

Juniper Advanced Threat Prevention Appliance Integration with the SRX Series Device

Published
2020-11-11

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Advanced Threat Prevention Appliance Integration with the SRX Series Device
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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 the Documentation | v

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

Overview

JATP and SRX Series Device Integration Overview | 11

2

Licensing

Licensing and Platform Support information | 13

JATP and SRX Series Integration Licensing | 13

Supported SRX Series Devices | 13

3

Getting Started

Getting Started with JATP and the SRX Series Device | 17

Configure the SRX Series Device to Begin | 17

Initial Configuration | 17

Configure Interfaces and a Default Route | 18

Configure Security Zones | 18

Configure DNS | 18

Configure NTP | 19

On JATP: Login to the Web UI and Enroll SRX Series Devices | 19

Enroll the SRX Series Device to JATP Web UI | 20

On the SRX Series Device: Configure Security Policies | 23

Configure the Anti-Malware Policy | 24

Configure the SSL Forward Proxy | 24

Optionally, Configure the Anti-Malware Source Interface | 25

Configure a Security Intelligence Profile | 25

Configure a Security Policy | 25

JATP and SRX Series Threat Level Comparison Chart | 26

4

JATP Configuration

Configure SMTP and IMAP Email Management | 29

Configure File Type Profiles | 30

Global Config | 32

Add SRX Series Devices to JATP Zones | 33

Configure MSSP Multi-Tenancy Zones | 33

Add SRX Series Devices to Existing Zones | 34

Add Proxy IP Addresses for SRX Series Devices to JATP | 37

5

SRX Series Configuration

Configure the SRX Series Device SMTP Email Policies for Integration with JATP | 40

Configure the SRX Series Device IMAP Email Policies for Integration with JATP | 46

Configure the SRX Series and Geolocation IP for Integration with JATP | 53

6

JATP Incidents

Viewing and Taking Action on Infected Hosts | 57

Viewing File and Command and Control Incidents | 59

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

Use this guide to integrate the SRX Series device with the JATP Core to provide file and email scanning and feeds for blocking infected hosts.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

[Table 1 on page vi](#) defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

Overview

JATP and SRX Series Device Integration Overview | **11**

JATP and SRX Series Device Integration Overview

The Juniper Advanced Threat Prevention Appliance integrates with the SRX Series device to protect all hosts in your network against evolving security threats by employing JATP's threat detection software with a next-generation firewall system.

For this release, the SRX Series device integrates with the JATP Core to provide the following features:

- File scanning with global allowlists and blocklists.
- File scanning for administrator-created file profiles for specified file types.
- Feeds for infected hosts, command and control servers, and GeolP.
- Email attachment scanning for SMTP and IMAP.

Configuration is required on both JATP and the SRX Series device for these features.

NOTE: JATP (previously Cyphort) already worked with the SRX Series device for "Auto-Mitigation" of infected hosts using address sets. The integration described in this guide is a more complete solution that requires the SRX Series device to enroll with JATP to make use of many more features explained here.

See the [Operator's Guide](#), and the section entitled "Verifying Auto-Mitigation Rule Operations," for more details about existing options for infected host mitigation using JATP and the SRX Series, that don't include enrollment.

RELATED DOCUMENTATION

[Licensing and Platform Support information](#) | 13

[Getting Started with JATP and the SRX Series Device](#) | 17

2

CHAPTER

Licensing

Licensing and Platform Support information | **13**

Licensing and Platform Support information

IN THIS SECTION

- [JATP and SRX Series Integration Licensing | 13](#)
- [Supported SRX Series Devices | 13](#)

The following sections provide information on licensing requirements and SRX Series device platform support.

JATP and SRX Series Integration Licensing

Unlike other Layer 7 features, there is no separate license required on the SRX Series device for integration with JATP. In this deployment, the JATP Core is the licensed component. If the Core has a valid license, then the SRX Series device can connect to the Core and enroll successfully. If not, the enrollment will fail.

For JATP license upload instructions, see *Setting the Juniper ATP Appliance License Key*.

NOTE: AppSecure functionality on the SRX Series device is a pre-requisite for integrating with JATP. Depending on the SRX Series platform, a separate license may be required to enable AppSecure. Please consult the SRX Series platform data sheet for the most accurate information.

Supported SRX Series Devices

This section describes the hardware and software components that are compatible with JATP.

Platform	Hardware Requirements	Software Versions
vSRX Series		Junos 18.2R1 and above
SRX Series	SRX320, SRX300	Junos 18.3R1 and above

Platform	Hardware Requirements	Software Versions
SRX Series	SRX4100, SRX4200, SRX4600	Junos 15.1X49-D65 and above for SRX4100 and SRX4200 Junos 17.4R1-S1 and above for SRX4600
SRX Series	SRX340, SRX345, SRX550m	Junos 15.1X49-D60 and above
SRX Series	SRX5800, SRX5600, SRX5400	Junos 15.1X49-D50 and above
SRX Series	SRX1500	Junos 15.1X49-D33 and above

The following devices support scanning SMTP e-mail attachments:

- SRX300 Series device
- SRX320 Series device
- SRX340 Series device
- SRX345 Series device
- SRX1500 Series device
- SRX4100 Series device
- SRX4200 Series device
- SRX4600 Series device
- SRX5400 Series device
- SRX5600 Series device
- SRX5800 Series device
- vSRX Series

The following devices support scanning IMAP e-mail attachments:

- SRX300 Series device
- SRX320 Series device
- SRX340 Series device
- SRX345 Series device
- SRX1500 Series device
- SRX4100 Series device
- SRX4200 Series device

- SRX4600 Series device
- SRX5400 Series device
- SRX5600 Series device
- SRX5800 Series device
- vSRX Series

RELATED DOCUMENTATION

Getting Started with JATP and the SRX Series Device | 17

3

CHAPTER

Getting Started

Getting Started with JATP and the SRX Series Device | 17

JATP and SRX Series Threat Level Comparison Chart | 26

Getting Started with JATP and the SRX Series Device

IN THIS SECTION

- [Configure the SRX Series Device to Begin | 17](#)
- [On JATP: Login to the Web UI and Enroll SRX Series Devices | 19](#)
- [On the SRX Series Device: Configure Security Policies | 23](#)

These are basic setup instructions to begin using the SRX Series Services Gateway with JATP (for those less familiar with SRX). Refer to the rest of the integration document for further configuration information such as email scanning, infected hosts, and viewing incidents.

Configure the SRX Series Device to Begin

IN THIS SECTION

- [Initial Configuration | 17](#)
- [Configure Interfaces and a Default Route | 18](#)
- [Configure Security Zones | 18](#)
- [Configure DNS | 18](#)
- [Configure NTP | 19](#)

Initial Configuration

To begin using the SRX Series device:

1. Load the factory defaults.

load factory-default

2. Set the root password.

set system root-authentication <password>

3. Set the host name.

```
set system host-name <hostname>
```

4. Commit the configuration. Once you commit, you should see the host name in the prompt.

```
commit
```

Configure Interfaces and a Default Route

On the SRX Series device, configure interfaces and the default route. (For the following instructions, these are generic examples. Please insert your own addresses and interfaces):

1. Enter the following commands for interfaces:

```
set interfaces ge-0/0/2 unit 0 family inet address x.x.x.x/x
```

```
set interfaces ge-0/0/4 unit 0 family inet address x.x.x.x/x
```

```
set interfaces ge-0/0/5 unit 0 family inet address x.x.x.x/x
```

2. Enter the following to configure the default route:

```
set routing-options static route 0.0.0.0/0 next-hop x.x.x.x
```

Configure Security Zones

The SRX Series device is a zone-based firewall. You must assign each interface to a zone in order to pass traffic through it: To configure security zones, enter the following commands:

```
set security zones security-zone untrust interfaces ge-0/0/2.0
```

```
set security zones security-zone untrust interfaces ge-0/0/5.0
```

```
set security zones security-zone trust host-inbound-traffic system-services all
```

```
set security zones security-zone trust host-inbound-traffic protocols all
```

```
set security zones security-zone trust interfaces ge-0/0/4.0
```

Configure DNS

On the SRX Series device, configure DNS using the following commands:

```
set groups global system name-server x.x.x.x
```

```
set groups global system name-server x.x.x.x
```

Configure NTP

On the SRX Series device, configure NTP using the following commands:

```
set groups global system processes ntp enable
```

```
set groups global system ntp boot-server x.x.x.x
```

```
set groups global system ntp server x.x.x.x
```

On JATP: Login to the Web UI and Enroll SRX Series Devices

IN THIS SECTION

- [Enroll the SRX Series Device to JATP Web UI | 20](#)

Enroll the SRX Series Device to JATP Web UI

Enrollment establishes a secure connection between JATP and the SRX Series device. It also performs basic configurations tasks such as:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series device
- Creates local certificates and enrolls them with JATP
- Establishes a secure connection to JATP



WARNING: If you are using a custom SSL certificate with JATP, before you enroll SRX Series devices, you must upload the CA bundle containing a CA certificate which validates the JATP certificate. This ONLY applies if you are using a Custom SSL certificate. See [The Juniper ATP Operator's Guide](#) for instructions. Search for the “Managing Certificates” heading. Once this is done, proceed to the enrollment instructions.



WARNING: If you already have SRX Series devices enrolled with JATP and you change the certificate (from the default to custom or vice-versa), you must re-enroll all SRX Series devices.

**WARNING:****Network Environment Considerations and Requirements**

- It is required that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Juniper ATP Appliance. (The Packet Forwarding Engine and the Routing Engine perform independently but communicate constantly through a 100-Mbps internal link. This arrangement provides streamlined forwarding and routing control and the ability to run Internet-scale networks at high speeds. Refer to Juniper Network's [Junos](#) documentation for more information.)
- You do not need to open any ports on the SRX Series device to communicate with JATP. However, if you have a device in the middle, such as a firewall, then that device must have port 443 open.
- You cannot use FXPO interfaces to communicate with JATP. You must use a separate revenue interface.
- If you are using addresses in the same subnet for JATP management and SRX Series management, you must use a virtual router instance to separate the management and revenue interfaces. If the addresses of JATP management and SRX Series management configured through FXPO are in different subnets, you do not need to configure an additional virtual router instance. Note that traffic must be routed through the revenue interface configured for JATP management.
- If you are registering JATP through a VPN tunnel, it must be a named tunnel. JATP expects an IP address on the interface. Therefore you must configure an IP address on the VPN tunnel interface before running the OP URL script to enroll the SRX Series device. Otherwise, the registration will fail.
- SRX Series Integration with JATP requires api keys to generate the enrollment script (op url). The JATP UI only allows generating API keys for local users. Therefore, if users authenticate using radius and attempt to generate an enrollment script to register an SRX Series device, it will fail because the remote user will not have an API key. As a workaround, you can log into the JATP UI using local credentials (https://<JATP IP>/cyadmin/?local_login) and continue with the instructions below. If your network policy doesn't allow local users, there is no workaround for this issue.

To enroll a SRX Series device with JATP, do the following:

1. From the JATP web UI, you must enable the API Key for the admin user. This is used for enrolling the SRX Series device.
From the **Config** tab, navigate to **System Profile > Users**. Select the admin user for JATP and enable the **Generate New API Key** checkbox. Click **Update User**.
2. From the **Config** tab, navigate to **> System Profile > SRX settings** and click the **Enrollment URL** button in top right side of the page. A screen with the enrollment command appears.
3. Copy the entire enrollment command to your clipboard and click **OK**.
4. Paste the command into the Junos OS CLI of the SRX Series device you want to enroll with JATP and press **Enter**.

NOTE: (Optional) Use the **show services advanced-anti-malware status** CLI command to verify that a connection is made to JATP from the SRX Series device.

Once configured, the SRX Series device communicates with JATP through multiple persistent connections established over a secure channel (TLS 1.2) and the SRX Series device is authenticated using SSL client certificates.

Use the **Delete** button in the JATP **SRX settings** page to remove the SRX Series device currently enrolled in JATP. To access the Delete button, click the arrow to the left of the device name to expand device information.

Use the **Search** field at the top of the page to search for enrolled devices in the list by serial number.

On the SRX Series Device: Configure Security Policies

IN THIS SECTION

- [Configure the Anti-Malware Policy | 24](#)
- [Configure the SSL Forward Proxy | 24](#)
- [Optionally, Configure the Anti-Malware Source Interface | 25](#)
- [Configure a Security Intelligence Profile | 25](#)
- [Configure a Security Policy | 25](#)

Configure the Anti-Malware Policy

On the SRX Series device, enter the following commands to create and configure the anti-malware policy. (Note that commands for both SMTP and IMAP are included here.):

```
set services advanced-anti-malware policy aamw-policy http inspection-profile default
set services advanced-anti-malware policy aamw-policy http action permit
set services advanced-anti-malware policy aamw-policy http notification log
set services advanced-anti-malware policy aamw-policy smtp inspection-profile default
set services advanced-anti-malware policy aamw-policy smtp notification log
set services advanced-anti-malware policy aamw-policy imap inspection-profile default
set services advanced-anti-malware policy aamw-policy imap notification log
set services advanced-anti-malware policy aamw-policy fallback-options notification log
set services advanced-anti-malware policy aamw-policy default-notification log
```

Configure the SSL Forward Proxy

SSL Forward Proxy is required to collect files from HTTPS traffic in the data plane.

1. On the SRX Series device, generate the local certificate.

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

2. Load the trusted root CA profiles.

```
request security pki ca-certificate ca-profile-group load ca-group-name trusted-ca-* filename default
```

3. Enter the following commands to configure the SSL forward proxy.

```
set services ssl proxy profile ssl-inspect-profile-dut root-ca ssl-inspect-ca
set services ssl proxy profile ssl-inspect-profile-dut actions log all
set services ssl proxy profile ssl-inspect-profile-dut actions ignore-server-auth-failure
set services ssl proxy profile ssl-inspect-profile-dut trusted-ca all
```


Optionally, Configure the Anti-Malware Source Interface

If you are using a routing instance, you must configure the source interface for the anti-malware connection. If you are using a non-default routing instance, you do not have to complete this step on the SRX Series device.

```
set services advanced-anti-malware connection source-interface ge-0/0/2
```

Configure a Security Intelligence Profile

JATP and SRX use different threat level thresholds. See the [“JATP and SRX Series Threat Level Comparison Chart” on page 26](#) for information.

On the SRX Series device, enter the following commands to create a security intelligence profile on the SRX Series device.

```
set services security-intelligence profile secintel_profile category CC

set services security-intelligence profile secintel_profile rule secintel_rule match threat-level [ 7 8 9 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 secintel_profile default-rule then action permit

set services security-intelligence profile secintel_profile default-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 [ 7 8 9 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
```

Configure a Security Policy

On the SRX Series device, enter the following commands to create a security policy on the SRX Series device for the inspection profiles.

```
set security policies from-zone trust to-zone untrust policy 1 match source-address any

set security policies from-zone trust to-zone untrust policy 1 match destination-address any
```

set security policies from-zone trust to-zone untrust policy 1 match application any

set security policies from-zone trust to-zone untrust policy 1 then permit application-services ssl-proxy
profile-name ssl-inspect-profile-dut

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

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

The initial configuration is complete.

RELATED DOCUMENTATION

[JATP and SRX Series Threat Level Comparison Chart](#) | 26

JATP and SRX Series Threat Level Comparison Chart

JATP uses a threat level threshold range of 0 - 1. While the SRX Series device uses a threshold range of 0 -10. When configuring SRX Series policies that use threat levels based on information provided by JATP, please refer to the following comparison table to understand how JATP levels match those set on the SRX Series.

Table 3: Threat Level Comparisons

Severity Level	SRX Series Device	JATP
Benign	0	0
Low	1 - 3	0.25
Medium	4 - 6	0.50
High	7 - 9	0.75
Critical	10	1.0

RELATED DOCUMENTATION

4

CHAPTER

JATP Configuration

Configure SMTP and IMAP Email Management | 29

Configure File Type Profiles | 30

Global Config | 32

Add SRX Series Devices to JATP Zones | 33

Add Proxy IP Addresses for SRX Series Devices to JATP | 37

Configure SMTP and IMAP Email Management

NOTE: There are configuration fields in the JATP Web UI for various SMTP options, but IMAP allows for no configuration at this time. IMAP is either permitted or denied based on scanning verdicts and policies configured on the SRX Series device.

By default, for both SMTP and IMAP, attachments are allowed unless they are found to be malicious. If an attachment is malicious, it appears in the Incidents tab with the threat source and target listed as an email address. Quarantining of email attachments is not supported at this time.

With Email Management, enrolled SRX devices transparently submit potentially malicious email attachments to JATP for inspection. Once an attachment is evaluated, JATP assigns the file a threat score. That score is between 0 and 1, with 1 being the most malicious.

JATP assigns threat scores using the following values. Note that JATP and SRX use different threat level thresholds. See the [“JATP and SRX Series Threat Level Comparison Chart” on page 26](#) for information.

Table 4: Threat Score Values

Value	Severity
0	Benign
.25	Low
.50	Medium
.75	High
1.0	Critical

NOTE: If an email contains no attachments, it is allowed to pass without any analysis.

Benefits of Email Management

- Allows attachments to be checked against allowlists and blocklists.
- Prevents users from opening potential malware received as an email attachment.

Emails are checked against global blocklists and allowlists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches the allowlist, that email is allowed through without any scanning. If an email matches the blocklist, it is considered to be malicious and is treated as such.

To configure SMTP email management options:

1. From the **Config** tab, navigate to **System Profiles > SRX settings**. The SMTP configuration fields are in the middle of the page.
2. You can configure JATP to take one of the following actions when an email attachment is determined to be malicious:

Action to take:

- **Deliver malicious messages with warning headers added**—When you select this option, headers are added to emails that most mail servers recognize and filter into Spam or Junk folders.
- **Permit**—You can select to permit the email and the recipient receives it intact.

SMTP header:

- **X-Distribution (Bulk, Spam)**—Use this header for messages that are sent to a large distribution list and are most likely spam. You can also select "Do not add this header."
- **X-Spam-Flag**—This is a common header added to incoming emails that are possibly spam and should be redirected into spam or junk folders. You can also select "Do not add this header."
- **Subject Prefix**—You can prepend headers with information for the recipient, such as "Possible Spam."

3. Click the **Submit** button to finish and save.

RELATED DOCUMENTATION

[Configure the SRX Series Device SMTP Email Policies for Integration with JATP | 40](#)

[Configure the SRX Series Device IMAP Email Policies for Integration with JATP | 46](#)

Configure File Type Profiles

File type profiles let you define which files to send to JATP for inspection. You can group types of files to be scanned together (such as .tar, .exe, and .java) under a common name and create multiple profiles based on the content you want scanned. You then enter the profile names on eligible SRX Series devices to apply them.

Benefits of File Inspection Profiles

- Allows you to create file categories to send JATP for scanning rather than having to list every single type of file you want scanned.
- Allows you to configure multiple scanning categories based on file type, adding and removing file types when necessary, increasing or decreasing granularity.
- You can manually submit files for inspection using the JATP file_submit API. Refer to the following document on Juniper.net for instructions: [Juniper ATP HTTP API Guide](#). See the “file_submit” command in the guide for instructions.

To configure a file type profile, do the following:

1. From the **Config** tab, navigate to **System Profiles > SRX settings**. The **File Type Profile** settings are near the bottom of the page.
2. Click the **Add New Profile** button to create a new file type profile. A window opens from which you can select file types and size limits in megabytes.

NOTE: The maximum file size limit for all file types is 32MB.

NOTE: JATP ships with a default profile already defined, which you can use. Click on the default profile in the JATP Web UI to view its contents.

3. Click **Save**.

NOTE: Once the profile is created, use the **set services advanced-anti-malware policy** CLI command to associate it with the JATP profile. See [“Getting Started with JATP and the SRX Series Device” on page 17](#).

To verify your updates are on your SRX Series devices, enter the following CLI command:

```
show services advanced-anti-malware profile
```

You can compare the version numbers or the contents to verify your profile is current.

Advanced Anti-malware inspection profile:

Profile Name:default_profile

```
version: 1573769866
disabled_file_types:
{ ...
```

RELATED DOCUMENTATION

| [Getting Started with JATP and the SRX Series Device](#) | 17

Global Config

You can configure JATP to consider a host to be infected when a certain threat level is reached based on malware downloaded by that host. For example, you can add a host to the infected hosts feed when threshold of .75 is met. That host then appears in the list under **Mitigation > Hosts**.

To configure the threshold for marking hosts as infected:

- 1. From the **Config** tab, navigate to **System Profiles > SRX settings**. The Global Config setting is at the bottom of the page.
- 2. From the pulldown, select a threshold:

Table 5: Threat Score Values

Value	Severity
.25	Low
.50	Medium
.75	High
1.0	Critical

Note that JATP and SRX use different threat level thresholds. See the [“JATP and SRX Series Threat Level Comparison Chart”](#) on page 26 for information.

- 3. Click the **Submit** button to save your setting.

RELATED DOCUMENTATION

[Viewing and Taking Action on Infected Hosts | 57](#)

Add SRX Series Devices to JATP Zones

IN THIS SECTION

- [Configure MSSP Multi-Tenancy Zones | 33](#)
- [Add SRX Series Devices to Existing Zones | 34](#)

Configure MSSP Multi-Tenancy Zones

NOTE: These instructions pertain to JATP zones and the SRX Series device. The full section for JATP Zone configuration can be found in the Operator's Guide. [Configuring MSSP Multi-Tenancy Zones](#).

You can now add SRX Series devices to zones along with traffic collectors. All tenant collectors and SRX Series devices are connected to the JATP Core cluster hosted at the MSSP multi-tenancy site. All management of incidents is performed by the MSSP; tenants do not have access to the Core cluster.

A configured zone identifies incidents and events per tenant. The MSSP defines a zone per tenant and groups all collectors and SRX devices associated with a tenant to a tenant-specific Zone. JATP's event correlation stages track all events per originating zone, and correlate events within the same zone. In this way, the multi-tenant MSSP manages incidents per zone/tenant and controls all zoned JATP Central Managers per tenant using the JATP Manager of Central Managers (MCM).

To configure MSSP Zones:

1. From the JATP Appliance Central Manager Web UI, navigate to Config>System Profiles>Zones.
2. Create the new MSSP Zone.
 - View Zone data from the JATP Appliance Central Manager Web UI Incidents page.
 - Generate Reports that include Zone analytics from the JATP Appliance Web UI Reports tab.

Figure 1: Zones Configuration

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications

System Profiles

Password Reset

Roles

Zones

Users

SAML Settings

RADIUS Settings

System Settings

Certificate Management

GSS Settings

Web Collectors

Email Collectors

Secondary Cores

Zone Name

Zone Description

Cancel

Current Zones

Zone Name	Zone Description	Actions
ABC Corp	Customer_1	Delete Edit
Acme Corp	Customer_2	Delete Edit

Add SRX Series Devices to Existing Zones

When an SRX Series device enrolls to JATP, it is automatically added to a “default zone.” Use the following instructions to move an SRX Series device to a different zone.

NOTE: A zone must already exist in JATP before you can add an SRX Series device to it.

To move an SRX Series device to a different zone, do the following:

1. At the JATP Appliance Central Manager Web UI, navigate to Config>System Profiles>SRX Settings.
2. Select the SRX Series device and click Edit.
3. In the window that appears, select the Zone to which you want to add the SRX Series device and click Submit.

Figure 2: Move SRX Series Device to a different JATP Zone

The screenshot shows the JATP Appliance Web UI. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings like 'Password Reset', 'Roles', 'Zones', 'Users', 'SAML Settings', 'RADIUS Settings', 'System Settings', 'Certificate Management', 'GSS Settings', 'Web Collectors', 'SRX Settings', 'Email Collectors', 'Secondary Cares', 'Golden Image VMs', 'Licensing', 'Backup/Restore', and 'Test Malware Detection'. The main content area is titled 'Enrolled Devices' and contains a table with columns: Name, Description, Serial Number, Hostname, Zone, Model Number, OS, Enabled, and Online. A device named 'sudhir-vrx' is listed with Serial Number '0E34ED854658@20161111' and is currently in the 'Default Zone'. An 'Update SRX Device Info' modal is open, showing fields for Name (pre-filled with 'sudhir-vrx'), Description, and Zone (a dropdown menu currently set to 'Default Zone'). There are 'Submit' and 'Delete' buttons in the modal. Below the table, there are sections for 'SMTP Configuration', 'File Type Profiles', and 'Global Config'.

Note the following:

- From the SRX Settings>Config tab, you can view a column that displays the zone to which the SRX Series device belongs.
- From the Mitigation>Hosts tab, you can view a column in the list of infected hosts that displays the zone to which the SRX Series device belongs.
- Infected host feeds are sent to SRX Series devices on a per zone basis.
- View zone data from the JATP Appliance Central Manager Web UI Incidents page.
- Generate reports that include zone analytics from the JATP Appliance Web UI Reports tab.

Figure 3: Enrolled SRX Series Devices with Zone Assignments

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications

System Profiles

Enrolled Devices

Name	Description	Serial Number	Hostname	Zone	Model Number	OS	Enabled	Online
kalsrv3	vSRX3.0	e29ef70f6b79@20161111	kalsrv3	Pepsi	VSRX-S	19.1-20181219.0	✓	✗
argon-srx550-02	-	DA31716AK0004	argon-srx550-02	Default Zone	srx550m	18.4I20181122_02 S8_Jydiazhao	✓	✗
srx550-01	srx550	DA1616AK0080	argon-srx550-09	Coke	srx550m	18.3-2018-03-25.1 _DEV_COMMON	✓	✓
argon-srx550-01	srx550	DA1416AK0104	argon-srx550-01	Pepsi	srx550m	18.3R1.4	✓	✓

Enrollment URL

SMTTP Configuration

Action to Take: Deliver with Warning Header

SMTTP Header

X-Distribution: Spam

X-Spam-Flag: Yes

Subject Prefix: SUBJECT_PREFIX_JATP1

Submit

File Type Profiles

Add New Profile

Profile Name	File Categories	Maximum File Size (MB)	Actions
--------------	-----------------	------------------------	---------

Global Config

Threat Level Threshold: 0.5

Submit

Environmental Settings

Powered by Juniper Version 5.5.5 Content Version 5.5.4

Support Resources Contact Us

Figure 4: Infected Hosts with Zone Assignments

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

IP Filtering URL Filtering IPS Signatures Endpoint Infection Verification Emails Hosts

Infected Hosts

Search: All Zones

Displaying Hosts with Threat Level at or above Threat Level: 0.5

Host IP	Threat Level	Threat First Seen	Threat Last Seen	Zone	CAC Hits	Malware Hits	Host Status	State of Investigation
5.0.0.104	0.75	2019-01-23 19:52:08.284304+00	2019-01-23 19:52:08.284304+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
5.0.0.101	0.75	2019-01-23 19:37:27.333336+00	2019-01-23 19:37:32.448179+00	Pepsi	0	1	High threat level, recommend blocking host and investigating further	Open
5.0.0.101	0.75	2019-01-23 19:18:53.853774+00	2019-01-23 19:18:53.853774+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Resolved - Fixed
192.168.3.101	0.75	2018-12-12 00:10:28.009513+00	2018-12-12 00:12:10.209413+00	Default Zone	0	2	High threat level, recommend blocking host and investigating further	Open
10.1.1.45	0.5	2018-11-30 23:30:17.693933+00	2018-11-30 23:42:11.887804+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
10.1.1.41	0.5	2018-11-30 23:30:17.591588+00	2018-11-30 23:42:11.783678+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
10.1.1.39	0.5	2018-11-30 23:30:17.053003+00	2018-11-30 23:42:11.241633+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
10.1.1.35	0.5	2018-11-30 23:30:15.949322+00	2018-11-30 23:42:10.140303+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
10.1.1.26	0.5	2018-11-30 23:30:15.851383+00	2018-11-30 23:42:10.044699+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
10.1.1.20	0.5	2018-11-30 23:30:14.934462+00	2018-11-30 23:42:09.328452+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open
10.1.1.2	0.5	2018-11-30 23:30:14.507277+00	2018-11-30 23:42:08.702641+00	Default Zone	0	1	High threat level, recommend blocking host and investigating further	Open

Powered by Juniper Version 5.5.5 Content Version 5.5.4

Support Resources Contact Us

RELATED DOCUMENTATION

Configuring MSSP Multi-Tenancy Zones

JATP and SRX Series Device Integration Overview | 11

Getting Started with JATP and the SRX Series Device | 17

Viewing and Taking Action on Infected Hosts | 57

Add Proxy IP Addresses for SRX Series Devices to JATP

If there is a proxy server between the endpoint device and the SRX Series device, the session data sent from the SRX Series to JATP will have the proxy IP address as the endpoint IP address. Therefore JATP may incorrectly identify the proxy IP address as the endpoint address.

By adding the proxy IP addresses to the JATP UI and making JATP aware of them, the correct endpoint IP addresses can be obtained from the X-forwarded-for (XFF) header. JATP can then use the trusted proxy IP address to validate the proxy IP address from the X-forwarded-for field and replace the real endpoint IP address.

To add proxy IP addresses to JATP:

1. Login to the JATP UI.
2. Select **Config > System Profiles > SRX Settings**.
3. Select the **SRX Series device** and click **Edit** as shown in [Figure 5 on page 37](#).

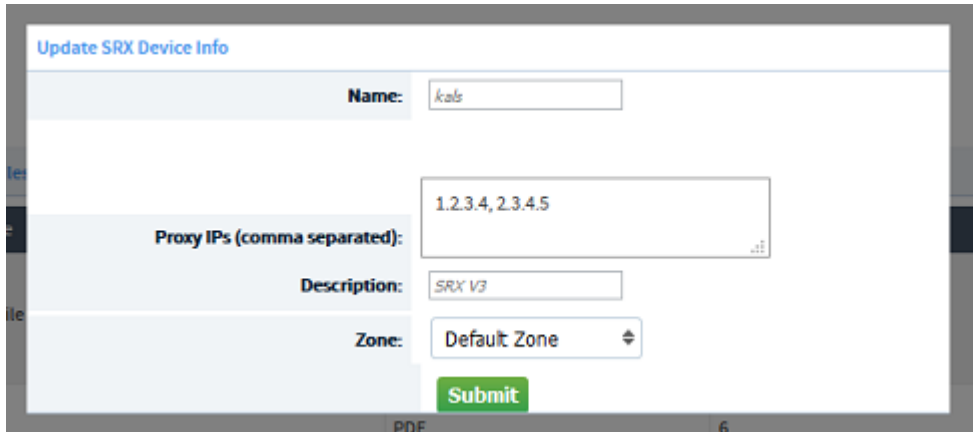
Figure 5: Enrolled Devices Page

[illegible]

The Update SRX Device Info page is displayed as shown in [Figure 6 on page 38](#).

4. Add the proxy IP address or addresses and click **Submit**.

Figure 6: Update SRX Device Info Page



The screenshot shows a web form titled "Update SRX Device Info". The form contains the following fields and controls:

- Name:** A text input field containing the value "kale".
- Proxy IPs (comma separated):** A text input field containing the value "1.2.3.4, 2.3.4.5".
- Description:** A text input field containing the value "SRX V3".
- Zone:** A dropdown menu with "Default Zone" selected.
- Submit:** A green button with the text "Submit".

At the bottom of the form, there is a "PDF" icon and a page number "6".

RELATED DOCUMENTATION

[Add SRX Series Devices to JATP Zones](#) | 33

5

CHAPTER

SRX Series Configuration

Configure the SRX Series Device SMTP Email Policies for Integration with JATP | 40

Configure the SRX Series Device IMAP Email Policies for Integration with JATP | 46

Configure the SRX Series and Geolocation IP for Integration with JATP | 53

Configure the SRX Series Device SMTP Email Policies for Integration with JATP

The SMTP email management action to take is defined in the **Config > System Profiles > SRX settings > SMTP**. All other actions are defined with CLI commands.

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

```
user@host# 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:

```
user@host> 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.

```
user@host# show security policies from-zone trust to-zone untrust {
  policy p1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
```



```

        client-certificate jatp-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.

```
user@host> 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 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.

For debugging purposes, you can also set SMTP trace options.

```
user@host# set services advanced-anti-malware traceoptions flag smtp
```

Before configuring the SMTP threat prevention policy, you can do the following:

- (Optional) Create a **File Type Profile** in the JATP UI 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 JATP policy.

- In this example, the policy name is **smtppolicy1**.

```
user@host# set services advanced-anti-malware policy smtppolicy1
```

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

```
user@host# set services advanced-anti-malware policy smtpolicy1
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.

```
user@host# set services advanced-anti-malware policy smtpolicy1
verdict-threshold 7
```

- Apply the SMTP protocol and turn on notification.

```
user@host# set services advanced-anti-malware policy smtpolicy1 smtp
notification log
```

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

```
set services advanced-anti-malware policy smtpolicy1 default-notification log
```

- When there is an error condition, send the email to the recipient and create a log entry.

```
set services advanced-anti-malware policy smtpolicy1 fallback-options action
permit
set services advanced-anti-malware policy smtpolicy1 fallback-options
notification log
```

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

```
[edit security zones]
user@host# set security policies from-zone untrust to-zone trust policy 1 then
permit application-services advanced-anti-malware smtpolicy1
```

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 device certificate repository.

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

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

```
user@host# set services ssl proxy profile server-protection-profile
server-certificate server1_cert_id
```

RELATED DOCUMENTATION

[Configure SMTP and IMAP Email Management](#) | 29

Configure the SRX Series Device IMAP Email Policies for Integration with JATP

IMAP email management has no configuration page in JATP. Similar to SMTP, actions are defined with CLI commands on the SRX Series device.

With IMAP, a default profile is send to the SRX Series device whereby all attachments are scanned and allowed unless an attachment is found to be malicious.

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

```
user@host# 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:

```

user@host> 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 placed in trust to untrust zone. See the example below.

```
user@host# 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, a verdict score of 8 and above indicates malware.

```
user@root> 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 the SRX Series documentation.

```

# show services ssl
initiation { # for cloud connection
  profile srx_to_jatp_tls_profile_name {
    trusted-ca jatp-secintel-ca;
    client-certificate jatp-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.

```

user@host> 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 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.

For debugging purposes, you can also set IMAP trace options.

```
user@host# set services advanced-anti-malware traceoptions flag imap
```

Before configuring the IMAP threat prevention policy, you can do the following:

- (Optional) Create a **File Type Profile** in the JATP UI 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 on the SRX Series device:

1. Create the JATP policy.

- In this example, the policy name is **imappolicy1**.

```
user@host# set services advanced-anti-malware policy imappolicy1
```

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

```
user@host# 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.

```
user@host# set services advanced-anti-malware policy imappolicy1
verdict-threshold 7
```

- Apply the IMAP protocol and turn on notification.

```
user@host# 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
```

- When there is an error condition, send the email to the recipient and create a log entry.

```
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 application service.

```
[edit security zones]
user@host# 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 device certificate repository.

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

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

```
user@host# set services ssl proxy profile server-protection-profile  
server-certificate server1_cert_id
```

RELATED DOCUMENTATION

| [Configure SMTP and IMAP Email Management](#) | 29

Configure the SRX Series and Geolocation IP for Integration with JATP

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

GeoIP uses a Dynamic Address Entry (DAE) infrastructure. A DAE is a group of IP addresses, not just a single IP prefix. 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.

NOTE: The feed URL is set up automatically for you when you run the script to enroll the SRX Series device. Currently, configuring GeoIP and security policies is done completely on the SRX Series device using CLI commands.

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](#).

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

```
root@host# set security dynamic-address address-name my-geoip profile category
GeoIP property country string US
root@host# 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:

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

[edit]
```

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**.

```
root@host# set security policies from-zone untrust to-zone trust policy
my-geoip-policy match source-address my-geoip destination-address any application
any
```

```
root@host# 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:

```
root@host# 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;
    }
  }
}
...
```

RELATED DOCUMENTATION

[Getting Started with JATP and the SRX Series Device](#) | 17

6

CHAPTER

JATP Incidents

Viewing and Taking Action on Infected Hosts | 57

Viewing File and Command and Control Incidents | 59

Viewing and Taking Action on Infected Hosts

View infected hosts by navigating to the **Mitigation > Infected Hosts** tab.

Infected hosts are systems where there is a high confidence that attackers have gained unauthorized access. When a host is compromised, the attacker can do several things to the computer, such as:

- Send junk or spam email to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.
- Disable your computer's security settings to allow easy access.

From the **Mitigation > Infected Hosts** tab, you can view infected hosts and set the status for the investigation and mitigation.

1. When viewing the list of infected hosts, click the link in the **State of Investigation** column for the host and a pop-up window with a pulldown appears. You can select one of the following: Open, In Progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.

NOTE: An infected host marked as resolved will remain in the Infected Hosts tab for 60 days, but it will have a threat level score of 0.

2. Click the **Submit** button.
3. To mitigate an infected host, locate the event in the **Incidents** tab. For each incident, you can view the **Summary** tab, which includes information about the threat, and the **Downloads** tab. From the Downloads tab, you can take the following actions:
 - Find on VirusTotal—VirusTotal is a web site that analyzes suspicious files and URLs to detect types of malware. You can also search for malware on this site by entering a URL, IP address, domain, or file hash.
 - Download PCAP trace—Click this link to download the pcap (packet capture) file data collected by the SRX Series device. You are prompted to save the file. (Note that there is no collector dashboard for the SRX Series at this time.)
 - Download Sample—Click this link to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the Download tab for the file in question..
 - Download Behavior Log—Click this link to download a zip file containing log information about the malware. You are prompted to save the file.

- **Add to Whitelist**—If you believe the file was incorrectly categorized as malware, click this link to add the file to the allowlist so that it will not be blocked.
- **Report False Positive**—Click this link to report a false positive. You are prompted to create a ticket and to fill in information to explain the issue.

More Information about Infected Hosts

Infected hosts are listed as data feeds (also called information sources). The feed lists the IP address or IP subnet of the host along with a threat level, for example, xxx.xxx.xxx.133 and threat level 1. Once identified, JATP recommends an action and you can create security policies on the SRX Series device to take enforcement actions on the inbound and outbound traffic on these infected hosts. JATP uses multiple indicators, such as a client attempting to contact a C&C server or a client attempting to download malware.

The process for determining infected hosts and acting on that determination is as follows:

Step	Description
1	A client with IP address 10.1.1.1 is located behind an SRX Series device and requests a file to be downloaded from the Internet.
2	The SRX Series device receives the file from the Internet and checks its security policies to see if any action needs to be taken before sending the file to the client.
3	<p>The SRX Series device has a JATP policy that requires files of the same type that was just downloaded to be sent to JATP for inspection.</p> <p>This file is not cached in JATP, meaning this is the first time this specific file has been sent to JATP for inspection, so the SRX Series device sends the file to the client while JATP performs an inspection.</p>
4	<p>In this example, the JATP analysis determines the file has a threat level greater than the threshold indicating that the file is malware, and sends this information back to the SRX Series device.</p> <p>The client is placed on the infected host list.</p>
5	<p>Using the infected hosts feed from JATP, the SRX Series device blocks the client from accessing the Internet.</p> <p>The client remains on the infected host list until an administrator performs further analysis and determines it is safe.</p>

RELATED DOCUMENTATION

Viewing File and Command and Control Incidents

In the JATP Web UI, view file and command and control detections from the **Incidents** tab.

- View downloaded file incidents by looking for **DL** in the Progression field. Select an incident to view the progression of the malware in the **Summary** tab at the bottom of the page. From the **Action** pulldown, you can select to Mitigate the incident or view the infection Timeline.
- View command and control server incidents by looking for **IN** in the Progression field. Select an incident to view the progression of the malware in the **Summary** tab at the bottom of the page. From the **Action** pulldown, you can select to Mitigate the incident or view the infection Timeline.
- In some cases, an incident may have both **DL** and **IN** in the progression field.

For each incident type, when you click on a log entry, additional information is provided at the bottom of the page in tabs.

Downloads Tab—For file incidents, in addition to the Summary tab, there is also a Downloads tab from which you can take the following actions:

- Find on VirusTotal—VirusTotal is a web site that analyzes suspicious files and URLs to detect types of malware. You can also search for malware on this site by entering a URL, IP address, domain, or file hash.
- Download PCAP trace—Click this link to download the pcap (packet capture) file data collected by the SRX Series device. You are prompted to save the file. (Note that there is no collector dashboard for the SRX Series at this time.)
- Download Sample—Click this link to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the Download tab for the file in question..
- Download Behavior Log—Click this link to download a zip file containing log information about the malware. You are prompted to save the file.
- Add to Whitelist—If you believe the file was incorrectly categorized as malware, click this link to add the file to the allowlist so that it will not be blocked.
- Report False Positive—Click this link to report a false positive. You are prompted to create a ticket and to fill in information to explain the issue.

Infections Tab—For command and control server hits, in addition to the Summary tab, there is also a Infections tab from which you can view more information on the threat such as the threat name, severity,

category of threat, and the name of the feed that blocked the threat. You can also add the threat to the allowlist and report it as a false positive.

RELATED DOCUMENTATION

| [Viewing and Taking Action on Infected Hosts](#) | 57