, visit Juniper Security Director, Juniper Security Director Cloud, and Juniper Secure Edge pages in the Juniper Networks TechLibrary.
- For more information about configuring Anti-malware and SecIntel policies using J-Web, see J-Web User Guide for SRX Series Devices.
- For information about the SRX Series Firewall, visit the SRX Series Services Gateways page in the Juniper Networks TechLibrary.