Juniper Sky ATP Getting Started

Ready. Set. Let's go!

Configure your SRX Series device, log into the Juniper Sky ATP web portal, and begin using Juniper Sky ATP.

Configure the SRX Series Device to Begin

Initial Configuration

To begin using the SRX Series device:

1. Load the factory defaults.

   root@host# load factory-default

2. Set the root password.

   root@host# set system root-authentication <password>

3. Set the host name. Note that Juniper Sky ATP requires your SRX Series device host name contain only alphanumeric ASCII characters (a-z, A-Z, 0-9), the underscore symbol (_), and the dash symbol (-).

   root@host# set system host-name <hostname>

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

   root@host# commit

Configure Interfaces and a Default Route

On the SRX Series device, configure interfaces and the default route. (For the following instructions, please insert your own addresses for "x.x.x.x."):

1. Enter the following commands for interfaces:

   user@host# set interfaces ge-x/x/2 unit 0 family inet address x.x.x.x/x

```
user@host# set interfaces ge-x/x/4 unit 0 family inet address x.x.x.x/x
user@host# set interfaces ge-x/x/5 unit 0 family inet address x.x.x.x/x
user@host# commit
```

2. Enter the following to configure the default route:

```
user@host# set routing-options static route 0.0.0.0/0 next-hop x.x.x.x
user@host# commit
```

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:

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

```
user@host# set security zones security-zone untrust interfaces ge-x/x/2
user@host# set security zones security-zone untrust interfaces ge-x/x/5
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-x/x/4
user@host# commit
```

Configure DNS

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

```
user@host# set groups global system name-server x.x.x.x
user@host# set groups global system name-server x.x.x.x
user@host# commit
```

Configure NTP

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

```
user@host# set groups global system processes ntp enable
user@host# set groups global system ntp boot-server x.x.x.x
user@host# set groups global system ntp server x.x.x.x
```

```
user@host# commit
```

On Juniper Sky ATP: Login to the Web Portal and Enroll SRX Series Devices

Obtain a License and Enroll the SRX Series Device

Contact your local sales office or Juniper Networks partner to place an order for a Juniper Sky ATP premium or basic license. Once the order is complete, an activation code is e-mailed to you. You will use this code in conjunction with your SRX Series device serial number to generate a premium or basic license entitlement. (Use the **show chassis hardware** CLI command to find the serial number of the SRX Series device.)

1. Go to https://www.juniper.net/generate_license/ and log in with your Juniper Networks Customer Support Center (CSC) credentials.

2. In the Generate Licenses list, select J Series Service Routers and SRX Series Devices.

3. Using your authorization code and SRX Series serial number, follow the instructions to generate your license key. (Note that you do not enter this license key anywhere.)

   Once generated, your license key is automatically transferred to the cloud server. It can take up to 24 hours for your activation to be updated in the Juniper Sky ATP cloud server.

NOTE: **For vSRX: If you are using Juniper Sky ATP with vSRX, the license is not automatically transferred. You must install the license.**

Create a Juniper Sky ATP Cloud Web Portal Login Account

1. Go to the customer portal URL for your location. On the next screen, click **Create a security realm**.

   The customer portal hostname varies by location. Please refer to the following table:

Location	Customer Portal URL
United States	Customer Portal: **https://amer.sky.junipersecurity.net**
European Union	Customer Portal: **https://euapac.sky.junipersecurity.net**
APAC	Customer Portal: **https://apac.sky.junipersecurity.net**
Canada	Customer Portal: **https://canada.sky.junipersecurity.net**

2. Enter the following required information and continue to click Next until you are finished:

   - Your single sign-on or Juniper Networks CSC credentials.
   - A security realm name — for example, Juniper-Mktg-Sunnyvale. Realm names can only contain alphanumeric characters and the dash ("-") symbol.
   - Your contact information.
   - An e-mail address and password. This will be your login information to access the Juniper Sky ATP management interface.

   When you click **Finish**, you are automatically logged in and taken to the Juniper Sky ATP Web UI dashboard.

Enroll SRX Series Devices with Juniper Sky ATP

Enrollment establishes a secure connection between the Juniper Sky ATP cloud server 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 the cloud server
- Establishes a secure connection to the cloud server

NOTE: Juniper Sky Advanced Threat Prevention 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 device to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have ports 80, 8080, and 443 open.

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

1. Go to https://amer.sky.junipersecurity.net and log in.

2. Navigate to **Devices** in the Juniper Sky ATP Web UI and click the **Enroll** button.

3. Run the provided command on the SRX Series device to enroll it.

NOTE: The "op url" command must be run from operational mode. Once generated, the op url command is valid for 7 days. If you generate a new op url command within that time, the old command is no longer valid. (Only the most recently generated op url command is valid.)

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

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

On the SRX Series Device: Configure Security Policies

Now you move back to the SRX Series device.

Configure the Anti-Malware Policy

On the SRX Series device, enter the following commands to create and configure the anti-malware policy.:

user@host# set services advanced-anti-malware policy *aamw-policy* verdict-threshold 7

user@host# set services advanced-anti-malware policy *aamw-policy* http inspection-profile default

user@host# set services advanced-anti-malware policy *aamw-policy* http action permit

user@host# set services advanced-anti-malware policy *aamw-policy* http notification log

user@host# set services advanced-anti-malware policy *aamw-policy* smtp inspection-profile default

user@host# set services advanced-anti-malware policy *aamw-policy* smtp notification log

user@host# set services advanced-anti-malware policy *aamw-policy* imap inspection-profile default

user@host# set services advanced-anti-malware policy *aamw-policy* imap notification log

user@host# set services advanced-anti-malware policy *aamw-policy* fallback-options notification log

user@host# set services advanced-anti-malware policy *aamw-policy* default-notification log

user@host# commit

Configure the SSL Forward Proxy

SSL Forward Proxy is required for HTTP(s) traffic in the data plane.

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

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

   user@host> 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.

   user@host> 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.

   user@host# set services ssl proxy profile *ssl-inspect-profile-dut* root-ca ssl-inspect-ca

   user@host# set services ssl proxy profile *ssl-inspect-profile-dut* actions log all

   user@host# set services ssl proxy profile *ssl-inspect-profile-dut* actions ignore-server-auth-failure

   user@host# set services ssl proxy profile *ssl-inspect-profile-dut* trusted-ca all

   user@host# commit

NOTE: Note that internal clients must trust certificates generated by the SRX Series device. Therefore you must import the root CA as a trusted CA into client browsers. This is required for the client browsers to trust the certificates signed by the SRX Series device. See Importing a Root CA Certificate into a Browser.

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.

user@host# set services advanced-anti-malware connection source-interface ge-x/x/2

Configure a Security Intelligence Profile

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

user@host# set services security-intelligence profile *secintel_profile* category CC

user@host# set services security-intelligence profile *secintel_profile* rule *secintel_rule* match threat-level [7 8 9 10]

user@host# set services security-intelligence profile *secintel_profile* rule *secintel_rule* then action block drop

user@host# set services security-intelligence profile *secintel_profile* rule *secintel_rule* then log

user@host# set services security-intelligence profile *secintel_profile* default-rule then action permit

user@host# set services security-intelligence profile *secintel_profile* default-rule then log

user@host# set services security-intelligence profile *ih_profile* category Infected-Hosts

user@host# set services security-intelligence profile *ih_profile* rule *ih_rule* match threat-level [7 8 9 10]

user@host# set services security-intelligence profile *ih_profile* rule *ih_rule* then action block drop

user@host# set services security-intelligence profile *ih_profile* rule *ih_rule* then log

user@host# set services security-intelligence policy *secintel_policy* Infected-Hosts *ih_profile*

user@host# set services security-intelligence policy *secintel_policy* CC *secintel_profile*

user@host# commit

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.

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

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

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

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

user@host# set security policies from-zone trust to-zone untrust policy 1 then permit application-services advanced-anti-malware-policy *aamw-policy*

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

user@host# commit and-quit

The initial configuration is complete.

Modified: 2018-08-30