Engineering
Simplicity

Data Center Next-Generation Firewall Use Case—Juniper Validated Design (JVD)

Published
2025-06-05

Table of Contents

Data Center Next-Generation Firewall Use Case—Juniper Validated Design (JVD)

Juniper Networks Validated Designs provide customers with a comprehensive, end-to-end blueprint for deploying Juniper solutions in their network. These designs are created by Juniper's expert engineers and tested to ensure they meet the customer's requirements. Using a validated design, customers can reduce the risk of costly mistakes, save time and money, and ensure that their network is optimized for maximum performance.

About this Document

This document covers the data center next-generation firewall use case with focus on optimal configuration of typical features in the data center. We also focus on the validation of each feature using a feature-based test plan and report the combined performance results delivered by these features. SRX4600 is the platform that is utilized in this validated design.

Solution Benefits

Juniper's approach to a data center security solution starts with operational efficiency, which is the most critical part of any architectural transformation. Following are the various components of this architecture:

In the data center:

- **Data center WAN gateway**—This is the main entryway to your data center where you control who and what can access your corporate resources. Using the analogy of fine art in a museum, this is where the balance between availability and security must be struck. Additionally, this is where you control who can access the data in the data center. It is your first line of defence, and access policies at the data center WAN gateway must align with user policies at your edge.
- **Cloud/Data Center Interconnect (DCI)**—This is the connection between your data center locations where information is exchanged between applications. The most important point to remember here is that the data in transit between data center locations must be secured.

- **Intra-data center**—Inside your data center, there are physical servers that house your applications and their components. There is a micro perimeter that needs to protect these resources. In a zero trust data center, segmentation between servers limiting the impact of a successful attack is a must.

- **Public Cloud**—Public Cloud offers tons of scale, redundance, and global reach. Many public cloud environments offer their own native security controls, but within the context of zero trust, access to public cloud resources must align with application access policies in your other data center environments.

- **Juniper Security Director Cloud (Management)**—Whether edge security is delivered on-premises or from the cloud, one management experience and one policy framework make it very easy to create a policy once and apply it anywhere, providing unbroken visibility regardless of architecture.

Examples of data center traffic profiles with security implemented:

- At the data center edge gateway—ensuring consistent zero trust access to private and public cloud environments.

- Traffic flow between servers (East-West traffic).

- Traffic flow between clouds (DCI).

- Traffic flow at the application level to protect data (microsegmentation).

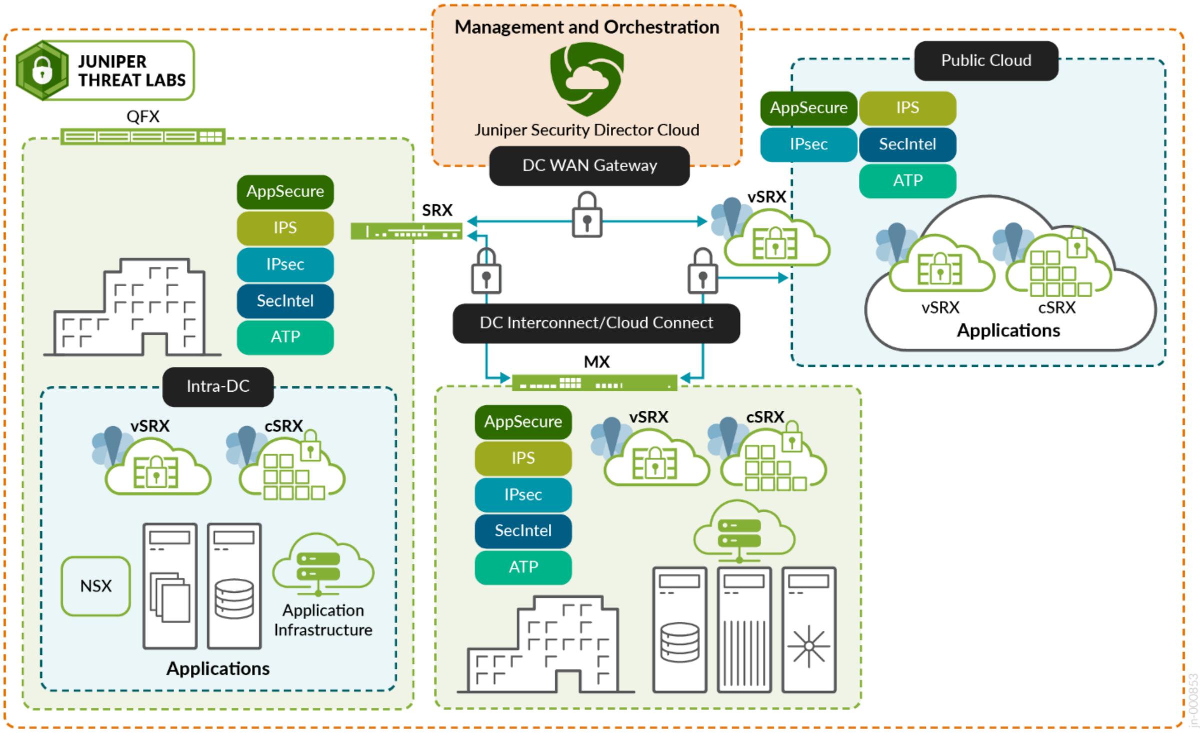
Features provided by Juniper Security Director Cloud with the same policy framework:

- Consistent threat protection.

- Easy extension of security policies to new environments and applications, reducing misconfigurations and lowering risk.

- Scaling data center security operations. Because visibility is unbroken in a unified console, security integration between multiple environments is not necessary, and automation is built in to identify and resolve threats quickly.

Figure 1: Data Center Reference Architecture



This JVD focuses on the next-generation firewall services that are typically used in the data center. This solution benefits you by providing an example of an optimized configuration for commonly utilized security services in the data center, and a validation that the deployed solutions are working as intended.

The following features are deployed and validated in this JVD:

- Application Security
- Intrusion detection and prevention (IDP)
- Advanced Threat Prevention (ATP)
- Security Intelligence (SecIntel)
- Advanced anti-malware (AAMW)
- DNS security
- Screens
- SSL Proxy (depends on use case implementation)

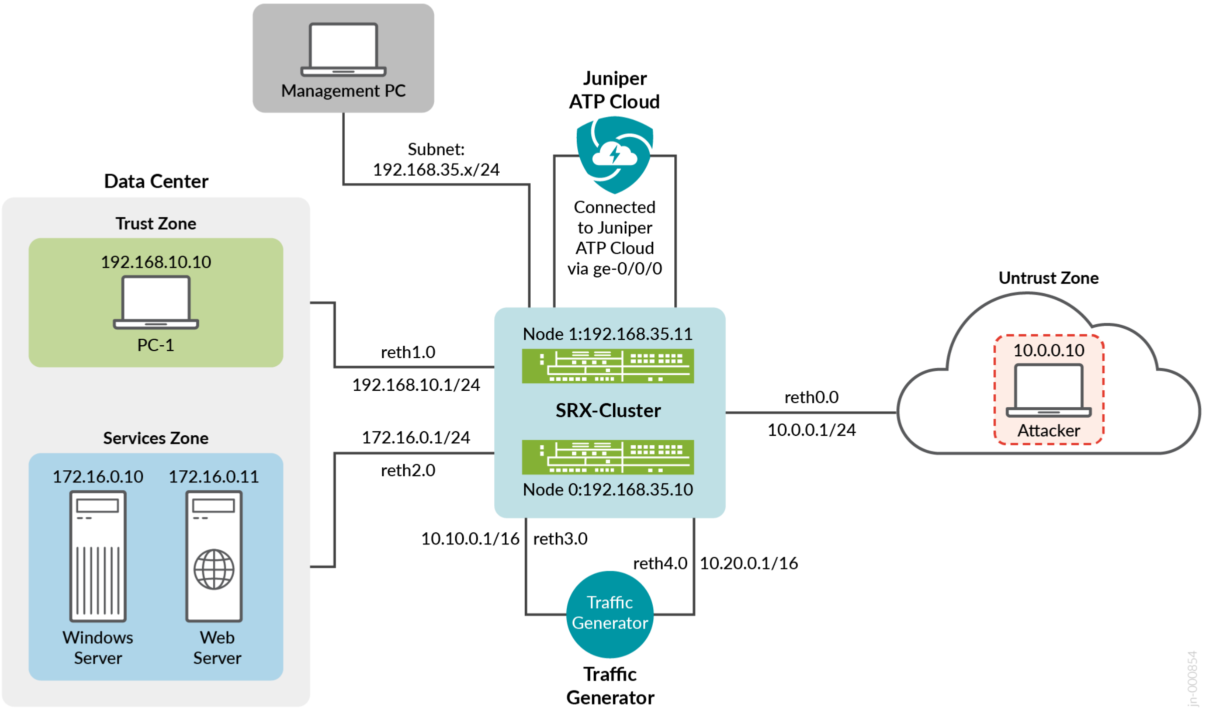
Use Case and Reference Architecture

IN THIS SECTION

In this section, we demonstrate how to implement next-generation firewall features in the data center environment. We test several use cases that present an example data center security implementation with a combination of next-generation firewall features. Each features contributes to a robust comprehensive implementation covering a holistic data center security deployment.

To test the JVD, a lab was built similar to the architecture shown in Figure 2 on page 4. The results of these tests are available in the associated Test Report document.

Figure 2: Reference Architecture



Data Center Next-Generation Firewall Use Cases

Table 1: Data Center Next-Generation Firewall Use Cases

Use Case	Purpose
Next-generation firewall and ATP.	Evaluates the usability and manageability of the firewall's ATP features and ensures the firewall can efficiently handle different types of traffic while maintaining performance. Also, detects and prevents zero-day threats through machine learning (ML) and behavioral analysis.
Validate data center traffic against threat on DNS traffic and validate DNS security features.	Protects data center traffic against common DNS exploits by employing heuristic analysis and behavior-based detection. Validates if DGA/DNS tunneling and SecIntel static blocks are effectively utilized by the SRX Series Firewall.
Effectiveness of IDP system (IDS/IPS) functionalities	Tests the effectiveness of IDP/IPS features by generating flood attacks, other attacks, and validates the effectiveness of the configured firewall settings.
Test security features with high availability use cases.	Tests security features with high availability use cases. Validates all the configured features are effective against a high availability scenario. Each security feature is tested against different failure scenarios.
Evaluate firewall performance with various traffic types and various ATP features enabled.	Evaluates the usability and manageability of the firewall's ATP features and ensures the firewall can efficiently handle different types of traffic while maintaining performance. Also detects and prevents zero-day threats through ML and behavioral analysis over constant base traffic across 20,000 users (HTTP traffic for 20,000 users).

Data Center Next-Generation Firewall Topology

The lab was configured with a basic data center architecture to emulate the following components:

- SRX Series Firewall (SRX4600) device in a Layer 2 high availability architecture.
- Baselined configuration covering:
  - Interface configuration.
  - Zone configuration.

    - Basic building blocks, such as DNS, NTP, System Logging, and so on.
    - Firewall policy enforcement between defined zones.

- Kali Linux server to emulate an attacker. This system emulates the following attack scenarios:
    - Generation of flooding attacks.
    - Generation of penetration testing attacks on webserver.
    - Generation and hosting of malware. Provides a reverse shell for exfiltration.
    - Assumes the role of C&C and hosts the malware for download.
- Linux server to host webserver services. This endpoint is protected from various attacks initiated by an attacker.
- Windows client to generate a web based traffic.
- Linux client to generate web based traffic and emulate malware download.

Validation Framework

IN THIS SECTION

Test Bed Overview

The test bed provides provision to emulate an attack environment to test all the next-generation firewall features on the SRX Series Firewall. The test bed is comprised of the following zone configurations:

Table 2: Test Bed

Test Bed		
Zone	Emulated Role	Description
untrust	Internet facing interface	Simulated untrusted zone facing the Internet edge.
services	Zone hosting services in data center environment	Simulated zone with webservers/ windows server hosting a range of services is configured.
trust	Zone hosting all trusted clients	Simulated environment with all trusted clients are connected that utilize services offered in the data center environment.

If this was a production environment, we need to configure public IP addresses on interfaces in the untrusted zone and private IP addresses on interfaces in the trust zone. NAT must be enabled for services that need access to Internet resources.

Platforms / Devices Under Test (DUT)

To review the software versions and platforms on which this JVD was validated by Juniper Networks, see the Validated Platforms and Software section in this document.

Test Bed Configuration

The appendix provides detailed next-generation firewall security configurations. Figure 3 on page 11 shows a workflow diagram regarding the high-level architecture of this JVD environment.

Test Objectives

IN THIS SECTION

Test Goals

The testing for this JVD was performed with the following goals in mind. See the Test Report for more information.

The goal for this testing was to test the following features and functions:

- Firewall configured as a data center WAN gateway.
- Implement features to protect hosted services in the services zone.
- Implement features to protect common services utilized within the data center environment.
- Implement data center WAN gateway in high availability architecture and test resiliency with different failure scenarios.
- Implement features to protect hosted services from DDoS attacks.
- Test performance of the Juniper SRX Series Firewall with long-lived and short-lived sessions and functionality of various security features with peak traffic conditions.

Test Non-Goals

The following roles were not tested in this JVD:

- Cloud/DCI
- Public Cloud
- Intra-DC

Recommendations

Ensure premium license is applied on the Juniper SRX Series Firewall to ensure availability of premium security features that are tested in the JVD.

Appendix: Next-Generation Firewall JVD Configuration

IN THIS SECTION

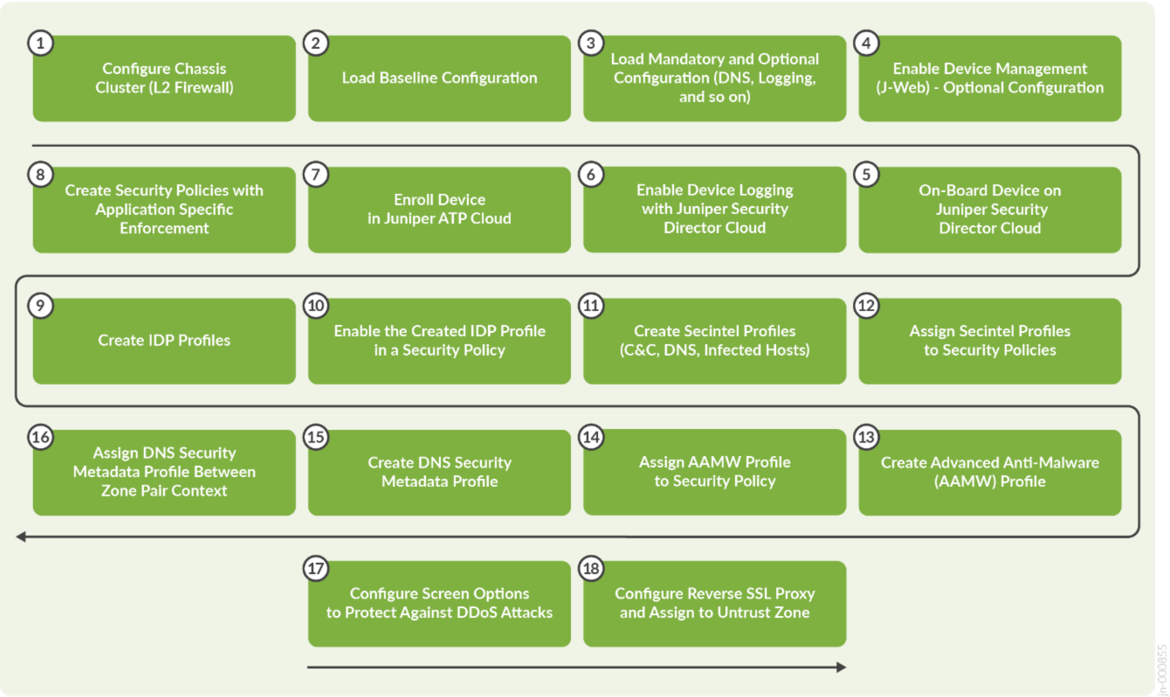
Generic Workflows and Operations for Creating the Data Center Next-Generation Firewall Topology

This overview illustrates how to use the Juniper SRX Series Firewall CLI and Juniper Security Director Cloud console (the GUI) to provision the data center next-generation firewall architecture. Conceptually, the Juniper SRX Series Firewall is configured on the data center edge to provide visibility and control of traffic that is originating from the following:

- Traffic originating from trusted clients outbound to the Internet. (South-North Traffic)
- Traffic originating from untrusted environment reaching inbound to services configured in the data center. (North-South Traffic)
- Traffic originating from the trusted clients using services hosted with in the data center. (East-West Traffic)

Figure 3 on page 11 illustrates the workflow for configuring the Juniper SRX Series Firewall using the Junos OS CLI and Juniper Security Director Cloud console.

Figure 3: Data Center Next-Generation Firewall Configuration Workflow


1 Configure Chassis Cluster (L2 Firewall)
2 Load Baseline Configuration
3 Load Mandatory and Optional Configuration (DNS, Logging, and so on)
4 Enable Device Management (J-Web) - Optional Configuration
5 On-Board Device on Juniper Security Director Cloud
6 Enable Device Logging with Juniper Security Director Cloud
7 Enroll Device in Juniper ATP Cloud
8 Create Security Policies with Application Specific Enforcement
9 Create IDP Profiles
10 Enable the Created IDP Profile in a Security Policy
11 Create Secintel Profiles (C&C, DNS, Infected Hosts)
12 Assign Secintel Profiles to Security Policies
13 Create Advanced Anti-Malware (AAMW) Profile
14 Assign AAMW Profile to Security Policy
15 Create DNS Security Metadata Profile
16 Assign DNS Security Metadata Profile Between Zone Pair Context
17 Configure Screen Options to Protect Against DDoS Attacks
18 Configure Reverse SSL Proxy and Assign to Untrust Zone
jn-000855

The sequence of configuration tasks in this example is as follows:

1. Configure chassis cluster through CLI: Clustering enables high availability.

2. Load baseline configuration with interface, zones, addresses, services, firewall policies, NAT, and default routing: Baseline the configuration for the device to carry traffic and able to reach out to Internet.

3. Configuring logging to an external SIEM: You can have multiple log streams configured in SRX Series Firewall and point the SRX logging mechanisms to multiple SIEMs.

4. Enable web management: Enable web management so that you can access SRX Series Firewall using the on-box management solution through J-Web.

5. Discover the device and import baseline configuration to Juniper Security Director Cloud: Discover the device and import the baseline configuration to Juniper Security Director Cloud.

6. Enable logging for Juniper Security Director Cloud: Enable logging so that the traffic is logged to Juniper Security Director Cloud from SRX Series Firewall.

7. Enroll the device to Juniper ATP Cloud: Juniper ATP Cloud is the threat intelligence component of this solution and the source of SecIntel threat feeds. It also can provide advanced malware detection.

8. Create security policies with application specific environment.

9. Create IDP profiles that cover the security landscape of the data center environment.

10. Assign the created IDP profile in a security policy.

11. Create SecIntel Profile: SecIntel Profile contains options for DNS, Command and Control (C&C), and Infected hosts.

12. Assign SecIntel Profile to rule: Assigning SecIntel Profile to rule ensures all the traffic using the rule is verified against the SecIntel feeds.

13. Create AAMW Profile: The AAMW profile allows you to select the type of traffic to be inspected for malware. Traffic includes HTTP, IMAP, SNB, and SMTP.

14. Assign AAMW Profile to Rule: Assign the profile to rule so that all traffic using the rule is inspected for malware based on the profile.

15. Create DNS security Meta Data Profile: DNS security allows you to identify DNS related threats such as DGA and DNS tunnelling.

16. Assign the DNS Meta Data to Zone Context: All the traffic between the zone set is inspected for DNS security.

17. Configure screen options to protect the untrust zone against DDoS attacks.

18. Configure reverse SSL proxy to analyze and protect webserver traffic. The traffic is subjected to advances security services.

The configuration for each tested JVD feature is as follows:

Chassis Configuration (CLI)

```
# Step 1:
cli
# Configure chassis cluster configuration and Reboot
set chassis cluster cluster-id 1 node 0 reboot
set chassis cluster cluster-id 1 node 1 reboot
# NOTE: Device would reboot and each device would assume a role either as primary or secondary.
# Step 2:
set interfaces fab0 fabric-options member-interfaces ge-0/0/3
set interfaces fab1 fabric-options member-interfaces ge-5/0/3
# Step 3:
Set the interface count to configure redundant interfaces and create the redundant interfaces.
cli
```

```
configure
set chassis cluster reth-count 5
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth3 redundant-ether-options redundancy-group 1
set interfaces reth4 redundant-ether-options redundancy-group 1
# Node 0 configuration
set interfaces ge-0/0/0 gigether-options redundant-parent reth0
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-0/0/2 gigether-options redundant-parent reth2
set interfaces ge-0/0/3 gigether-options redundant-parent reth3
set interfaces ge-0/0/4 gigether-options redundant-parent reth4
# Node 1 configuration
set interfaces ge-5/0/0 gigether-options redundant-parent reth0
set interfaces ge-5/0/1 gigether-options redundant-parent reth1
set interfaces ge-5/0/2 gigether-options redundant-parent reth2
set interfaces ge-5/0/3 gigether-options redundant-parent reth3
set interfaces ge-5/0/4 gigether-options redundant-parent reth4
# Step 4 - Set Hostname and Management IP:
set groups node0 system host-name SRX-NODE0
set groups node0 interfaces fxp0 unit 0 family inet address 192.16.35.10/24
set groups node1 system host-name SRX-NODE1
set groups node1 interfaces fxp0 unit 0 family inet address 192.16.35.11/24
# Step 5: Enable interface monitoring.
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/1 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/2 weight 255
# Step 6: Set chassis options.
set chassis cluster redundancy-group 1 node 0 priority 150
set chassis cluster redundancy-group 1 node 1 priority 100
set chassis cluster redundancy-group 1 preempt
```

Baseline Configuration (CLI)

```
UNTRUST:
set security zones security-zone untrust screen root-screen
set security zones security-zone untrust interfaces reth0.0 host-inbound-traffic system-services
ssh
```

```
set security zones security-zone untrust interfaces reth0.0 host-inbound-traffic system-services
ping
set security zones security-zone untrust interfaces reth0.0 host-inbound-traffic system-services
all
set security zones security-zone untrust interfaces reth5.2000 host-inbound-traffic system-
services ssh
set security zones security-zone untrust interfaces reth2.0 host-inbound-traffic system-services
ping
TRUST:
set security zones security-zone trust interfaces reth1.0 host-inbound-traffic system-services
all
set security zones security-zone trust interfaces reth3.0 host-inbound-traffic system-services
all
set security zones security-zone trust interfaces reth4.1200 host-inbound-traffic system-
services all
SERVICES:
set security zones security-zone services screen root-screen
set security zones security-zone services interfaces xe-1/1/2.0 host-inbound-traffic system-
services ping
DEFAULT ROUTE:
set routing-options static route 0.0.0.0/0 next-hop 80.80.80.1
set routing-options static route 90.0.0.0/16 next-hop 21.0.0.2
set routing-options static route 190.0.0.0/16 next-hop 30.30.30.2
NAT: Outgoing Internet Traffic
set security nat source pool abc address 50.0.0.0/24
set security nat source rule-set nat_to_internet from zone services
set security nat source rule-set nat_to_internet from zone trust
set security nat source rule-set nat_to_internet to zone untrust
set security nat source rule-set nat_to_internet rule 1 match source-address 0.0.0.0/0
set security nat source rule-set nat_to_internet rule 1 match destination-address 0.0.0.0/0
set security nat source rule-set nat_to_internet rule 1 match application any
set security nat source rule-set nat_to_internet rule 1 then source-nat pool abc
NAT: Incoming destination traffic for web server:
set security nat destination pool web-svr-pool address 172.16.0.11/32
set security nat destination pool web-svr-pool address port 443
set security nat destination rule-set WS-NAT rule 1 match destination-address 10.0.0.100/32
set security nat destination rule-set WS-NAT rule 1 match destination-port 443
set security nat destination rule-set WS-NAT rule 1 then destination-nat pool web-svr-pool
Global Addresses:
set security address-book global address WebSvr-Local 7.7.7.2/32
set security address-book global address win-server 172.16.0.10/32
set security address-book global address web-server 172.16.0.11/32
set security address-book global address client1 192.168.10.10/32
```

```
Set security address-book global address web-server-ext 10.0.0.100/32
Services:
set applications application-set Internet-services application junos-http
set applications application-set Internet-services application junos-https
set applications application-set Internet-services application junos-smtp
set applications application-set Internet-services application junos-smtps
set applications application-set Internet-services application junos-imap
set applications application-set Internet-services application junos-imaps
set applications application-set Internet-services application junos-dns-udp
set applications application-set Internet-services application junos-dns-tcp
set applications application-set Internet-services application junos-icmp-all
Security Policies:
Security Policies between trust to untrust:
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
source-address any
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
destination-address any
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
application any
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
source-identity "domain08.net\ks_windows1_user_1"
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
source-identity "domain08.net\ks_user1_user_1"
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
source-identity unknown-user
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
source-identity unauthenticated-user
deactivate security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule
match source-identity
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule match
dynamic-application any
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule then permit
application-services idp-policy Recommended_WithAudit
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule then permit
application-services utm-policy junos-default-utm-policy
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule then permit
application-services security-intelligence-policy default-secintel
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule then permit
application-services advanced-anti-malware-policy default-antimalware
set security policies from-zone trust to-zone untrust policy t2u-allow_internet_rule then log
session-close
set security policies from-zone trust to-zone untrust policy Block_Offending_Apps match source-
address any
```

```
set security policies from-zone trust to-zone untrust policy Block_Offending_Apps match
destination-address any
set security policies from-zone trust to-zone untrust policy Block_Offending_Apps match
application junos-defaults
set security policies from-zone trust to-zone untrust policy Block_Offending_Apps match dynamic-
application Block_HighBW_Apps
set security policies from-zone trust to-zone untrust policy Block_Offending_Apps then deny
set security policies from-zone trust to-zone untrust policy Block_Offending_Apps then log
session-close
set security policies from-zone trust to-zone untrust application-services security-metadata-
streaming-policy apt_services
Security Policies between services to untrust:
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule match
source-address any
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule match
destination-address any
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule match
application any
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule match
dynamic-application any
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule then
permit application-services security-intelligence-policy default-secintel
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule then
permit application-services advanced-anti-malware-policy default-antimalware
set security policies from-zone services to-zone untrust policy s2u-allow_internet_rule then log
session-close
Security Policies between trust and services:
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule match
source-address any
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule match
destination-address any
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule match
application junos-http
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule match
application junos-https
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule match
dynamic-application junos:HTTP
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule match
dynamic-application junos:SSL
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule then
permit application-services idp-policy CS-To-Web-Protection-Rules
set security policies from-zone trust to-zone services policy t2s-allow_web_svcs_rule then log
session-close
```

```
Security Policies between untrust to services:
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs match
source-address any
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs match
destination-address WebSvr-Local
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs match
application junos-defaults
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs match
dynamic-application junos:HTTP
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs match
dynamic-application junos:SSL
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs then permit
application-services idp-policy CS-To-Web-Protection-Rules
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs then log
session-init
set security policies from-zone untrust to-zone services policy u2s-protect_web_svcs then log
session-close
NETCONF SERVICE:
set system services ssh sftp-server
set system services rlogin
set system services netconf ssh
set system services netconf rfc-compliant
set system services web-management https system-generated-certificate
set system services web-management limits debug-level 9
set system services web-management session idle-timeout 1440
DNS SERVER:
set system name-server 8.8.8.8
```

System and Security Logging Configuration (CLI)

```
set security log utc-timestamp
set security log mode stream
set security log format sd-syslog
set security log report
set security log source-interface reth0.0
set security log transport
set security log stream sd-cloud-logs category all
set security log stream sd-cloud-logs host srx.sdcloud.juniperclouds.net
set security log stream sd-cloud-logs host port 6514
set security log stream sd-cloud-logs transport division line-based
set security log stream sd-cloud-logs transport protocol tls
set security log stream sd-cloud-logs transport tls-profile syslog-profile
```

Management Configuration (CLI)

```
HTTP:
set system services web-management http interface reth1.0
HTTPS:
set system services web-management https system-generated-certificate
set system services web-management https interface reth1.0
set system services web-management https interface fxp0.0
HTTP:
set system services rest http
HTTPS:
set system services rest https server-certificate system-generated-certificate
set system services rest enable-explorer
```

GUI driven feature configuration through Juniper Security Director Cloud:

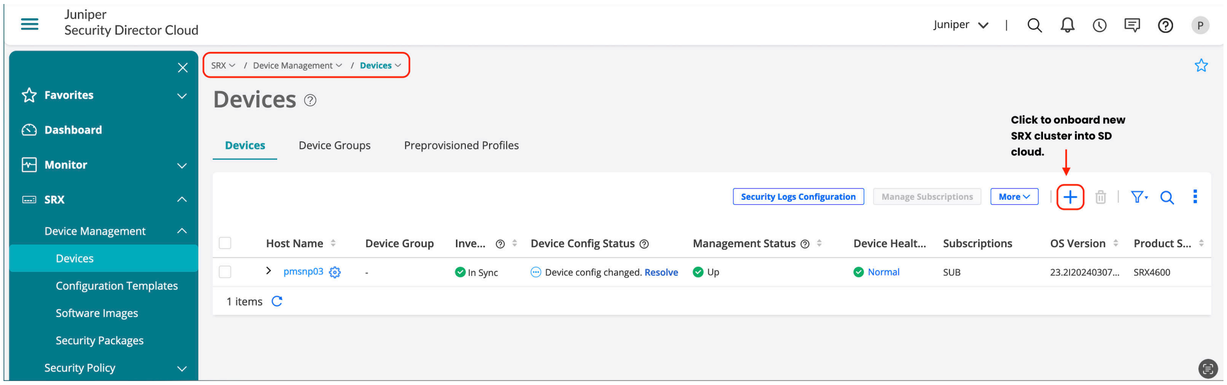
- Discover device in Juniper Security Director Cloud and import baselined configuration.
- Onboard device in Juniper Security Director Cloud.

To onboard the SRX Series Firewall, follow the procedure below:

1. Go to **SRX** > **Device Management** > **Device** and then click **+.**
2. Select **Adopt SRX Devices**.
3. Select **SRX Clusters**.
4. Enter **1** in the Number of SRX clusters to be adopted field.
5. Click **OK** and then click **Close**.

The action above creates a temporary device and to complete the on-boarding process, click **Adopt Cluster** as seen in Figure 6 on page 20 . Copy paste the CLI commands on to the node0 of the SRX Cluster.

Figure 4: Juniper Security Director Cloud Device Page

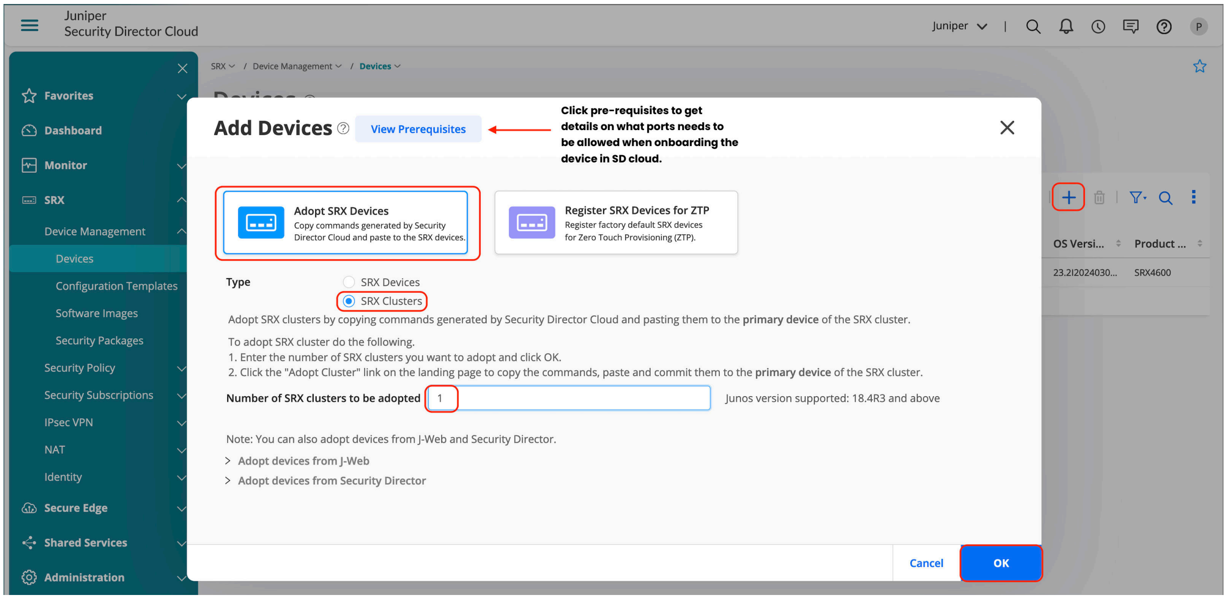


Click to onboard new SRX cluster into SD cloud.

Host Name	Device Group	Inve...	Device Config Status	Management Status	Device Healt...	Subscriptions	OS Version	Product S...
pmsnp03	-	In Sync	Device config changed. Resolve	Up	Normal	SUB	23.2I20240307...	SRX4600

1 items

Figure 5: Juniper Security Director Cloud Device: Onboard SRX Cluster



Click pre-requisites to get details on what ports needs to be allowed when onboarding the device in SD cloud.

Adopt SRX Devices
Copy commands generated by Security Director Cloud and paste to the SRX devices.

Register SRX Devices for ZTP
Register factory default SRX devices for Zero Touch Provisioning (ZTP).

Type ○ SRX Devices ● SRX Clusters

Adopt SRX clusters by copying commands generated by Security Director Cloud and pasting them to the **primary device** of the SRX cluster.

To adopt SRX cluster do the following.
1. Enter the number of SRX clusters you want to adopt and click OK.
2. Click the "Adopt Cluster" link on the landing page to copy the commands, paste and commit them to the **primary device** of the SRX cluster.

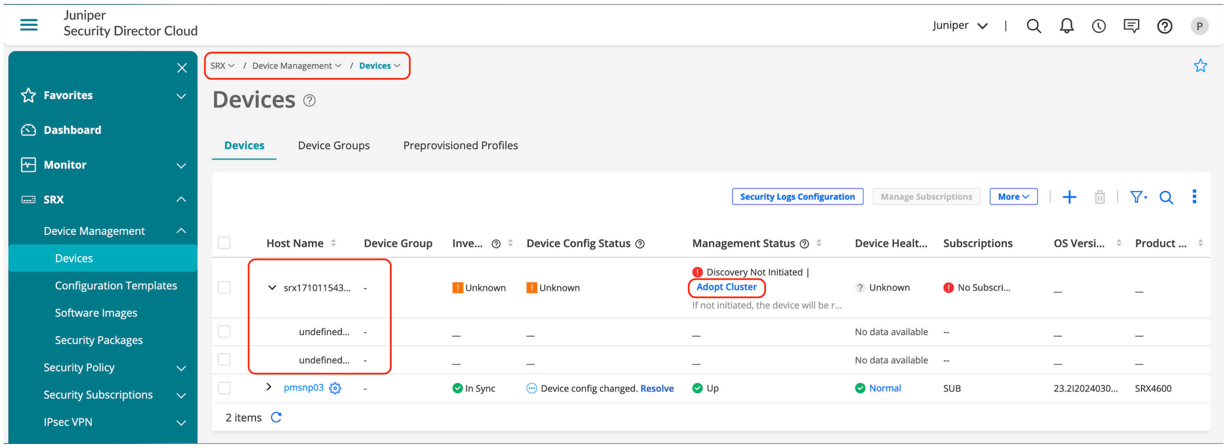
Number of SRX clusters to be adopted: 1 Junos version supported: 18.4R3 and above

Note: You can also adopt devices from J-Web and Security Director.

> Adopt devices from J-Web

> Adopt devices from Security Director

Figure 6: Juniper Security Director Cloud: Adopt Device

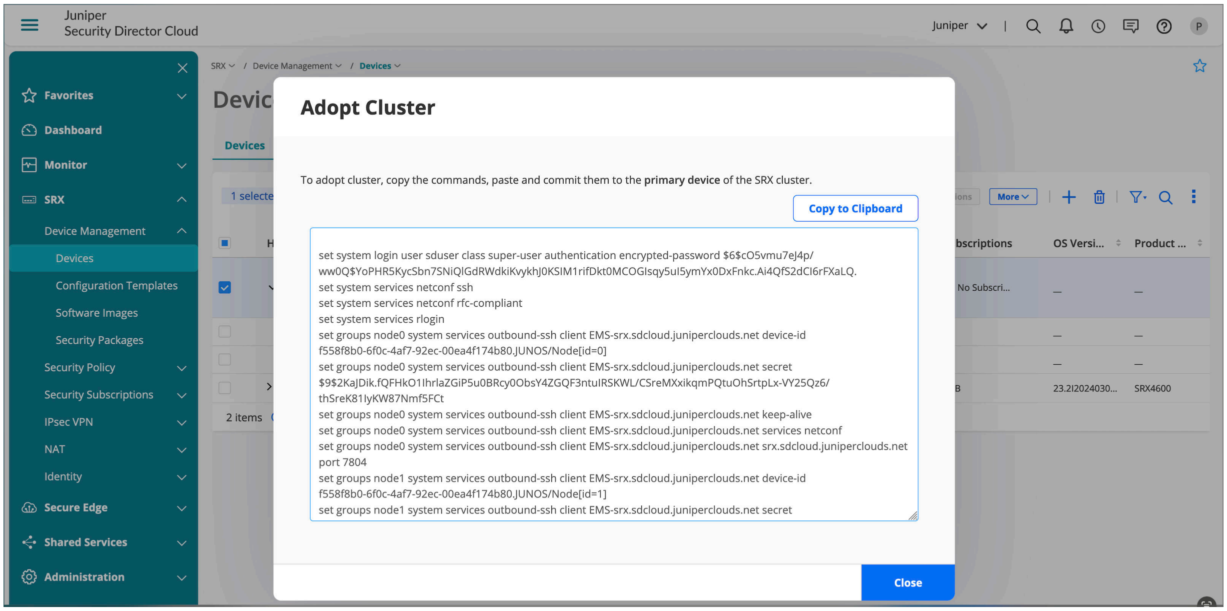


Devices

	Host Name	Device Group	Inve...	Device Config Status	Management Status	Device Healt...	Subscriptions	OS Versi...	Product ...
□	srx171011543...	-	Unknown	Unknown	Discovery Not Initiated | Adopt Cluster If not initiated, the device will be r...	Unknown	No Subscri...	_	_
□	undefined...	-	_	_	_	No data available	--	_	_
□	undefined...	-	_	_	_	No data available	--	_	_
□	pmsnp03	-	In Sync	Device config changed. Resolve	Up	Normal	SUB	23.2I2024030...	SRX4600

2 items

Figure 7: Juniper Security Director Cloud: Copy Paste CLI Commands to Onboard SRX Cluster



Adopt Cluster

To adopt cluster, copy the commands, paste and commit them to the **primary device** of the SRX cluster.

```
set system login user sduser class super-user authentication encrypted-password $6$cO5vmu7eJ4p/
ww0Q$YoPHR5KycSbn7SNiQlGdRWdkiKvykhJ0KSIM1rifDkt0MCOGIsqy5uI5ymYx0DxFnkc.Ai4QfS2dCI6rFXaLQ.
set system services netconf ssh
set system services netconf rfc-compliant
set system services rlogin
set groups node0 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net device-id
f558f8b0-6f0c-4af7-92ec-00ea4f174b80.JUNOS/Node[id=0]
set groups node0 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net secret
$9$2KaJDik.fQFHkO1IhrlaZGiP5u0BRcy0ObsY4ZGQF3ntuIRSKWL/CSreMXxikqmPQtuOhSrtpLx-VY25Qz6/
thSreK81IyKW87Nmf5FCt
set groups node0 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net keep-alive
set groups node0 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net services netconf
set groups node0 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net srx.sdcloud.juniperclouds.net
port 7804
set groups node1 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net device-id
f558f8b0-6f0c-4af7-92ec-00ea4f174b80.JUNOS/Node[id=1]
set groups node1 system services outbound-ssh client EMS-srx.sdcloud.juniperclouds.net secret
```

Enroll Device to Juniper ATP Cloud After Device Discovery

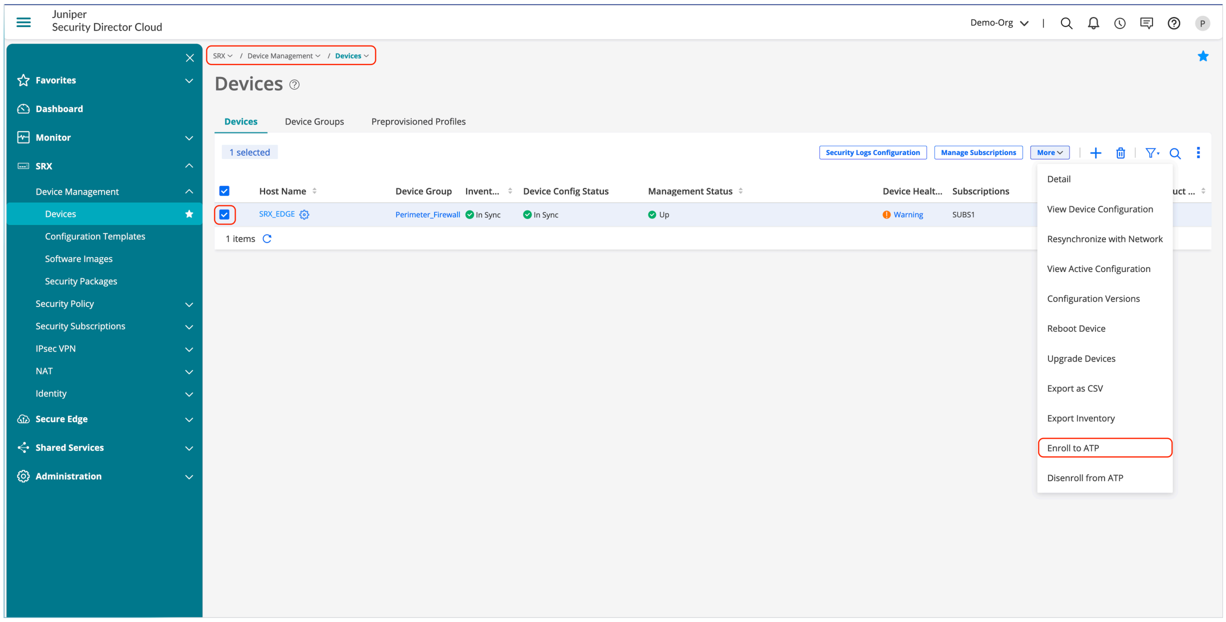
1. Go to SRX > Device Management > Device.

2. Select **Devices**.

3. Click **More** and then select **Enroll to ATP**.

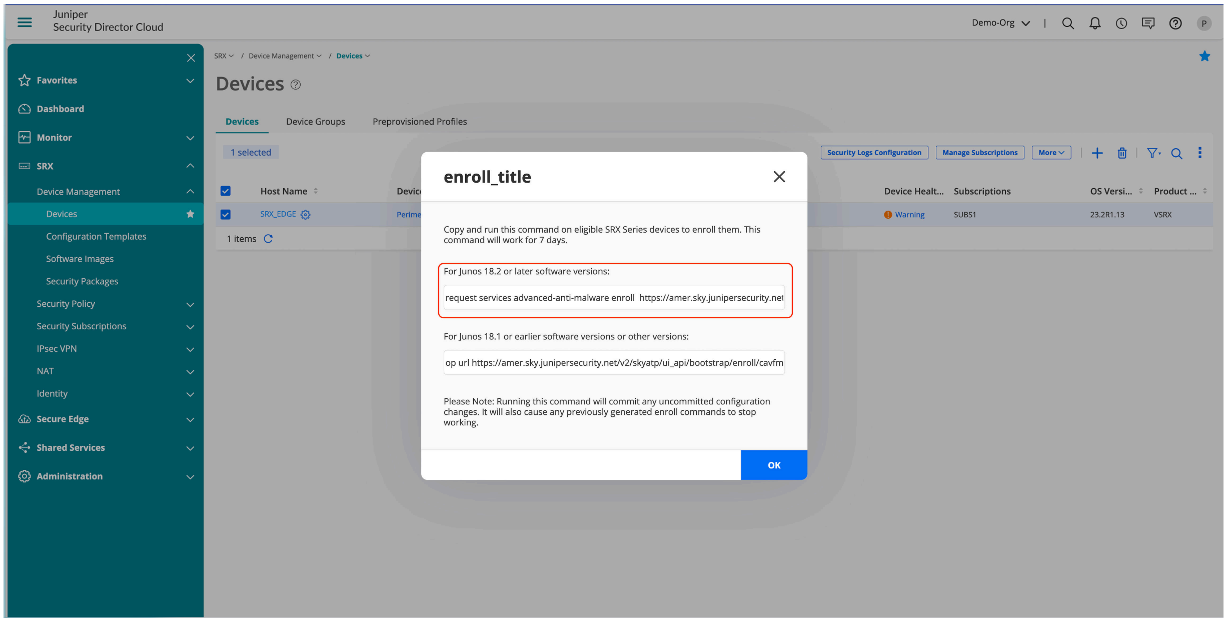
4. Log on to your SRX Series Firewall and paste the command into the Junos OS CLI.

Figure 8: Juniper Security Director Cloud—ATP Enrollment



	Host Name	Device Group	Invent...	Device Config Status	Management Status	Device Healt...	Subscriptions
☑	SRX_EDGE	Perimeter_Firewall	In Sync	In Sync	Up	Warning	SUBS1

Figure 9: Juniper Security Director Cloud—ATP Enrollment



Copy and run this command on eligible SRX Series devices to enroll them. This command will work for 7 days.

For Junos 18.2 or later software versions:

```
request services advanced-anti-malware enroll  https://amer.sky.junipersecurity.net
```

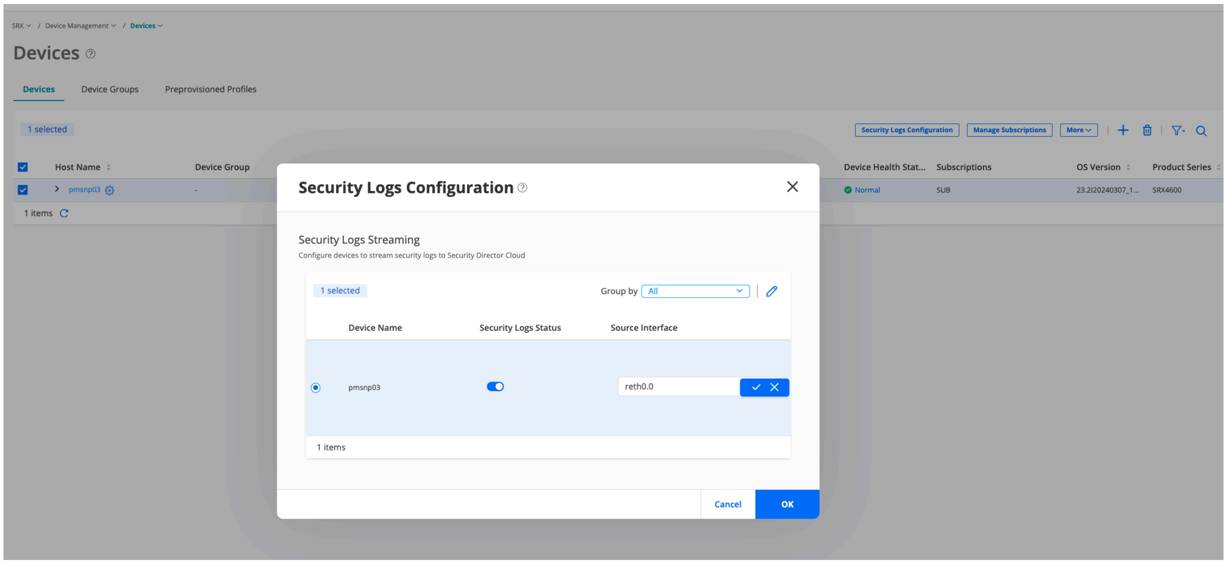
For Junos 18.1 or earlier software versions or other versions:

```
op url https://amer.sky.junipersecurity.net/v2/skyatp/ui_api/bootstrap/enroll/cavfm
```

Please Note: Running this command will commit any uncommitted configuration changes. It will also cause any previously generated enroll commands to stop working.

Enable Logging on SRX Series Firewall to Log the Traffic to Juniper Security Director Cloud

Figure 10: Juniper Security Director Cloud—Enable Juniper Security Director Cloud Logging



☑	Host Name	Device Group	Device Health Stat...	Subscriptions	OS Version	Product Series
☑	pmsnp03	-	Normal	SUB	23.2I20240307_1...	SRX4600

1 items

Configure devices to stream security logs to Security Director Cloud

	Device Name	Security Logs Status	Source Interface
●	pmsnp03	●	reth0.0

1 items

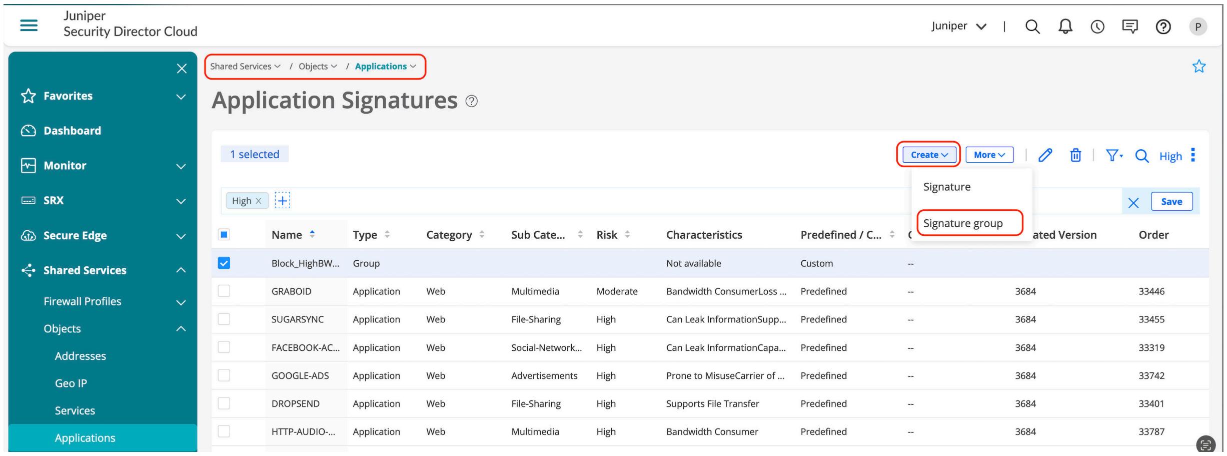
Application Security

Configure firewall policy to implement application security in a data center environment. We'll create a firewall policy to block any high bandwidth social media / shopping websites and apps (Facebook, Amazon) and video sharing websites such as YouTube, Vimeo, and so on.

Create an Application Group that you'll use in the firewall policy:

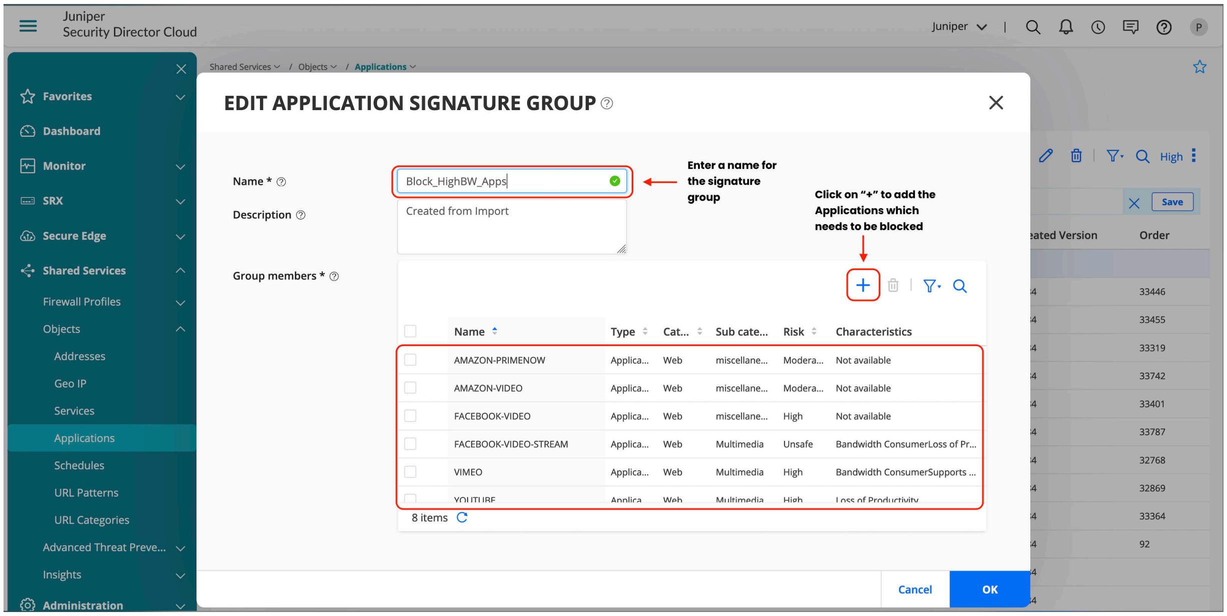
1. Go to **Shared Services** > **Applications.**
2. Click **Create** drop-down and then select **Signature group**.
3. Enter a name for the Application Group.
4. Click **+** to add all the applications that needs to be blocked.
5. Click **OK** to save the Application Group.

Figure 11: Juniper Security Director Cloud—Enable Juniper Security Director Cloud Logging



	Name	Type	Category	Sub Cate...	Risk	Characteristics	Predefined / C...	C	ated Version	Order
☑	Block_HighBW...	Group				Not available	Custom	--		
□	GRABOID	Application	Web	Multimedia	Moderate	Bandwidth ConsumerLoss ...	Predefined	--	3684	33446
□	SUGARSYNC	Application	Web	File-Sharing	High	Can Leak InformationSupp...	Predefined	--	3684	33455
□	FACEBOOK-AC...	Application	Web	Social-Network...	High	Can Leak InformationCapa...	Predefined	--	3684	33319
□	GOOGLE-ADS	Application	Web	Advertisements	High	Prone to MisuseCarrier of ...	Predefined	--	3684	33742
□	DROPSEND	Application	Web	File-Sharing	High	Supports File Transfer	Predefined	--	3684	33401
□	HTTP-AUDIO-...	Application	Web	Multimedia	High	Bandwidth Consumer	Predefined	--	3684	33787

Figure 12: Juniper Security Director Cloud—Creating the Application Signature Group



EDIT APPLICATION SIGNATURE GROUP

Name * Block_HighBW_Apps

Description Created from Import

Group members *

	Name	Type	Cat...	Sub cate...	Risk	Characteristics
□	AMAZON-PRIMENOW	Applica...	Web	miscellane...	Modera...	Not available
□	AMAZON-VIDEO	Applica...	Web	miscellane...	Modera...	Not available
□	FACEBOOK-VIDEO	Applica...	Web	miscellane...	High	Not available
□	FACEBOOK-VIDEO-STREAM	Applica...	Web	Multimedia	Unsafe	Bandwidth ConsumerLoss of Pr...
□	VIMEO	Applica...	Web	Multimedia	High	Bandwidth ConsumerSupports ...
□	YOUTUBE	Applica...	Web	Multimedia	High	Loss of Productivity

8 items

Include the Application Group in a Security Policy for enforcement:

1. Go to **SRX** > **Security Policy** > **SRX Policy**.

2. Click + to add new firewall rule.

3. Enter **Source Zone** and **Source Address**.

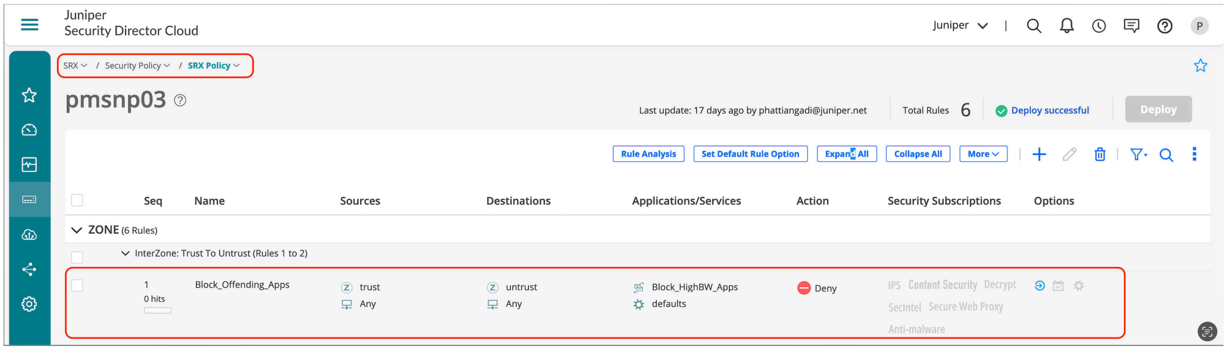
4. Enter **Destination Zone** and **Destination Address**.

5. Select **Services and Application Group** that we created with apps that need to be blocked.

6. Select **Action**.

7. Enable **Logging** if needed from Options.

Figure 13: Juniper Security Director Cloud—Deployment of SRX Policy



ZONE (6 Rules)

InterZone: Trust To Untrust (Rules 1 to 2)

Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
1 0 hits	Block_Offending_Apps	trust Any	untrust Any	Block_HighBW_Apps defaults	Deny	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	

Intrusion Detection and Prevention (IDP)

When implementing IDP, you can consider the following settings when designing the IDP policy:

- Environment (Services running within the data center)
- Applications (Applications that are currently being served through the firewall)
- Exempt any services or protocols that are not be scanned (for example, SSH)

Based on the services implemented for this JVD, we choose to clone the client-to-server based protection and add a few rules that cater to the server-to-client based traffic.

The policy created considers the following settings:

- Services running in the data center (HTTP, HTTPS, MAIL, ICMP, DB, DNS, and so on)
- Signatures to detect malicious activity
- Signatures to detect network / services scanning
- Signatures to detect any DOS and DDOS based attacks

Workflow to create IDP policies and enforce the policies.

To clone predefined policy:

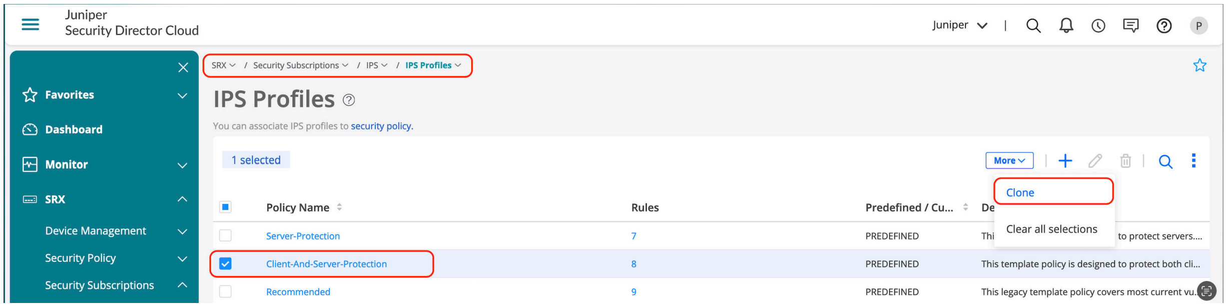
1. Go to **SRX** > **Security Subscription** > **IPS** > **IPS Profiles**.

2. Select the predefined policy to clone.

3. Click **More** and then select **Clone**.

4. Enter a new policy name.

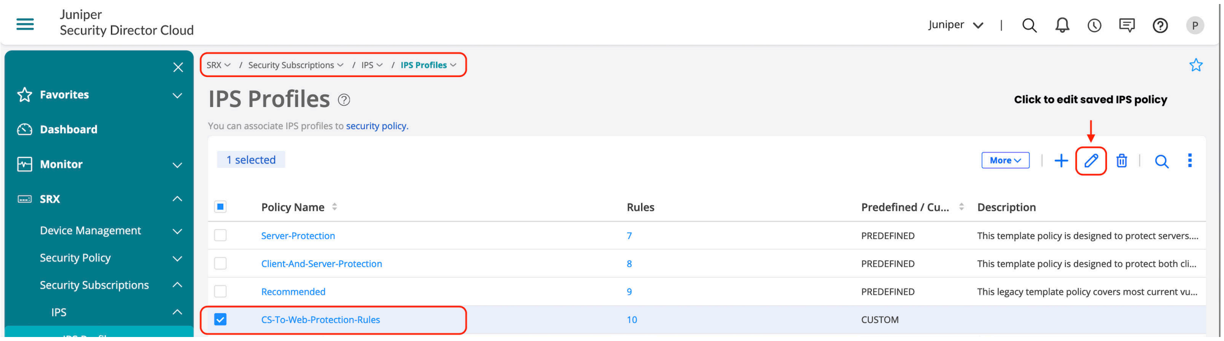
Figure 14: Juniper Security Director Cloud—Creation of IPS Profile



Policy Name	Rules	Predefined / Cu...	De
Server-Protection	7	PREDEFINED	Thi ... to protect servers....
☑ Client-And-Server-Protection	8	PREDEFINED	This template policy is designed to protect both cli...
Recommended	9	PREDEFINED	This legacy template policy covers most current vu...

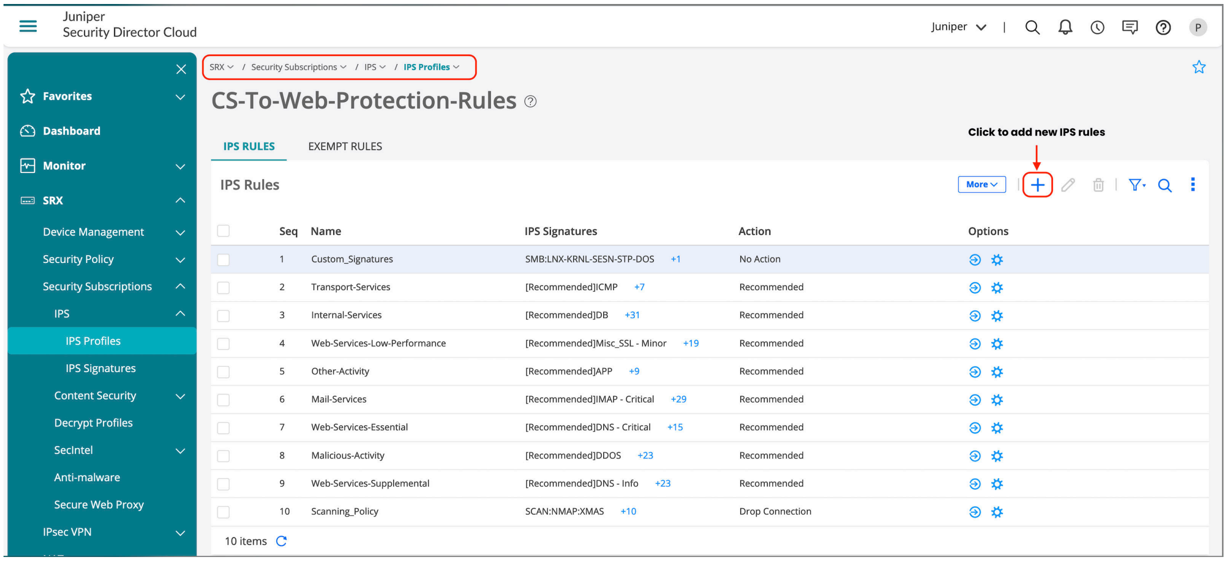
In this JVD, we've named the policy **CS-To-Web-Protection-Rules** and added a few rules which caters to server-to-client protection.

Figure 15: Juniper Security Director Cloud—Creation of IPS Profile



Policy Name	Rules	Predefined / Cu...	Description
Server-Protection	7	PREDEFINED	This template policy is designed to protect servers....
Client-And-Server-Protection	8	PREDEFINED	This template policy is designed to protect both cli...
Recommended	9	PREDEFINED	This legacy template policy covers most current vu...
☑ CS-To-Web-Protection-Rules	10	CUSTOM	

Figure 16: Juniper Security Director Cloud—Add New IPS Rule



CS-To-Web-Protection-Rules

IPS Rules

□	Seq	Name	IPS Signatures	Action	Options
□	1	Custom_Signatures	SMB:LNX-KRNL-SESN-STP-DOS +1	No Action	
□	2	Transport-Services	[Recommended]ICMP +7	Recommended	
□	3	Internal-Services	[Recommended]DB +31	Recommended	
□	4	Web-Services-Low-Performance	[Recommended]Misc_SSL - Minor +19	Recommended	
□	5	Other-Activity	[Recommended]APP +9	Recommended	
□	6	Mail-Services	[Recommended]IMAP - Critical +29	Recommended	
□	7	Web-Services-Essential	[Recommended]DNS - Critical +15	Recommended	
□	8	Malicious-Activity	[Recommended]DDOS +23	Recommended	
□	9	Web-Services-Supplemental	[Recommended]DNS - Info +23	Recommended	
□	10	Scanning_Policy	SCAN:NMAP:XMAS +10	Drop Connection	

10 items

Once new IPS rule is added, update the following:

1. Name of the IPS rule.

2. Add new IDP signatures.

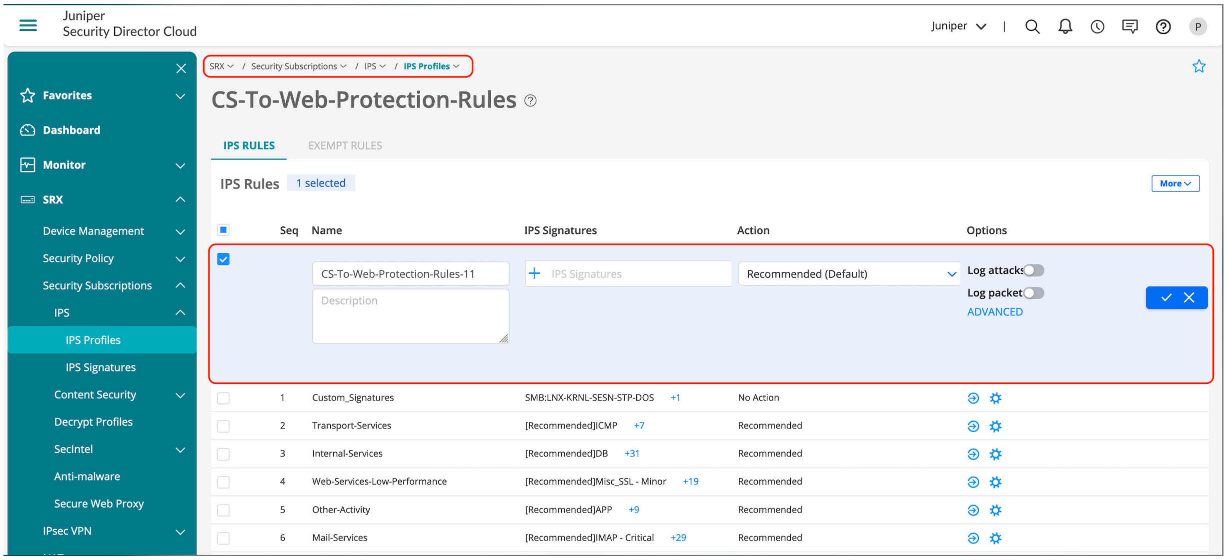
3. Select action if a threat is detected.

4. Optional. Log detected attacks.

5. IPS rules also have advanced options to enable IP actions on detected attacks.

NOTE: Each signature that is added comes with a recommended action to take if detected. You can set the action as Recommended. For more information on the signatures and the recommended action, see: https://threatlabs.juniper.net/home/search/#/list/ips?page_number=1&page_size=20

Figure 17: Juniper Security Director Cloud—Add New IPS Rule



CS-To-Web-Protection-Rules

IPS Rules 1 selected

☑	Seq	Name	IPS Signatures	Action	Options
☑		CS-To-Web-Protection-Rules-11 Description	+ IPS Signatures	Recommended (Default)	Log attacks Log packet ADVANCED
□	1	Custom_Signatures	SMB:LNX-KRNL-SESN-STP-DOS +1	No Action	
□	2	Transport-Services	[Recommended]ICMP +7	Recommended	
□	3	Internal-Services	[Recommended]DB +31	Recommended	
□	4	Web-Services-Low-Performance	[Recommended]Misc_SSL - Minor +19	Recommended	
□	5	Other-Activity	[Recommended]APP +9	Recommended	
□	6	Mail-Services	[Recommended]IMAP - Critical +29	Recommended	

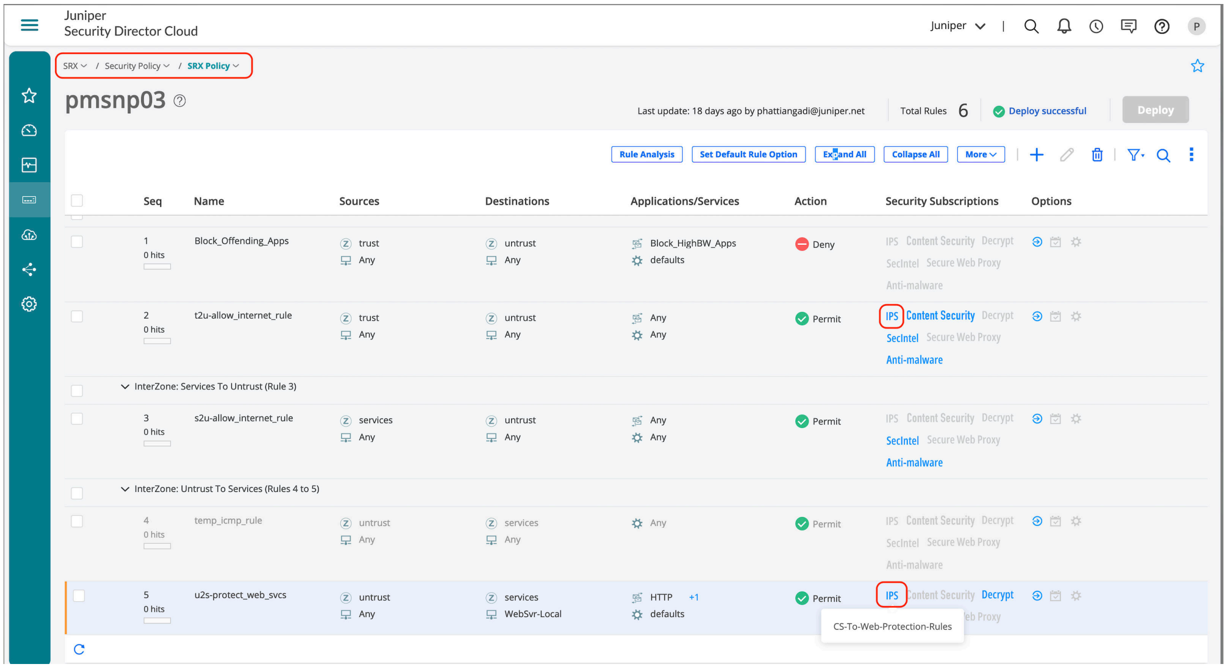
Once IPS profile and rules are created, enforce the IPS profile on a security policy:

1. Click on the firewall rule where IPS needs to be enabled.

2. Click **Security Subscriptions**.

3. Either use the global options and turn on just the IPS toggle or click **Customize** to select a new policy.

Figure 18: Juniper Security Director Cloud—Deployment of Rule with IPS

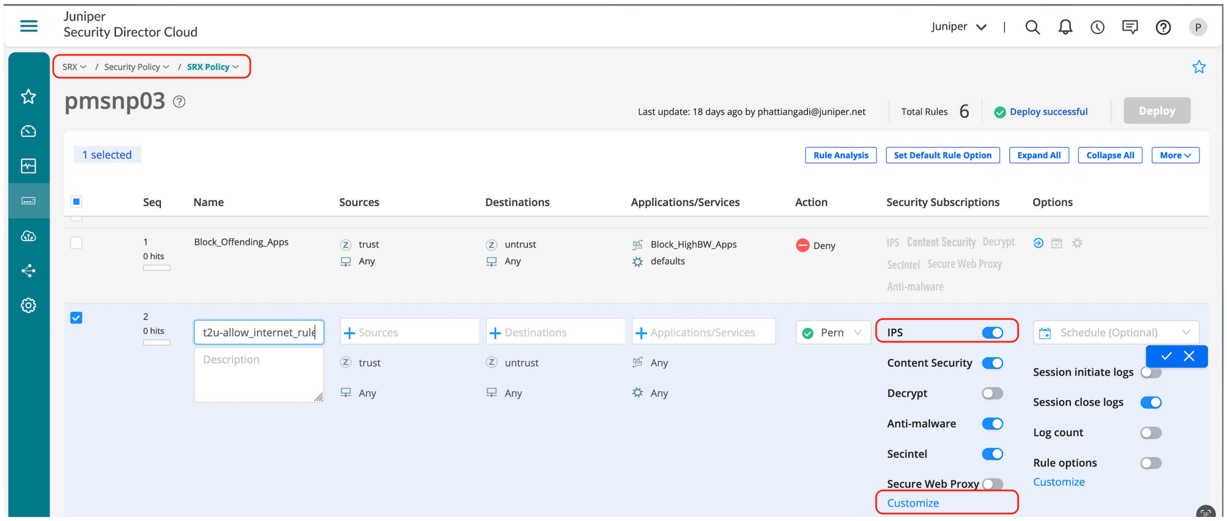


pmsnp03

Last update: 18 days ago by phattiangadi@juniper.net Total Rules 6 Deploy successful

	Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
□	1 0 hits	Block_Offending_Apps	trust Any	untrust Any	Block_HighBW_Apps defaults	Deny	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	
□	2 0 hits	t2u-allow_internet_rule	trust Any	untrust Any	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	
□	InterZone: Services To Untrust (Rule 3)							
□	3 0 hits	s2u-allow_internet_rule	services Any	untrust Any	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	
□	InterZone: Untrust To Services (Rules 4 to 5)							
□	4 0 hits	temp_icmp_rule	untrust Any	services Any	Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	
□	5 0 hits	u2s-protect_web_svcs	untrust Any	services WebSvr-Local	HTTP +1 defaults	Permit	IPS Content Security Decrypt CS-To-Web-Protection-Rules eb Proxy	

Figure 19: Juniper Security Director Cloud—Deployment of Rule with IPS



pmsnp03

Last update: 18 days ago by phattiangadi@juniper.net Total Rules 6 Deploy successful

1 selected

■	Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
□	1 0 hits	Block_Offending_Apps	trust Any	untrust Any	Block_HighBW_Apps defaults	Deny	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	
☑	2 0 hits	t2u-allow_internet_rule Description	+ Sources trust Any	+ Destinations untrust Any	+ Applications/Services Any Any	Perm	IPS ● Content Security ● Decrypt ○ Anti-malware ● Secintel ● Secure Web Proxy ○ Customize	Schedule (Optional) Session initiate logs ○ Session close logs ● Log count ○ Rule options ○ Customize

You can set the Global Options on the main SRX Policy page.

Figure 20: Juniper Security Director Cloud—Deployment of Rule with IPS

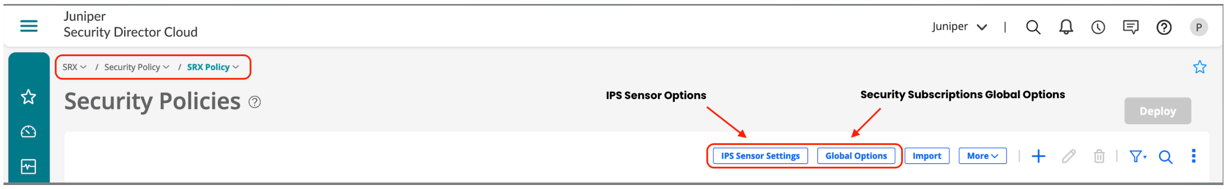
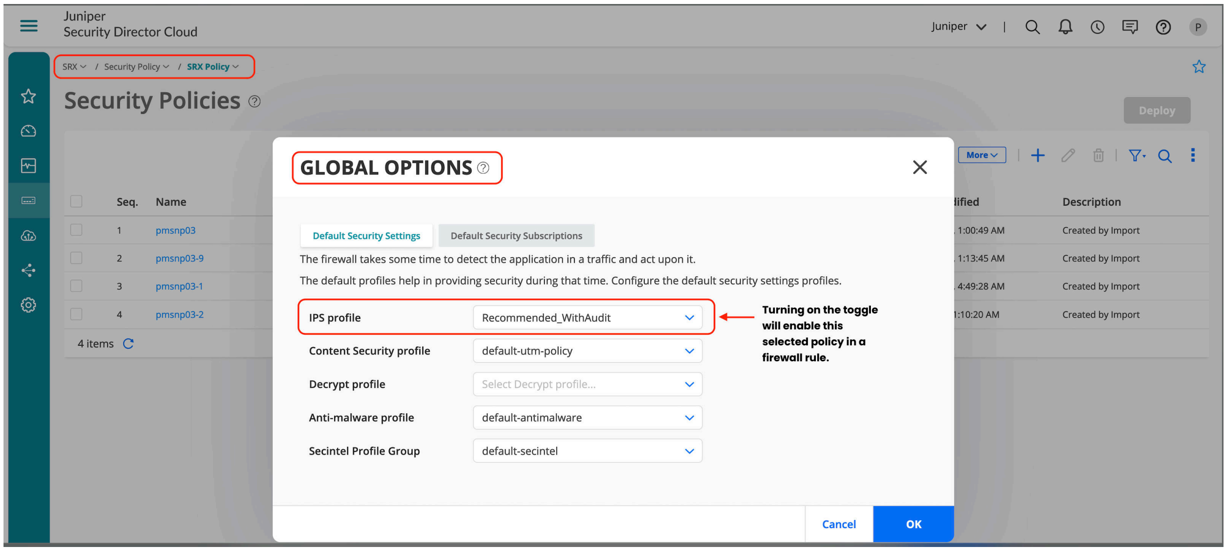


Figure 21: Juniper Security Director Cloud—Deployment of Rule with IPS



The firewall takes some time to detect the application in a traffic and act upon it.

The default profiles help in providing security during that time. Configure the default security settings profiles.

IPS profile: Recommended_WithAudit

Content Security profile: default-utm-policy

Decrypt profile: Select Decrypt profile...

Anti-malware profile: default-antimalware

Secintel Profile Group: default-secintel

Turning on the toggle will enable this selected policy in a firewall rule.

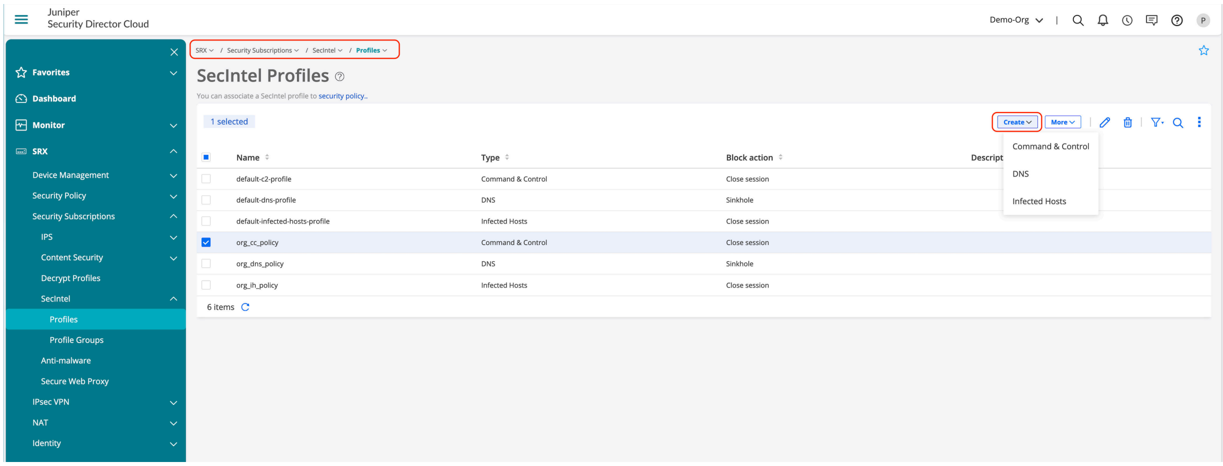
SecIntel Configuration

1. Go to **SRX** > **Security Subscriptions** > **SecIntel** > **Profiles**.

2. Click **Create**.

3. Configure the profiles for required services.

Figure 22: Juniper Security Director Cloud—SecIntel Profile Configuration



SecIntel Profiles

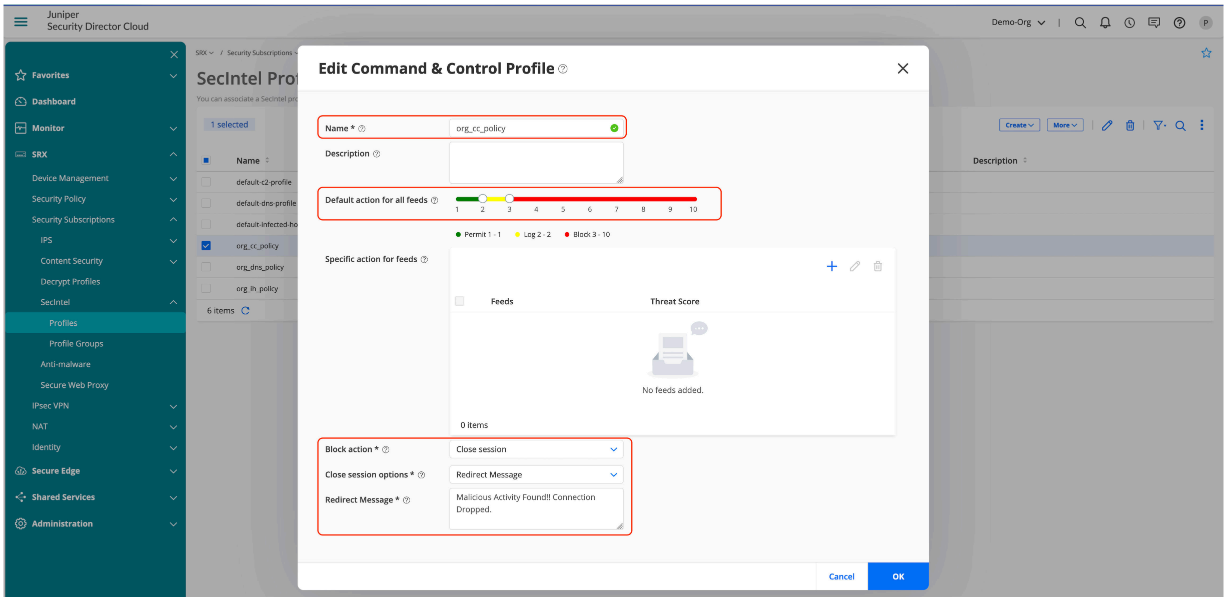
You can associate a SecIntel profile to security policy..

1 selected

	Name	Type	Block action	Descript
☐	default-c2-profile	Command & Control	Close session	
☐	default-dns-profile	DNS	Sinkhole	
☐	default-infected-hosts-profile	Infected Hosts	Close session	
☑	org_cc_policy	Command & Control	Close session	
☐	org_dns_policy	DNS	Sinkhole	
☐	org_ih_policy	Infected Hosts	Close session	

6 items

Figure 23: Juniper Security Director Cloud—SecIntel Command and Control Profile Configuration



Edit Command & Control Profile

Name *: org_cc_policy

Description:

Default action for all feeds: ● Permit 1 - 1 ● Log 2 - 2 ● Block 3 - 10

Specific action for feeds:

☐	Feeds	Threat Score

No feeds added.

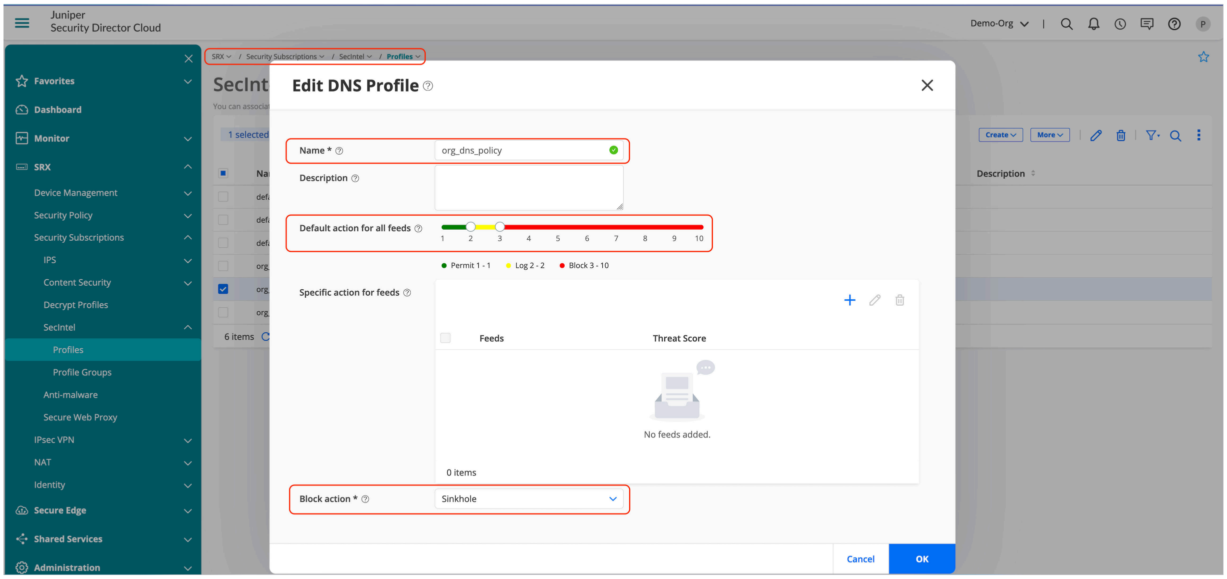
0 items

Block action *: Close session

Close session options *: Redirect Message

Redirect Message *: Malicious Activity Found!! Connection Dropped.

Figure 24: Juniper Security Director Cloud—SecIntel DNS Profile Configuration



Edit DNS Profile

Name * org_dns_policy

Description

Default action for all feeds 1 2 3 4 5 6 7 8 9 10

● Permit 1 - 1 ● Log 2 - 2 ● Block 3 - 10

Specific action for feeds

□	Feeds	Threat Score

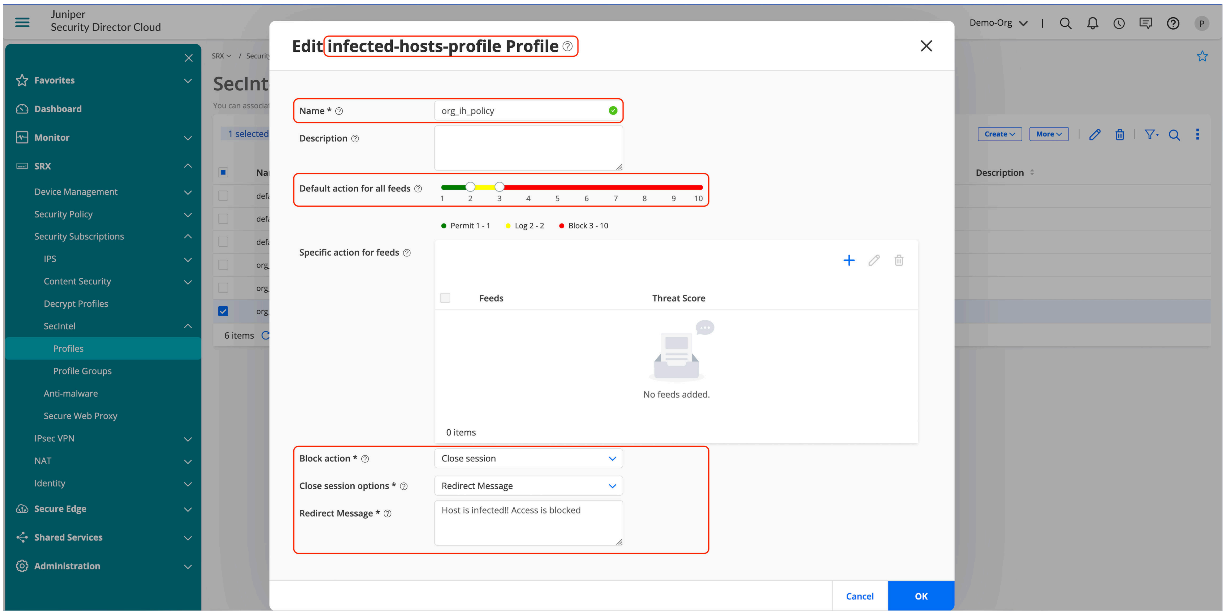
No feeds added.

0 items

Block action * Sinkhole

Cancel OK

Figure 25: Juniper Security Director Cloud—SecIntel Infected-Hosts Profile Configuration



Edit infected-hosts-profile Profile

Name * org_ih_policy

Description

Default action for all feeds 1 2 3 4 5 6 7 8 9 10

● Permit 1 - 1 ● Log 2 - 2 ● Block 3 - 10

Specific action for feeds

□	Feeds	Threat Score

No feeds added.

0 items

Block action * Close session

Close session options * Redirect Message

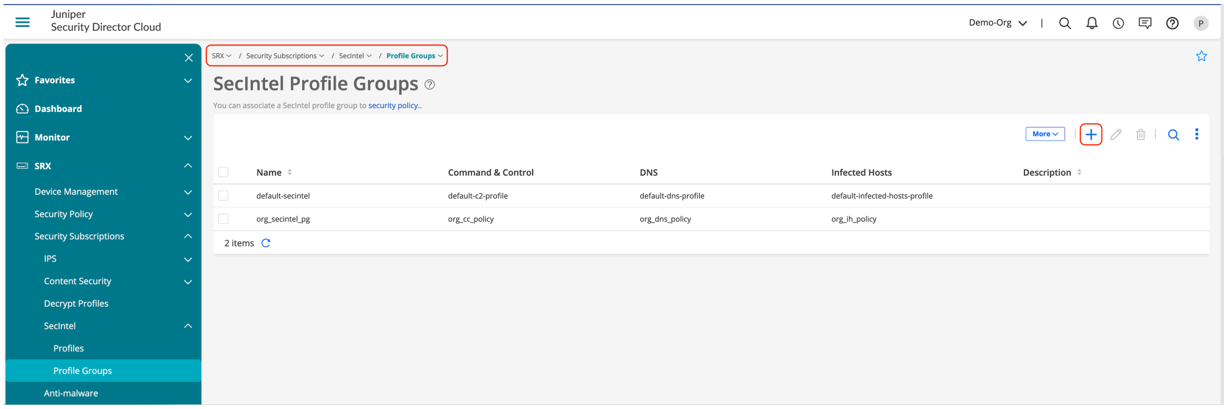
Redirect Message * Host is infected!! Access is blocked

Cancel OK

To create profile groups:

1. Go to **SRX** > **Security Subscriptions** > **SecIntel** > **Profile Groups**.
2. Click **+** to create a new profile group.

Figure 26: Juniper Security Director Cloud—SecIntel Profile Group



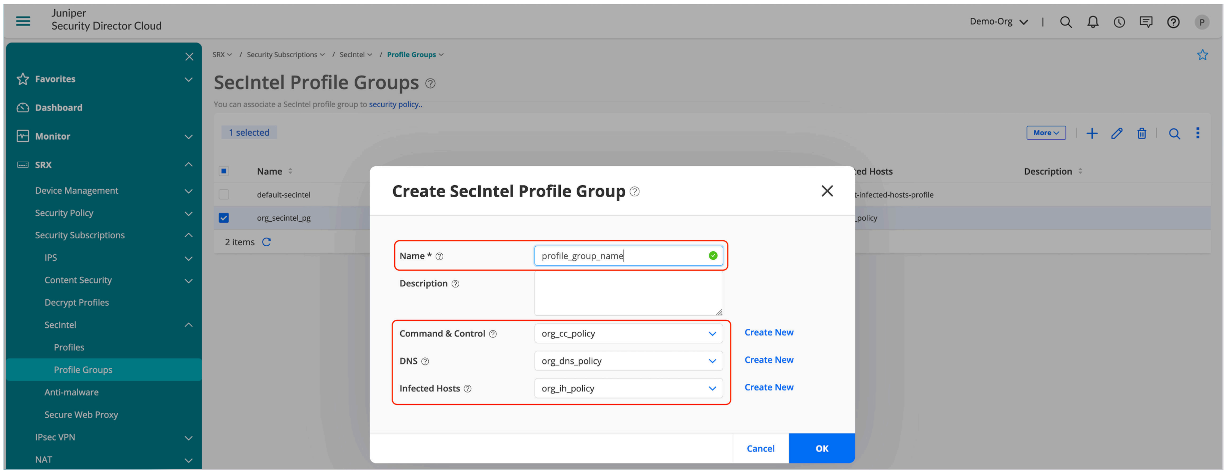
SecIntel Profile Groups

You can associate a SecIntel profile group to security policy..

Name	Command & Control	DNS	Infected Hosts	Description
default-secintel	default-c2-profile	default-dns-profile	default-infected-hosts-profile	
org_secintel_pg	org_cc_policy	org_dns_policy	org_ih_policy	

2 items

Figure 27: Juniper Security Director Cloud—SecIntel Profile Group Configuration



Create SecIntel Profile Group

Name *: profile_group_name

Description:

Command & Control: org_cc_policy

DNS: org_dns_policy

Infected Hosts: org_ih_policy

As a final step, let's enable the SecIntel profile group in a security policy that enforces the detection and remediation for SecIntel profiles based on reputation.

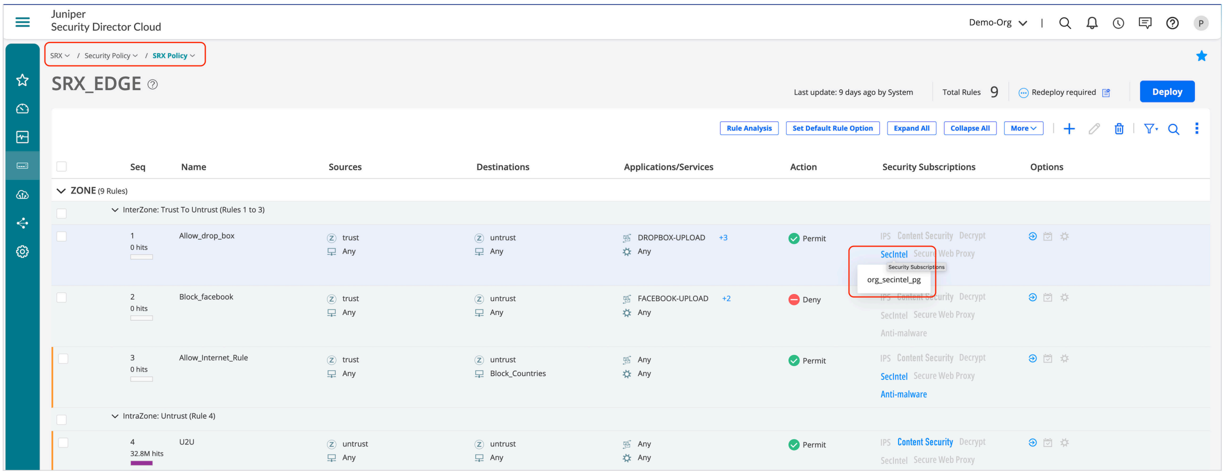
To enable SecIntel profile group in a security policy:

1. Go to **SRX** > **Security Policy** > **SRX Policy**.

2. Select the policy you want to modify and click the pencil icon.

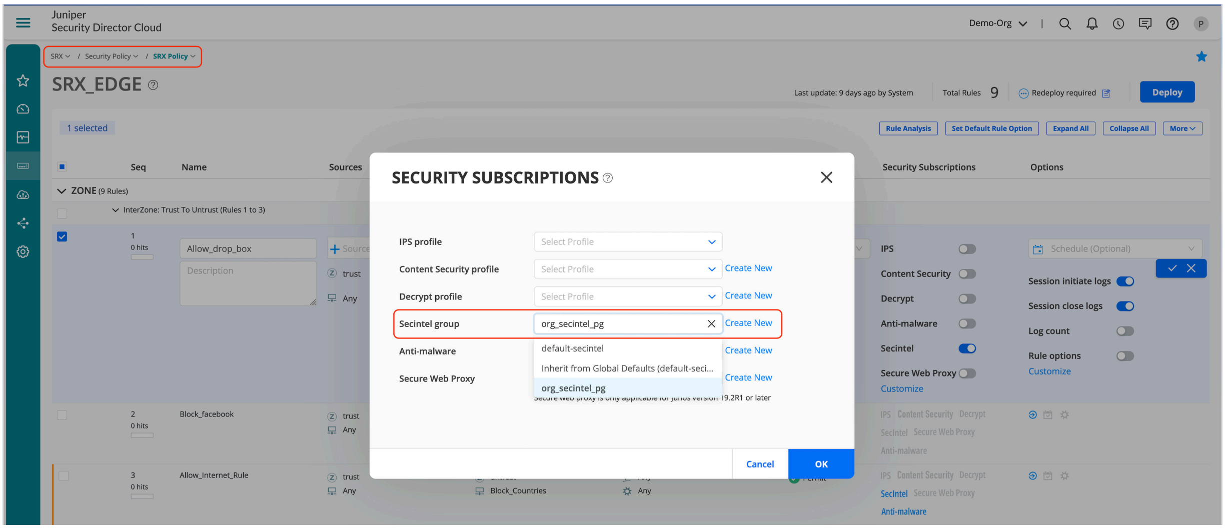
3. Edit policy to enable SecIntel profile group or click on **Create New** to select a different profile.

Figure 28: Juniper Security Director Cloud—Assign SecIntel Profile Group



Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions
ZONE (9 Rules)						
InterZone: Trust To Untrust (Rules 1 to 3)						
1 0 hits	Allow_drop_box	trust Any	untrust Any	DROPBOX-UPLOAD +3 Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy org_secintel_pg
2 0 hits	Block_facebook	trust Any	untrust Any	FACEBOOK-UPLOAD +2 Any	Deny	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware
3 0 hits	Allow_Internet_Rule	trust Any	untrust Block_Countries	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware
IntraZone: Untrust (Rule 4)						
4 32.8M hits	U2U	untrust Any	untrust Any	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy

Figure 29: Juniper Security Director Cloud—Assign SecIntel Group to Security Policy



SECURITY SUBSCRIPTIONS

IPS profile	Select Profile
Content Security profile	Select Profile
Decrypt profile	Select Profile
Secintel group	org_secintel_pg
Anti-malware	
Secure Web Proxy	

default-secintel
Inherit from Global Defaults (default-seci...
org_secintel_pg

Secure web proxy is only applicable for Junos version 19.2R1 or later

IPS ○
Content Security ○
Decrypt ○
Anti-malware ○
Secintel ●
Secure Web Proxy ○
Customize

Session initiate logs ●
Session close logs ●
Log count ○
Rule options ○
Customize

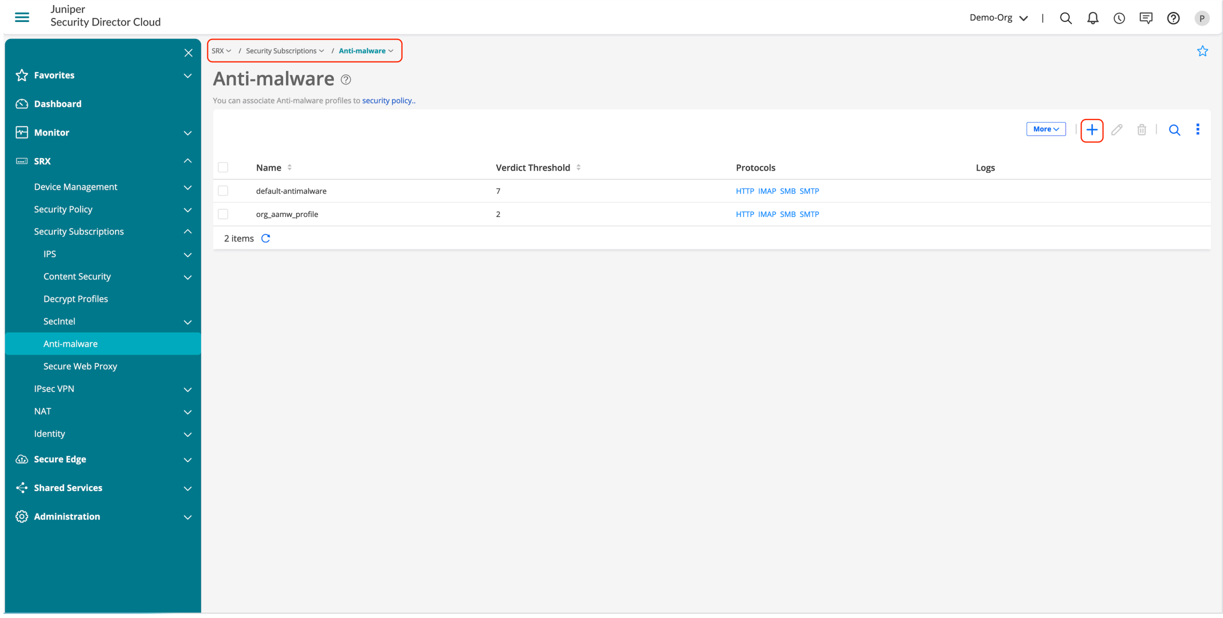
Advanced Anti-Malware

1. Go to **SRX** > **Security Subscriptions** > **Anti-malware**.

2. Click **+**.

3. Configure the protocols that you need to enable and click **OK** to save the AAMW profile.

Figure 30: Juniper Security Director Cloud—Advanced Anti-Malware Profiles



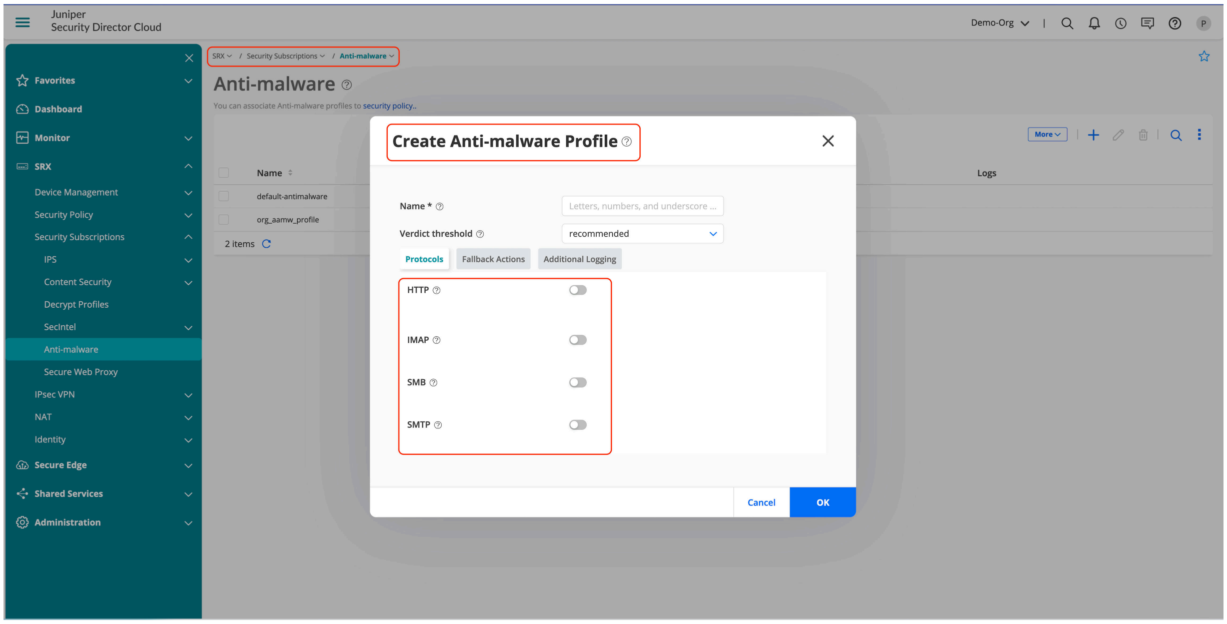
Anti-malware

You can associate Anti-malware profiles to security policy..

Name	Verdict Threshold	Protocols	Logs
default-antimalware	7	HTTP IMAP SMB SMTP	
org_aamw_profile	2	HTTP IMAP SMB SMTP	

2 items

Figure 31: Juniper Security Director Cloud—Advanced Anti-Malware Profile Configuration



Create Anti-malware Profile

Name * Letters, numbers, and underscore ...

Verdict threshold recommended

Protocols | Fallback Actions | Additional Logging

HTTP

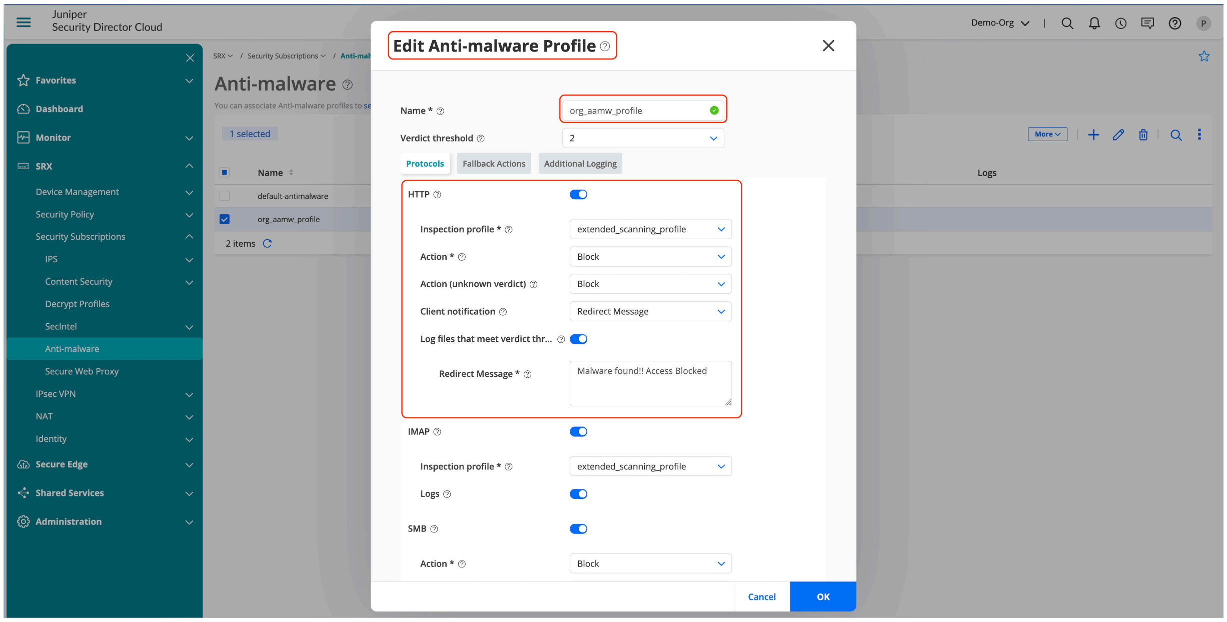
IMAP

SMB

SMTP

Cancel | OK

Figure 32: Juniper Security Director Cloud—Advanced Anti-Malware Profile Configuration



Edit Anti-malware Profile

Name *: org_aamw_profile

Verdict threshold: 2

Protocols | Fallback Actions | Additional Logging

HTTP: on

- Inspection profile *: extended_scanning_profile
- Action *: Block
- Action (unknown verdict): Block
- Client notification: Redirect Message
- Log files that meet verdict thr...: on
- Redirect Message *: Malware found!! Access Blocked

IMAP: on

- Inspection profile *: extended_scanning_profile
- Logs: on

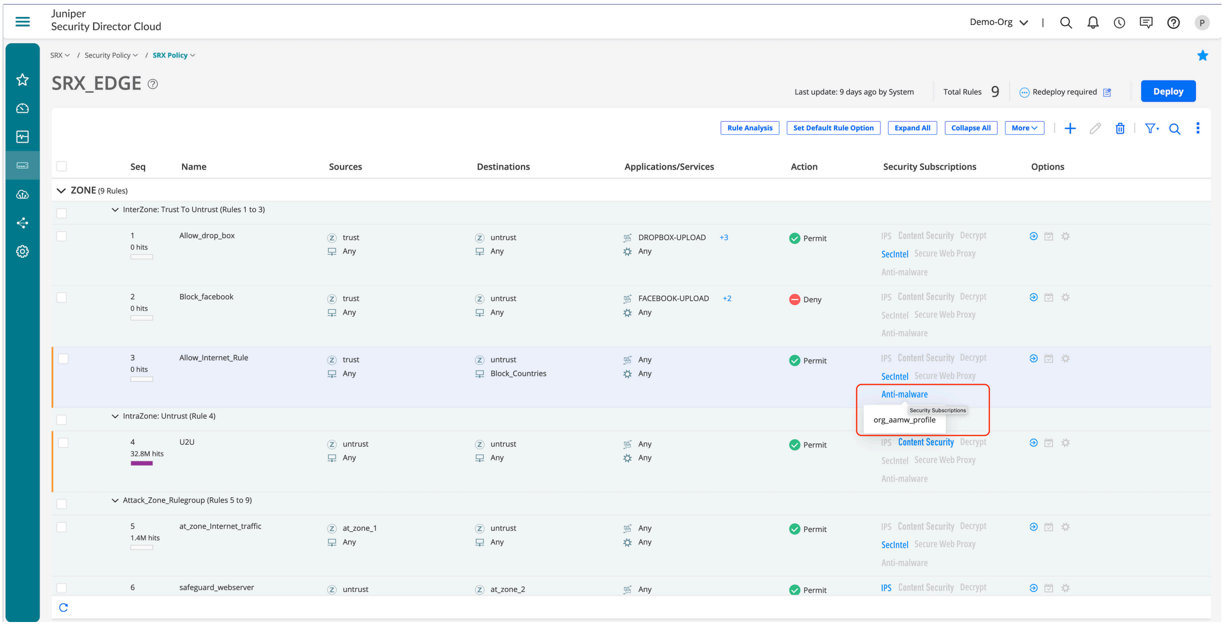
SMB: on

- Action *: Block

Cancel | OK

Created AAMW profile is configured in a security policy.

Figure 33: Juniper Security Director Cloud—Assign Advanced Anti-Malware Profile to Security Policy



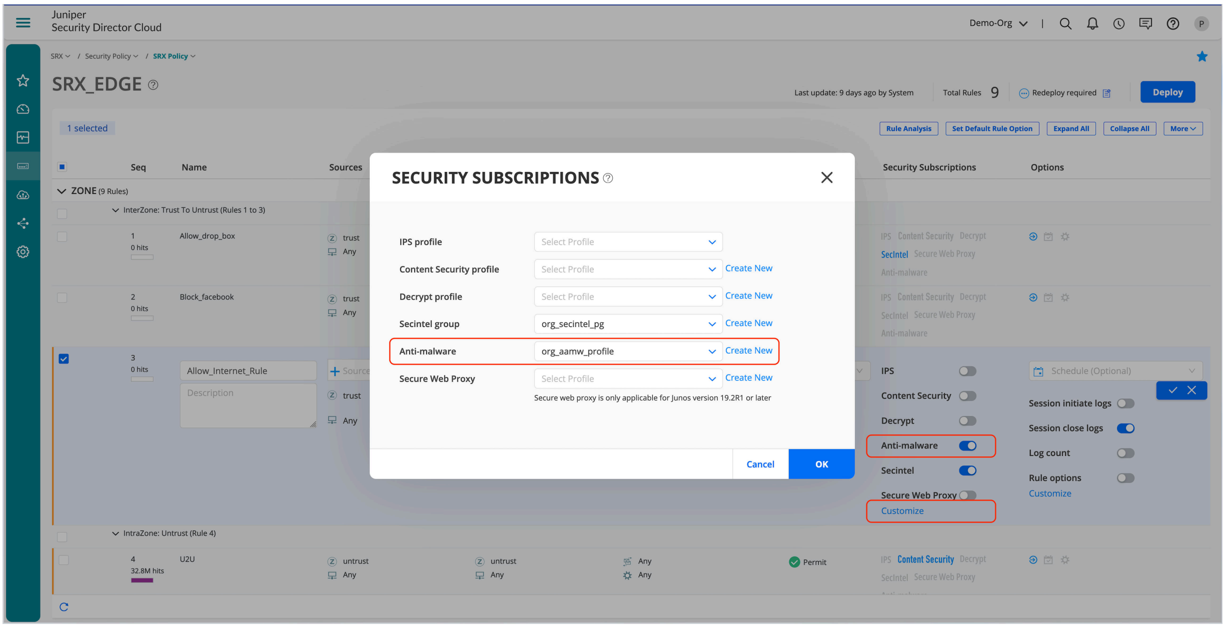
SRX_EDGE

Last update: 9 days ago by System | Total Rules 9 | Redeploy required

ZONE (9 Rules)

Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions
InterZone: Trust To Untrust (Rules 1 to 3)						
1 0 hits	Allow_drop_box	trust Any	untrust Any	DROPBOX-UPLOAD +3 Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware
2 0 hits	Block_facebook	trust Any	untrust Any	FACEBOOK-UPLOAD +2 Any	Deny	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware
3 0 hits	Allow_Internet_Rule	trust Any	untrust Block_Countries	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware Security Subscriptions: org_aamw_profile
IntraZone: Untrust (Rule 4)						
4 32.8M hits	U2U	untrust Any	untrust Any	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware
Attack_Zone_Rulegroup (Rules 5 to 9)						
5 1.4M hits	at_zone_Internet_traffic	at_zone_1 Any	untrust Any	Any Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware
6	safeguard_webserver	untrust	at_zone_2	Any	Permit	IPS Content Security Decrypt

Figure 34: Juniper Security Director Cloud—Assign Advanced Anti-Malware Profile to Security Policy



SECURITY SUBSCRIPTIONS

IPS profile: Select Profile

Content Security profile: Select Profile — Create New

Decrypt profile: Select Profile — Create New

Secintel group: org_secintel_pg — Create New

Anti-malware: org_aamw_profile — Create New

Secure Web Proxy: Select Profile — Create New

Secure web proxy is only applicable for Junos version 19.2R1 or later

DNS Security

DNS security is configured in two phases:

- Enabling SecIntel phase, which is covered under the SecIntel section.
- Enabling core DNS security features such as DNS DGA and DNS Tunneling, which are covered in this section.

To enable DNS security, follow the path to configure the settings on Juniper Security Director Cloud:

1. Go to **SRX** > **Device Management** > **Devices.**
2. Click the device we want to configure DNS security.
3. Click **Junos Detailed Configurations**.
4. Enter **DNS filtering** in the search section.
5. Select **Services** > **Dns Filtering**.
6. Enter the details.
7. Click **Save** once done.

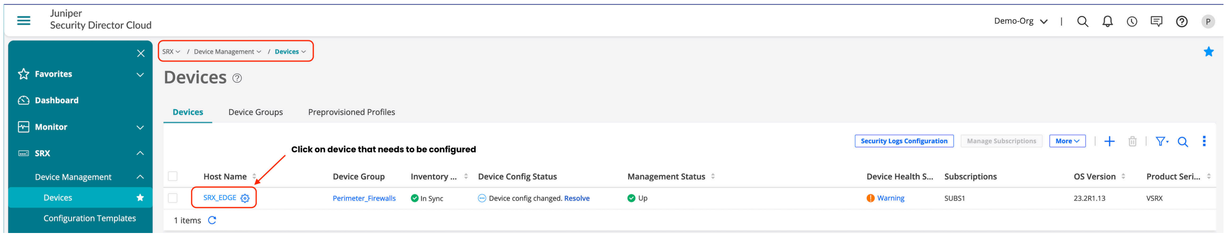
8. Optional. Click **Preview** if you want to view saved configuration.

9. Click **Deploy** to deploy the configuration to the device.

> **NOTE**: You can always complete all the configuration sections and save before deploying the final configuration.

Also, this configuration is the same for implementing IoT Security as well.

Figure 35: Juniper Security Director Cloud—DNS Security Configuration

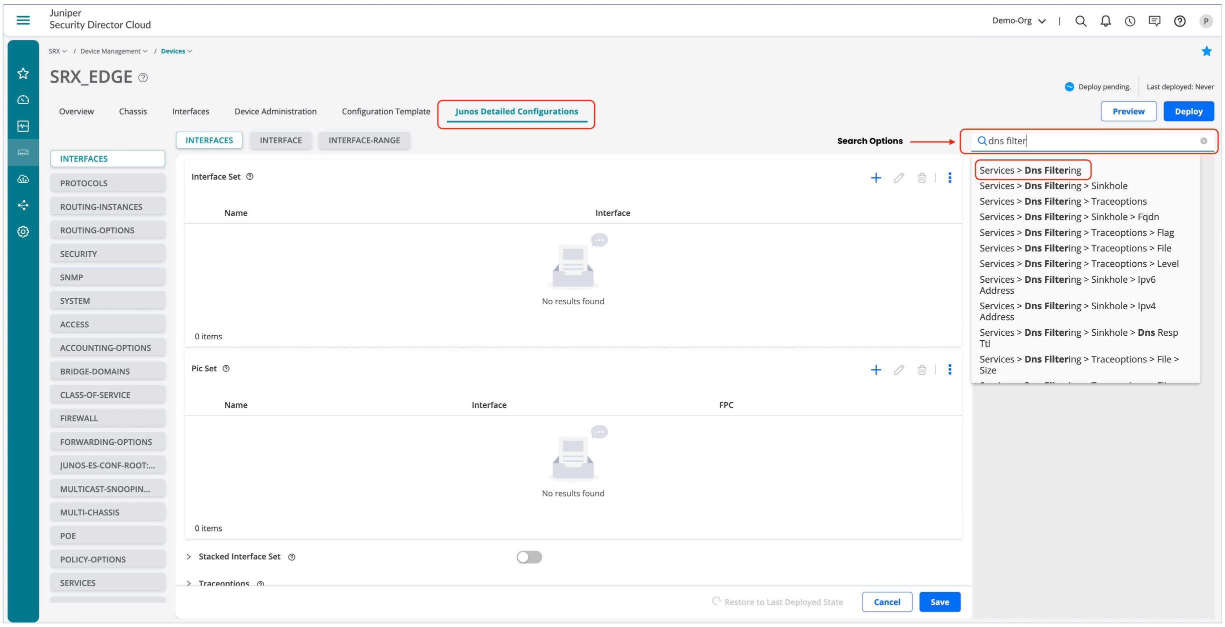


Click on device that needs to be configured

Host Name	Device Group	Inventory ...	Device Config Status	Management Status	Device Health S...	Subscriptions	OS Version	Product Seri...
SRX_EDGE	Perimeter_Firewalls	In Sync	Device config changed. Resolve	Up	Warning	SUBS1	23.2R1.13	VSRX

1 items

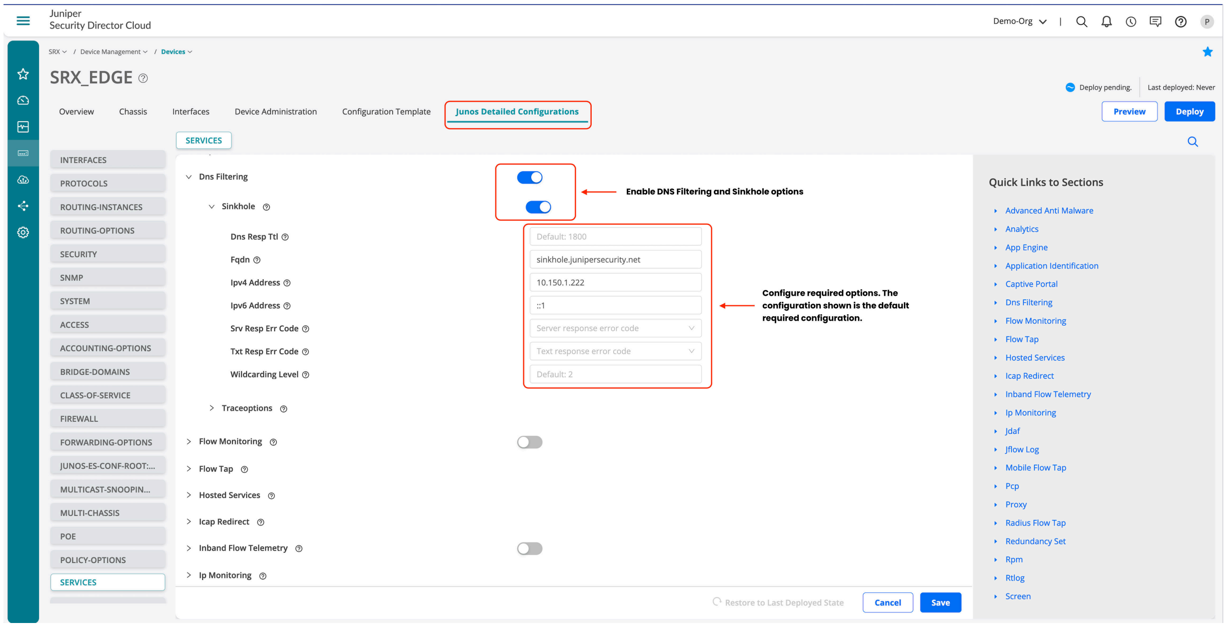
Figure 36: Juniper Security Director Cloud—Junos Detailed Configuration



dns filter

Services > **Dns Filter**ing
Services > **Dns Filter**ing > Sinkhole
Services > **Dns Filter**ing > Traceoptions
Services > **Dns Filter**ing > Sinkhole > Fqdn
Services > **Dns Filter**ing > Traceoptions > Flag
Services > **Dns Filter**ing > Traceoptions > File
Services > **Dns Filter**ing > Traceoptions > Level
Services > **Dns Filter**ing > Sinkhole > Ipv6 Address
Services > **Dns Filter**ing > Sinkhole > Ipv4 Address
Services > **Dns Filter**ing > Sinkhole > **Dns** Resp Ttl
Services > **Dns Filter**ing > Traceoptions > File > Size

Figure 37: Juniper Security Director Cloud—Junos Detailed Configuration—DNS Filtering



Dns Filtering: enabled
Sinkhole: enabled

Enable DNS Filtering and Sinkhole options

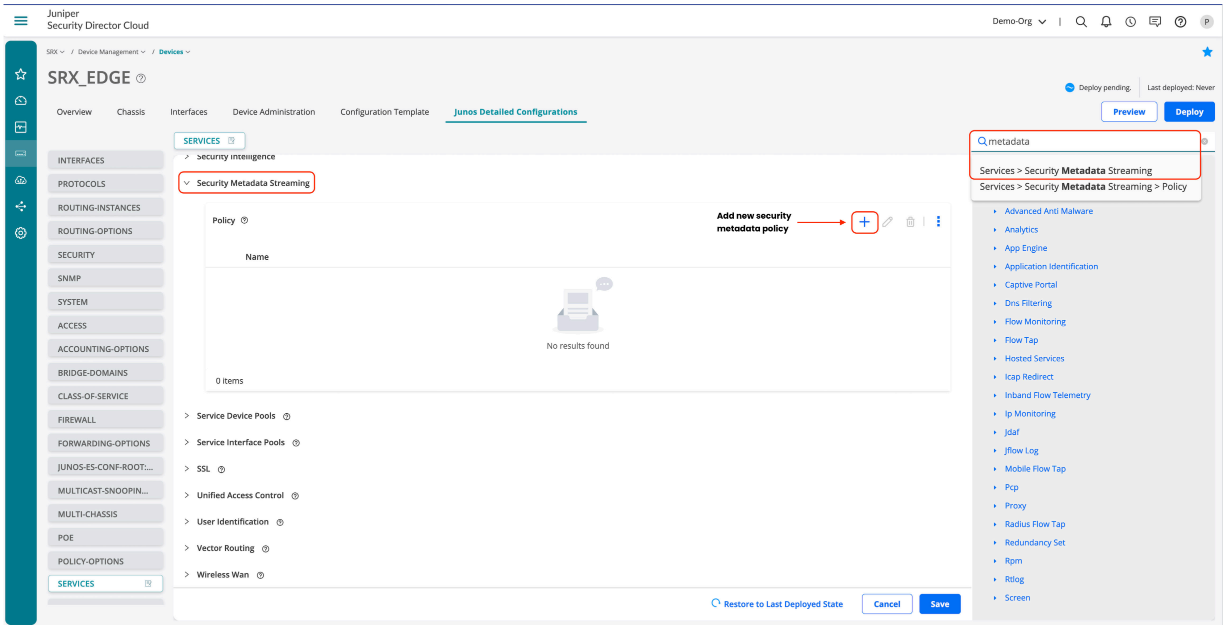
Dns Resp Ttl: Default: 1800
Fqdn: sinkhole.junipersecurity.net
Ipv4 Address: 10.150.1.222
Ipv6 Address: ::1
Srv Resp Err Code: Server response error code
Txt Resp Err Code: Text response error code
Wildcarding Level: Default: 2

Configure required options. The configuration shown is the default required configuration.

Let’s configure the core DNS security features:

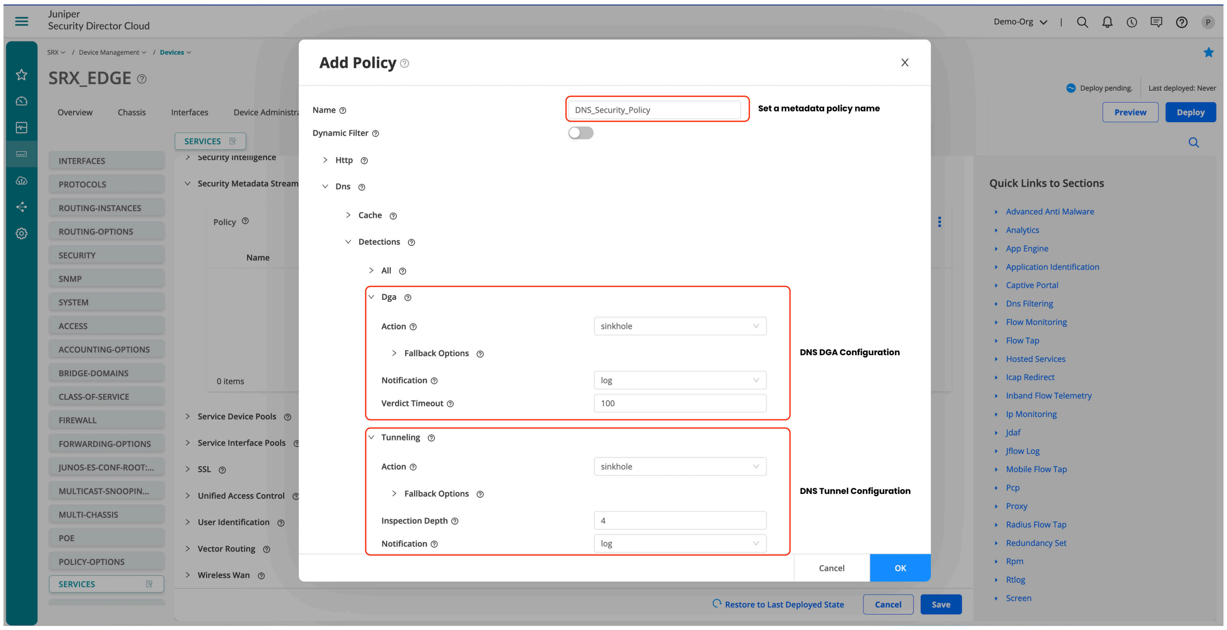
1. Enter **metadata** in the search section.
2. Select **Services** > **Security Metadata Streaming**.
3. Click to proceed to the configuration section.
4. Click **+** to enable DNS metadata configuration.
5. Click **Save** once done.
6. Optional. Click **Preview** if you want to view saved configuration.
7. Click **Deploy** to deploy the configuration to the device.

Figure 38: Juniper Security Director Cloud—Junos Detailed Configuration—Security Metadata



Add new security metadata policy

Figure 39: Juniper Security Director Cloud—Junos Detailed Configuration—Security Metadata



Name: DNS_Security_Policy

Dynamic Filter: ○ (off)

Set a metadata policy name

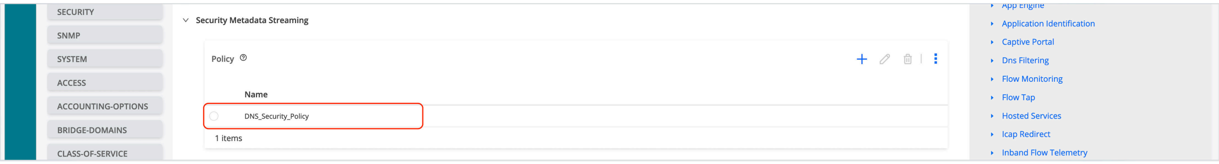
Dga
- Action: sinkhole
- Notification: log
- Verdict Timeout: 100

DNS DGA Configuration

Tunneling
- Action: sinkhole
- Inspection Depth: 4
- Notification: log

DNS Tunnel Configuration

Figure 40: Juniper Security Director Cloud— Junos Detailed Configuration—Security Metadata Policy



NOTE: Ensure to save and deploy the configuration once its completed.

Let's use CLI to configure the metadata streaming policy on a zone pair to enforce DNS security settings.

Ensure that the configuration is deployed before configuring the next steps through CLI.

```
# Add the security metadata streaming policy:
set security policies from-zone trust to-zone untrust application-services security-metadata-
streaming-policy DNS_Security_Policy
```

Security Screens

To configure Security IDS Screen option on Juniper Security Director Cloud:

1. Go to **SRX** > **Device Management** > **Devices**.

2. Click on the device.

3. Click **Junos Detailed Configurations**.

4. Search for screens.

5. Select **Security** > **Screen**.

6. Click **+** to add a new profile.

Figure 41: Juniper Security Director Cloud—Screens Configuration

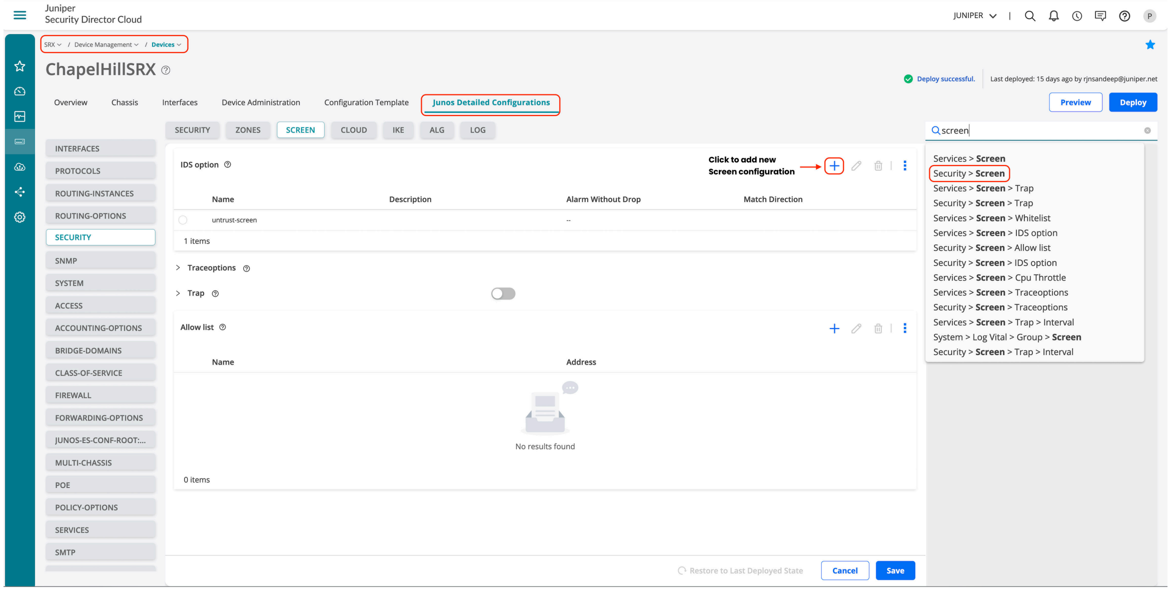
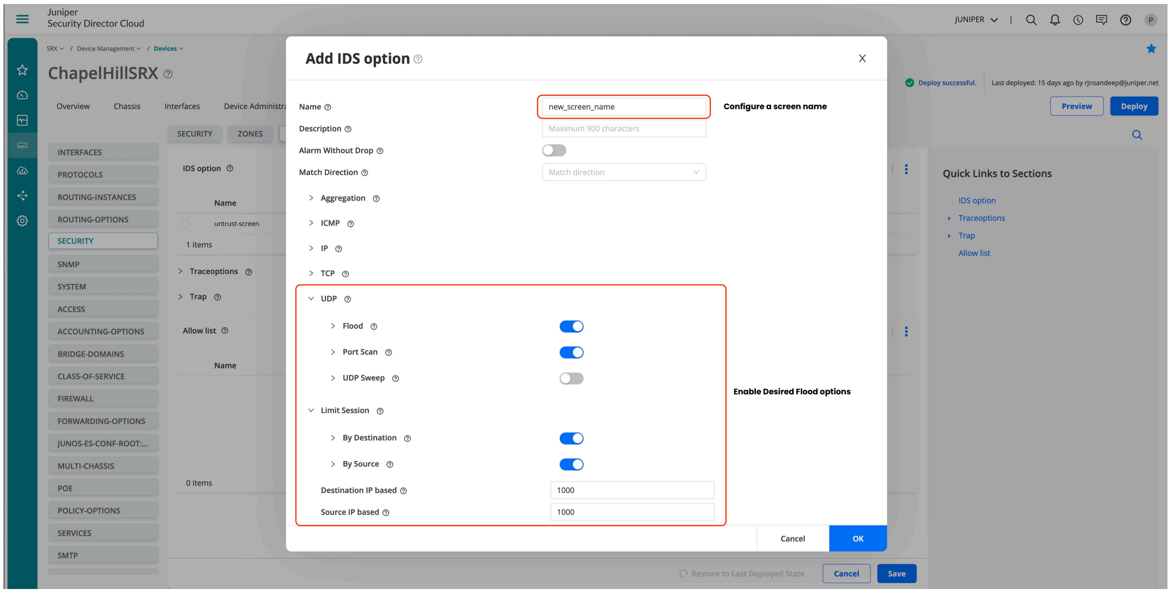


Figure 42: Juniper Security Director Cloud—Screens Flood Attack Options


Add IDS option

Name: new_screen_name

Description: Maximum 900 characters

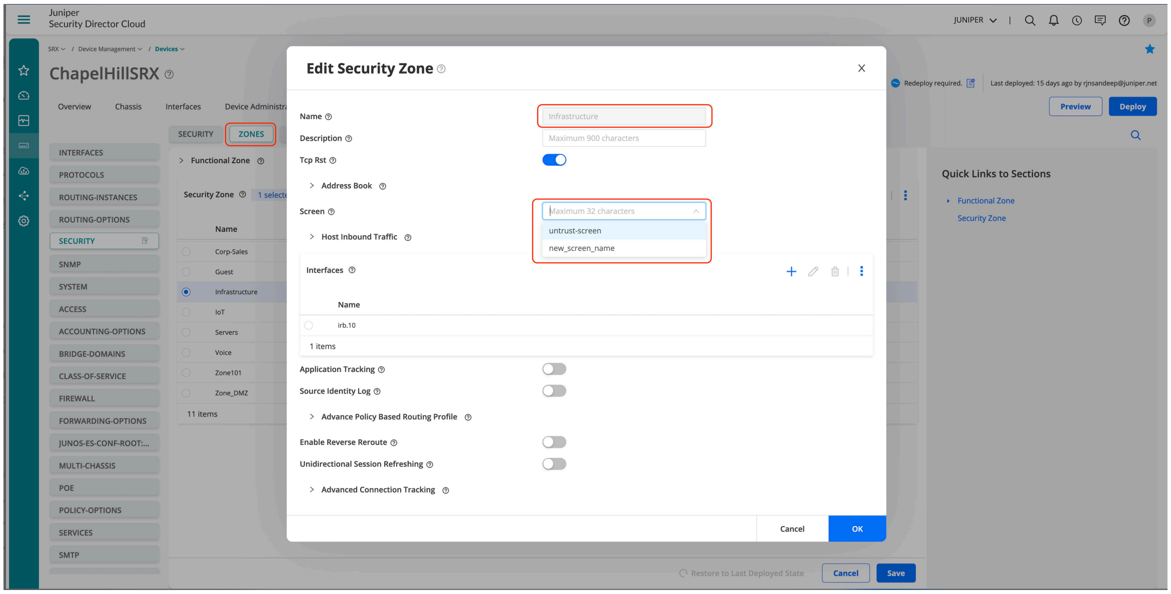
Destination IP based: 1000

Source IP based: 1000

7. Click **OK** to save the screen configuration once the desired configuration is completed.

8. Click **Zones** to enforce the screen on a specific zone.

Figure 43: Juniper Security Director Cloud—Assign Screens Options to Zone



Edit Security Zone

Name: Infrastructure

Description: Maximum 900 characters

Tcp Rst: on

> Address Book

Screen: Maximum 32 characters
- untrust-screen
- new_screen_name

> Host Inbound Traffic

Interfaces

Name
irb.10

1 items

Application Tracking: off

Source Identity Log: off

> Advance Policy Based Routing Profile

Enable Reverse Reroute: off

Unidirectional Session Refreshing: off

> Advanced Connection Tracking

9. Click **OK** to save the configuration once the new screen configuration is applied to the zone.

10. Click **Deploy** to deploy the configuration to the device.

Reverse SSL Proxy

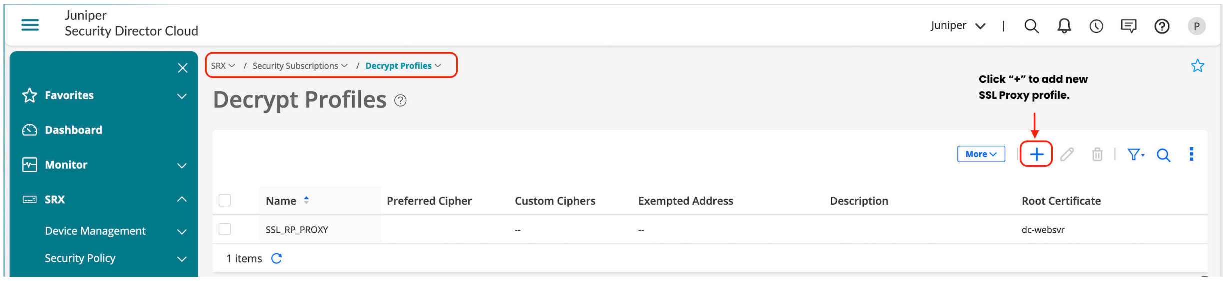
As the data center next-generation firewall use case focuses on protecting internal resources such as webservers, we can optionally implement SSL reverse proxy. SSL reverse proxy ensures advanced services are applied to decrypted webserver traffic and inspected before leaving the firewall to gain the webserver resources.

The creation of the webserver certificates is not covered in this section. You must import this certificate into Juniper Security Director Cloud. This certificate is used when creating the SSL proxy profile.

To create the SSL reverse proxy profile:

1. Import webserver certificates.
2. Create the SSL reverse proxy profile.
3. Go to **SRX** > **Security Subscriptions** > **Decrypt Profiles**.
4. Click **+** to add a new profile.

Figure 44: Juniper Security Director Cloud—Assign Screens Options to Zone



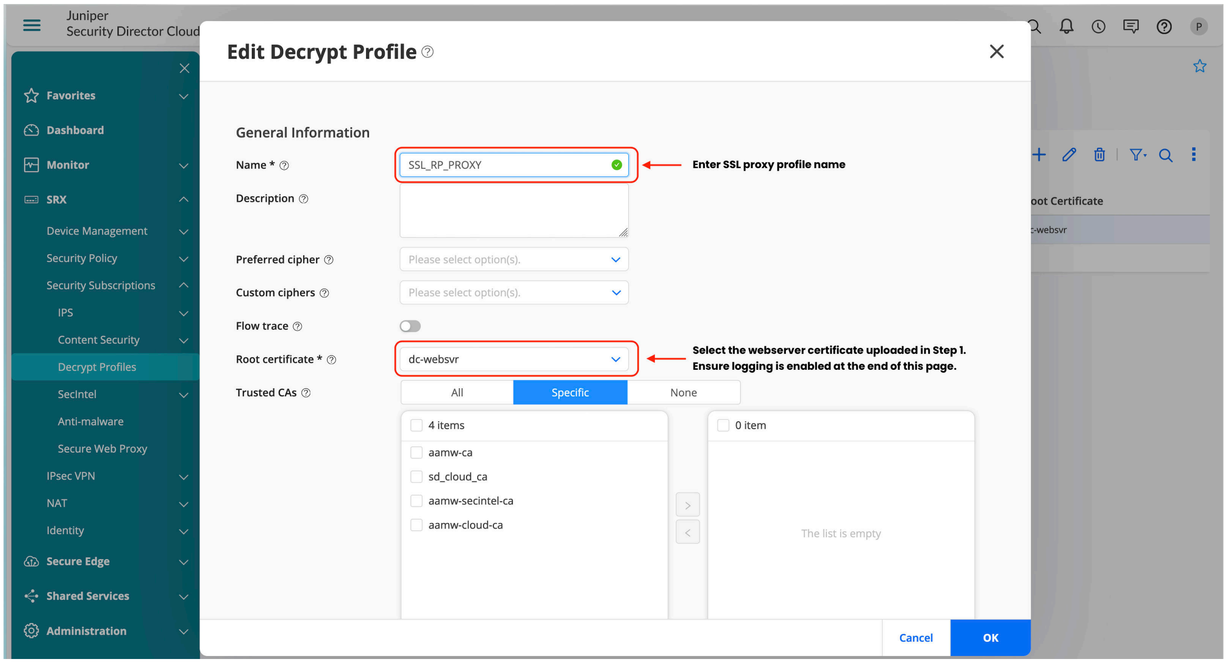
Decrypt Profiles

Click "+" to add new SSL Proxy profile.

	Name	Preferred Cipher	Custom Ciphers	Exempted Address	Description	Root Certificate
□	SSL_RP_PROXY		--	--		dc-websvr

1 items

Figure 45: Juniper Security Director Cloud—Assign Screens Options to Zone



Edit Decrypt Profile

General Information

Name * SSL_RP_PROXY

Enter SSL proxy profile name

Description

Preferred cipher Please select option(s).

Custom ciphers Please select option(s).

Flow trace

Root certificate * dc-websvr

Select the webserver certificate uploaded in Step 1. Ensure logging is enabled at the end of this page.

Trusted CAs All | Specific | None

□ 4 items
□ aamw-ca
□ sd_cloud_ca
□ aamw-secintel-ca
□ aamw-cloud-ca

□ 0 item
The list is empty

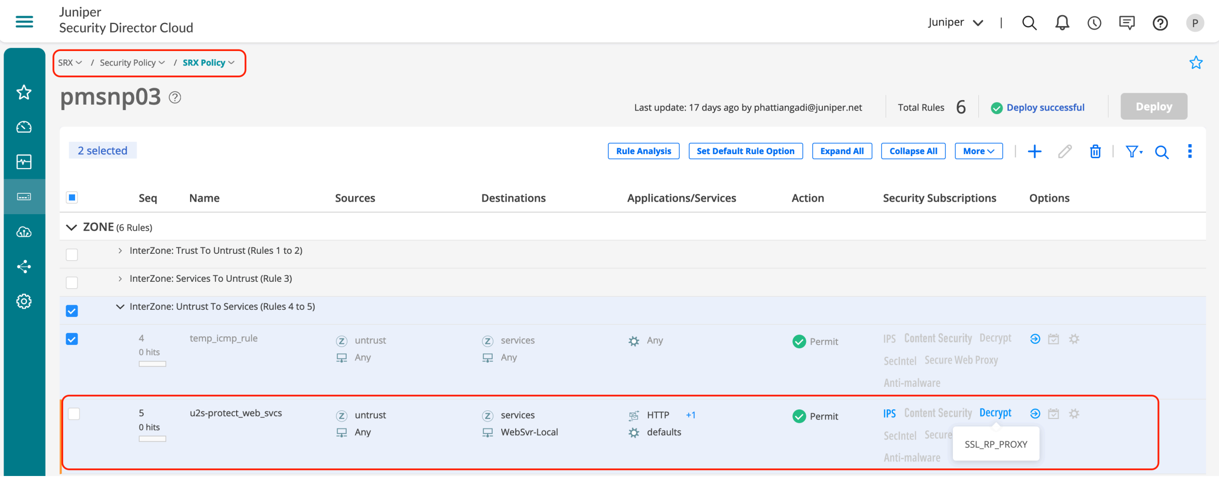
Cancel OK

Include the profile in a firewall rule for enforcement:

1. Go to **SRX** > **Security Policy** > **SRX Policy**.
2. Click + to add new firewall rule.
3. Enter **Source Zone** and **Source Address**.
4. Enter **Destination Zone** and **Destination Address**.
5. Select **Services and Applications**.
6. Select **Advanced Services** under security subscriptions that must be enabled. In this example, IPS is selected.

7. Select the SSL Reverse proxy profile created in the previous step.

Figure 46: Juniper Security Director Cloud—Assign Screens Options to Zone



pmsnp03

Last update: 17 days ago by phattiangadi@juniper.net Total Rules 6 Deploy successful

	Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
	ZONE (6 Rules)							
☐	InterZone: Trust To Untrust (Rules 1 to 2)							
☐	InterZone: Services To Untrust (Rule 3)							
☑	InterZone: Untrust To Services (Rules 4 to 5)							
☑	4 0 hits	temp_icmp_rule	untrust Any	services Any	Any	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware	
☐	5 0 hits	u2s-protect_web_svcs	untrust Any	services WebSvr-Local	HTTP +1 defaults	Permit	IPS Content Security Decrypt SecIntel Secure Anti-malware	

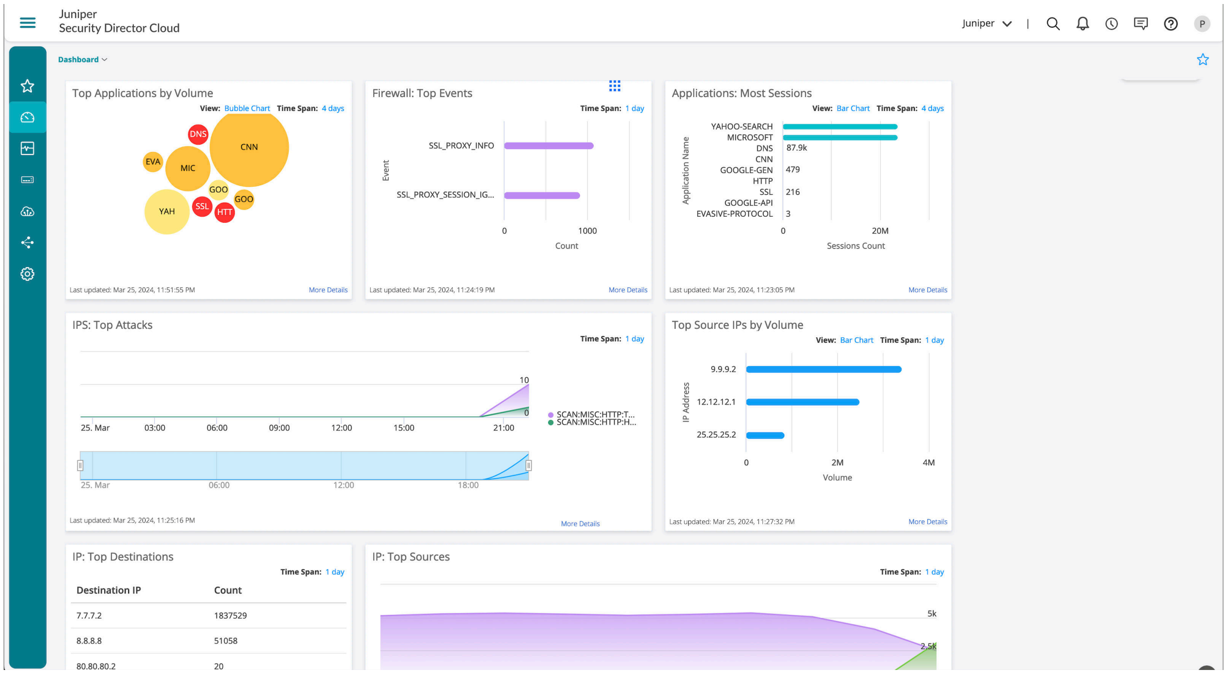
SSL_RP_PROXY

Data Center Next-Generation Firewall Solution Validation

The configuration provides advanced security services in data center environment using next-generation firewalls. In this section, we'll focus on validating the solution that is implemented with this JVD.

Let's start with the Juniper Security Director Cloud Dashboard, which is the landing page when logged in. The Dashboard page provides a landscape of what is happening in the environment through various readily available widgets.

Figure 47: Juniper Security Director Cloud—Dashboard Page



Destination IP	Count
7.7.7.2	1837529
8.8.8.8	51058
80.80.80.2	20

The **Monitor** > **Logs** > **Session** page provides a snapshot of the traffic flow through the environment. Using Session page, you can filter information based on various options that's provided on the page.

Table 3: Filter Options

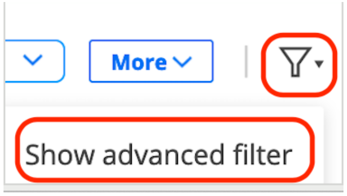
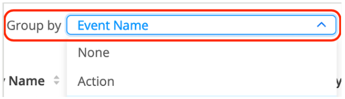
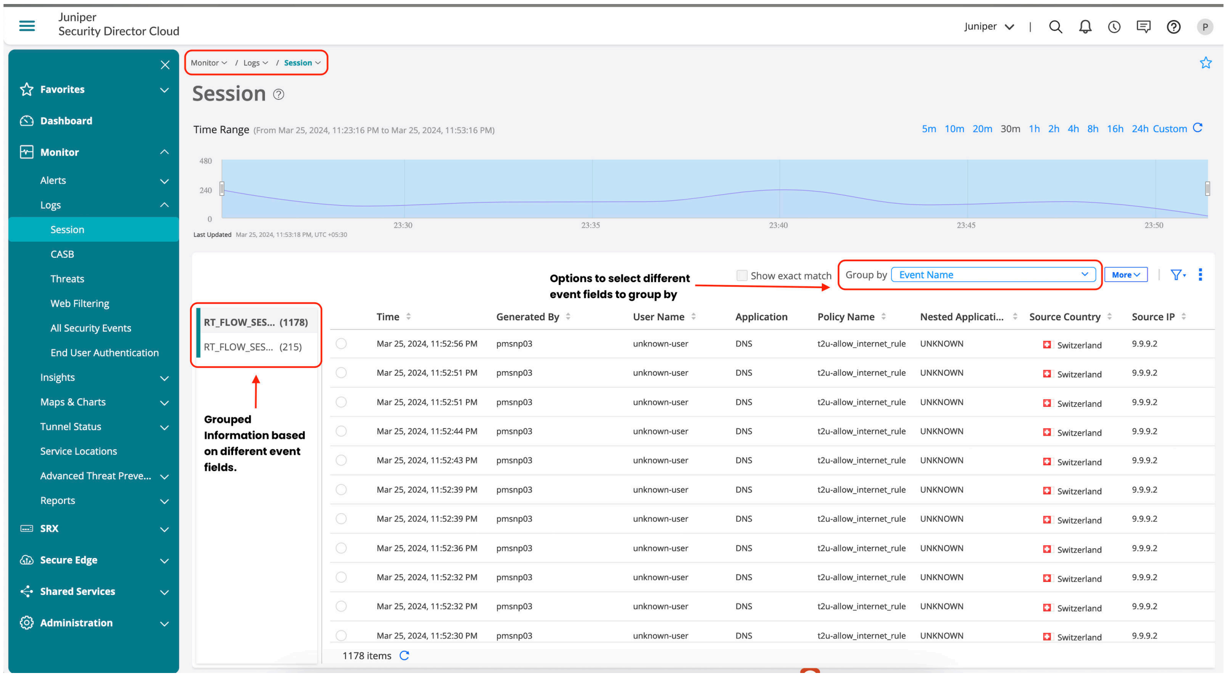
Filter Options	Description
	Use **Show advanced filter** to search through the logs. All the event fields are used to run through the search.
	Use **Group by** to sort through the logs based on predefined field. Which is shown in the next screenshots.

Figure 48: Juniper Security Director Cloud—Session Traffic Logs



Session

Time Range (From Mar 25, 2024, 11:23:16 PM to Mar 25, 2024, 11:53:16 PM)

Last Updated Mar 25, 2024, 11:53:18 PM, UTC +05:30

Options to select different event fields to group by

□ Show exact match Group by Event Name

RT_FLOW_SES... (1178)
RT_FLOW_SES... (215)

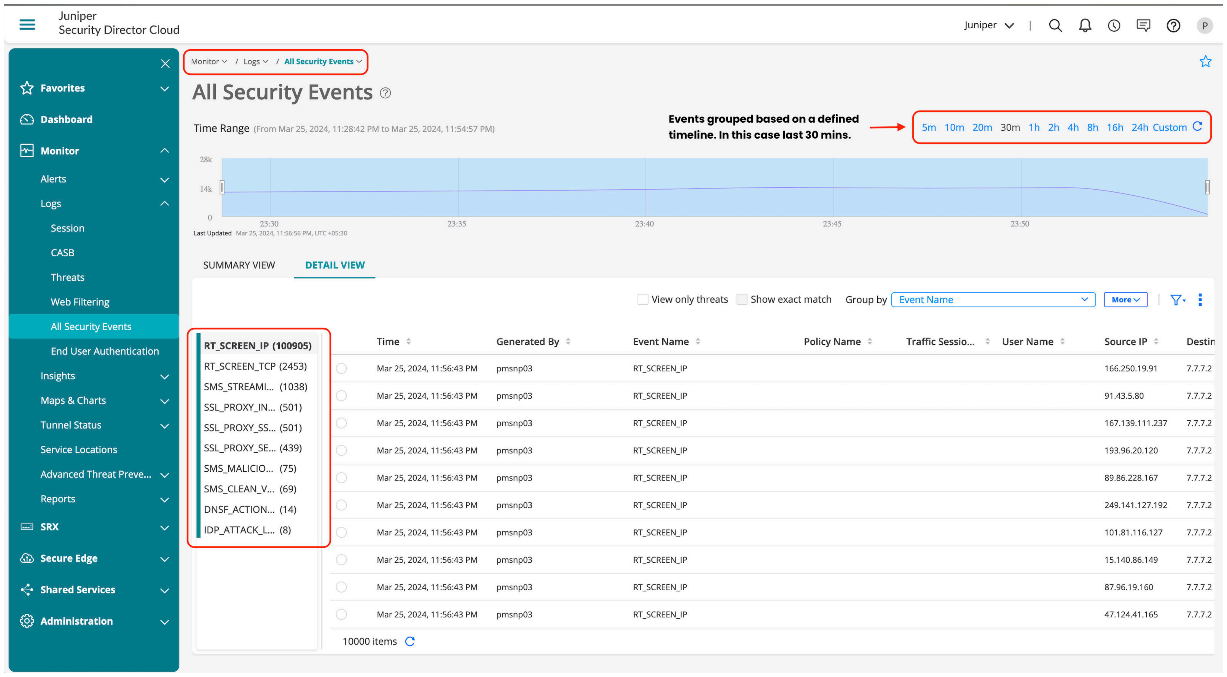
Grouped Information based on different event fields.

Time	Generated By	User Name	Application	Policy Name	Nested Applicati...	Source Country	Source IP
Mar 25, 2024, 11:52:56 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:51 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:51 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:44 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:43 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:39 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:39 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:36 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:32 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:32 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2
Mar 25, 2024, 11:52:30 PM	pmsnp03	unknown-user	DNS	t2u-allow_internet_rule	UNKNOWN	Switzerland	9.9.9.2

1178 items

All Security Events page provide details on all the security events received from the device.

Figure 49: Juniper Security Director Cloud—Grouped Events



All Security Events

Time Range (From Mar 25, 2024, 11:28:42 PM to Mar 25, 2024, 11:54:57 PM)

Events grouped based on a defined timeline. In this case last 30 mins.

Last Updated Mar 25, 2024, 11:56:56 PM, UTC +05:30

□ View only threats □ Show exact match Group by Event Name

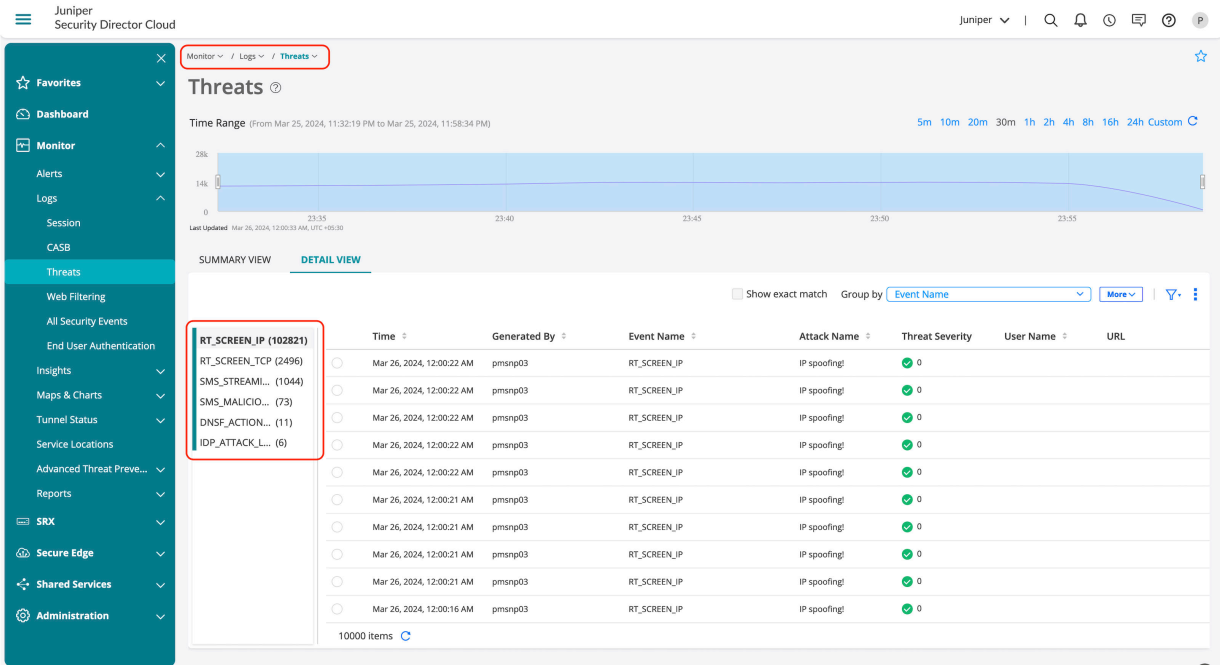
RT_SCREEN_IP (100905)
RT_SCREEN_TCP (2453)
SMS_STREAMI... (1038)
SSL_PROXY_IN... (501)
SSL_PROXY_SS... (501)
SSL_PROXY_SE... (439)
SMS_MALICIO... (75)
SMS_CLEAN_V... (69)
DNSF_ACTION... (14)
IDP_ATTACK_L... (8)

Time	Generated By	Event Name	Policy Name	Traffic Sessio...	User Name	Source IP	Destin
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				166.250.19.91	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				91.43.5.80	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				167.139.111.237	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				193.96.20.120	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				89.86.228.167	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				249.141.127.192	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				101.81.116.127	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				15.140.86.149	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				87.96.19.160	7.7.7.2
Mar 25, 2024, 11:56:43 PM	pmsnp03	RT_SCREEN_IP				47.124.41.165	7.7.7.2

10000 items

Threats page focuses only on the threats identified in the environment.

Figure 50: Juniper Security Director Cloud—Grouped Events



Threats

Time Range (From Mar 25, 2024, 11:32:19 PM to Mar 25, 2024, 11:58:34 PM)

Last Updated Mar 26, 2024, 12:00:33 AM, UTC +05:30

□ Show exact match Group by Event Name

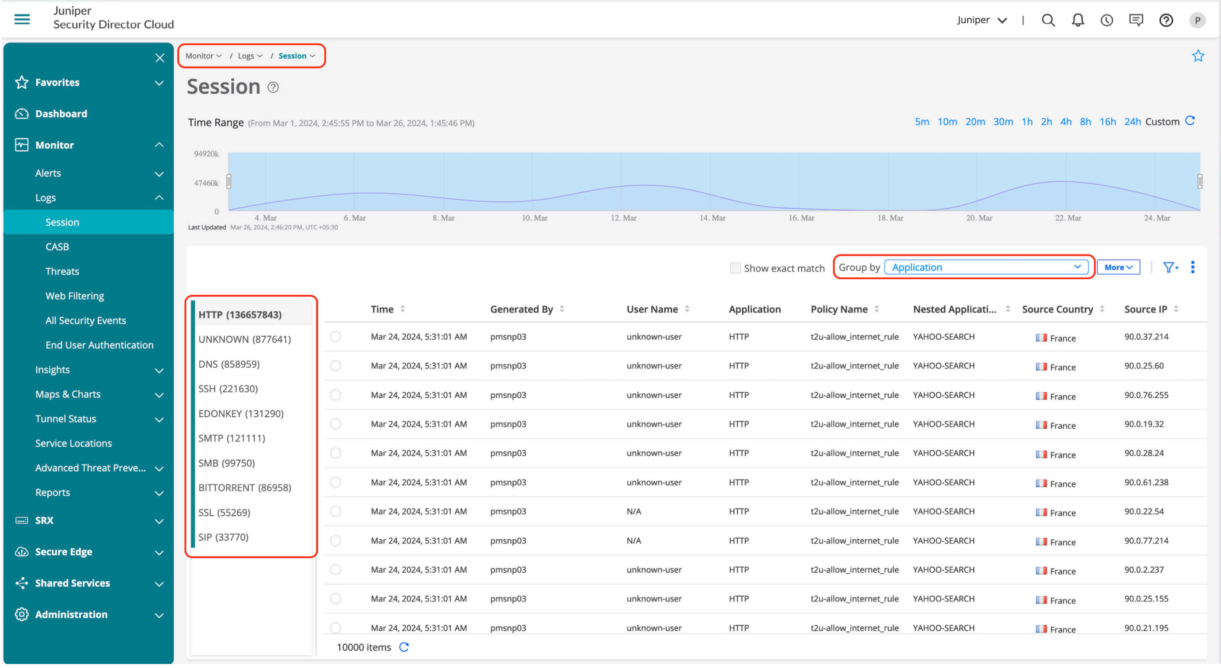
RT_SCREEN_IP (102821)
RT_SCREEN_TCP (2496)
SMS_STREAMI... (1044)
SMS_MALICIO... (73)
DNSF_ACTION... (11)
IDP_ATTACK_L... (6)

	Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
○	Mar 26, 2024, 12:00:22 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:22 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:22 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:22 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:22 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:21 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:21 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:21 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:21 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
○	Mar 26, 2024, 12:00:16 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		

Application Security Validation

Grouped applications provide a view on identified applications from the traffic where the firewall has processed.

Figure 51: Juniper Security Director Cloud—Grouped Application View



Session

Time Range (From Mar 1, 2024, 2:45:55 PM to Mar 26, 2024, 1:45:46 PM)

Last Updated Mar 26, 2024, 2:46:20 PM, UTC +05:30

□ Show exact match Group by Application

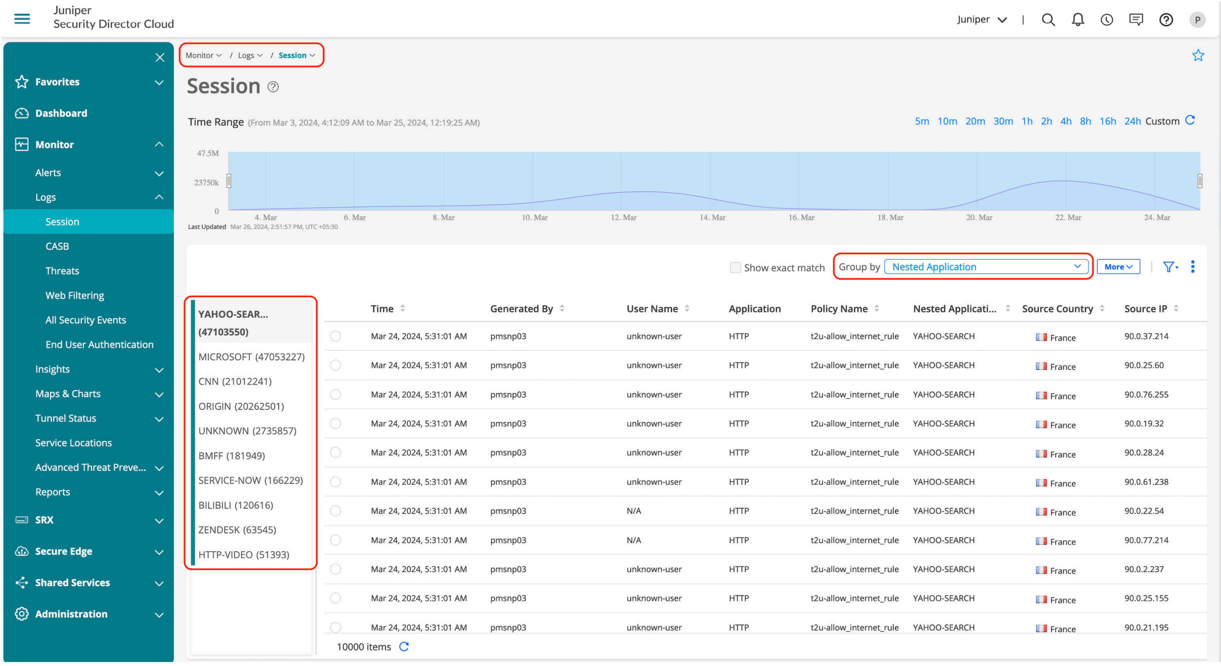
HTTP (136657843)
UNKNOWN (877641)
DNS (858959)
SSH (221630)
EDONKEY (131290)
SMTP (121111)
SMB (99750)
BITTORRENT (86958)
SSL (55269)
SIP (33770)

	Time	Generated By	User Name	Application	Policy Name	Nested Applicati...	Source Country	Source IP
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.37.214
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.25.60
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.76.255
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.19.32
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.28.24
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.61.238
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	N/A	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.22.54
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	N/A	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.77.214
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.2.237
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.25.155
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.21.195

10000 items

Grouping using Nested Applications provides information on the actual applications using the applications that is shown in Figure 51 on page 48.

Figure 52: Juniper Security Director Cloud—Grouped Nested Application View



Session

Time Range (From Mar 3, 2024, 4:12:09 AM to Mar 25, 2024, 12:19:25 AM)

Last Updated Mar 26, 2024, 2:51:57 PM, UTC +05:30

□ Show exact match Group by Nested Application

YAHOO-SEAR... (47103550)
MICROSOFT (47053227)
CNN (21012241)
ORIGIN (20262501)
UNKNOWN (2735857)
BMFF (181949)
SERVICE-NOW (166229)
BILIBILI (120616)
ZENDESK (63545)
HTTP-VIDEO (51393)

	Time	Generated By	User Name	Application	Policy Name	Nested Applicati...	Source Country	Source IP
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.37.214
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.25.60
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.76.255
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.19.32
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.28.24
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.61.238
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	N/A	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.22.54
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	N/A	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.77.214
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.2.237
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.25.155
○	Mar 24, 2024, 5:31:01 AM	pmsnp03	unknown-user	HTTP	t2u-allow_internet_rule	YAHOO-SEARCH	France	90.0.21.195

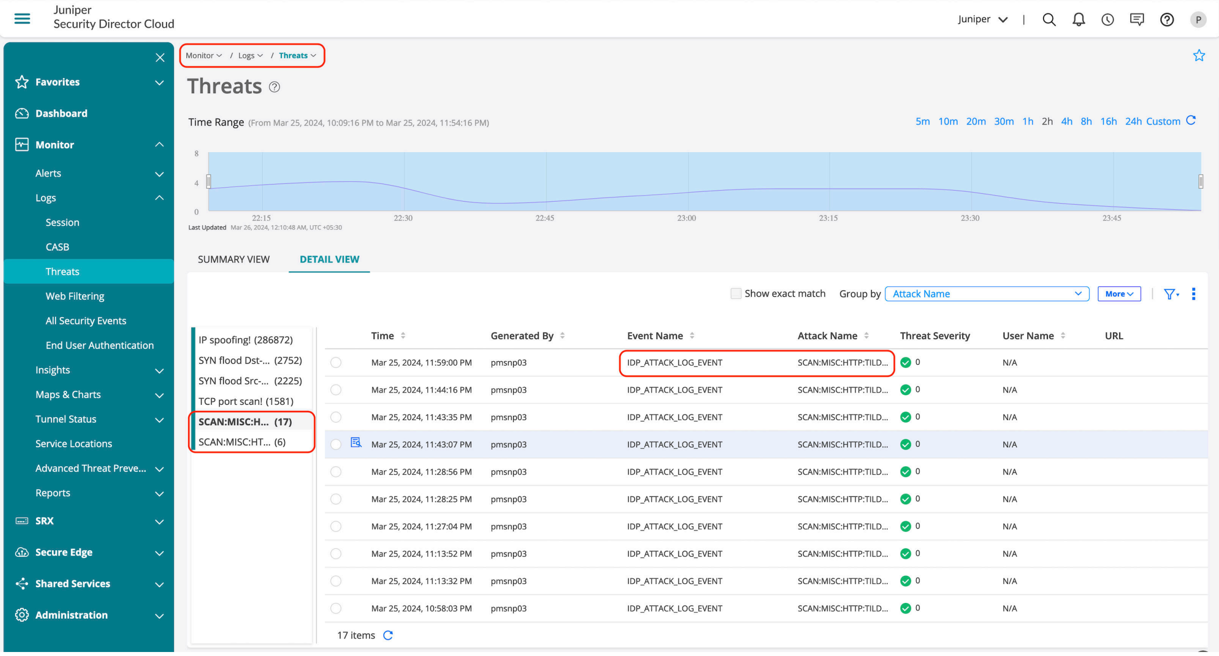
10000 items

IDP Feature Validation

Threats page provides information on the detected IDP attacks in the environment. You can also view the detailed information of the following:

- Source and destination zone
- Source and destination IP addresses
- IDP policy and rule that triggered the detection
- Detected attack and its severity
- Action taken on the detected attack

Figure 53: Juniper Security Director Cloud—IDP Attacks



Threats

Time Range (From Mar 25, 2024, 10:09:16 PM to Mar 25, 2024, 11:54:16 PM)

Last Updated Mar 26, 2024, 12:10:48 AM, UTC +05:30

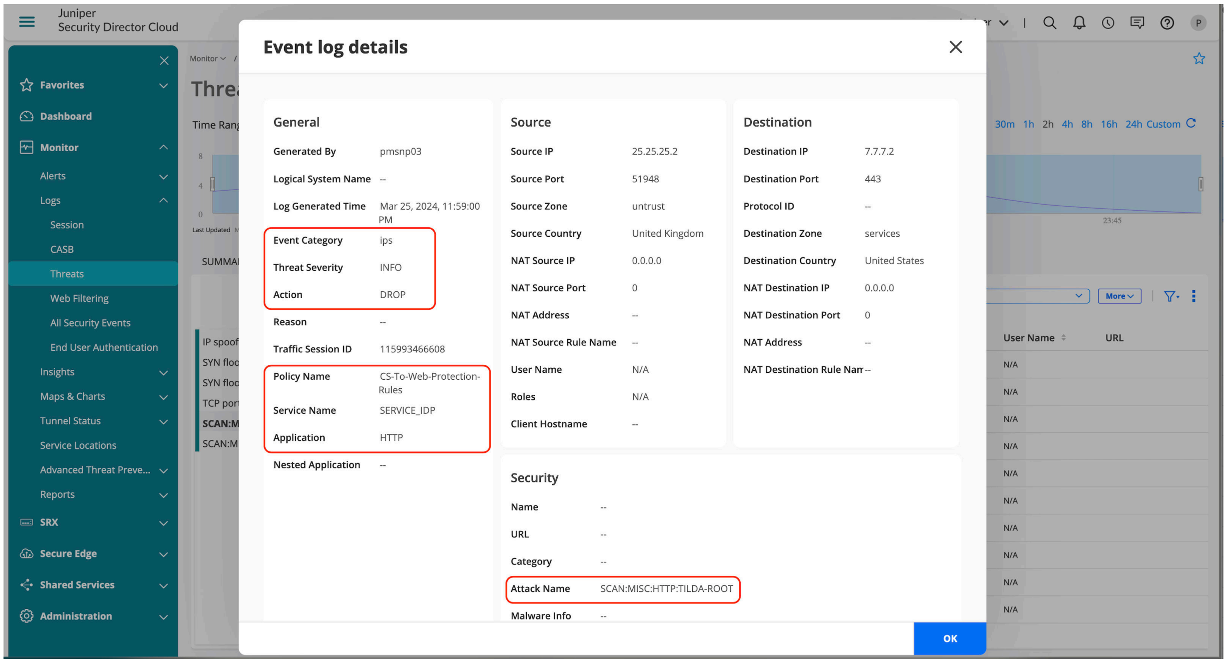
□ Show exact match   Group by Attack Name

Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
Mar 25, 2024, 11:59:00 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:44:16 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:43:35 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:43:07 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:28:56 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:28:25 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:27:04 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:13:52 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 11:13:32 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	
Mar 25, 2024, 10:58:03 PM	pmsnp03	IDP_ATTACK_LOG_EVENT	SCAN:MISC:HTTP:TILD...	✓ 0	N/A	

17 items

IDP Detailed Information

Figure 54: Juniper Security Director Cloud—IDP Attack Detail View



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 25, 2024, 11:59:00 PM
Event Category	ips
Threat Severity	INFO
Action	DROP
Reason	--
Traffic Session ID	115993466608
Policy Name	CS-To-Web-Protection-Rules
Service Name	SERVICE_IDP
Application	HTTP
Nested Application	--

Source

Source IP	25.25.25.2
Source Port	51948
Source Zone	untrust
Source Country	United Kingdom
NAT Source IP	0.0.0.0
NAT Source Port	0
NAT Address	--
NAT Source Rule Name	--
User Name	N/A
Roles	N/A
Client Hostname	--

Destination

Destination IP	7.7.7.2
Destination Port	443
Protocol ID	--
Destination Zone	services
Destination Country	United States
NAT Destination IP	0.0.0.0
NAT Destination Port	0
NAT Address	--
NAT Destination Rule Nam	--

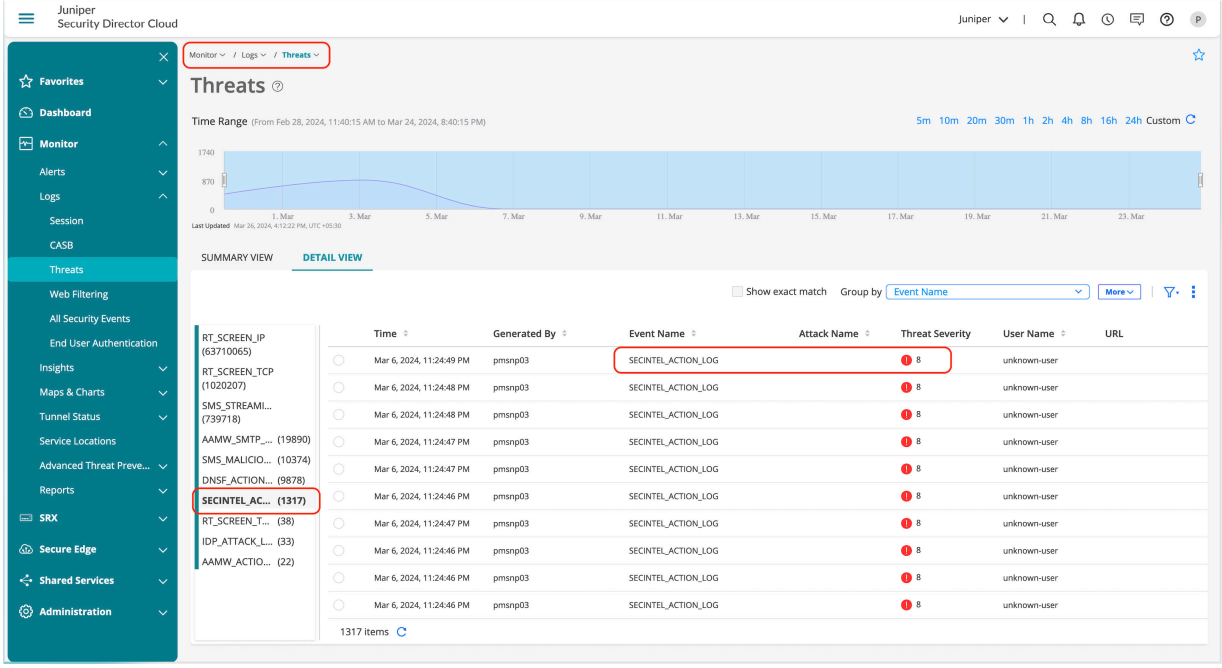
Security

Name	--
URL	--
Category	--
Attack Name	SCAN:MISC:HTTP:TILDA-ROOT
Malware Info	--

SecIntel Feature Validation

SecIntel feeds applied on the firewall policy generates logs when the traffic matches the configured risk level.

Figure 55: Juniper Security Director Cloud—SecIntel Threat Logs



Threats

Time Range (From Feb 28, 2024, 11:40:15 AM to Mar 24, 2024, 8:40:15 PM)

Last Updated Mar 26, 2024, 4:12:22 PM, UTC +05:30

☐ Show exact match Group by Event Name

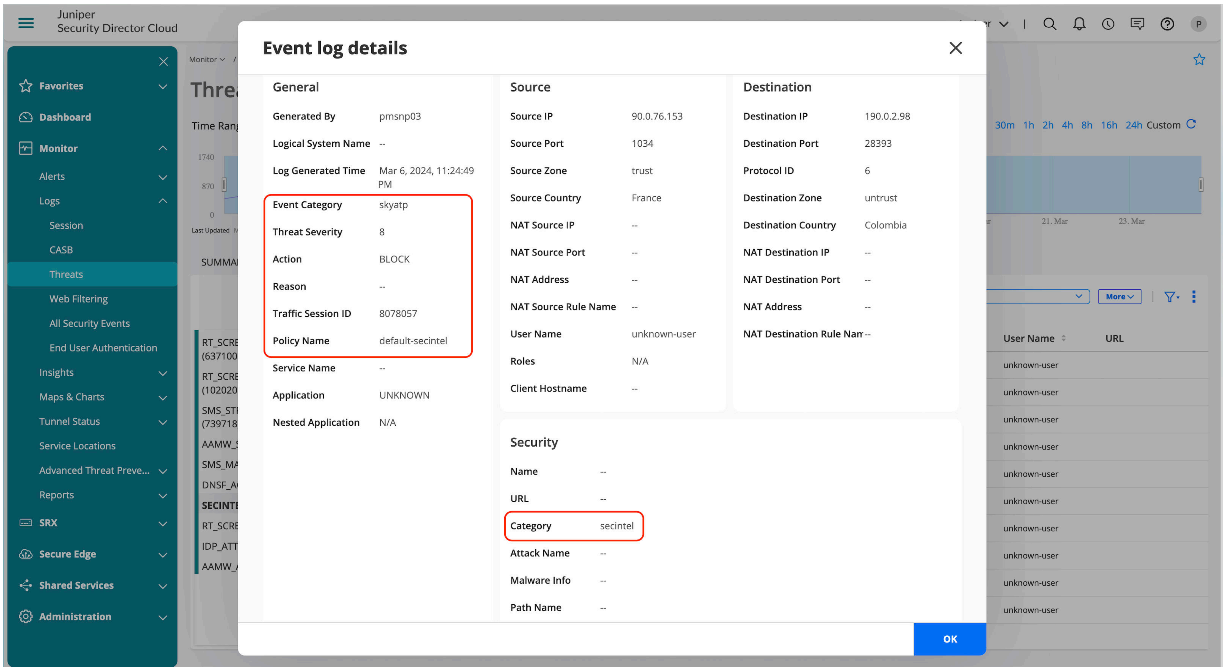
RT_SCREEN_IP (63710065)
RT_SCREEN_TCP (1020207)
SMS_STREAMI... (739718)
AAMW_SMTP_... (19890)
SMS_MALICIO... (10374)
DNSF_ACTION... (9878)
SECINTEL_AC... (1317)
RT_SCREEN_T... (38)
IDP_ATTACK_L... (33)
AAMW_ACTIO... (22)

	Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
○	Mar 6, 2024, 11:24:49 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:48 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:48 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:47 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:47 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:46 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:47 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:46 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:46 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	
○	Mar 6, 2024, 11:24:46 PM	pmsnp03	SECINTEL_ACTION_LOG		8	unknown-user	

1317 items

Detailed view shows information on the category and SecIntel policy that enforced the action including the source, destination, and corresponding zones.

Figure 56: Juniper Security Director Cloud—SecIntel Threat Log Detail View



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 6, 2024, 11:24:49 PM
Event Category	skyatp
Threat Severity	8
Action	BLOCK
Reason	--
Traffic Session ID	8078057
Policy Name	default-secintel
Service Name	--
Application	UNKNOWN
Nested Application	N/A

Source

Source IP	90.0.76.153
Source Port	1034
Source Zone	trust
Source Country	France
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	unknown-user
Roles	N/A
Client Hostname	--

Destination

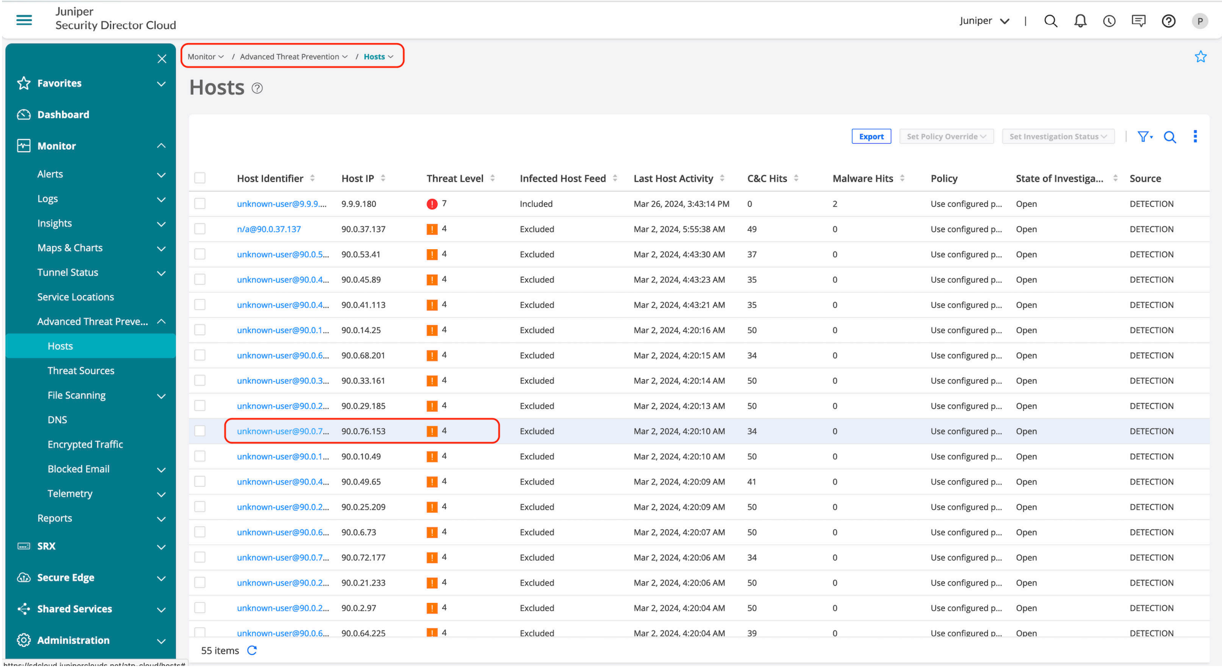
Destination IP	190.0.2.98
Destination Port	28393
Protocol ID	6
Destination Zone	untrust
Destination Country	Colombia
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Nar	--

Security

Name	--
URL	--
Category	secintel
Attack Name	--
Malware Info	--
Path Name	--

Advanced Threat Prevention dashboard also provides details on the client that initiated the traffic and the history of when the event occurred.

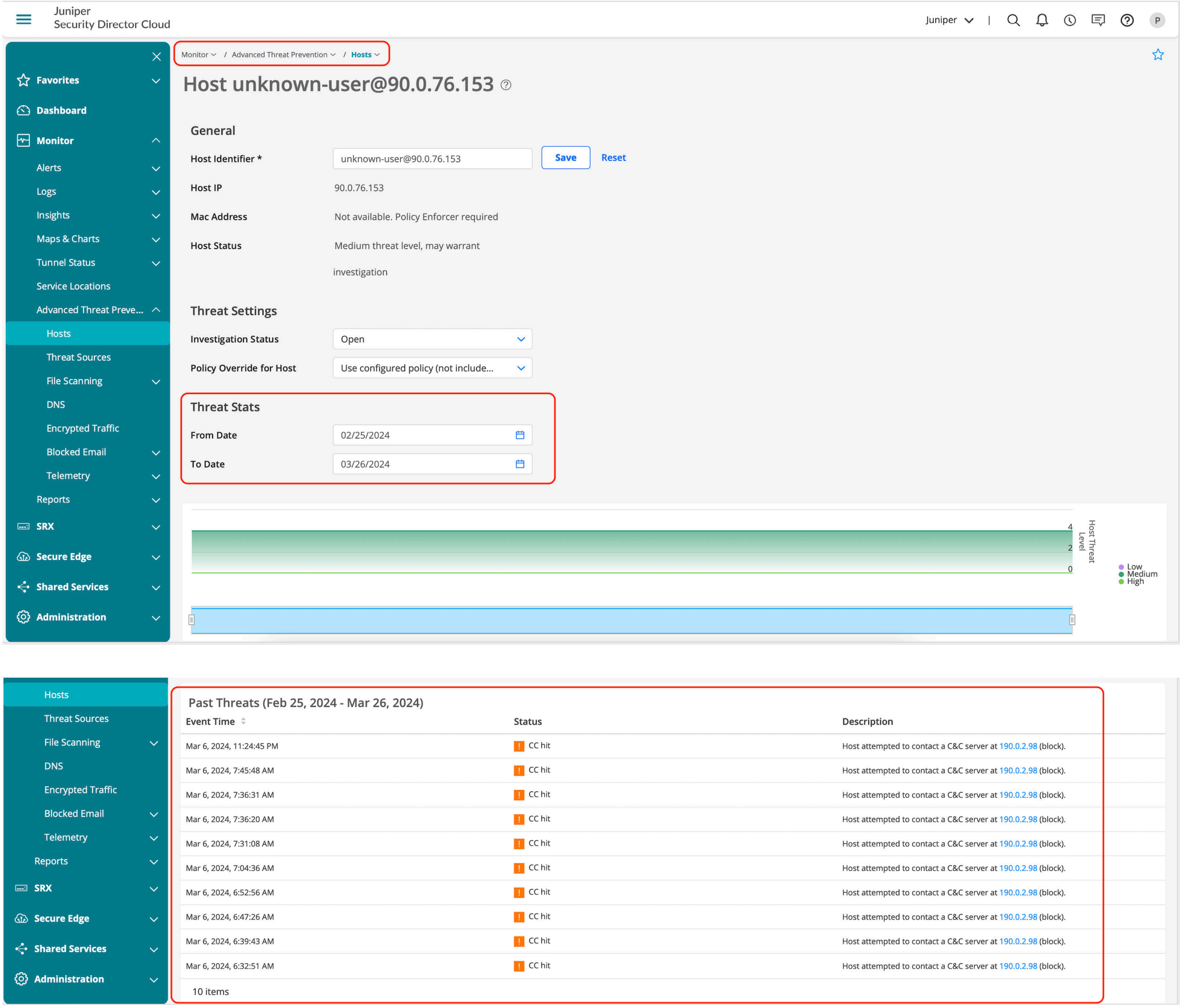
Figure 57: Juniper Security Director Cloud—SecIntel Identified Clients



Host Identifier	Host IP	Threat Level	Infected Host Feed	Last Host Activity	C&C Hits	Malware Hits	Policy	State of Investiga...	Source
unknown-user@9.9.9....	9.9.9.180	7	Included	Mar 26, 2024, 3:43:14 PM	0	2	Use configured p...	Open	DETECTION
n/a@90.0.37.137	90.0.37.137	4	Excluded	Mar 2, 2024, 5:55:38 AM	49	0	Use configured p...	Open	DETECTION
unknown-user@90.0.5...	90.0.53.41	4	Excluded	Mar 2, 2024, 4:43:30 AM	37	0	Use configured p...	Open	DETECTION
unknown-user@90.0.4...	90.0.45.89	4	Excluded	Mar 2, 2024, 4:43:23 AM	35	0	Use configured p...	Open	DETECTION
unknown-user@90.0.4...	90.0.41.113	4	Excluded	Mar 2, 2024, 4:43:21 AM	35	0	Use configured p...	Open	DETECTION
unknown-user@90.0.1...	90.0.14.25	4	Excluded	Mar 2, 2024, 4:20:16 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.6...	90.0.68.201	4	Excluded	Mar 2, 2024, 4:20:15 AM	34	0	Use configured p...	Open	DETECTION
unknown-user@90.0.3...	90.0.33.161	4	Excluded	Mar 2, 2024, 4:20:14 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.2...	90.0.29.185	4	Excluded	Mar 2, 2024, 4:20:13 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.7...	90.0.76.153	4	Excluded	Mar 2, 2024, 4:20:10 AM	34	0	Use configured p...	Open	DETECTION
unknown-user@90.0.1...	90.0.10.49	4	Excluded	Mar 2, 2024, 4:20:10 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.4...	90.0.49.65	4	Excluded	Mar 2, 2024, 4:20:09 AM	41	0	Use configured p...	Open	DETECTION
unknown-user@90.0.2...	90.0.25.209	4	Excluded	Mar 2, 2024, 4:20:09 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.6...	90.0.6.73	4	Excluded	Mar 2, 2024, 4:20:07 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.7...	90.0.72.177	4	Excluded	Mar 2, 2024, 4:20:06 AM	34	0	Use configured p...	Open	DETECTION
unknown-user@90.0.2...	90.0.21.233	4	Excluded	Mar 2, 2024, 4:20:06 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.2...	90.0.2.97	4	Excluded	Mar 2, 2024, 4:20:04 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.6...	90.0.64.225	4	Excluded	Mar 2, 2024, 4:20:04 AM	39	0	Use configured p...	Open	DETECTION

55 items

Figure 58: Juniper Security Director Cloud—SecIntel Client Details



Host unknown-user@90.0.76.153

General

Host Identifier *: unknown-user@90.0.76.153

Host IP: 90.0.76.153

Mac Address: Not available. Policy Enforcer required

Host Status: Medium threat level, may warrant investigation

Threat Settings

Investigation Status: Open

Policy Override for Host: Use configured policy (not include...

Threat Stats

From Date: 02/25/2024

To Date: 03/26/2024

Past Threats (Feb 25, 2024 - Mar 26, 2024)

Event Time	Status	Description
Mar 6, 2024, 11:24:45 PM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 7:45:48 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 7:36:31 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 7:36:20 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 7:31:08 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 7:04:36 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 6:52:56 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 6:47:26 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 6:39:43 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).
Mar 6, 2024, 6:32:51 AM	! CC hit	Host attempted to contact a C&C server at 190.0.2.98 (block).

10 items

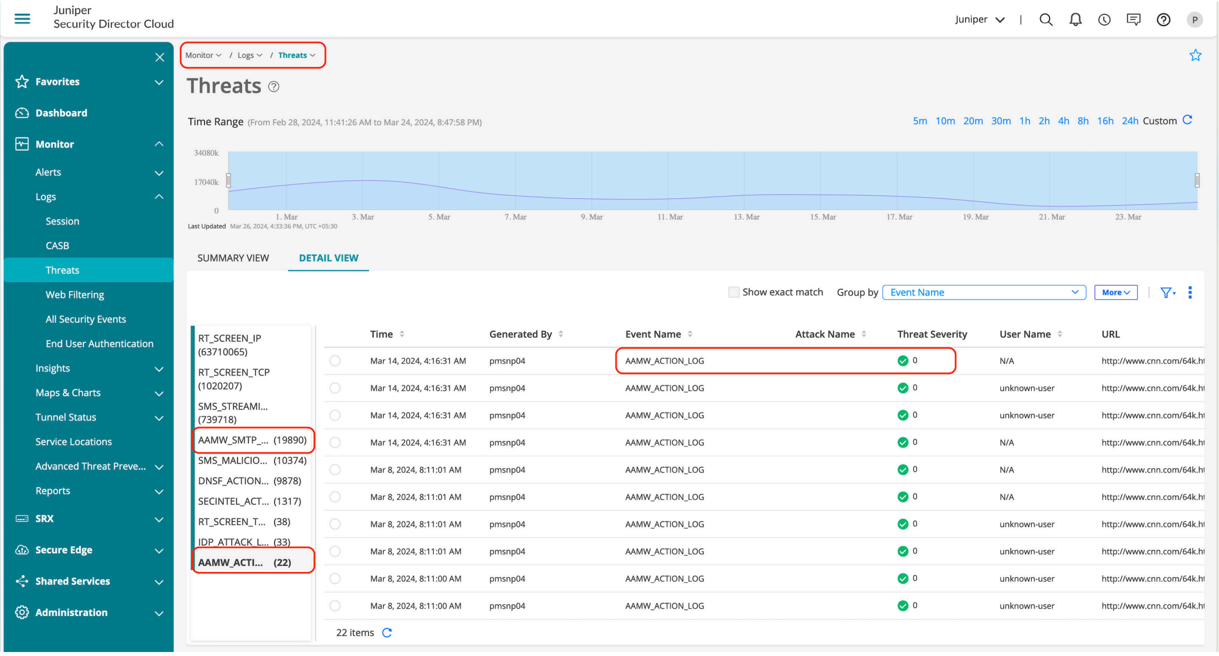
Advanced Anti-Malware Feature Validation

Configured AAMW policy might result in several logs depending on what protocol is identified. Few key logs provide information on the action enforced by AAMW.

Table 4: Advanced Anti-Malware Logs

Log Information	Description
AAMW_ACTION_LOG	Action taken based on the verdict delivered based on the sandboxing result by Juniper ATP Cloud and defined risk profile on the SRX Series Firewall.
AAMW_HOST_INFECTED_EVENT_LOG	If the verdict found is malicious, the host infected event log is generated.
AAMW_MALWARE_EVENT_LOG	If the verdict as a result of the sandboxing is malicious, the malware event log is generated.

Figure 59: Juniper Security Director Cloud—AAMW Logs



Threats

Time Range (From Feb 28, 2024, 11:41:26 AM to Mar 24, 2024, 8:47:58 PM)

Last Updated Mar 26, 2024, 4:33:36 PM, UTC +05:30

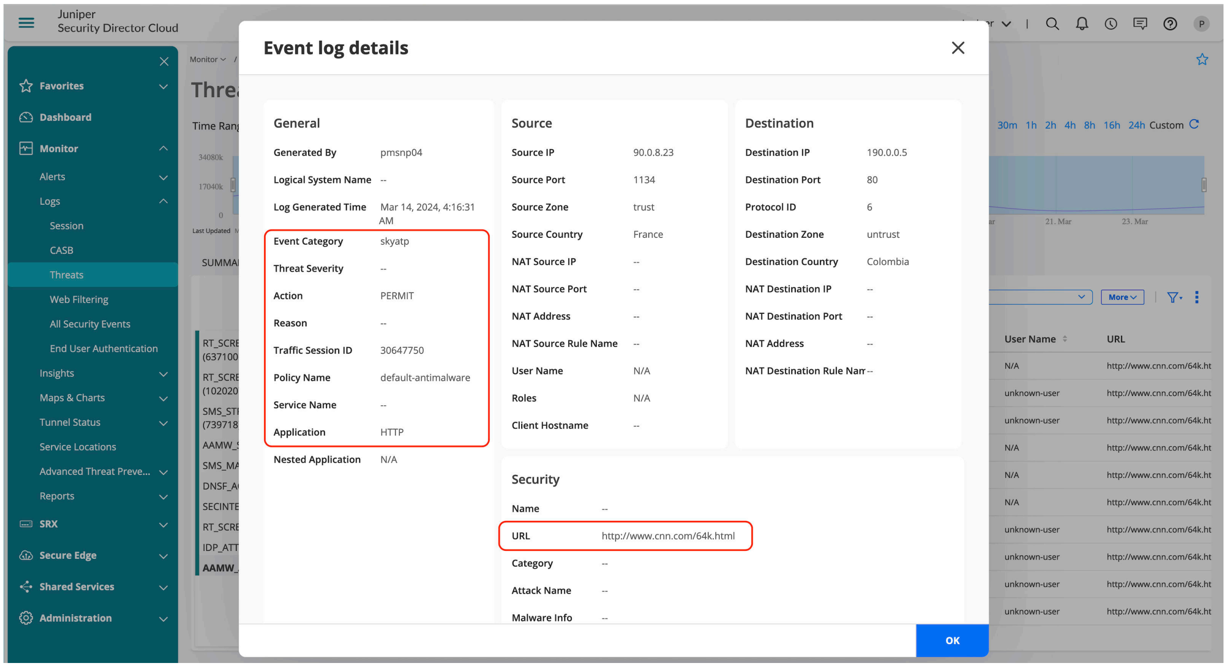
□ Show exact match Group by Event Name

RT_SCREEN_IP	(63710065)
RT_SCREEN_TCP	(1020207)
SMS_STREAMI...	(739718)
AAMW_SMTP_...	(19890)
SMS_MALICIO...	(10374)
DNSF_ACTION...	(9878)
SECINTEL_ACT...	(1317)
RT_SCREEN_T...	(38)
IDP_ATTACK_L...	(33)
AAMW_ACTI...	**(22)**

	Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
○	Mar 14, 2024, 4:16:31 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	N/A	http://www.cnn.com/64k.ht
○	Mar 14, 2024, 4:16:31 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	unknown-user	http://www.cnn.com/64k.ht
○	Mar 14, 2024, 4:16:31 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	unknown-user	http://www.cnn.com/64k.ht
○	Mar 14, 2024, 4:16:31 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	N/A	http://www.cnn.com/64k.ht
○	Mar 8, 2024, 8:11:01 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	N/A	http://www.cnn.com/64k.ht
○	Mar 8, 2024, 8:11:01 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	N/A	http://www.cnn.com/64k.ht
○	Mar 8, 2024, 8:11:01 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	unknown-user	http://www.cnn.com/64k.ht
○	Mar 8, 2024, 8:11:01 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	unknown-user	http://www.cnn.com/64k.ht
○	Mar 8, 2024, 8:11:00 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	unknown-user	http://www.cnn.com/64k.ht
○	Mar 8, 2024, 8:11:00 AM	pmsnp04	AAMW_ACTION_LOG		✓ 0	unknown-user	http://www.cnn.com/64k.ht

22 items

Figure 60: Juniper Security Director Cloud—AAMW Log Detail



Event log details

General

Generated By	pmsnp04
Logical System Name	--
Log Generated Time	Mar 14, 2024, 4:16:31 AM
Event Category	skyatp
Threat Severity	--
Action	PERMIT
Reason	--
Traffic Session ID	30647750
Policy Name	default-antimalware
Service Name	--
Application	HTTP
Nested Application	N/A

Source

Source IP	90.0.8.23
Source Port	1134
Source Zone	trust
Source Country	France
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	N/A
Roles	N/A
Client Hostname	--

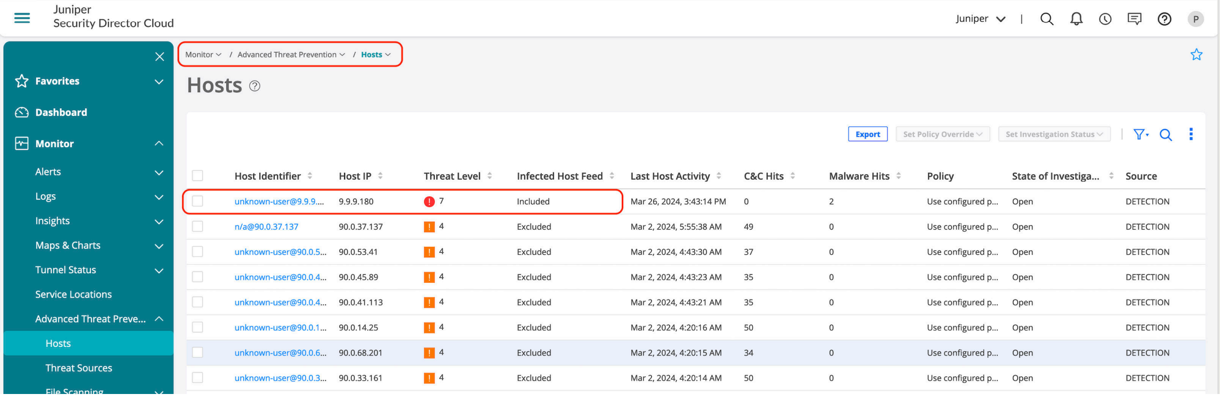
Destination

Destination IP	190.0.0.5
Destination Port	80
Protocol ID	6
Destination Zone	untrust
Destination Country	Colombia
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Nam	--

Security

Name	--
URL	http://www.cnn.com/64k.html
Category	--
Attack Name	--
Malware Info	--

Figure 61: Juniper Security Director Cloud—ATP Infected Host

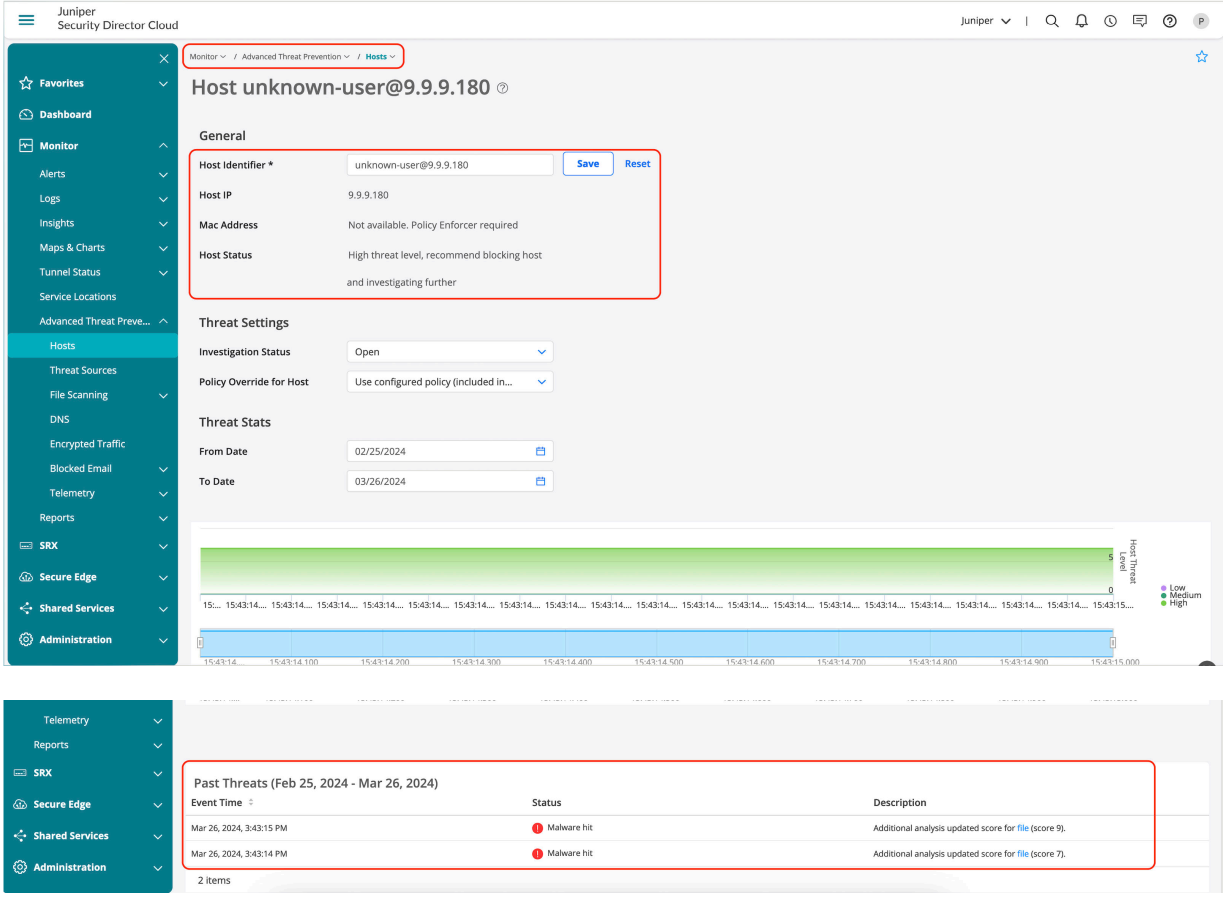


Monitor / Advanced Threat Prevention / Hosts

Hosts

Host Identifier	Host IP	Threat Level	Infected Host Feed	Last Host Activity	C&C Hits	Malware Hits	Policy	State of Investiga...	Source
unknown-user@9.9.9....	9.9.9.180	7	Included	Mar 26, 2024, 3:43:14 PM	0	2	Use configured p...	Open	DETECTION
n/a@90.0.37.137	90.0.37.137	4	Excluded	Mar 2, 2024, 5:55:38 AM	49	0	Use configured p...	Open	DETECTION
unknown-user@90.0.5...	90.0.53.41	4	Excluded	Mar 2, 2024, 4:43:30 AM	37	0	Use configured p...	Open	DETECTION
unknown-user@90.0.4...	90.0.45.89	4	Excluded	Mar 2, 2024, 4:43:23 AM	35	0	Use configured p...	Open	DETECTION
unknown-user@90.0.4...	90.0.41.113	4	Excluded	Mar 2, 2024, 4:43:21 AM	35	0	Use configured p...	Open	DETECTION
unknown-user@90.0.1...	90.0.14.25	4	Excluded	Mar 2, 2024, 4:20:16 AM	50	0	Use configured p...	Open	DETECTION
unknown-user@90.0.6...	90.0.68.201	4	Excluded	Mar 2, 2024, 4:20:15 AM	34	0	Use configured p...	Open	DETECTION
unknown-user@90.0.3...	90.0.33.161	4	Excluded	Mar 2, 2024, 4:20:14 AM	50	0	Use configured p...	Open	DETECTION

Figure 62: Juniper Security Director Cloud—ATP Infected Host Detailed View



Host unknown-user@9.9.9.180

General

Host Identifier * unknown-user@9.9.9.180

Host IP 9.9.9.180

Mac Address Not available. Policy Enforcer required

Host Status High threat level, recommend blocking host and investigating further

Threat Settings

Investigation Status Open

Policy Override for Host Use configured policy (included in...

Threat Stats

From Date 02/25/2024

To Date 03/26/2024

Past Threats (Feb 25, 2024 - Mar 26, 2024)

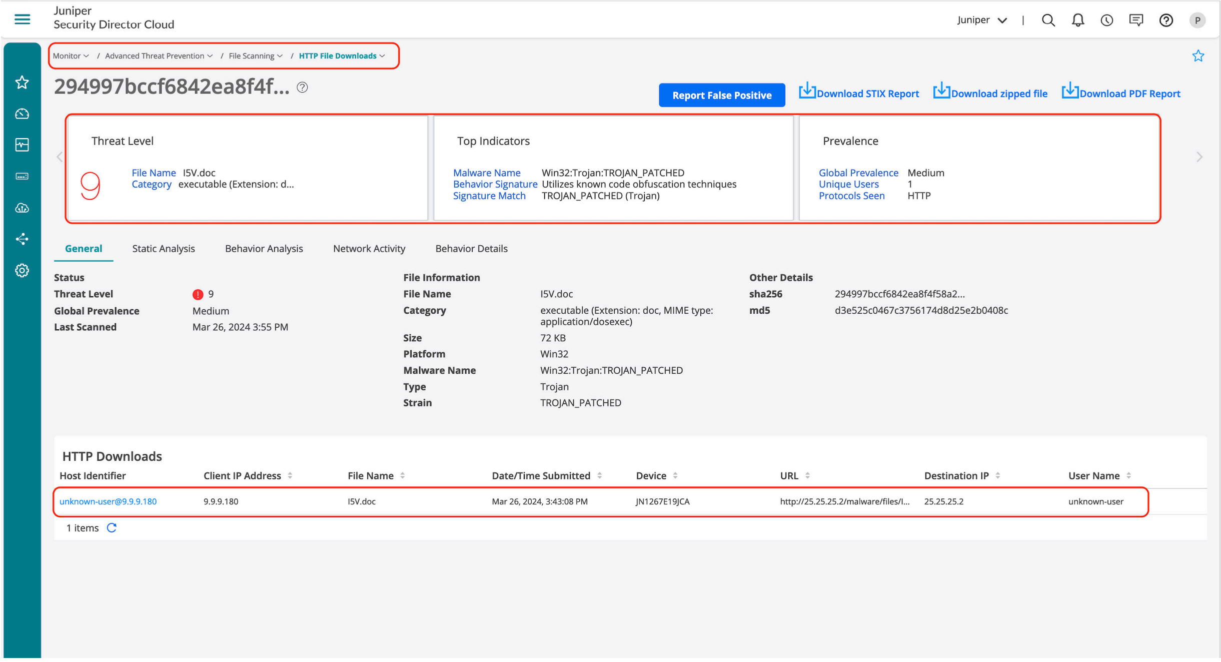
Event Time	Status	Description
Mar 26, 2024, 3:43:15 PM	● Malware hit	Additional analysis updated score for file (score 9).
Mar 26, 2024, 3:43:14 PM	● Malware hit	Additional analysis updated score for file (score 7).

2 items

ATP Infected host view provides the following details:

- Indicators of compromise (IOC).
- Static analysis of the identified malicious file.
- Behavior analysis to identify key behaviors based on the assigned threat level to derive how malicious is the identified file.
- Network activity provides details on the malware activity identified during sandboxing.
- Behavior details outline the behavioural steps identified during sandboxing.

Figure 63: Juniper Security Director Cloud—ATP Malware IOC



Juniper
Security Director Cloud

294997bccf6842ea8f4f...

Threat Level

9

File Name I5V.doc
Category executable (Extension: d...

Top Indicators

Malware Name Win32:Trojan:TROJAN_PATCHED
Behavior Signature Utilizes known code obfuscation techniques
Signature Match TROJAN_PATCHED (Trojan)

Prevalence

Global Prevalence Medium
Unique Users 1
Protocols Seen HTTP

Status	
Threat Level	9
Global Prevalence	Medium
Last Scanned	Mar 26, 2024 3:55 PM

File Information	
File Name	I5V.doc
Category	executable (Extension: doc, MIME type: application/dosexec)
Size	72 KB
Platform	Win32
Malware Name	Win32:Trojan:TROJAN_PATCHED
Type	Trojan
Strain	TROJAN_PATCHED

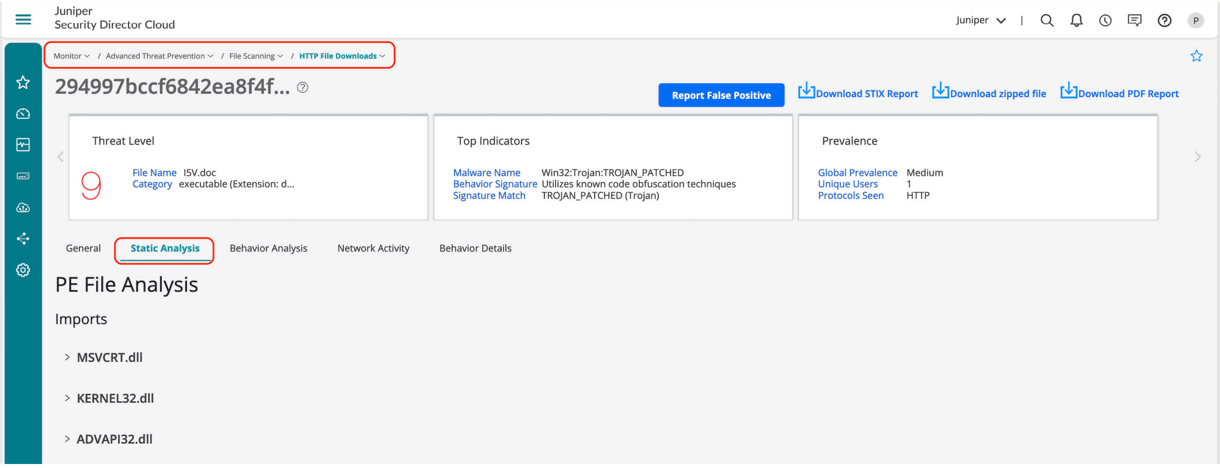
Other Details	
sha256	294997bccf6842ea8f4f58a2...
md5	d3e525c0467c3756174d8d25e2b0408c

HTTP Downloads

Host Identifier	Client IP Address	File Name	Date/Time Submitted	Device	URL	Destination IP	User Name
unknown-user@9.9.9.180	9.9.9.180	I5V.doc	Mar 26, 2024, 3:43:08 PM	JN1267E19JCA	http://25.25.25.2/malware/files/I...	25.25.25.2	unknown-user

1 items

Figure 64: Juniper Security Director Cloud—ATP Malware Static Analysis



Juniper
Security Director Cloud

294997bccf6842ea8f4f...

Threat Level

9

File Name I5V.doc
Category executable (Extension: d...

Top Indicators

Malware Name Win32:Trojan:TROJAN_PATCHED
Behavior Signature Utilizes known code obfuscation techniques
Signature Match TROJAN_PATCHED (Trojan)

Prevalence

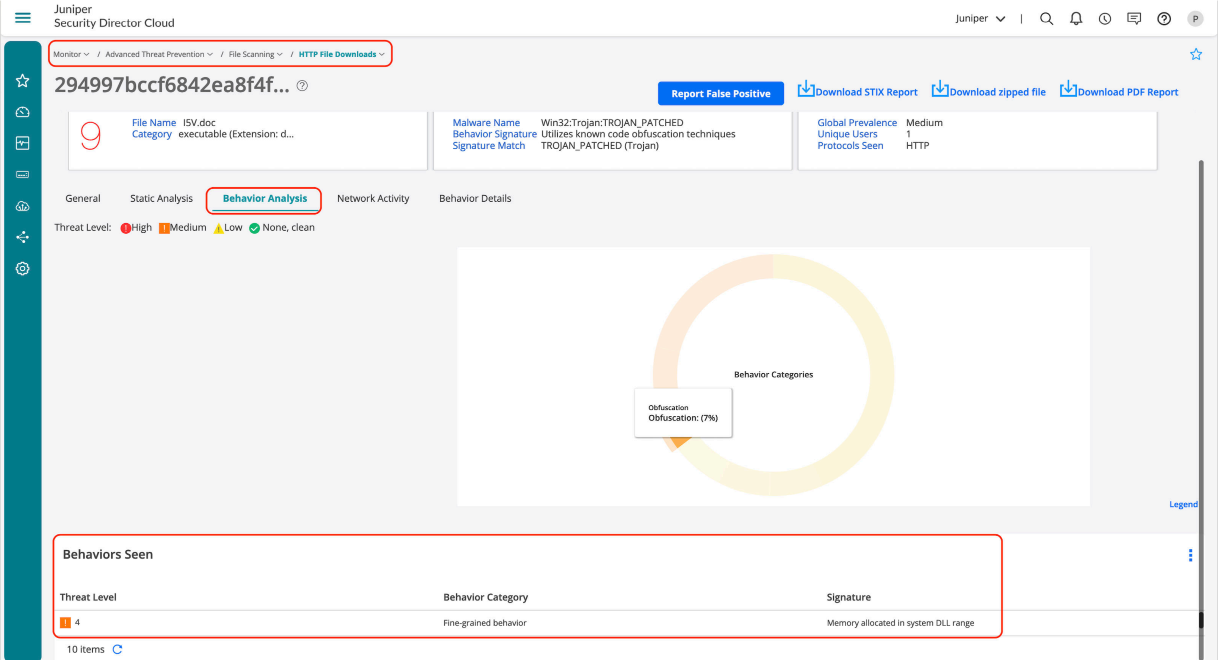
Global Prevalence Medium
Unique Users 1
Protocols Seen HTTP

PE File Analysis

Imports

- MSVCRT.dll
- KERNEL32.dll
- ADVAPI32.dll

Figure 65: Juniper Security Director Cloud—ATP Malware Behavior Analysis



294997bccf6842ea8f4f...

9

File Name I5V.doc
Category executable (Extension: d...

Malware Name Win32:Trojan:TROJAN_PATCHED
Behavior Signature Utilizes known code obfuscation techniques
Signature Match TROJAN_PATCHED (Trojan)

Global Prevalence Medium
Unique Users 1
Protocols Seen HTTP

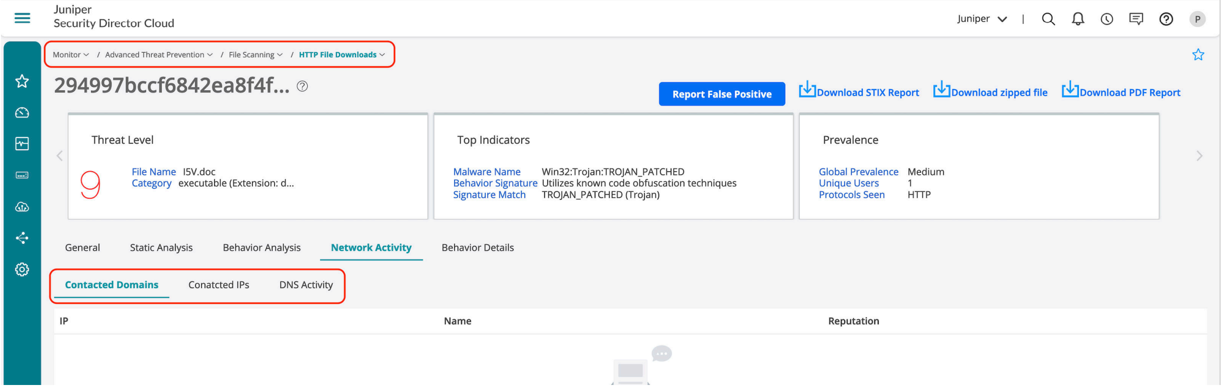
Threat Level: ❗High 🟧Medium ⚠Low ✓None, clean

Behaviors Seen

Threat Level	Behavior Category	Signature
🟧 4	Fine-grained behavior	Memory allocated in system DLL range

10 items

Figure 66: Juniper Security Director Cloud—ATP Malware Network Activity



294997bccf6842ea8f4f...

Threat Level

9

File Name I5V.doc
Category executable (Extension: d...

Top Indicators

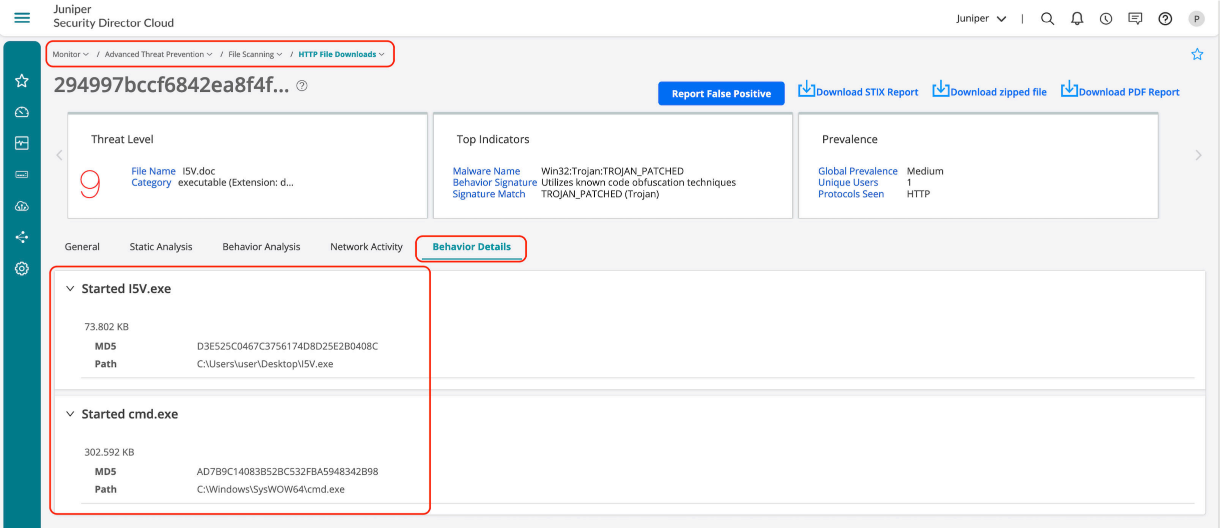
Malware Name Win32:Trojan:TROJAN_PATCHED
Behavior Signature Utilizes known code obfuscation techniques
Signature Match TROJAN_PATCHED (Trojan)

Prevalence

Global Prevalence Medium
Unique Users 1
Protocols Seen HTTP

IP	Name	Reputation

Figure 67: Juniper Security Director Cloud—ATP Malware Behavioral Details



294997bccf6842ea8f4f...

Threat Level

9

File Name I5V.doc
Category executable (Extension: d...

Top Indicators

Malware Name Win32:Trojan:TROJAN_PATCHED
Behavior Signature Utilizes known code obfuscation techniques
Signature Match TROJAN_PATCHED (Trojan)

Prevalence

Global Prevalence Medium
Unique Users 1
Protocols Seen HTTP

Started I5V.exe

73.802 KB
MD5 D3E525C0467C3756174D8D25E2B0408C
Path C:\Users\user\Desktop\I5V.exe

Started cmd.exe

302.592 KB
MD5 AD7B9C14083B52BC532FBA5948342B98
Path C:\Windows\SysWOW64\cmd.exe

DNS Security Feature Validation

DNS security logs are generated based on each DNS security features such as DGA and DNS tunneling, if any identified DNS traffic is found to be malicious appropriate logs are generated.

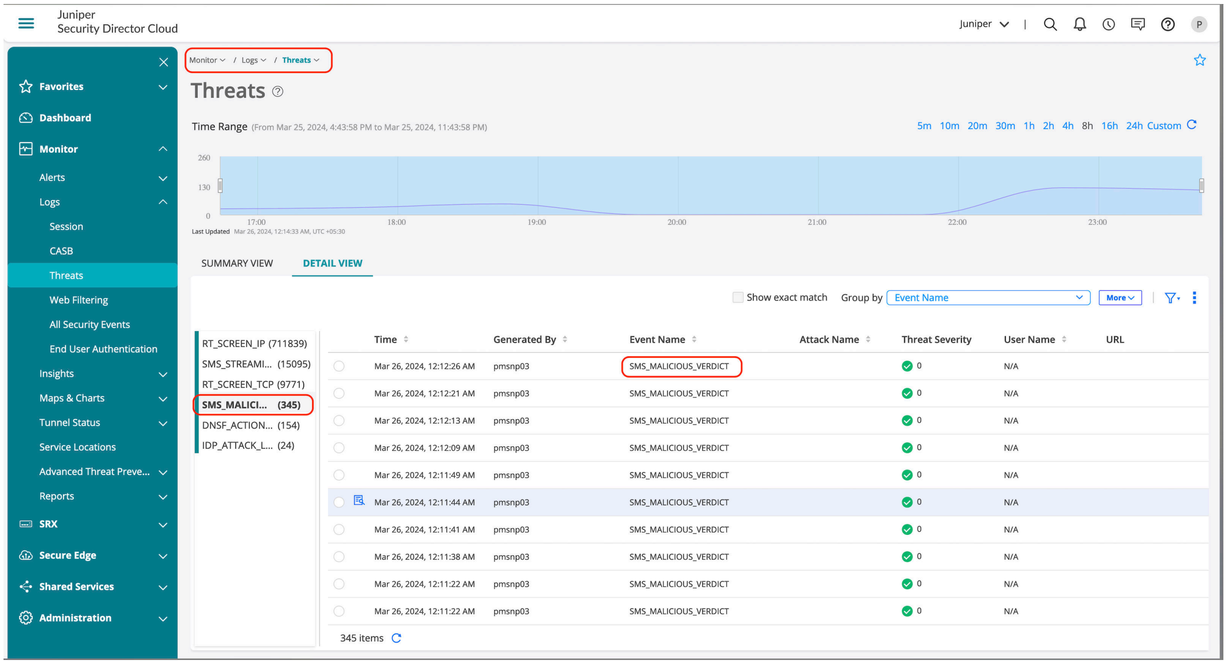
Table 5: DNS Security Logs

Log Information	Description
SMS_STREAMING	Log is generated for DNS REQ when 'notification log' is configured under any detections (dga, tunneling, and all).
SMS_CLEAN_VERDICT	Log is generated when the cloud verdict is 'clean' and 'notification log-detection' is configured under any detections (dga and all).
SMS_MALICIOUS_VERDICT	Log is generated when the cloud verdict is malicious or tunneling is detected and 'notification log-detection' is configured under any detections (dga, tunneling and all).
SMS_FALLBACK_EVENT	Log is generated when the cloud verdict is not received in verdict-timeout interval. Log is generated only when 'fallback-options notification log' is configured under any detection (dga, tunneling and all).

Apart from generated logs, you can also view the offense details from Advanced Threat Prevention section, which provides information on the following:

- Client which generated the offense.
- Offense details if its DGA or DNS Tunneling.
- Information on the IOC and exfiltration attempts.

Figure 68: Juniper Security Director Cloud—DNS Logs



Time Range (From Mar 25, 2024, 4:43:58 PM to Mar 25, 2024, 11:43:58 PM)

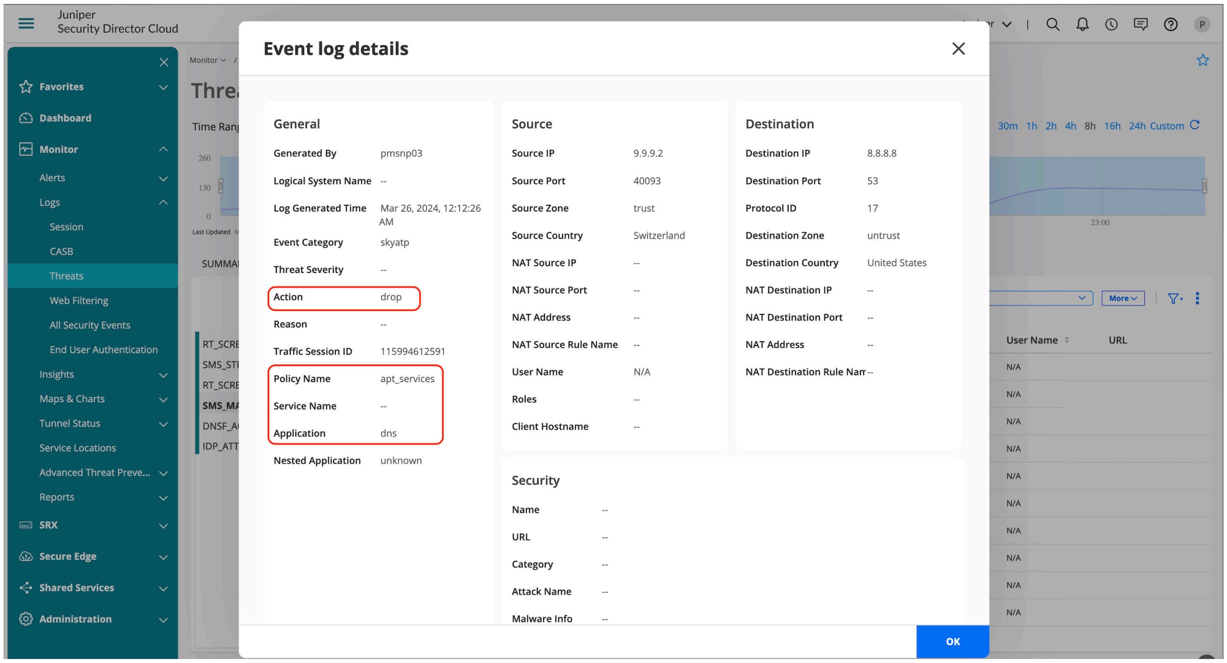
Last Updated Mar 26, 2024, 12:14:33 AM, UTC +05:30

□ Show exact match Group by Event Name

RT_SCREEN_IP (711839)
SMS_STREAMI... (15095)
RT_SCREEN_TCP (9771)
SMS_MALICI... (345)
DNSF_ACTION... (154)
IDP_ATTACK_L... (24)

	Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
○	Mar 26, 2024, 12:12:26 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:12:21 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:12:13 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:12:09 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:11:49 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:11:44 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:11:41 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:11:38 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:11:22 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	
○	Mar 26, 2024, 12:11:22 AM	pmsnp03	SMS_MALICIOUS_VERDICT		✓ 0	N/A	

Figure 69: Juniper Security Director Cloud—DNS Log Detail



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 26, 2024, 12:12:26 AM
Event Category	skyatp
Threat Severity	--
Action	drop
Reason	--
Traffic Session ID	115994612591
Policy Name	apt_services
Service Name	--
Application	dns
Nested Application	unknown

Source

Source IP	9.9.9.2
Source Port	40093
Source Zone	trust
Source Country	Switzerland
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	N/A
Roles	--
Client Hostname	--

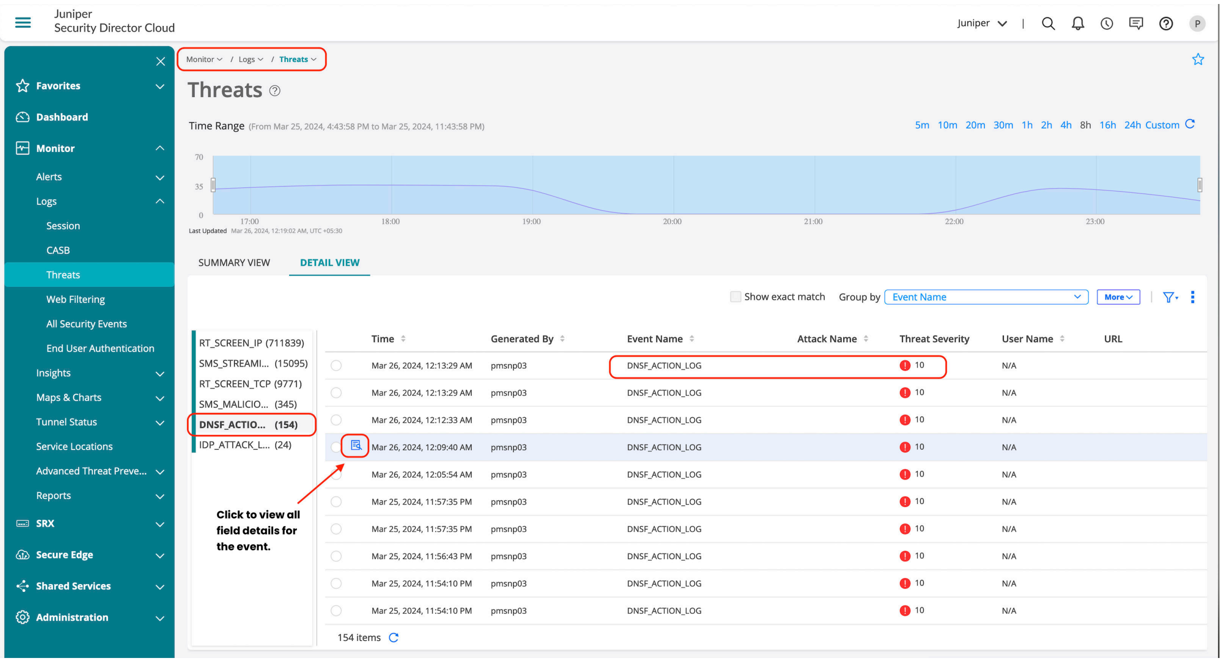
Destination

Destination IP	8.8.8.8
Destination Port	53
Protocol ID	17
Destination Zone	untrust
Destination Country	United States
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Nam	--

Security

Name	--
URL	--
Category	--
Attack Name	--
Malware Info	--

Figure 70: Juniper Security Director Cloud—SecIntel Based DNS Log



Threats

Time Range (From Mar 25, 2024, 4:43:58 PM to Mar 25, 2024, 11:43:58 PM)

Last Updated Mar 26, 2024, 12:19:02 AM, UTC +05:30

□ Show exact match Group by Event Name

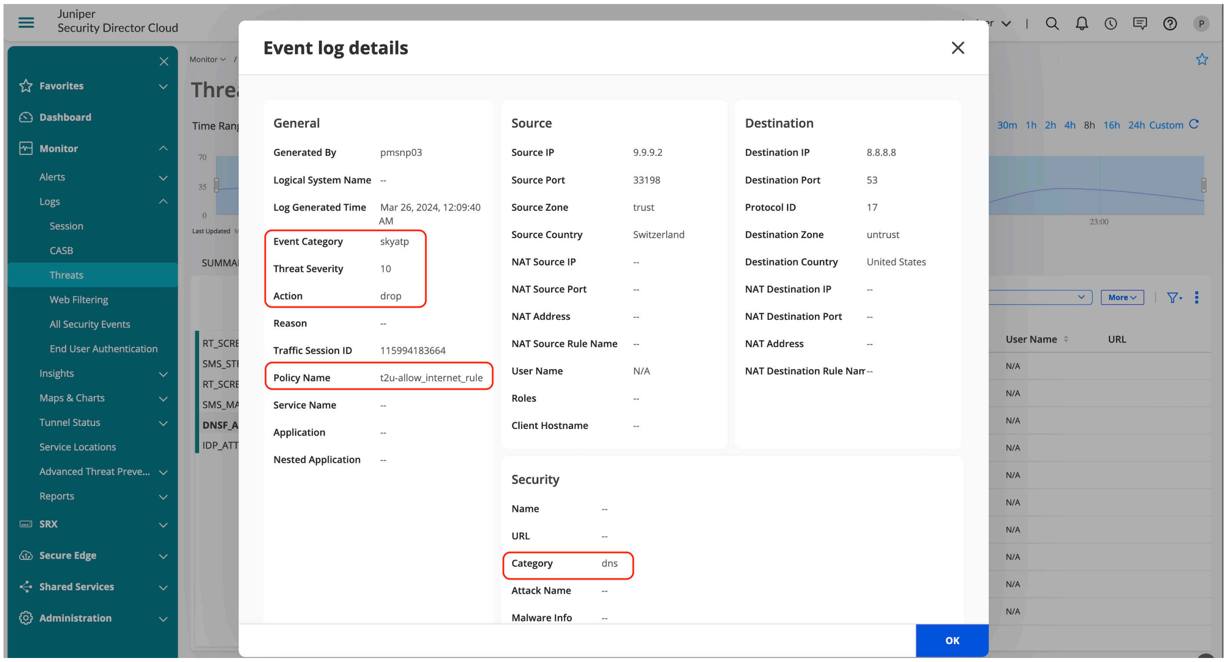
RT_SCREEN_IP (711839)
SMS_STREAMI... (15095)
RT_SCREEN_TCP (9771)
SMS_MALICIO... (345)
DNSF_ACTIO... (154)
IDP_ATTACK_L... (24)

Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
Mar 26, 2024, 12:13:29 AM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 26, 2024, 12:13:29 AM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 26, 2024, 12:12:33 AM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 26, 2024, 12:09:40 AM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 26, 2024, 12:05:54 AM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 25, 2024, 11:57:35 PM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 25, 2024, 11:57:35 PM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 25, 2024, 11:56:43 PM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 25, 2024, 11:54:10 PM	pmsnp03	DNSF_ACTION_LOG		10	N/A	
Mar 25, 2024, 11:54:10 PM	pmsnp03	DNSF_ACTION_LOG		10	N/A	

154 items

Click to view all field details for the event.

Figure 71: Juniper Security Director Cloud—SecIntel Based DNS Log Details



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 26, 2024, 12:09:40 AM
Event Category	skyatp
Threat Severity	10
Action	drop
Reason	--
Traffic Session ID	115994183664
Policy Name	t2u-allow_internet_rule
Service Name	--
Application	--
Nested Application	--

Source

Source IP	9.9.9.2
Source Port	33198
Source Zone	trust
Source Country	Switzerland
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	N/A
Roles	--
Client Hostname	--

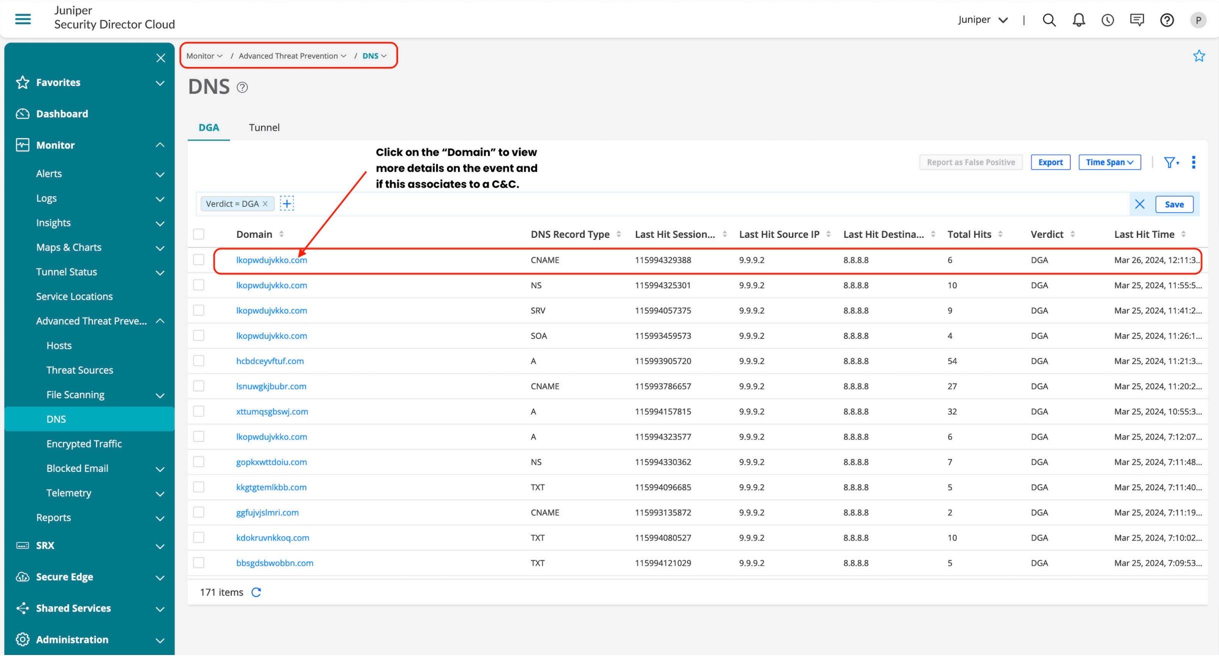
Destination

Destination IP	8.8.8.8
Destination Port	53
Protocol ID	17
Destination Zone	untrust
Destination Country	United States
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Nar	--

Security

Name	--
URL	--
Category	dns
Attack Name	--
Malware Info	--

Figure 72: Juniper Security Director Cloud—ATP DNS DGA Offense



DNS

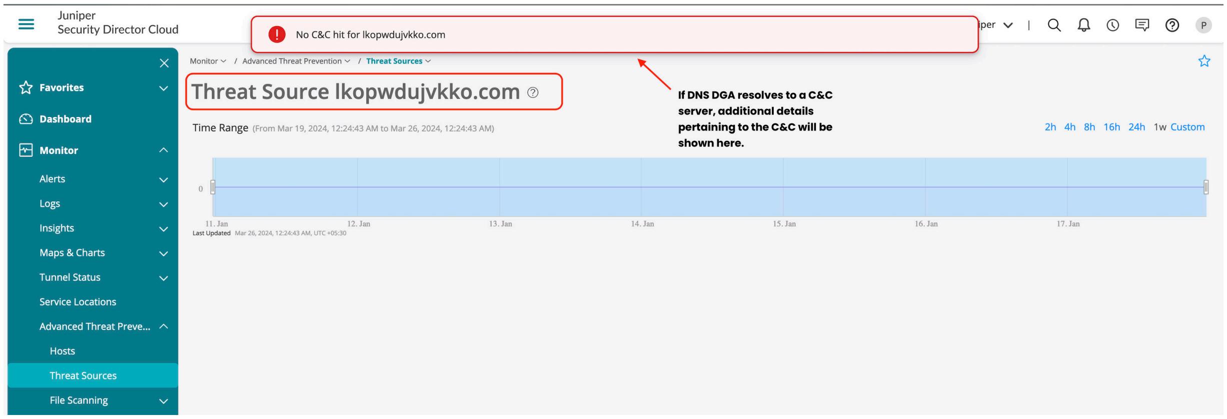
Click on the "Domain" to view more details on the event and if this associates to a C&C.

Domain	DNS Record Type	Last Hit Session...	Last Hit Source IP	Last Hit Destina...	Total Hits	Verdict	Last Hit Time
lkopwdujvkko.com	CNAME	115994329388	9.9.9.2	8.8.8.8	6	DGA	Mar 26, 2024, 12:11:3...
lkopwdujvkko.com	NS	115994325301	9.9.9.2	8.8.8.8	10	DGA	Mar 25, 2024, 11:55:5...
lkopwdujvkko.com	SRV	115994057375	9.9.9.2	8.8.8.8	9	DGA	Mar 25, 2024, 11:41:2...
lkopwdujvkko.com	SOA	115993459573	9.9.9.2	8.8.8.8	4	DGA	Mar 25, 2024, 11:26:1...
hcbdceyvftuf.com	A	115993905720	9.9.9.2	8.8.8.8	54	DGA	Mar 25, 2024, 11:21:3...
lsnuwgkjbubr.com	CNAME	115993786657	9.9.9.2	8.8.8.8	27	DGA	Mar 25, 2024, 11:20:2...
xttumqsgbswj.com	A	115994157815	9.9.9.2	8.8.8.8	32	DGA	Mar 25, 2024, 10:55:3...
lkopwdujvkko.com	A	115994323577	9.9.9.2	8.8.8.8	6	DGA	Mar 25, 2024, 7:12:07...
gopkxwttdoiu.com	NS	115994330362	9.9.9.2	8.8.8.8	7	DGA	Mar 25, 2024, 7:11:48...
kkgtgtemlkbb.com	TXT	115994096685	9.9.9.2	8.8.8.8	5	DGA	Mar 25, 2024, 7:11:40...
ggfujvjslmri.com	CNAME	115993135872	9.9.9.2	8.8.8.8	2	DGA	Mar 25, 2024, 7:11:19...
kdokruvnkkoq.com	TXT	115994080527	9.9.9.2	8.8.8.8	10	DGA	Mar 25, 2024, 7:10:02...
bbsgdsbwobbn.com	TXT	115994121029	9.9.9.2	8.8.8.8	5	DGA	Mar 25, 2024, 7:09:53...

171 items

-

Figure 73: Juniper Security Director Cloud—ATP DNS DGA Offense Details



No C&C hit for lkopwdujvkko.com

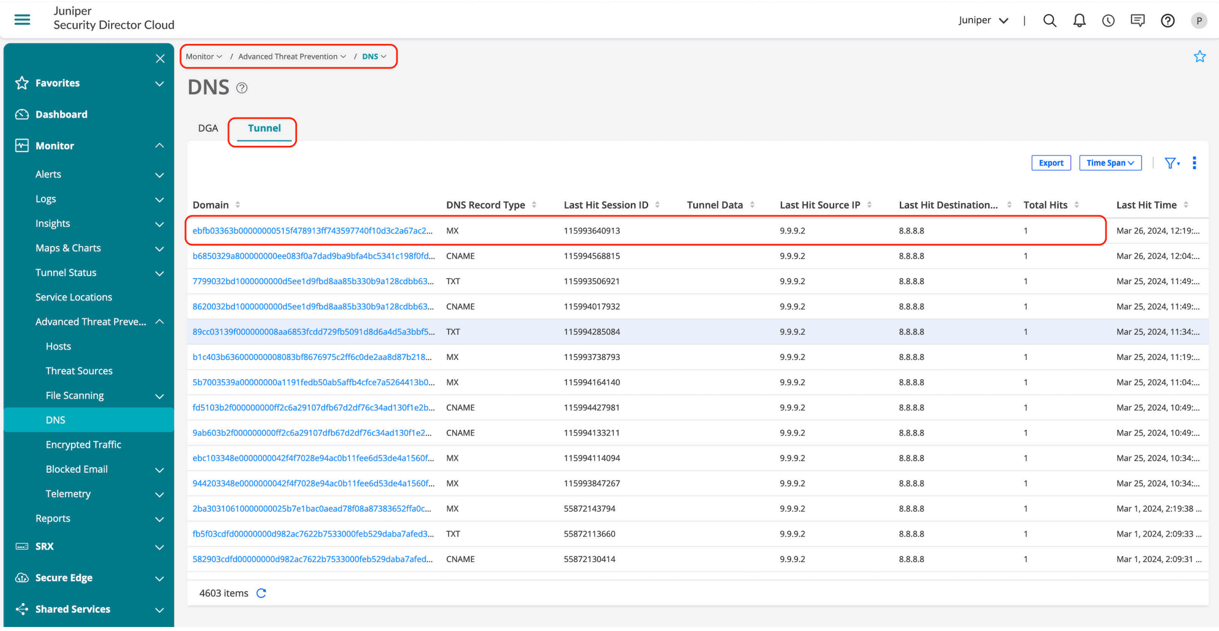
Threat Source lkopwdujvkko.com

Time Range (From Mar 19, 2024, 12:24:43 AM to Mar 26, 2024, 12:24:43 AM)

Last Updated Mar 26, 2024, 12:24:43 AM, UTC +05:30

If DNS DGA resolves to a C&C server, additional details pertaining to the C&C will be shown here.

Figure 74: Security Director Clou—ATP DNS Tunnel Offense

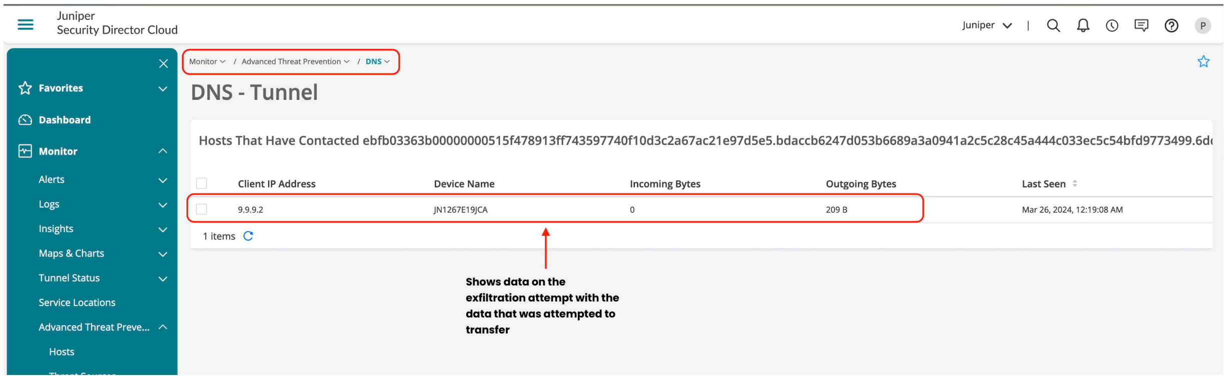


DNS

Domain	DNS Record Type	Last Hit Session ID	Tunnel Data	Last Hit Source IP	Last Hit Destination...	Total Hits	Last Hit Time
ebfb03363b00000000515f478913ff743597740f10d3c2a67ac2...	MX	115993640913		9.9.9.2	8.8.8.8	1	Mar 26, 2024, 12:19:...
b6850329a800000000ee083f0a7dad9ba9bfa4bc5341c198f0fd...	CNAME	115994568815		9.9.9.2	8.8.8.8	1	Mar 26, 2024, 12:04:...
7799032bd1000000000d5ee1d9fbd8aa85b330b9a128cdbb63...	TXT	115993506921		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 11:49:...
8620032bd1000000000d5ee1d9fbd8aa85b330b9a128cdbb63...	CNAME	115994017932		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 11:49:...
89cc03139f000000008aa6853fcdd729fb5091d8d6a4d5a3bbf5...	TXT	115994285084		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 11:34:...
b1c403b636000000008083bf8676975c2ff6c0de2aa8d87b218...	MX	115993738793		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 11:19:...
5b7003539a00000000a1191fedb50ab5affb4cfce7a5264413b0...	MX	115994164140		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 11:04:...
fd5103b2f000000000ff2c6a29107dfb67d2df76c34ad130f1e2b...	CNAME	115994427981		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 10:49:...
9ab603b2f000000000ff2c6a29107dfb67d2df76c34ad130f1e2...	CNAME	115994133211		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 10:49:...
ebc103348e0000000042f4f7028e94ac0b11fee6d53de4a1560f...	MX	115994114094		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 10:34:...
944203348e0000000042f4f7028e94ac0b11fee6d53de4a1560f...	MX	115993847267		9.9.9.2	8.8.8.8	1	Mar 25, 2024, 10:34:...
2ba30310610000000025b7e1bac0aead78f08a87383652ffa0c...	MX	55872143794		9.9.9.2	8.8.8.8	1	Mar 1, 2024, 2:19:38 ...
fb5f03cdfd00000000d982ac7622b7533000feb529daba7afed3...	TXT	55872113660		9.9.9.2	8.8.8.8	1	Mar 1, 2024, 2:09:33 ...
582903cdfd00000000d982ac7622b7533000feb529daba7afed...	CNAME	55872130414		9.9.9.2	8.8.8.8	1	Mar 1, 2024, 2:09:31 ...

4603 items

Figure 75: Juniper Security Director Cloud—ATP DNS Tunnel Offense Detail



DNS - Tunnel

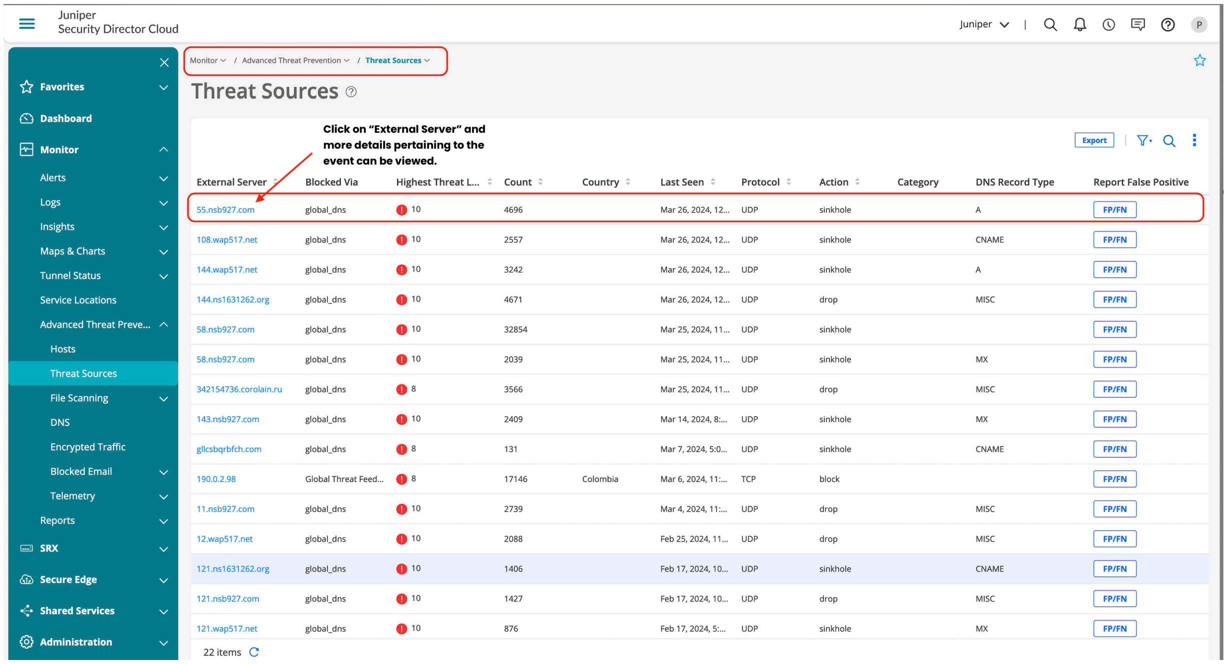
Hosts That Have Contacted ebfb03363b00000000515f478913ff743597740f10d3c2a67ac21e97d5e5.bdaccb6247d053b6689a3a0941a2c5c28c45a444c033ec5c54bfd9773499.6d

□	Client IP Address	Device Name	Incoming Bytes	Outgoing Bytes	Last Seen
□	9.9.9.2	JN1267E19JCA	0	209 B	Mar 26, 2024, 12:19:08 AM

1 items

Shows data on the exfiltration attempt with the data that was attempted to transfer

Figure 76: Juniper Security Director Cloud—SecIntel Identified DNS Offense



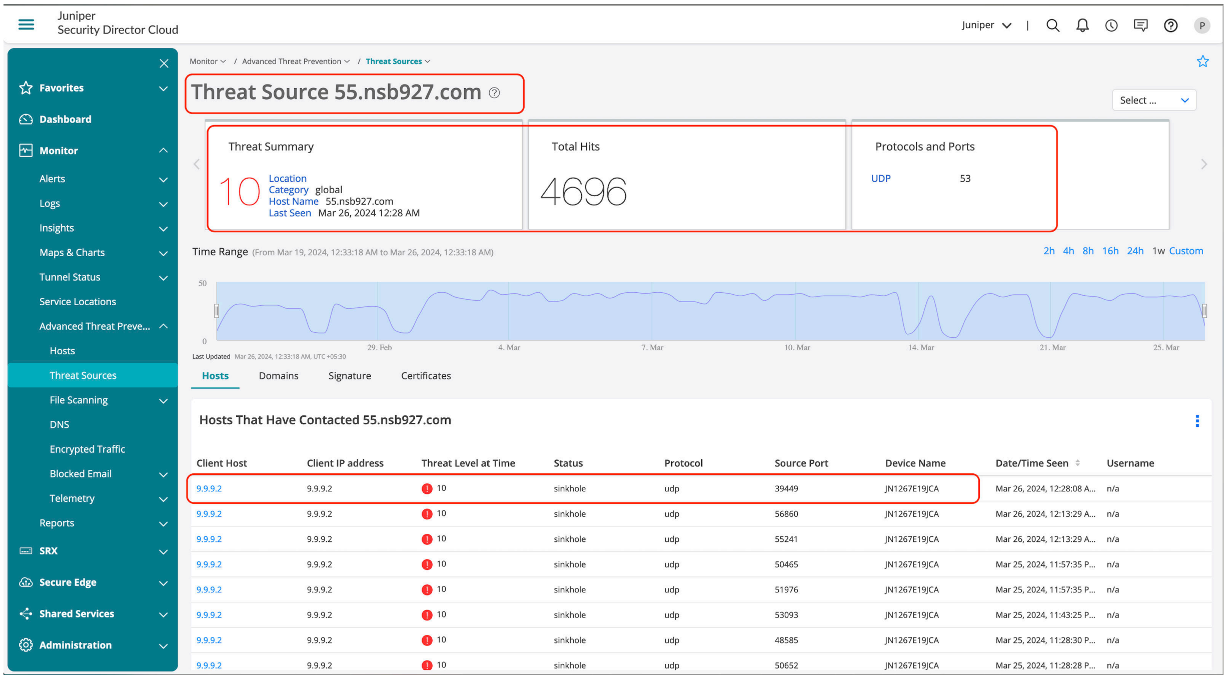
Threat Sources

Click on "External Server" and more details pertaining to the event can be viewed.

External Server	Blocked Via	Highest Threat L...	Count	Country	Last Seen	Protocol	Action	Category	DNS Record Type	Report False Positive
55.nsb927.com	global_dns	! 10	4696		Mar 26, 2024, 12...	UDP	sinkhole		A	FP/FN
108.wap517.net	global_dns	! 10	2557		Mar 26, 2024, 12...	UDP	sinkhole		CNAME	FP/FN
144.wap517.net	global_dns	! 10	3242		Mar 26, 2024, 12...	UDP	sinkhole		A	FP/FN
144.ns1631262.org	global_dns	! 10	4671		Mar 26, 2024, 12...	UDP	drop		MISC	FP/FN
58.nsb927.com	global_dns	! 10	32854		Mar 25, 2024, 11...	UDP	sinkhole			FP/FN
58.nsb927.com	global_dns	! 10	2039		Mar 25, 2024, 11...	UDP	sinkhole		MX	FP/FN
342154736.corolain.ru	global_dns	! 8	3566		Mar 25, 2024, 11...	UDP	drop		MISC	FP/FN
143.nsb927.com	global_dns	! 10	2409		Mar 14, 2024, 8:...	UDP	sinkhole		MX	FP/FN
gllcsbqrbfch.com	global_dns	! 8	131		Mar 7, 2024, 5:0...	UDP	sinkhole		CNAME	FP/FN
190.0.2.98	Global Threat Feed...	! 8	17146	Colombia	Mar 6, 2024, 11:...	TCP	block			FP/FN
11.nsb927.com	global_dns	! 10	2739		Mar 4, 2024, 11:...	UDP	drop		MISC	FP/FN
12.wap517.net	global_dns	! 10	2088		Feb 25, 2024, 11...	UDP	drop		MISC	FP/FN
121.ns1631262.org	global_dns	! 10	1406		Feb 17, 2024, 10...	UDP	sinkhole		CNAME	FP/FN
121.nsb927.com	global_dns	! 10	1427		Feb 17, 2024, 10...	UDP	drop		MISC	FP/FN
121.wap517.net	global_dns	! 10	876		Feb 17, 2024, 5:...	UDP	sinkhole		MX	FP/FN

22 items

Figure 77: Juniper Security Director Cloud—SecIntel Identified DNS Offense Detail



Threat Source 55.nsb927.com

Threat Summary

10 Location
Category global
Host Name 55.nsb927.com
Last Seen Mar 26, 2024 12:28 AM

Total Hits

4696

Protocols and Ports

UDP 53

Time Range (From Mar 19, 2024, 12:33:18 AM to Mar 26, 2024, 12:33:18 AM) 2h 4h 8h 16h 24h 1w Custom

Last Updated Mar 26, 2024, 12:33:18 AM, UTC +05:30

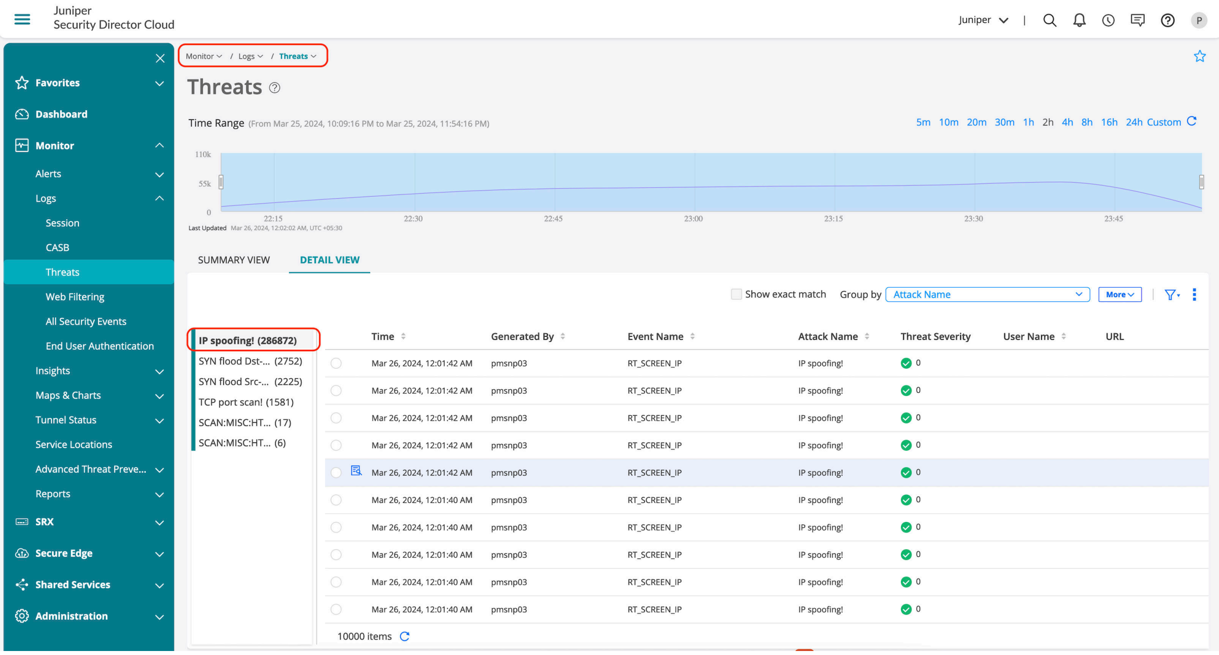
Hosts That Have Contacted 55.nsb927.com

Client Host	Client IP address	Threat Level at Time	Status	Protocol	Source Port	Device Name	Date/Time Seen	Username
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	39449	JN1267E19JCA	Mar 26, 2024, 12:28:08 A...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	56860	JN1267E19JCA	Mar 26, 2024, 12:13:29 A...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	55241	JN1267E19JCA	Mar 26, 2024, 12:13:29 A...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	50465	JN1267E19JCA	Mar 25, 2024, 11:57:35 P...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	51976	JN1267E19JCA	Mar 25, 2024, 11:57:35 P...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	53093	JN1267E19JCA	Mar 25, 2024, 11:43:25 P...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	48585	JN1267E19JCA	Mar 25, 2024, 11:28:30 P...	n/a
9.9.9.2	9.9.9.2	! 10	sinkhole	udp	50652	JN1267E19JCA	Mar 25, 2024, 11:28:28 P...	n/a

Screens Feature Validation

IP Spoofing

Figure 78: Juniper Security Director Cloud—IP Spoofing Log



Monitor / Logs / Threats

Threats

Time Range (From Mar 25, 2024, 10:09:16 PM to Mar 25, 2024, 11:54:16 PM)

5m 10m 20m 30m 1h 2h 4h 8h 16h 24h Custom

Last Updated Mar 26, 2024, 12:02:02 AM, UTC +05:30

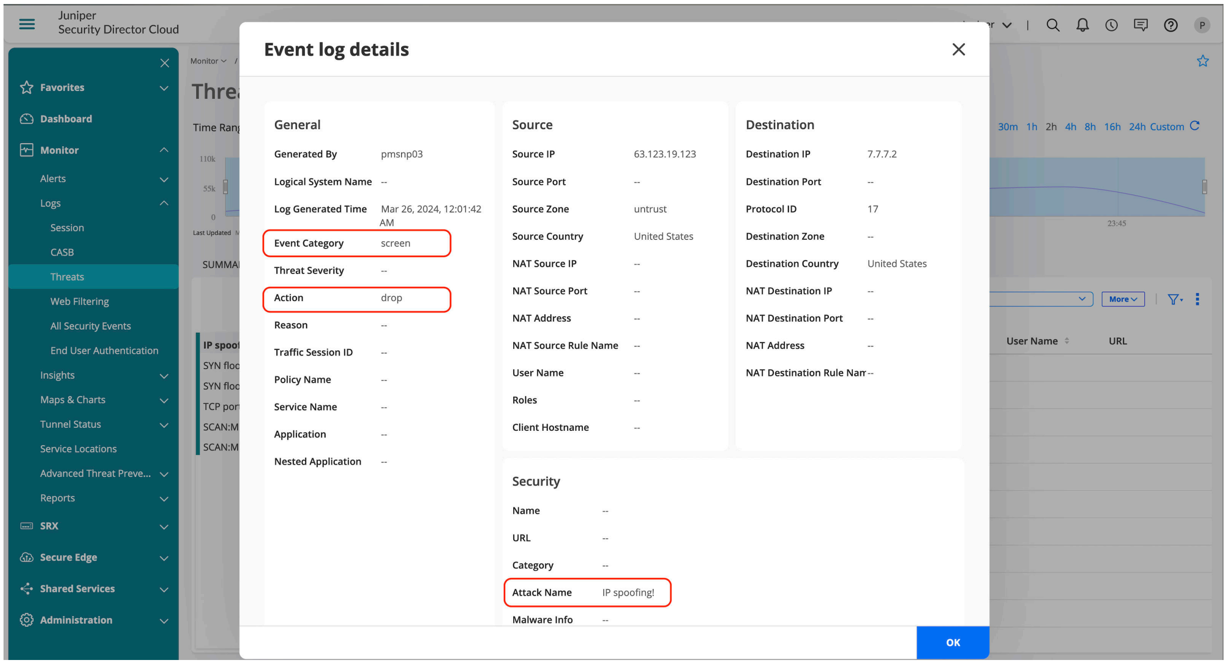
□ Show exact match Group by Attack Name

IP spoofing! (286872)
SYN flood Dst-... (2752)
SYN flood Src-... (2225)
TCP port scan! (1581)
SCAN:MISC:HT... (17)
SCAN:MISC:HT... (6)

Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:40 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:40 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:40 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:40 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		
Mar 26, 2024, 12:01:40 AM	pmsnp03	RT_SCREEN_IP	IP spoofing!	✓ 0		

10000 items

Figure 79: Juniper Security Director Cloud—IP Spoofing Log Detail



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 26, 2024, 12:01:42 AM
Event Category	screen
Threat Severity	--
Action	drop
Reason	--
Traffic Session ID	--
Policy Name	--
Service Name	--
Application	--
Nested Application	--

Source

Source IP	63.123.19.123
Source Port	--
Source Zone	untrust
Source Country	United States
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	--
Roles	--
Client Hostname	--

Destination

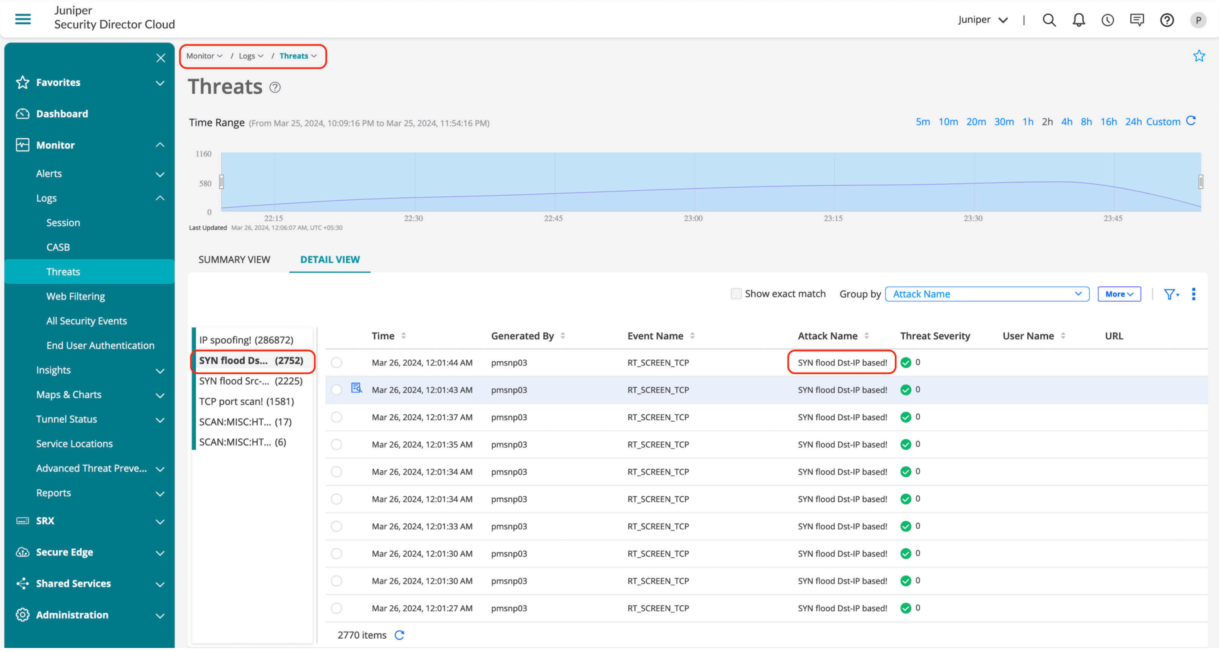
Destination IP	7.7.7.2
Destination Port	--
Protocol ID	17
Destination Zone	--
Destination Country	United States
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Nar	--

Security

Name	--
URL	--
Category	--
Attack Name	IP spoofing!
Malware Info	--

SYN Flood—(Apply Source and Destination Limits)

Figure 80: Juniiper Security Director Cloud—Syn Flood dst-ip Filter



Time Range (From Mar 25, 2024, 10:09:16 PM to Mar 25, 2024, 11:54:16 PM)

Last Updated Mar 26, 2024, 12:06:07 AM, UTC +05:30

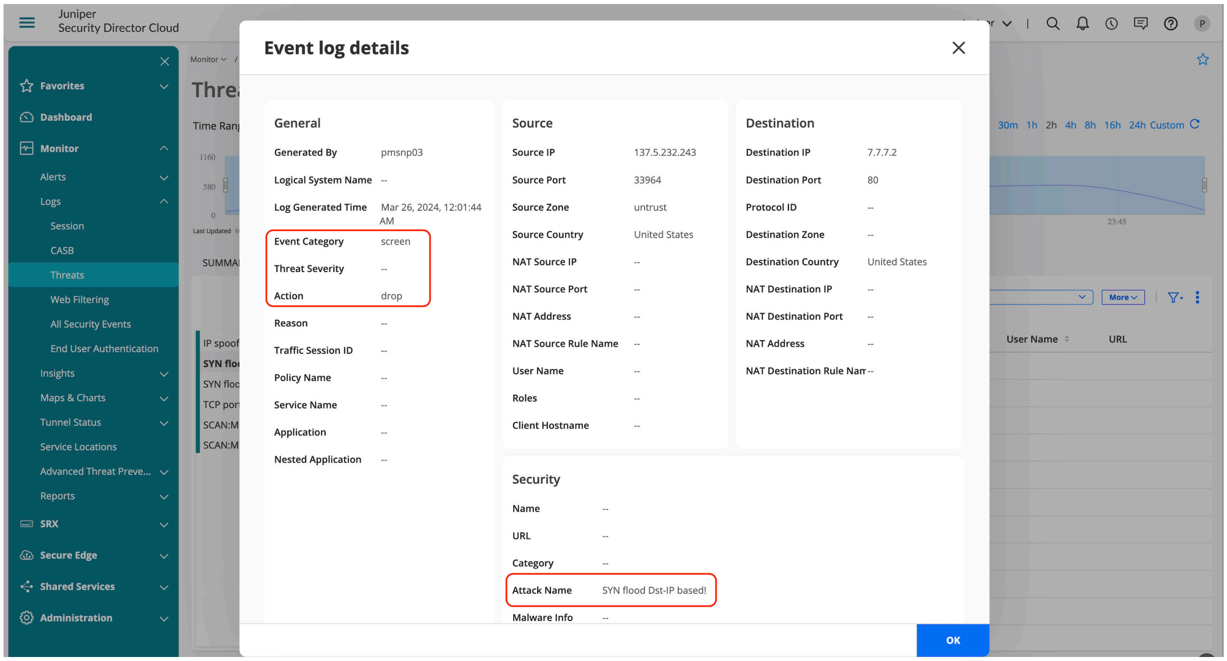
□ Show exact match Group by Attack Name

IP spoofing! (286872)
SYN flood Ds... (2752)
SYN flood Src-... (2225)
TCP port scan! (1581)
SCAN:MISC:HT... (17)
SCAN:MISC:HT... (6)

Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
Mar 26, 2024, 12:01:44 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:43 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:37 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:35 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:34 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:34 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:33 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:30 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:30 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		
Mar 26, 2024, 12:01:27 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Dst-IP based!	✓ 0		

2770 items

Figure 81: Juniper Security Director Cloud—Syn Flood dst-ip Filter Detail



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 26, 2024, 12:01:44 AM
Event Category	screen
Threat Severity	--
Action	drop
Reason	--
Traffic Session ID	--
Policy Name	--
Service Name	--
Application	--
Nested Application	--

Source

Source IP	137.5.232.243
Source Port	33964
Source Zone	untrust
Source Country	United States
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	--
Roles	--
Client Hostname	--

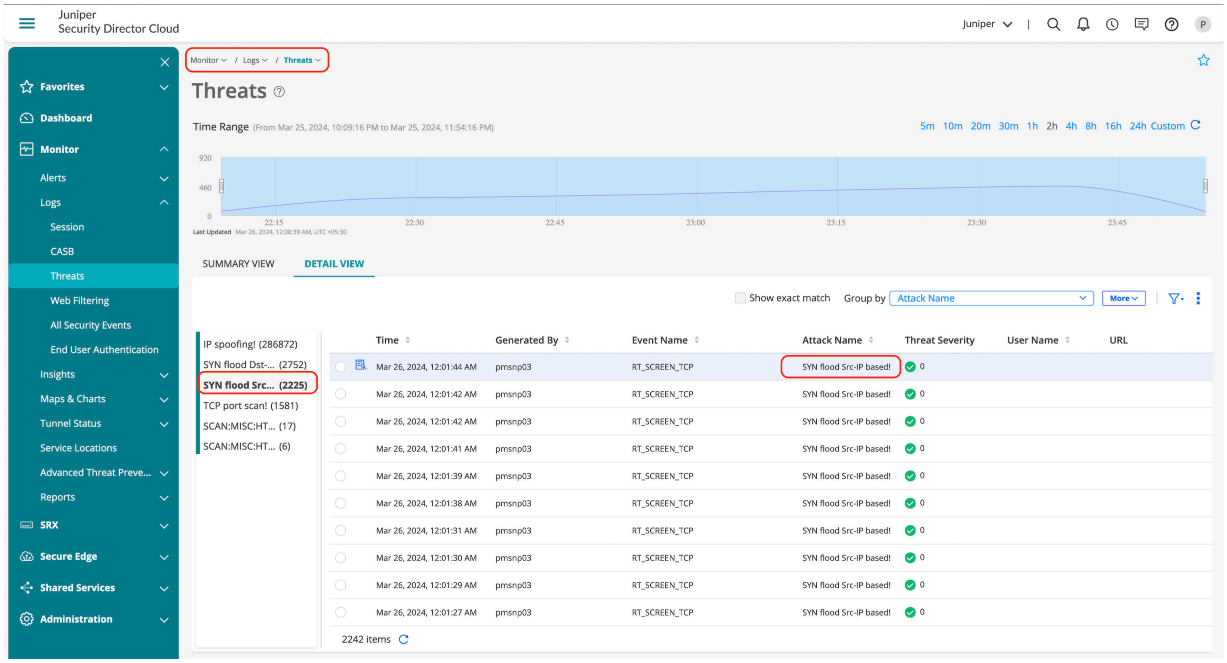
Destination

Destination IP	7.7.7.2
Destination Port	80
Protocol ID	--
Destination Zone	--
Destination Country	United States
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Narr	--

Security

Name	--
URL	--
Category	--
Attack Name	SYN flood Dst-IP based!
Malware Info	--

Figure 82: Juniper Security Director Cloud— Syn Flood src-ip Filter



Threats

Time Range (From Mar 25, 2024, 10:09:16 PM to Mar 25, 2024, 11:54:16 PM)

Last Updated Mar 26, 2024, 12:08:39 AM, UTC +05:30

□ Show exact match Group by Attack Name

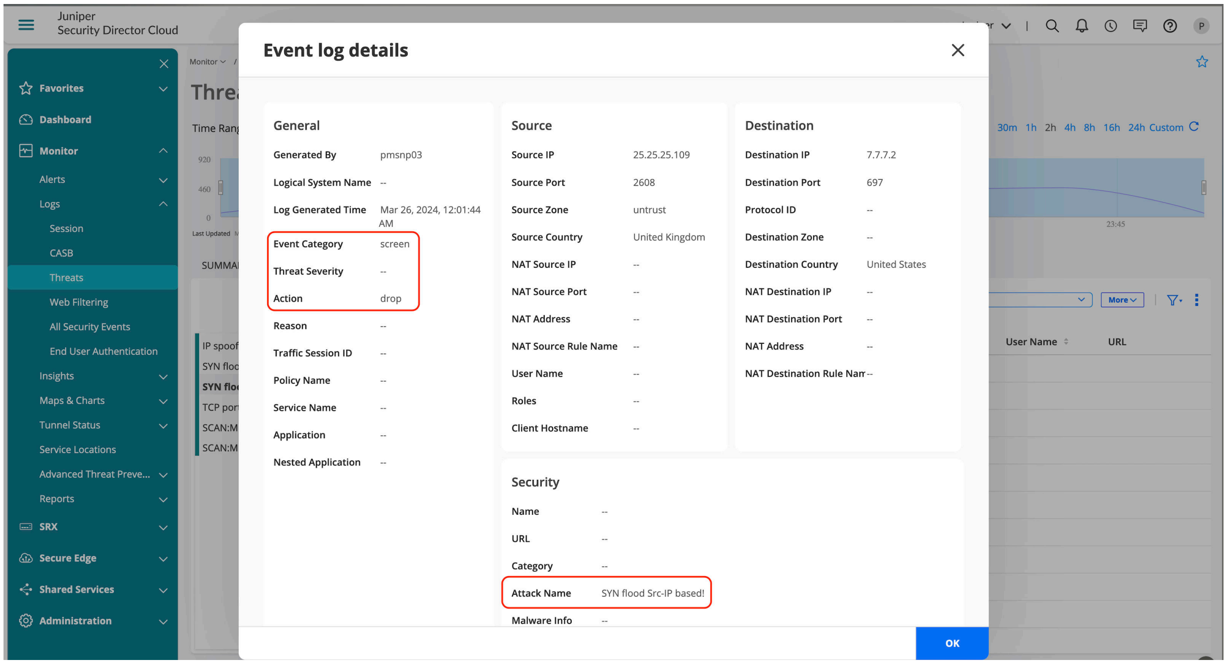
- IP spoofing! (286872)
- SYN flood Dst-... (2752)
- **SYN flood Src... (2225)**
- TCP port scan! (1581)
- SCAN:MISC:HT... (17)
- SCAN:MISC:HT... (6)

Time	Generated By	Event Name	Attack Name	Threat Severity	User Name	URL
Mar 26, 2024, 12:01:44 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:42 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:41 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:39 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:38 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:31 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:30 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:29 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		
Mar 26, 2024, 12:01:27 AM	pmsnp03	RT_SCREEN_TCP	SYN flood Src-IP based!	✓ 0		

2242 items

.

Figure 83: Figure 83:Junioer Security Director Cloud – Syn Flood src-ip Filter Detail



Event log details

General

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 26, 2024, 12:01:44 AM
Event Category	screen
Threat Severity	--
Action	drop
Reason	--
Traffic Session ID	--
Policy Name	--
Service Name	--
Application	--
Nested Application	--

Source

Source IP	25.25.25.109
Source Port	2608
Source Zone	untrust
Source Country	United Kingdom
NAT Source IP	--
NAT Source Port	--
NAT Address	--
NAT Source Rule Name	--
User Name	--
Roles	--
Client Hostname	--

Destination

Destination IP	7.7.7.2
Destination Port	697
Protocol ID	--
Destination Zone	--
Destination Country	United States
NAT Destination IP	--
NAT Destination Port	--
NAT Address	--
NAT Destination Rule Nam	--

Security

Name	--
URL	--
Category	--
Attack Name	SYN flood Src-IP based!
Malware Info	--

Reverse SSL Proxy Validation

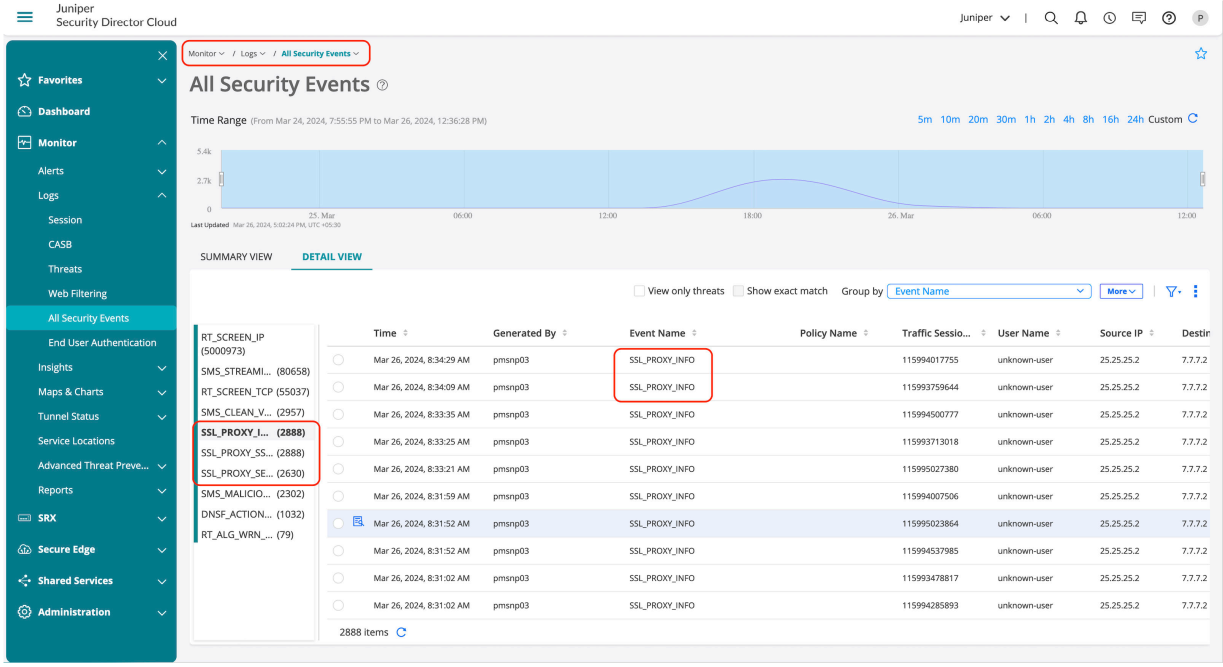
Reverse SSL proxy enables to decrypt specific traffic destined to a webserver for subjecting the traffic through advanced security services.

Once applied on a security policy, you'll notice several logs that might define the action that SSL proxy takes.

Table 6: Reverse SSL Proxy Logs

Log Information	Description
SSL_PROXY_SSL_SESSION_DROP	Log is generated when SSL proxy drop a session.
SSL_PROXY_SSL_SESSION_ALLOW	Log is generated when SSL session is processed by SSL proxy even after encountering minor errors.
SSL_PROXY_SESSION_IGNORE	Log is generated after detection of non-SSL sessions which are initially mistaken as SSL sessions.
SSL_PROXY_SESSION_WHITELIST	Log is generated when a SSL proxy session is whitelisted.
SSL_PROXY_ERROR	Log is generated for reporting errors during SSL proxy.
SSL_PROXY_WARNING	Log is generated for reporting warnings during SSL proxy.
SSL_PROXY_INFO	Log is generated for reporting general information during SSL proxy.

Figure 84: Juniper Security Director Cloud—SSL Proxy Log



All Security Events

Time Range (From Mar 24, 2024, 7:55:55 PM to Mar 26, 2024, 12:36:28 PM)

Last Updated Mar 26, 2024, 5:02:24 PM, UTC +05:30

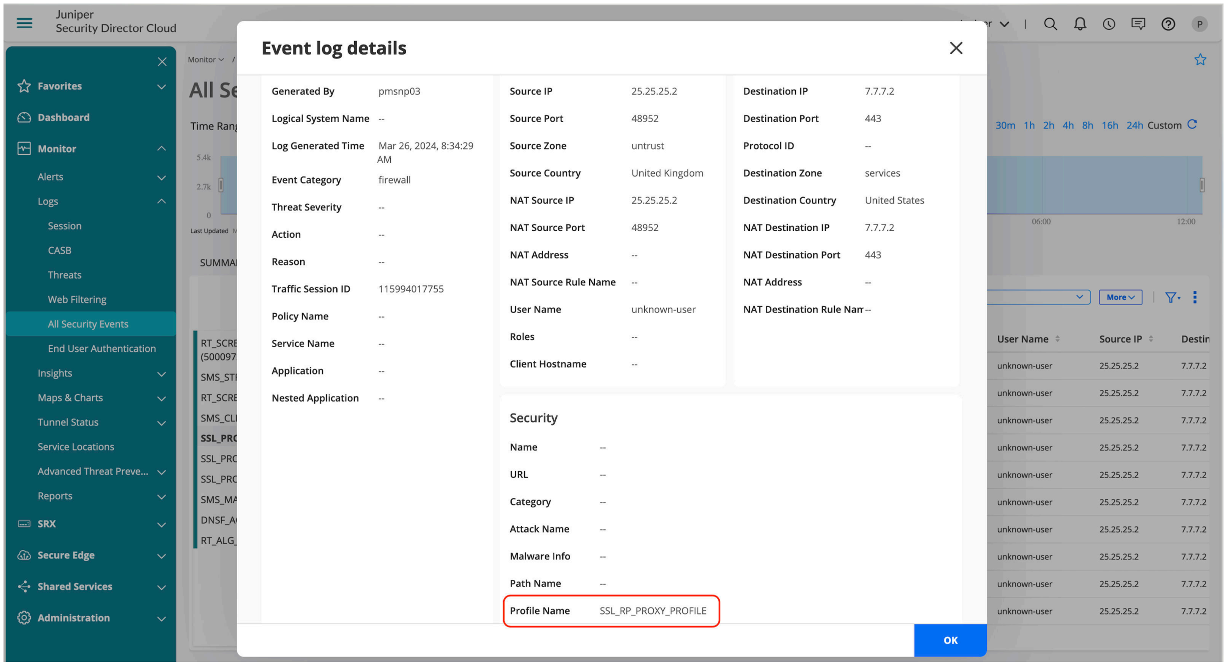
□ View only threats □ Show exact match Group by Event Name

RT_SCREEN_IP (5000973)
SMS_STREAMI... (80658)
RT_SCREEN_TCP (55037)
SMS_CLEAN_V... (2957)
SSL_PROXY_I... (2888)
SSL_PROXY_SS... (2888)
SSL_PROXY_SE... (2630)
SMS_MALICIO... (2302)
DNSF_ACTION... (1032)
RT_ALG_WRN_... (79)

Time	Generated By	Event Name	Policy Name	Traffic Sessio...	User Name	Source IP	Destin
Mar 26, 2024, 8:34:29 AM	pmsnp03	SSL_PROXY_INFO		115994017755	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:34:09 AM	pmsnp03	SSL_PROXY_INFO		115993759644	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:33:35 AM	pmsnp03	SSL_PROXY_INFO		115994500777	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:33:25 AM	pmsnp03	SSL_PROXY_INFO		115993713018	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:33:21 AM	pmsnp03	SSL_PROXY_INFO		115995027380	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:31:59 AM	pmsnp03	SSL_PROXY_INFO		115994007506	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:31:52 AM	pmsnp03	SSL_PROXY_INFO		115995023864	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:31:52 AM	pmsnp03	SSL_PROXY_INFO		115994537985	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:31:02 AM	pmsnp03	SSL_PROXY_INFO		115993478817	unknown-user	25.25.25.2	7.7.7.2
Mar 26, 2024, 8:31:02 AM	pmsnp03	SSL_PROXY_INFO		115994285893	unknown-user	25.25.25.2	7.7.7.2

2888 items

Figure 85: Juniper Security Director Cloud—SSL Proxy Log Details



Event log details

Generated By	pmsnp03
Logical System Name	--
Log Generated Time	Mar 26, 2024, 8:34:29 AM
Event Category	firewall
Threat Severity	--
Action	--
Reason	--
Traffic Session ID	115994017755
Policy Name	--
Service Name	--
Application	--
Nested Application	--

Source IP	25.25.25.2
Source Port	48952
Source Zone	untrust
Source Country	United Kingdom
NAT Source IP	25.25.25.2
NAT Source Port	48952
NAT Address	--
NAT Source Rule Name	--
User Name	unknown-user
Roles	--
Client Hostname	--

Destination IP	7.7.7.2
Destination Port	443
Protocol ID	--
Destination Zone	services
Destination Country	United States
NAT Destination IP	7.7.7.2
NAT Destination Port	443
NAT Address	--
NAT Destination Rule Nam	--

Security

Name	--
URL	--
Category	--
Attack Name	--
Malware Info	--
Path Name	--
Profile Name	SSL_RP_PROXY_PROFILE