JUNIPER NETWORKS | Engineering Simplicity

Junos OS

Security IoT User Guide

Published
2025-08-06

JUNOS

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

Junos OS Security IoT User 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 learn about IoT device discovery and classification feature on your security device. Knowledge of IoT devices in a network helps network administrators to better manage network security and reduce the IoT attack surface

1
CHAPTER

Overview

IN THIS CHAPTER

IoT Security Overview

SUMMARY

Read this guide to understand about the IoT security solution available on your SRX Series/NFX Series devices and learn how to start using the feature.

IN THIS SECTION

Read this topic to learn about Juniper Networks security IoT and how it helps to get visibility into IoT devices in your network.

Introduction

In terms of scale, the Internet of Things (IoT) is taking over the network. As a technology, IoT is transformational, enriching data, adding context into processes, and providing unprecedented levels of visibility across organizations. The volume and variety of IoT devices such as IP cameras, smart elevators, medical equipment, and industrial controllers can add complexity in your network security. With so many devices on the network, you need real-time visibility, intelligent policy enforcement capabilities that work seamlessly across the network. Most IoT endpoints have limited footprints and unknown devices the network can be a reason for security incident.

Knowledge of IoT devices in a network allows users or network administrators to better manage their network security. It is even more important to have visibility of IoT devices in a network especially since zero-day vulnerabilities are exploding.

Juniper Networks security IoT solution provides discovery, visibility, and classification of IoT devices in the network. IoT device visibility helps you to continuously discover, monitor and enforce security policies across all connected IoT devices.

Security IoT Solution

IN THIS SECTION

The Juniper Networks Security IoT solution involves the integration of security devices with Juniper ATP Cloud to:

- Provide deep insight into IOT devices in the network in real-time
- Create security policies using the discovered IoT device's attributes
- Enforce security policies to prevent attacks and reduce attack surface

IOT device discovery provides basis for enforcing security policies and address security risk by identifying abnormal behavior of discovered devices.

Features

- Discovery of IoT devices behind Wi-Fi access point
- Support for broad range of IoT devices
- Granular fingerprints on each device including type, brand, model, IP, MAC address
- Single pane of glass for efficient IoT device inventory and classification
- Granular security rules based on IoT device attributes

Benefits of Security IOT

- Discovering and managing all IoT devices in a network without manual intervention increases security operations efficiency and productivity
- Having an real-time inventory of IoT devices and related security policies helps in reducing attack surface within your network.

Use Cases

Security IoT solution is adaptable different environments including healthcare/medical industry, organizations with campus/branch offices, and other industries with smart buildings and offices.

IoT Device Discovery and Security Enforcement - Workflow

IN THIS SECTION

Terminology

Let's get familiar with some of the terminologies in this document before we deep-dive into IoT device discovery and security enforcement.

Table 1: Security IoT Terminology

IOT Terms	Description
IoT devices	IoT devices are the physical devices that establish a wireless connection to a network and can transmit data over the Internet or other networks. IoT devices can be sensors, gadgets, appliances, or machines or embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, and more.
Data streaming	Process of transmitting packets and related metadata from IoT devices to a Juniper ATP Cloud to identify and classify IoT devices.
Web socket	A communications protocol is used for bi-directional data transfer between the security device and Juniper ATP cloud to provide confidentiality.

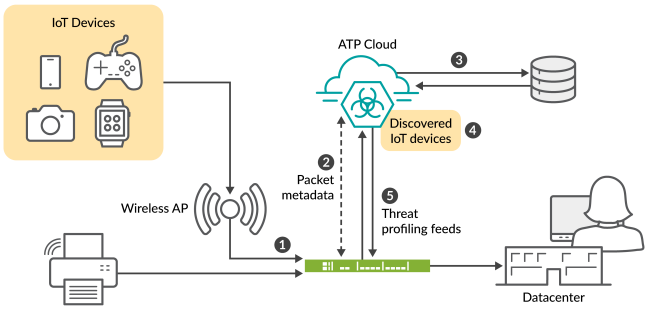
Table 1: Security IoT Terminology *(Continued)*

IOT Terms	Description
Serialization	Protocol buffers (gpb) format used to serialize structured data and enable communication between security device and ATP cloud.
Authentication	Process of enabling secure communication between security device and Juniper ATP cloud using TLS1.2 or later versions to ensure authentication, encryption, and integrity of the shared data.
IoT device discovery	Process of identifying IoT devices by searching through an internal database using the streamed data. The details of the discovered IoT devices includes-device brand, type, model, operating system, manufacturer, and so on. Security IoT supports HTTP, DNS, DHCP, SSL, and UPNP protocols for IoT device discovery.
IoT device classification	Building a profile for the discovered IoT devices. Since an IoT device can belong to a wide range of device types, knowing the class of the IoT device is important for enforcing the right type of security policy. Example: An infotainment IoT device has a different traffic profile compared to an industrial IoT device.
Data Filtering	Using data filter helps Juniper ATP Cloud to control the amount of data, type of data it receives from the security device. Filters are especially useful where a large number of IoT devices are available in the network. Security IoT does not support IPv6-based filters.
IP address feeds/dynamic address groups	A dynamic address entry is a group of IP addresses, that share a common purpose or attribute such as a geographical origin, a threat type, or a threat level. IP addresses of discovered IoT devices are grouped into a dynamic address group. You can use IP address feeds to enforce policy in real time secure network.

IoT Device Discovery and Enforcement Workflow

Following illustration depicts a typical workflow involved in IOT device discovery.

Figure 1: Security IoT Workflow



1. Security device inspects network traffic from IoT devices.
2. Security device connects to Juniper ATP cloud and streams details to the Juniper ATP cloud. The details include metadata about traffic flow, and packet payloads.
3. Juniper ATP Cloud uses the streamed data to get the details of the IoT device such as brand, device model, class, vendor, IP, MAC address, and other properties of IoT devices.
4. Juniper ATP Cloud successfully classifies the IoT device. The devices that Juniper ATP Cloud discovers and identifies appear on the Juniper ATP Cloud page. You can use the device details to create a IP address feeds in the form of dynamic address group using adaptive threat profiling feature.
5. The security device downloads the feed. You can create security rules based on the IP address feeds to enforce granular security rules based on the IoT device attributes.

The security device continues to analyze the traffic pattern of the discovered IoT devices and detect any traffic deviation (for example, reachability and amount of traffic it might send) for these devices. You can

isolate an IoT device from the network depending on the policy, and enforce a customized security policy to limit the reach of these devices in the network.

What's Next?

In the next section, you'll learn how to configure IoT device discovery and enforcement on your security device.

2

CHAPTER

Configuration

IN THIS CHAPTER

Example: Configure IoT Device Discovery and Policy Enforcement

SUMMARY

In this example, you'll configure your security device for IoT device discovery and security policy enforcement.

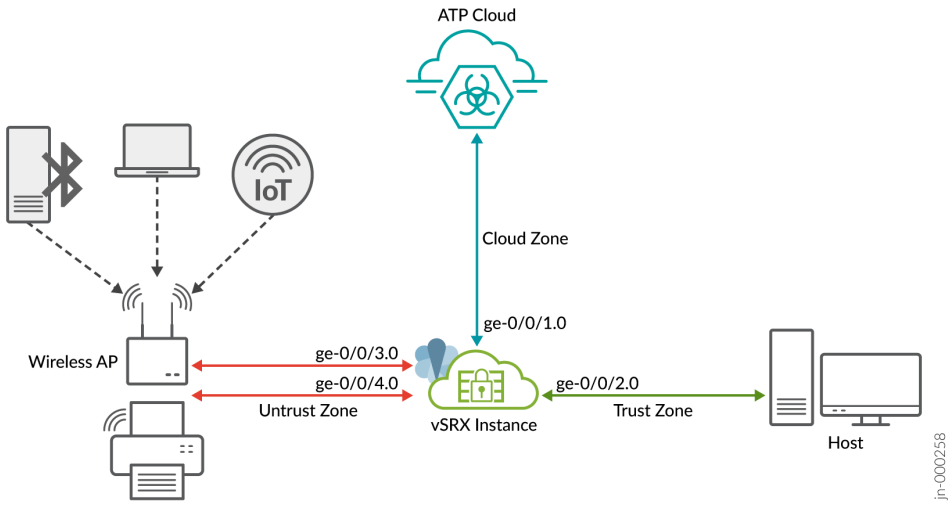
IN THIS SECTION

Overview

IN THIS SECTION

To get started with IoT device discovery in your network, all you need is a security device connected to Juniper ATP Cloud. Figure 2 on page 10 shows the topology used in this example.

Figure 2: IoT Device Discovery and Policy Enforcement Topology



As shown in the topology, the network includes some IoT devices connected to an SRX Series Firewall through wireless access point (AP). The security device is connected to the Juniper Cloud ATP server, and to a host device.

The security device collects IoT device metadata and streams the relevant information to the Juniper ATP Cloud. To enable streaming of IoT metadata, you'll need to create security metadata streaming policies and attach these policies to security policies. Streaming of the IoT device traffic pauses automatically when Juniper Cloud server has sufficient details to classify the IoT device.

Juniper ATP cloud discovers and classifies IoT devices. Using the inventory of discovered IoT devices, you'll create threat feeds in the form of dynamic address groups. Once the security device downloads dynamic address groups, you can use the dynamic address groups to create and enforce security policies for the IoT traffic.

Table 2 on page 10 and Table 3 on page 11 provide details of the parameters used in this example.

Table 2: Security Zone Configuration Parameters

Zones	Interfaces	Connected To
trust	ge-0/0/2.0	Client device
untrust	ge-0/0/4.0 and ge-0/0/3.0	Access points to manage IoT traffic
cloud	ge-0/0/1.0	Internet (to connect to Juniper ATP cloud)

Table 3: Security Policy Configuration Parameters

Policy	Type	Application
P1	Security policy	Allows traffic from trust zone to untrust zone
P2	Security policy	Allows traffic from untrust zone to trust zone
P3	Security policy	Allows traffic from trust zone to cloud zone
p1	Metadata streaming Policy	Streams untrust zone to trust zone traffic metadata
p2	Metadata streaming Policy	Streams trust zone to clod zone traffic metadata
Unwanted_Applications	Global Security Policy	Prevents IoT traffic based on the threat feed and security policy at global-context

Requirements

- SRX Series Firewall or NFX Series device
- IoT security is a premium ATP feature and requires a premium license (Premium 1 or Premium 2) for entitlement. For details, check Software Licenses for ATP Cloud.
- Junos OS Release 22.1R1 or later
- Juniper Advanced Threat Prevention Cloud Account. See Registering a Juniper Advanced Threat Prevention Cloud Account.

We've verified and tested the configuration using a vSRX Virtual Firewall instance with Junos OS Release 22.1R1.

Configuration

IN THIS SECTION

Get Your SRX Series Firewall Ready to Work with Juniper ATP Cloud

You'll need to configure your SRX Series Firewall to communicate with the Juniper ATP Cloud Web Portal. Ensure your SRX Series Firewall is connected to Internet. Ensure that you complete the following initial configuration to set your SRX Series Firewall to Internet.

1. Configure the interface. In this example, we're using the interface ge-0/0/1.0 as Internet-facing interface on SRX Series Firewall.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.50.50.1/24
```

2. Add the interface to a security zones.

```
[edit]
user@host# set security zones security-zone cloud interfaces ge-0/0/1.0 host-inbound-traffic
system-services all
user@host# set security zones security-zone cloud interfaces ge-0/0/1.0 host-inbound-traffic
protocols all
```

3. Configure DNS.

```
[edit]
user@host# set groups global system name-server 172.16.1.1
```

4. Configure NTP.

```
[edit]
user@host# set groups global system processes ntp enable
user@host# set groups global system ntp boot-server 192.168.1.20
user@host# set groups global system ntp server 192.168.1.20
```

Once your SRX Series can reach the Internet through the ge-0/0/1.0 interface, proceed with next steps.

Check Required Licenses and Application Signature Package

- Ensure that you have an appropriate Juniper ATP cloud license. Use the `show system license` command to check the license status. The output might show the legacy ATP Cloud branding (SkyATP) based on the SRX device type (SRX or vSRX) and the JUNOS version as shown in the following samples:

```
user@host> show system license
  License identifier: JUNOS123456
  License version: 4
  Software Serial Number: 1234567890
  Customer ID: JuniperTest
  Features:
    Sky ATP          - Sky ATP: Cloud Based Advanced Threat Prevention on SRX firewalls
      date-based, 2016-07-19 17:00:00 PDT - 2016-07-30 17:00:00 PDT
```

```
root@host> show system license

  License identifier: JUNOS123456
  License version: 4
  Software Serial Number: 1234567890
  Customer ID: JuniperTest
  Features:
    ATP Cloud          - Cloud Based Advanced Threat Prevention on SRX firewalls
      date-based, 2016-07-19 17:00:00 PDT - 2016-07-30 17:00:00 PDT
```

NOTE: The `show system license` command on an SRX Series Firewall might not display an ATP Cloud license if the entitlement is managed in the cloud. This is because the SRX Series devices do not require an installed license key for ATP Cloud; instead, the entitlement is automatically transferred to the cloud server when you generate the license key using your SRX Series serial number and authorization code. For vSRX Virtual Firewalls, an installed license is required.

- Ensure your device has the latest application signature pack on your security device.
  - Verify the application identification license is installed on your device.

```
user@host> show system license
License usage:
Licenses Licenses Licenses Expiry
Feature name used installed needed
logical-system 4 1 3 permanent
License identifier: JUNOSXXXXXX
License version: 2
Valid for device: AA4XXXX005
Features:
appid-sig - APPID Signatur
```

  - Download latest version of application signature pack.

```
user@host> request services application-identification download
```

  - Check the download status.

```
user@host> request services application-identification download status
Downloading application package 3475 succeeded.
```

  - Install the application identification signature pack.

```
user@host> request services application-identification install
```

- Check the installed application signature pack version.

```
user@host> show services application-identification version
  Application package version: 3418
  Release date: Tue Sep 14 14:40:55 2021 UTC
```

Enroll Security Device with Juniper ATP Cloud

Lets start with enrolling the security device with Juniper ATP cloud. If you've already enrolled your device, you can skip this step and jump directly to "Configure IoT Traffic Streaming Settings" on page 18. If not, use one of the following method for device enrollment.

Method 1: Enrolling Security Device Using CLI

1. On your SRX Series Firewall, run the following command to initiate the enrollment process.

```
user@host> 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 new realm.

```
Enroll SRX to:
1. A new SkyATP security realm (you will be required to create it first)
2. An existing SkyATP security realm
```

Select option 1 to create a realm. Use the following steps:

a.
```
You are going to create a new Sky ATP realm, please provide the required information:
```

b.
```
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
```

c.
```
Please enter your company name:
Company name: Example Company A
```

d.
```
Please enter your e-mail address. This will be your username for your Sky ATP account:
Email: me@example-company-a.com
```

e.
```
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: **********
```

f.
```
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
```

g.
```
Create a new realm with the above information? [yes,no]
yes
Device enrolled successfully!
```

You can also use an existing realm for enrolling your SRX Series with Juniper ATP Cloud.

3. Use the `show services advanced-anti-malware` status CLI command to confirm that your SRX Series Firewall is connected to the cloud server.

```
root@idpreg-iot-v2# run show services advanced-anti-malware dynamic-filter status
Feb 09 18:36:46
Dynamic Filter Server Connection Status:
  Server Hostname: srxapi.us-west-2.sky.junipersecurity.net
  Server Port: 443
  Proxy Hostname: None
  Proxy Port: None
```

```
  Control Plane
    Connection Status: Connected
    Last Successful Connect: 2022-02-09 18:36:07 PST
    Pkts Sent: 2
    Pkts Received: 6
```

Method 2: Enrolling Security Device in Juniper ATP Cloud Web Portal

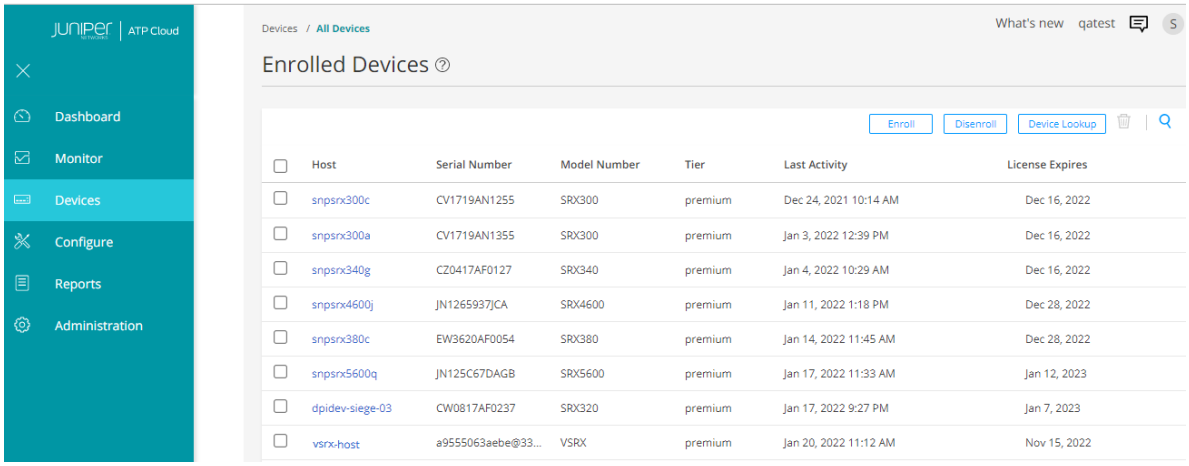
You can use a Junos OS operation (op) script to configure your SRX Series Firewall to connect to the Juniper Advanced Threat Prevention Cloud service.

1. On Juniper ATP Cloud Web portal, click the Enroll button on the Devices page.
2. Copy the command to your clipboard and click OK.
3. Paste the command into the Junos OS CLI of the SRX Series Firewall in operational mode.
4. Use the `show services advanced-anti-malware` status command to verify that a connection is made to the cloud server from the SRX Series Firewall. The server host name in the following sample is an example only.

```
                        user@host> show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.us-west-2.sky.junipersecurity.net
  Server realm: qatest
  Server port: 443
  Proxy hostname: None
  Proxy port: None
    Control Plane:
      Connection time: 2022-02-15 21:31:03 PST
      Connection status: Connected
    Service Plane:
      fpc0
        Connection active number: 18
        Connection retry statistics: 48
```

   In the sample, the connection status indicates that the cloud server is connected to your security device.

5. You can also view the enrolled devices in Juniper ATP Cloud portal. Go to **Devices > All Devices** page. The page lists all the enrolled devices.



Configure IoT Traffic Streaming Settings

In this procedure, you'll create metadata streaming policies and enable security services on your security device.

1. Complete cloud connection configuration.

```
[edit]
user@host# set services security-intelligence url https://
cloudfeeds.sky.junipersecurity.net/api/manifest.xml
user@host# set services security-intelligence authentication tls-profile aamw-ssl
```

2. Create a security metadata streaming policy.

```
[edit]
user@host# set services security-metadata-streaming policy p1 dynamic-filter
user@host# set services security-metadata-streaming policy p2 dynamic-filter
```

   We'll later attach these security metadata streaming policy to security policies to enable the IoT traffic streaming for the session.

3. Enable security services such as application tracking, application identification, and PKI.

```
[edit]
user@host# set services application-identification
user@host# set security pki
user@host# set security application-tracking
```

Configure SRX Series Firewall

Use this procedure to configure interfaces, zones, policies enable IoT packet filtering and streaming services on your security device.

1. Configure interfaces.

```
[edit]
user@host# set interfaces ge-0/0/2 mtu 9092
user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.60.60.1/24
user@host# set interfaces ge-0/0/3 mtu 9092
user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.70.70.1/24
user@host# set interfaces ge-0/0/4 mtu 9092
user@host# set interfaces ge-0/0/4 unit 0 family inet address 10.80.80.1/24
```

2. Configure security zones and enable application traffic for each configured zone.

```
[edit]
user@host# set security zones security-zone trust interfaces ge-0/0/2.0 host-inbound-traffic
system-services all
user@host# set security zones security-zone trust interfaces ge-0/0/2.0 host-inbound-traffic
protocols all
user@host# set security zones security-zone trust application-tracking
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic protocols all
user@host# set security zones security-zone untrust interfaces ge-0/0/3.0 host-inbound-
traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/3.0 host-inbound-
traffic protocols all
user@host# set security zones security-zone untrust application-tracking
user@host# set security zones security-zone cloud application-tracking
```

   As shown in the topology, the untrust zone receives transit and host-bound traffic from IOT devices in network. The client device is in trust zone and the Juniper ATP Cloud is in cloud zone.

3. Configure security policy P1.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy P1 match source-
```

```
address any
user@host# set security policies from-zone trust to-zone untrust policy P1 match destination-
address any
user@host# set security policies from-zone trust to-zone untrust policy P1 match application
any
user@host# set security policies from-zone trust to-zone untrust policy P1 then permit
```

This configuration allows traffic from trust zone to untrust zone.

4. Configure security policy P2.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy P2 match source-
address any
user@host# set security policies from-zone untrust to-zone trust policy P2 match destination-
address any
user@host# set security policies from-zone untrust to-zone trust policy P2 match application
any
user@host# set security policies from-zone untrust to-zone trust policy P2 then permit
user@host# set security policies from-zone untrust to-zone trust application-services
security-metadata-streaming-policy p1
```

The configuration allows traffic from untrust zone to trust zone and applies the security metadata streaming policy p1 to enable IoT traffic streaming for the session.

5. Configure security policy P3.

```
[edit]
user@host# set security policies from-zone trust to-zone cloud policy P3 match source-address
any
user@host# set security policies from-zone trust to-zone cloud policy P3 match destination-
address any
user@host# set security policies from-zone trust to-zone cloud policy P3 match application any
user@host# set security policies from-zone trust to-zone cloud policy P3 then permit
user@host# set security policies from-zone trust to-zone cloud application-services security-
metadata-streaming-policy p2
```

This configuration allows traffic from trust zone to cloud zone and applies the security metadata streaming policy p2 to enable IoT traffic streaming for the session.

6. Commit the configuration.

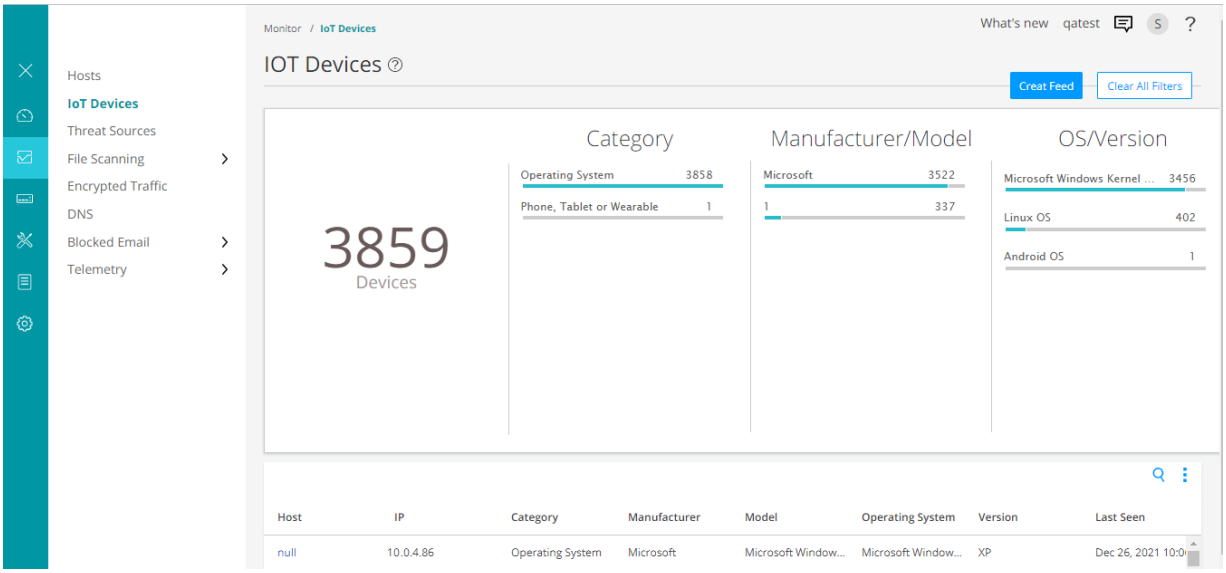
```
[edit]
user@host# commit
```

Now your security device is ready to stream IoT traffic to Juniper ATP Cloud.

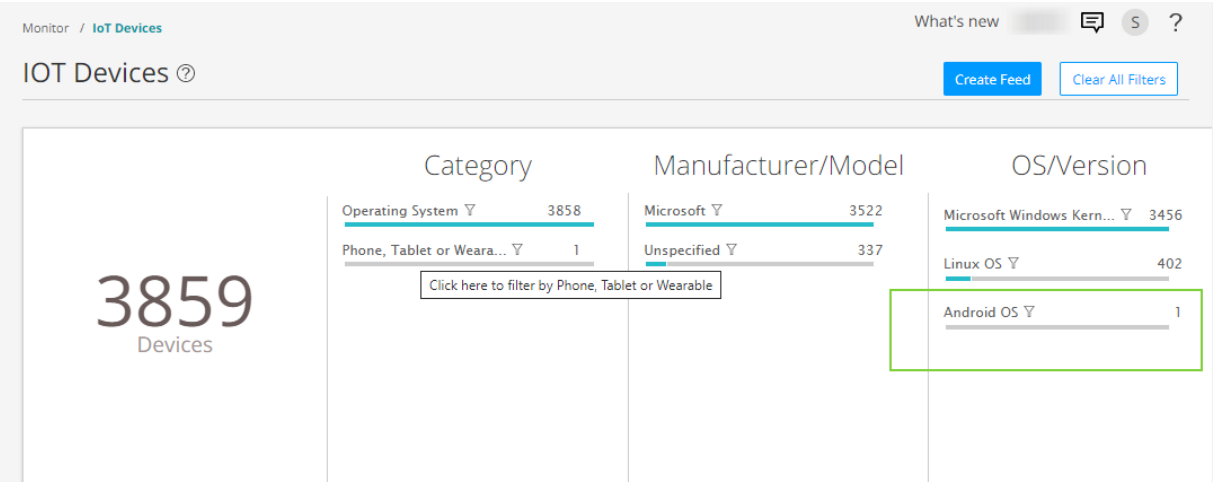
Lets check all the discovered IoT devices in Juniper ATP Cloud portal.

Viewing Discovered IOT Devices in ATP Cloud

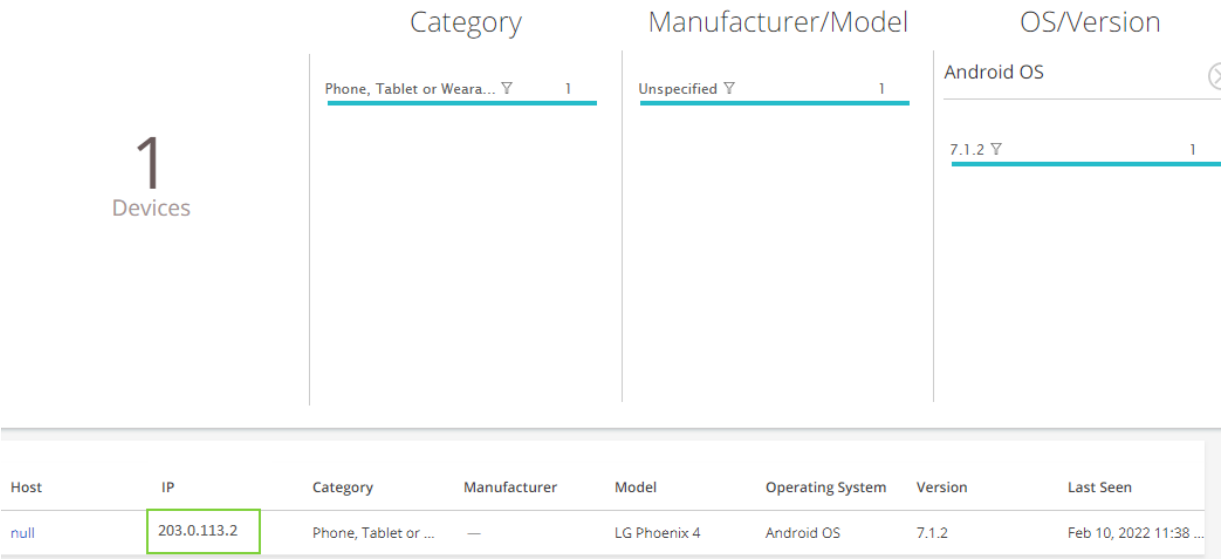
To view discovered IoT devices in Juniper ATP Cloud portal, navigate to **Minotor > IoT Devices** page.



You can click and filter the IoT devices based on device category, manufacturer, type of operating system.



In the following image, we're filtering devices with Android OS.

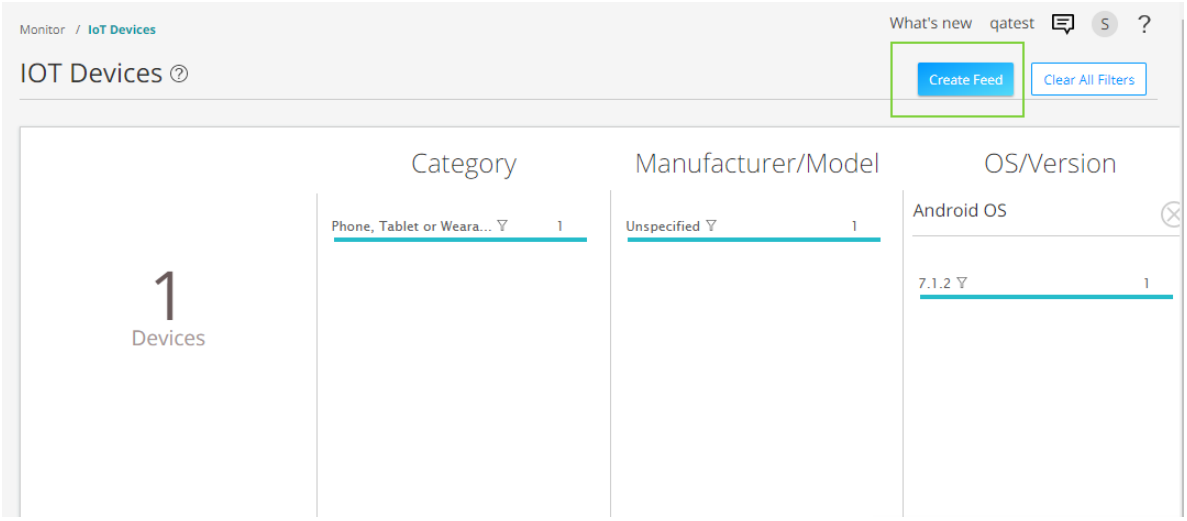


The page lists IoT devices with details such as IP address, type, manufacturer, models, and so on. Using these details, you can monitor and create threat feeds to enforce security policy.

Create Threat Feeds

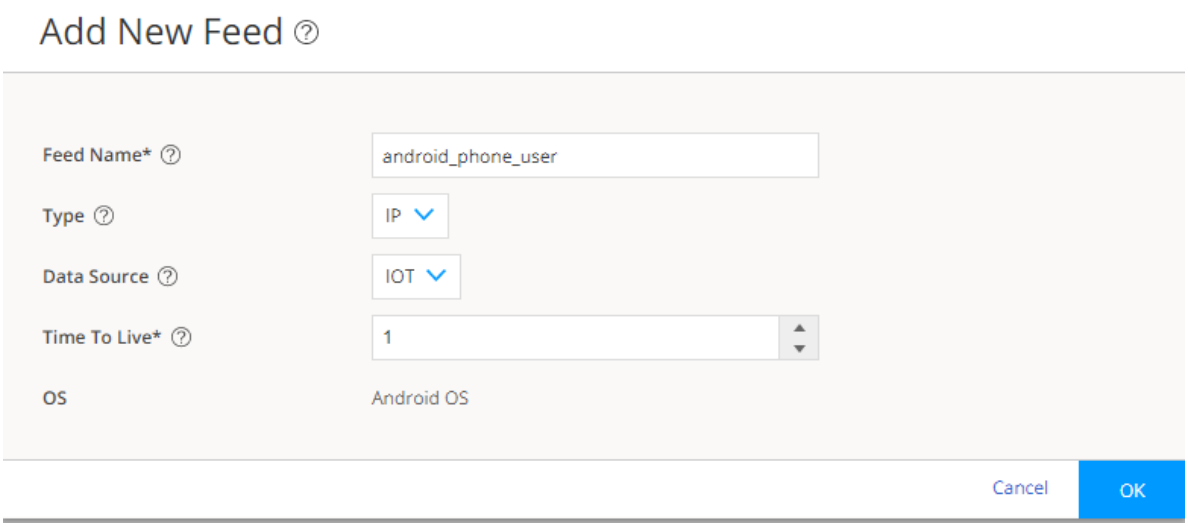
Once Juniper ATP Cloud identifies IoT devices, you can create threat feeds. When your security device downloads threat feeds in the form of dynamic address groups, you can use the feed your security policies to take enforcement actions on the inbound and outbound traffic on these IoT devices.

1. Go to **Minotor > IoT Devices** page and click **Create Feeds** option.



2. Click the plus sign (+). The Add New Feed page appears.

   In this example, we will use the feed name **android_phone_user** with a time-to-live (TTL) of seven days.



Complete the configuration for the following fields:

- **Feed Name:**

  Enter a unique name for the threat feed. The feed name must begin with an alpha-numeric character and can include letters, numbers, and underscores; no spaces are allowed. The length is 8–63 characters.

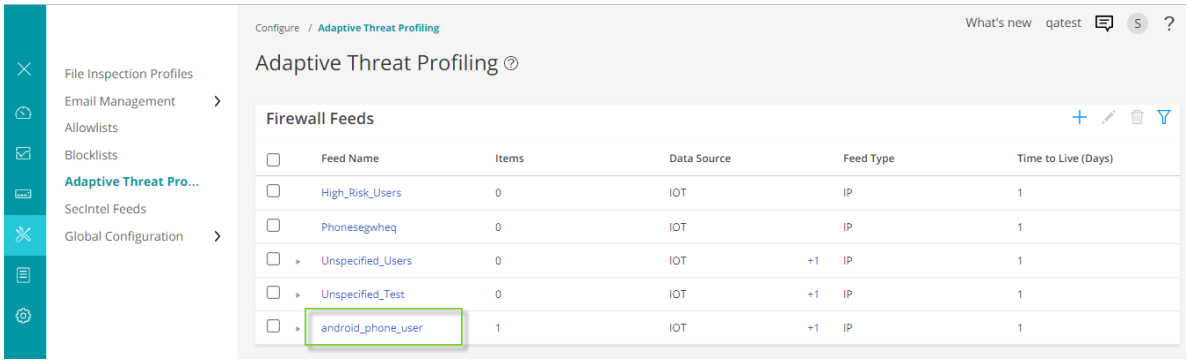
- **Type:** Select the content type of the feed as **IP**.

- **Data Source:** Select the data source for creating the feed as **IOT**.

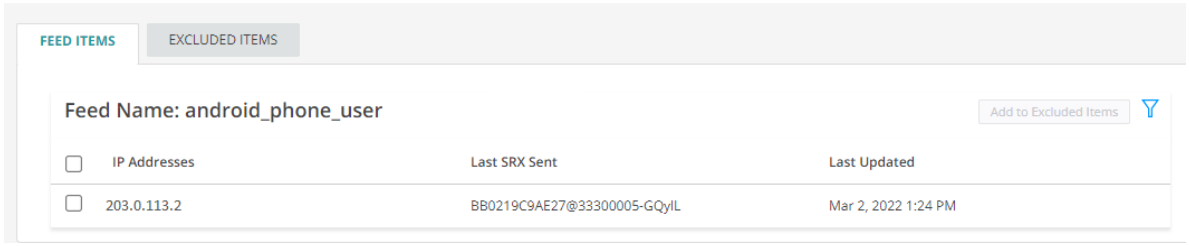
- **Time to Live:** Enter the number of days for the required feed entry to be active. After the feed entry crosses the time to live (TTL) value, the feed entry is automatically removed. The available range is 1–365 days.

3. Click **OK** to save the changes.

4. Go to **Configure > Adaptive Threat Profiling**. The page displays all threat feeds created. You can see the threat feed **android_phone_user** listed on the page.



Click on the threat feed to display the IP address included in the threat feed.



5.

6. Ensure that your security device has downloaded the feed. Downloading happens automatically at regular intervals but can take a few minutes.

```
user@host> show services security-intelligence sec-profiling-feed status
Category name            :SecProfiling
  Feed name              :Android_Phone_User
    Feed type            :IP
    Last post time       :N/A
    Last post status code:N/A
    Last post status     :N/A
  Feed name              :IT_feed
    Feed type            :IP
    Last post time       :N/A
    Last post status code:N/A
```

```
    Last post status     :N/A
  Feed name              :High_Risk_Users
    Feed type            :IP
    Last post time       :N/A
    Last post status code:N/A
    Last post status     :N/A
```

You can manually download the threat feeds using the following command:

```
request services security-intelligence download status ||match android_phone_user
```

Lets proceed with creating security policies with the downloaded threat feeds.

Create Security Policy Using Adaptive Threat Profiling Feeds

Once your security device downloads the threat feed, you can refer it as dynamic address group in a security policy. A dynamic address is a group of IP addresses of IoT devices belonging to a specific domain.

In this example, we create a policy that detects traffic from android phones and blocks the traffic.

1. Define security policy match criteria.

```
[edit]
user@host# set security policies global policy Block_Android_Traffic match source-address
android_phone_user
user@host# set security policies global policy Block_Android_Traffic match destination-
address any
user@host# set security policies global policy Block_Android_Traffic match application any
```

2. Define security policy action.

```
[edit]
user@host# set security policies global policy Block_Android_Traffic then deny
```

In this example, when you commit the configuration, your security device blocks HTTP traffic for the IoT devices belonging to the specific domain.

For more information, see Configure Adaptive Threat Profiling.

Results

From configuration mode, confirm your configuration by entering the show security command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
              [edit]


              user@host# show security policies
from-zone trust to-zone untrust {
    policy P1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy P2 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    application-services {
        security-metadata-streaming-policy p1;
    }
}
from-zone trust to-zone cloud {
    policy P3 {
        match {
```

```
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    application-services {
        security-metadata-streaming-policy p2;
    }
}
```

```
user@host# show security policies global
policy Block_Android_Traffic {
    match {
        source-address android_phone_user;
        destination-address any;
        application any;
    }
    then {
        deny;
    }
}
```

Check security zones.

```
              [edit]

              user@host# show security zones
security-zone trust {
    interfaces {
        ge-0/0/2.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
```

```
                    all;
                }
            }
        }
    }
    application-tracking;
}
security-zone untrust {
    interfaces {
        ge-0/0/4.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
        }
        ge-0/0/3.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
        }
    }
    application-tracking;
}
security-zone cloud {
    interfaces {
        ge-0/0/0.1 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
```

```
        }
    }
    application-tracking;
}
```

show services

```
[edit]

user@host# show services
advanced-anti-malware {
    dynamic-filter {
        traceoptions {
            file dyn-filterd-log size 1g world-readable;
            level all;
            flag all;
        }
    }
    connection {
        url https://srxapi.us-west-2.sky.junipersecurity.net;
        authentication {
            tls-profile aamw-ssl;
        }
    }
}
ssl {
    initiation {
        profile aamw-ssl {
            trusted-ca [ aamw-secintel-ca aamw-cloud-ca ];
            client-certificate aamw-srx-cert;
            actions {
                crl {
                    disable;
                }
            }
        }
    }
}
security-metadata-streaming {
```

```
    policy p1 {
        dynamic-filter;
    }
    policy p2 {
        dynamic-filter;
    }
}
security-intelligence {
    url https://cloudfeeds.sky.junipersecurity.net/api/manifest.xml;
    authentication {
        tls-profile aamw-ssl;
    }
}
```

If you are done configuring the feature on your device, enter commit from configuration mode.

Verification

IN THIS SECTION

Check Feed Summary and Status

Purpose: Verify if your security device is receiving IP address feeds in the form of dynamic address groups.

Action: Run the following command:

```
user@host> show services advanced-anti-malware dynamic-filter status
Dynamic Filter Server Connection Status:
  Server Hostname: srxapi.us-west-2.sky.junipersecurity.net
  Server Port: 443
  Proxy Hostname: None
  Proxy Port: None
```

```
Control Plane
  Connection Status: Connected
  Last Successful Connect: 2022-02-12 09:51:50 PST
  Pkts Sent: 3
  Pkts Received: 42
```

Meaning The output displays the connection status and other details of the Juniper ATP Cloud server.

3

CHAPTER

Configuration Statements and Operational Commands

IN THIS CHAPTER

Junos CLI Reference Overview

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

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands