Release Notes

Published
2023-07-25

Juniper Advanced Threat Prevention Cloud

SOFTWARE HIGHLIGHTS

- Webhook for audit log notifications
- DAG Filter for Amazon AWS feeds
- Quick Start: Use this new setup guide to get your Juniper ATP Cloud up and running in three quick steps.

Table of Contents

Introduction to Juniper ATP Cloud

Juniper® Advanced Threat Prevention Cloud (Juniper ATP Cloud) is the threat intelligence hub for your network. It comprises of built-in advanced threat services that use the power of AI to detect attacks and optimize enforcement.

Juniper ATP Cloud detects and stops zero-day and commodity malware within web, email, data center, and application traffic targeted for Windows, Mac, and IoT devices.

The service assesses risk from encrypted and decrypted network traffic and connecting devices, including IoT, and distributes that intelligence throughout the network to stop attacks and drastically decrease the attack surface before a breach occurs. It provides a real-time window into security events that security operations staff can use to quickly correlate activity and remediate issues.

Juniper ATP Cloud's identification technology uses different techniques to quickly identify a threat and prevent an impending attack. These methods include:

- Powerful machine learning algorithms.
- Dynamic analysis with techniques to trick malware into activating and self-identifying.
- Rapid cache lookups to speed up previous malware identification.
- Antivirus signature-based engine to identify known files.
- Static analysis that analyzes software code to identify possible dangerous fragments.

The following are the highlights of the features available in Juniper ATP Cloud release:

- SecIntel—Curate and distribute threat feeds verified by Juniper Threat Labs across the network to routers, switches, access points, and firewalls for orchestrated action. Use the threat intelligence feeds to detect and block verified threats, compromised devices, and malicious connections in real time.
- Threat Mitigation— Automatically discover and mitigate known and unknown threats. Block or segment malicious outbreaks on the network using an SRX Series firewall, MX Series router, or an EX Series or QFX Series switch. Integrates with existing network access control (NAC) solutions and third-party firewalls, switches, and wireless technology.
- Encrypted Traffic Insights —Detect and stop threats hiding within encrypted traffic without decrypting, which means privacy and security are no longer at odds.
- Adaptive Threat Profiling —Detect targeted attacks on your network, including high-risk users and devices, and automatically mobilize your defenses. Create security intelligence feeds based on real-time events happening on your network. You have the flexibility to take action against emerging threats as they are detected.

- AI-Driven Risk Profiling—Automatically discover and mitigate known and unknown threats. Assess the risk of user and IoT devices connecting to Mist AI-managed wired and wireless solutions based on endpoint information and behavior. Pinpoint and mitigate potential compromise with geospatial location and one-touch mitigation.

Supportability Information

IN THIS SECTION

Juniper ATP Cloud Component Support Table

The following product versions have been tested and are supported with Juniper ATP Cloud.

Table 1: Juniper ATP Cloud Component Support Table

Platform	Hardware Requirements	Software Versions
MX Series	MX5, MX10, MX40, MX80, MX104, MX240, MX480, MX960, MX2010, MX2020	Junos 16.1R1 and above
MX Series	MX204	Junos 17.4R1 and above
MX Series	MX2008	Junos 17.2R1 and above
MX Series	MX10003	Junos 17.3R1 and above

Table 1: Juniper ATP Cloud Component Support Table *(Continued)*

Platform	Hardware Requirements	Software Versions
MX Series	MX10008	Junos 18.2R1 and above
MX Series	MX10016	Junos 19.2R1
vSRX Series		Junos 15.1X49-D60 and above
SRX Series	SRX300, SRX320	Junos 18.3R1 and above
SRX Series	SRX340, SRX345, SRX550HM	Junos 15.1X49-D60 and above
SRX Series	SRX380	Junos 20.1R1
SRX Series	SRX1500	Junos 15.1X49-D40 and above
SRX Series	SRX4100, SRX4200	Junos 15.1X49-D65 and above
SRX Series	SRX4600	Junos 17.4R1-S1 and above
SRX Series	SRX5400, SRX5600, SRX5800	Junos 15.1X49-D50 and above

Juniper ATP Cloud Web UI Browser Support Table

The following operating systems and browsers are supported with the Juniper ATP Cloud web-based service portal (web UI).

Table 2: Juniper ATP Cloud Component Support Table

OS	Browser
Windows 10 Enterprise, 64 bit	• Google Chrome 33.x and above • Microsoft Edge • Firefox 31 ESR and above • Spartan
Windows 8.1 Enterprise, 64 bit	• Google Chrome 33.x and above • Microsoft Edge • Firefox 31 ESR and above
Windows 8 Enterprise, 64 bit	• Google Chrome 33.x and above • Microsoft Edge • Firefox 31 ESR and above
Windows 7 Enterprise SP1, 64 bit	• Google Chrome 33.x and above • Microsoft Edge • Firefox 31 ESR and above
Mac OS X 10.10, 64 bit	Safari 7.0
Mac OS X 10.9, 64 bit	Safari 7.0

Sandbox OS Support

Sandboxing supports the following operating systems:

- Windows 7
- Windows 10
- Android

JSA and QRadar SIEM Support Table

The following product versions support Juniper ATP Cloud syslog messages.

Table 3: Juniper ATP Cloud Component Support Table

Product	Software Version
QRadar SIEM	7.2 and above
JSA	2014.4x and above

Release 2023

IN THIS SECTION

July, 2023 Release

IN THIS SECTION

New and Changed Features: July, 2023

Webhook for audit log notifications

You can use Audit Log Webhook to send ATP Cloud audit log notifications to a remote server. Webhook is an automated message or real-time notification sent to your application when an event is triggered. You can enable webhook and configure the remote server URL to receive the audit log notifications in your chat application that can process JSON responses.

[See Configure Webhook.]

DAG Filter

You can filter and view the DAG feeds from the AWS regions and services that are relevant to you. Use DAG Filter to add feeds for the AWS regions and services that you select. You can configure a maximum of 10 DAG filters.

[See Configure DAG Filter.]

April, 2023 Release

IN THIS SECTION

New and Changed Features: April, 2023

Enhancements to Blocklists

We have increased the limit for the maximum number of blocklists. You can now configure up to 15000 IP addresses in the blocklist.

[See Creating Allowlists and Blocklists.]

Enhancements to Customer Portal

We have updated the following pages in Juniper ATP Cloud Portal for better user experience:

- Allowlists – We have added ETI and DNS to the allowlist types. To configure allowlist, navigate to **Configure > Allowlists**.
- Allowlists – We have added Threat and DAG feeds to SecIntel feeds. To configure allowlist, navigate to **Configure > Allowlists**.
- Global Configuration – We have renamed Global Configuration as Misc Configuration. To access Misc Configuration, navigate to **Configure > Misc Configuration**.
- Infected Hosts – We have moved Infected Hosts tab out of Misc Configuration. To configure Infected Hosts, navigate to **Configure > Infected Hosts**.
- Threat Intelligence Sharing – We have moved Threat Intelligence Sharing tab out of Misc Configuration. To configure Threat Intelligence Sharing, navigate to **Configure > Threat Intelligence Sharing**.

OpenAPI support to pull Audit logs

OpenAPI support is enabled for Audit API to manually pull Audit logs. Now you can get the Audit details with API /v2/skyatp/ui_api/audit along with the Application Token.

January, 2023 Release

IN THIS SECTION

New and Changed Features: January, 2023

Alert message for false positive events

When you report an event as false positive, we now display an alert. The alert message states that an event with threat level below 7 is considered as non-malicious and does not need any action. However, you can still report the event as false positive.

Category enrichment for C&C server hits

Starting with this release, we have discontinued category enrichment for C&C server hits from a custom feed.

Release 2022

IN THIS SECTION

October, 2022 Release

IN THIS SECTION

New and Changed Features: October, 2022

Enhancements in the threat assessment report

We have added new report data for DNS. The new report includes DNS Event Counts and Top DNS Tunnel Destination Domains.

[See Reports Overview.]

Setting up the initial login password

When the administrator creates your profile in the Juniper ATP Cloud Web UI, you will receive an email with a link to set the password.

[See Set Password.]

July, 2022 Release

IN THIS SECTION

New and Changed Features: July, 2022

Enhancements in the Threat Assessment Report

In the executive summary page, we have introduced the report data for the following categories:

- DNS DGA
- DNS Tunnels
- ETI Source Hosts
- ETI Destinations

[See Reports Overview.]

May, 2022 Release

IN THIS SECTION

New and Changed Features: May, 2022

Notification for session expiry

We have added a new notification to let you know that the session is about to expire in few minutes. You can choose to extend the current session or logout from the session. You can extend the session for maximum 25 times.

[See Juniper Advanced Threat Prevention Cloud Web UI Overview.]

Support to display behavior information for partial file downloads

Juniper ATP Cloud now provides more insights into the behavior information of signatures for partial file downloads with sandbox results. You can now view the sample behavior, network activity, and behavior details for the signatures.

[See Signature Details.]

Support to display static analysis information for full file downloads

You can now view static file information such as document type, certificate details, signer information and so on for full file downloads with static analysis results.

[See HTTP File Download Details.]

March, 2022 Release

IN THIS SECTION

New and Changed Features: March, 2022

IoT Device Detection and Classification

Juniper ATP Cloud provides discovery, visibility, and classification of Internet of Things (IoT) devices in the network. IoT device visibility helps you to continuously discover, monitor, and enforce security policies across all connected IoT devices.

[See Security IoT User Guide and IoT Device Overview.]

Enhancement in File Scanning

The Behavior Analysis tab now shows a new radar chart to provide a quick overview of the malware category information. Note that the new radar chart may not exist for some possibly malicious samples after sandboxing.

[See HTTP File Download Details.]

Support for Feodo Tracker and Threatfox as Third Party Threat Feed

We now support Feodo Tracker IP, Threatfox IP, Threatfox URL, and Threatfox domains feeds under third-party threat feeds category. By default, the feeds are disabled in the Juniper ATP Cloud Portal. Log in to the portal and enable the new feeds at **Configure > SecIntel Feeds**.

[See SecIntel Feeds Overview.]

January, 2022 Release

IN THIS SECTION

New and Changed Features: January, 2022

Support for SecIntel feeds on MX Series routers

MX Series routers can now download global SecIntel feeds directly from Cloud Feeds without enrolling to Juniper ATP Cloud.

[See Configure SecIntel Feeds for MX Series Routers.]

Enhancement to SMTP email notifications

When an email attachment is determined to be malicious, you can configure Juniper ATP Cloud to permit the email and also notify user about the permitted message containing an unknown malware.

[See Email Management: Configure SMTP.]

Enhancements to Customer Portal

We have updated the following pages in Juniper ATP Cloud Portal for better user experience:

- Single Sign-On Configuration—We have categorized the Single Sign-On (SSO) settings as Service Provider settings and Identity Provider settings. To configure SSO settings, navigate to **Administration > Single Sign-On Settings**.
- Allowlists—We have categorized the allowlist types as Antimalware and SecIntel. To configure allowlist, navigate to **Configure > Allowlists**.
- Blocklists—We have categorized the blocklist types as Antimalware and SecIntel. To configure blocklist, navigate to **Configure > Blocklists**.
- SecIntel Feeds—We have categorized the SecIntel feeds as Juniper Threat Feeds, Third Party Threat Feeds, and Dynamic Address Group (DAG) Feeds. To enable the feeds, navigate to **Configure > SecIntel Feeds**.

[See Configure SSO Settings, Allowlist and Blocklist Overview, Creating Allowlists and Blocklists, and SecIntel Feeds Overview.]

Release 2021

IN THIS SECTION

September, 2021 Release

IN THIS SECTION

New and Changed Features: September, 2021

Advanced Strike Engine

Starting in Junos OS Release 21.3R1, a new high performance malware inspection engine has been added to SRX Series Firewalls. The device can block a malicious file immediately inline when an advanced anti-malware (AAMW) policy is configured with the block action. This enhancement to Juniper ATP Cloud block mode is supported on HTTP, IMAP and, SMB protocols.

NOTE: Starting in Junos OS Release 21.3R1, AAMW HTTP hash solution is deprecated.

Use the existing `set services advanced-anti-malware policy` *`policy-name`* `http action block` command to configure block mode. To view the malware statistics, use the `show services advanced-anti-malware malware-db-statistics` operational command.

To view the malware signature details, log in to Juniper ATP Cloud Web portal and go to the following page:

- **Monitor > File Scanning > HTTP File Downloads > Partial File**.
- **Monitor > File Scanning > Email Attachments > Partial File**.
- **Monitor > File Scanning > SMB File Downloads > Partial File**.

[See Signature Details, advanced-anti-malware policy, and show services advanced-anti-malware statistics.]

Support for New Third-Party Internet Service Feeds

We've added new third-party Internet service feeds in addition to the existing office365 feeds. By default, the feeds are disabled in the Juniper ATP Cloud Portal. Log in to the portal and enable the new feeds at **Configure > SecIntel Feeds**.

[See SecIntel Feeds Overview.]

Support for Multiple Mist Deployments

We now support multiple Mist deployments to a single region in Juniper ATP Cloud. You can select the Mist cloud to which you want to stream the security events. To select the Mist cloud, log in to Juniper ATP Cloud Portal, navigate to **Configure > Global Configuration > Mist**, and select the Target Mist Cloud from the drop-down list.

[See Enable Mist with Juniper ATP Cloud.]

Deprecation of Malware Domain List Feeds

The third party IP threat feed, **Malware Domain list** is deprecated and hence it is no longer supported on Juniper ATP Cloud. If you had enabled this feed earlier, you will stop receiving the feed.

[See SecIntel Feeds Overview.]

Change in Update Interval for Adaptive Threat Profiling Feeds

We've optimized the update interval for adaptive threat profiling feed in Juniper ATP Cloud. The SRX Series Firewalls will now receive the feeds 10 times faster than earlier releases.

June, 2021 Release

IN THIS SECTION

New and Changed Features: June, 2021

DNS DGA Detection

Starting in Junos OS Release 21.2R1, Juniper ATP Cloud supports Domain Name System (DNS) Domain Generation Algorithm (DGA) detection. DNS DGA generates seemingly random domain names that are used as rendezvous points with potential C&C servers. DNS DGA detection uses machine learning models as well as known pre-computed DGA domain names and provides domain verdicts, which will help in in-line blocking and sinkholing of DNS queries on SRX Series Firewalls.

Use the `set security-metadata-streaming policy` *`policy-name`* `detections dga` command at the `[edit services]` hierarchy to configure DNS DGA detections.

To view the DNS DGA detections, log in to Juniper ATP Cloud Web portal and navigate to **Monitor > DNS**.

[See DNS DGA Detection Overview, DNS DGA Tunnel Detection Details, and security-metadata-streaming.]

DNS Tunnel Detection

Starting in Junos OS Release 21.2R1, Juniper ATP Cloud supports DNS tunnel detection. DNS Tunneling is a cyber-attack method that encodes the data of malicious programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beaconing.

Use the `set security-metadata-streaming policy` *`policy-name`* `detections tunneling` command at the `[edit services]` hierarchy to configure DNS tunneling detections.

To view the list of DNS tunnel detections on SRX Series Firewalls, log in to Juniper ATP Cloud Web portal, navigate to **Monitor > DNS** and click **Tunnel** tab.

[See DNS Tunnel Detection Overview, DNS DGA Tunnel Detection Details, and security-metadata-streaming.]

SSO with SAML 2.0

Juniper ATP Cloud supports Single sign-on (SSO) with SAML 2.0 protocol. SSO is an authentication method that allows you to securely log in to multiple applications and websites with a single set of login credentials.

You can now configure the SSO settings to sign into the ATP Cloud Web portal using an external Identity Provider (IdP), such as Okta and Microsoft Azure that supports SSO using SAML 2.0 protocol. To configure, activate, or deactivate SSO settings, log in to Juniper ATP Cloud Web portal and navigate to **Administration > SSO Settings** page.

[See Set Up Single Sign-on with SAML 2.0 Identity Provider and Configure SSO Settings.]

March, 2021 Release

IN THIS SECTION

New and Changed Features: March, 2021

Server Message Block (SMB) protocol support for file inspection

Starting in Junos OS Release 21.1R1, SRX Series Firewalls support the Server Message Block (SMB) protocol in advanced anti-malware (AAMW) file inspection. Users and applications can use the SMB protocol to access files and other resources on a remote server. Navigate to **Monitor > File Scanning > SMB File Downloads** in the Juniper ATP Cloud UI to view the list of files downloaded by hosts for SMB protocol inspection.

[See SMB File Download Overview, SMB File Download Details, advanced-anti-malware policy, and show services advanced-anti-malware statistics.]

Support for username feed type in adaptive threat profiling feeds

Starting in Junos OS Release 21.1R1, you can add user the source identity (username) feed type to adaptive threat profiling feeds. Navigate to **Configure > Threat Profiling** in the Juniper ATP Cloud UI to configure adaptive threat profiling feed.

[See Adaptive Threat Profiling Overview , Create an Adaptive Threat Profiling Feed, security-intelligence (security policies), and show services security-intelligence.]

Audit logs

You can now view audit logs for login activity and specific tasks that are completed successfully using the ATP Cloud Web portal. Audit log entries include details about user-initiated tasks, such as the username, task name, task details, and date and time of execution of the task. You can view audit logs for a specific time span, search for and filter for audit logs, and export audit logs in comma-separated values (CSV) format. The retention period for audit logs is five years.

[See Viewing Audit Logs.]

Virtual routing and forwarding (VRF) behavior for adaptive threat profiling feeds

In earlier releases, malware and CC submissions from all VRF instances under root logical domain were accepted even though they were not associated with the sub-realm. From this release onwards, you can see similar behavioral change for adaptive threat profiling feeds as well. Feeds from SRX Series Firewalls are accepted for all VRF instances under the root logical domain even though they are not associated with any sub-realm.

January, 2021 Release

IN THIS SECTION

New and Changed Features: January, 2021

Support for filtering DNS requests for disallowed domains (SRX4100, SRX4200, SRX4600, and vSRX)

Starting in Junos OS Release 20.4R1, you can configure DNS filtering to identify DNS requests for disallowed domains. You can either:

- Block access to the domain by sending a DNS response that contains the IP address or fully qualified domain name (FQDN) of a DNS sinkhole server. This ensures that when the client attempts to send traffic to the disallowed domain, the traffic instead goes to the sinkhole server.
- Log the DNS request and reject access.

[See DNS Sinkhole, dns-filtering, security-intelligence(services), clear services security-intelligence dns-statistics, and show services security-intelligence dns-statistics.]

Enhancements to adaptive threat profiling feed

You can now directly exclude specific feed entries (IP addresses) from the threat profiling feed.

[See Adaptive Threat Profiling Overview.]

Inclusion and Diversity (I&D) terminology updates

We have changed some of the terminologies in the Juniper ATP Cloud GUI and documentation. The changed terms represent the inclusion and diversity principles we value.

[See Creating Allowlists and Blocklists.]

Support for TLS version 1.3

We now support Transport Layer Security (TLS) version 1.3 for encrypted traffic insights feature.

Release 2020

IN THIS SECTION

October, 2020 Release

IN THIS SECTION

New and Changed Feature: October, 2020

Support to integrate AWS GuardDuty with vSRX Firewalls

Starting with Junos OS Release 20.3R1, we support threat feeds from Amazon Web Services (AWS) GuardDuty. The threats are sent as a security feed to the vSRX firewalls in the AWS environment. The vSRX firewalls can access the feeds either by directly downloading it from the AWS S3 bucket or, if the vSRX firewall is enrolled with Juniper ATP Cloud, the feed is pushed to the firewall device along with the security intelligence (SecIntel) feeds.

[See Integrate AWS GuardDuty with vSRX Firewalls.]

September, 2020 Release

IN THIS SECTION

New and Changed Features: September, 2020

Support to add adaptive threat profiling feed to infected host feed

You can now add adaptive threat profiling feed content, such as source IP address or destination IP address, to the infected host feed.

[See Adaptive Threat Profiling Overview and Create an Adaptive Threat Profiling Feed.]

Increase in maximum number of feeds per category for adaptive threat profiling

You can now create up to 64 feeds per category for adaptive threat profiling feeds. Based on your requirement, you can choose to add all 64 feeds to infected host feeds.

[See Create an Adaptive Threat Profiling Feed.]

Support to retain malicious file samples

After analyzing malicious file samples, we now retain them for further investigation. For more information, please refer to Juniper ATP Cloud Privacy Policy Supplement.

Support to Integrate Mist with vSRX Firewalls

You can enable Mist integration with ATP Cloud to share the threat alerts detected by Juniper SRX Series firewalls and Juniper ATP Cloud with Mist customers.

[See Enable Mist Integration with Juniper ATP Cloud.]

SecIntel Feeds

We have renamed the Third-party Threat Feeds menu to SecIntel Feeds in Juniper ATP Cloud Web portal. To view SecIntel feeds, navigate to **Configure > SecIntel in Juniper ATP Cloud Web** portal. You can now view Juniper SecIntel feeds (Command and Control Feed, Attacker IP Feed, GeoIP Feed, and Infected Host Feed) that are available for ATP Cloud license.

Note that the Infected Host feed is enabled by default for all license tiers. All other Juniper SecIntel feeds are enabled by default with a premium license.

[See SecIntel Feeds Overview and Juniper Threat Feeds Overview.]

Change in Whitelist and Blacklist pages

We have separated the IP and URL tabs in the Whitelist and Blacklist pages.

[See Creating Allowlists and Blocklists.]

Encrypted Traffic Insights

Starting with this release, we have renamed Encrypted Traffic Analysis menu to Encrypted Traffic Insights.

[See Encrypted Traffic Insights Overview.]

Reports

We have changed the terminology Infected Hosts to Hosts with Malicious Activities in the Threat Assessment reports.

[See Reports Overview.]

Rebranding ATP

Juniper Sky™ Advanced Threat Prevention (Juniper Sky ATP) is now Juniper® Advanced Threat Prevention Cloud (Juniper ATP Cloud).

June, 2020 Release

IN THIS SECTION

New and Changed Features: June, 2020

Adaptive Threat Profiling

Adaptive threat profiling enables SRX Series Firewalls to generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events. You can generate adaptive threat profiling feeds with traditional policies, unified policies with application identification (AppID) or URL-based match criteria, and IDP. Navigate to **Configure > Threat Profiling** in the Juniper Sky ATP UI to configure adaptive threat profiling.

[See Adaptive Threat Profiling Overview and Create an Adaptive Threat Profiling Feed.]

Encrypted Traffic Analysis

You can use encrypted traffic analysis to detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic. Navigate to **Monitor > Encrypted Traffic** in the Juniper Sky ATP UI to view detections based on encrypted traffic analysis. To configure encrypted traffic analysis, use the security-metadata-streaming command at [edit services] hierarchy level. Use the show services security-metadata-streaming statistics command to view the statistics of the sessions.

[See Encrypted Traffic Insights Overview and Encrypted Traffic Insights Details.]

Enhancements to VRF Workflow

You can associate Virtual Routing and Forwarding (VRF) to sub-realms only after clearing or resolving the infected host feed list in the managed security service provider (MSSP) feeds for all devices. This is to avoid any overlapping IP addresses that may have come through from submissions or CC hits of root-logical-system VRFs (if any) in the MSSP realm. Starting in Junos OS Release 20.2R1, all submissions and CC hits from any VRFs under root logical system are allowed. This behavior was not supported in Junos OS Release 19.4R1.

Realm Recovery

You can recover realm names using the following methods:

- When you create a new realm, an e-mail is sent to your registered e-mail address. The e-mail contains the realm name, which you can save for future use.
- Click the Forgot Realm link on the Juniper Sky ATP login page and enter your registered realm creator e-mail address. You will receive an e-mail with the list of realm names that are associated with your e-mail address.

[See Recover Realm Name.]

URLhaus as a Third-Party Feed

Juniper Sky ATP UI supports URLhaus as a third-party feed. URLhaus is a threat intelligence feed that shares malicious URLs that are used for malware distribution. Log in to the Juniper Sky ATP UI and navigate to **Configure > Third Party Feeds** to enable the URLhaus feed.

[See SecIntel Feeds Overview.]

April, 2020 Release

IN THIS SECTION

New and Changed Features: April, 2020

New Platform Support

Junos OS Release 20.1R1 supports Juniper Sky ATP on SRX380 device. Please refer to the Supported Platforms Guide for details.

Default Settings for SMTP and IMAP

The default setting for SMTP and IMAP for the new realms is “permit”.

Change in Default Threat Level

The default threat level for HTTP file downloads and e-mail attachments is changed from 4 to 7.

Enhancements to Monthly Reports

The monthly reports now include the following additional information:

- Devices expiring in the next 60 days
- Devices that have not submitted files to the Sky ATP in the past 30 days.

January, 2020 Release

IN THIS SECTION

New and Changed Features: January, 2020

Virtual Routing and Forwarding (VRF)

Juniper Sky ATP now supports multiple virtual routing and forwarding (VRF) instances per logical domain. The VRF instance name or ID is unique for each logical domain and is used to uniquely identify the infected hosts. Each virtual instance:logical domain combination is unique and can be assigned to a

sub-realm in Juniper Sky ATP. The user or a managed security service provider (MSSP) maps that combination to a corresponding realm.

[See Flow Management in SRX Series Firewalls Using VRF Routing Instance, Configuring Security Policies for a VRF Routing Instance, and Configuring Security Policies Using VRF Group.]

Third-Party URL Feeds

You can now enable URL feeds for third parties in the Juniper Sky ATP Web UI. Navigate to **Configure > Third Party Feeds > URL Feeds** and enable the URL feeds.

[See SecIntel Feeds Overview.]

Detailed Threat Information in E-Mails

The Juniper Sky ATP alert e-mail for an infected host now includes the source and destination hostnames or IP addresses, threat level, details of the downloaded file, and the login URL to check the details.

Release 2019

IN THIS SECTION

November, 2019 Release

IN THIS SECTION

New and Changed Feature: November, 2019

Enhanced Email Alerts

These alerts now include more detailed information and improved formatting.

September, 2019 Release

IN THIS SECTION

New and Changed Features: September, 2019

Automatically Expire Blocked Hosts

In the Juniper Sky ATP Web UI, you can navigate to **Configure>Global Configuration>Infected Hosts** to set an expiration time, based on IP address and threat level, for hosts marked as infected. After the designated time-frame, all hosts or a range of IP addresses are no longer blocked. This is useful if your network allocates new IP addresses on a regular schedule using DHCP.

[See Configuration for Infected Hosts.]

Enhanced Static Detection of IOT Malware

The ELF (Executable and Linkable Format) file type is now supported for static analysis using machine learning and is automatically included in the **Executable** category under **File Inspection Profiles.**

Alternative Enrollment Procedure

Starting in Junos OS Release 19.3R1, there is now an alternative onboarding procedure you can use to perform all enrollment steps using the CLI on the SRX Series Firewall without having to access the Sky ATP Web Portal. Run the “request services advanced-anti- malware enroll” command on the SRX Series device to begin the process. Both the original enrollment process that obtains an op script from the Web Portal and the new CLI-only enroll process are valid procedures. Use either one.

[See Configuration for Infected Hosts.]

Block File with Unknown Verdict and Send User Notification on Block

Starting in Junos OS Release 19.3R1, for advanced anti-malware policies, you can now block a file when the verdict is unknown. You can also send a user notification when a block occurs. We’ve introduced the following new commands (for example): “set services advanced-anti-malware policy p1 http file-verdict-unknown (block|permit)” and “set services advanced-anti-malware policy p1 http client-notify (message|file|redirect-URL)”.

[See Enroll an SRX Series Firewall with the CLI.]

July, 2019 Release

IN THIS SECTION

New and Changed Features: July, 2019

Report Generation

In the Juniper Sky ATP Web UI, you can navigate to Reports>Report Definitions to configure threat assessment reports to be run on-demand or on scheduled intervals. Scheduled reports can run daily, weekly, or monthly and can be automatically emailed as PDF files to designated recipients.

[See Reports Overview.]

Security Intelligence HTTPS and SNI Support

Starting in Junos OS Release 19.2R1, SRX Series Firewalls support inspection of encrypted traffic (HTTPS) in security-intelligence policies. Server name identification (SNI) checks are also supported. Note that these changes do not introduce any new CLI commands. All existing commands and configurations can make use of this expanded functionality.

March, 2019 Release

IN THIS SECTION

New and Changed Feature: March, 2019

Multi-Factor Authentication for Administrators

Multi-Factor Authentication requires a user to pass at least two different types of authentication before gaining access to a requested page. Juniper Sky ATP lets you configure multi-factor authentication (over SMS or Email) for administrators who are logging into the Juniper Sky ATP Web UI. This is an optional setting that when enabled, applies globally to all administrators in a realm.

[See Configure Multi-Factor Authentication for Administrators.]

January, 2019 Release

IN THIS SECTION

New and Changed Features: January, 2019

Tenant System (TSYS) Support

Starting in Junos OS Release 18.4R1, SRX Series Firewalls support tenant systems for anti-malware and security-intelligence policies. When you associate a tenant system with a realm in Juniper Sky ATP, that tenant system receives the threat management features configured for the realm. The SRX Series Firewall will then perform policy enforcement based on tenant system and the associated Juniper Sky ATP realm.

[See Tenant Systems: Security-Intelligence and Anti-Malware Policies.]

Realm Management

From the **Configure > Global Configuration > Realm Management** page, you can attach realms to the current realm and associate devices with realms. When an SRX Series Firewall enrolls to Sky ATP, all associated tenant systems are also enrolled. The SRX Series Firewall can then perform policy enforcement based on tenant system and an associated Juniper Sky ATP realm.

[See Realm Overview.]

Release 2018

IN THIS SECTION

December, 2018 Release

IN THIS SECTION

New and Changed Features: December, 2018

Whitelist Command and Control Servers

You can now whitelist C&C servers by entering an IP address or hostname in the **Configure > Whitelist > C&C Server** page. This information is then sent to the SRX Series Firewall to be excluded from any security intelligence blacklists or C&C feeds (both Juniper's global threat feed and third party feeds). You can also whitelist C&C servers directly from the C&C Monitoring page details view.

[See Creating Allowlists and Blocklists.]

November, 2018 Release

IN THIS SECTION

New and Changed Feature: November, 2018

Support for Deep Analysis and Sandboxing

There is now support for deep analysis and sandboxing for Mac OS X Mach-O, PKG and DMG file types (in US and EU regions). These files are automatically included in existing file inspection profile categories.

September, 2018 Release

IN THIS SECTION

New and Changed Features: September, 2018

Added Platform Support

Junos OS 18.3R1 adds support for the following SRX Series Firewalls: SRX320 and SRX300.

See Juniper Sky Advanced Threat Prevention Supported Platforms Guide for details.

Enhancement in the Threat Level of a Host

A fine adjustment was made to the threat level of a host for more proper and accurate detection. (Some customers may want to change their global configurations as a result of this change.)

June, 2018 Release

IN THIS SECTION

New and Changed Features: June, 2018

Unified Policy support

(Support starting in Junos OS 18.2R1) Unified policies allow you to use dynamic applications as one of the policy match criteria rules in each application. Application identification (AppID) is applied on the traffic, and the application is identified after several packets are checked. The **set services security-intelligence default-policy** and **set services advanced-anti-malware default-policy** commands are introduced to create default policies.

During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list, which contains different security intelligence or anti-malware policies, the SRX Series Firewall applies the default policy until a more explicit match has occurred.

Explicit Web Proxy Support

(Support starting in Junos OS 18.2R1) This is configured using the set services proxy profile command on the SRX Series Firewall. To configure HTTP(S) connections to use a web proxy, you create one or more proxy profiles and refer to those profiles in your anti-malware and security intelligence policies. When using a web proxy, you must enroll your SRX Series Firewalls to Sky ATP using a slightly different process.

[See Explicit Web Proxy Support.]

File Scanning PDF Reports

You can now download PDF reports from the HTTP File Downloads, Details page. Navigate to **File Scanning > HTTP File Downloads** and click on a file hash from the list. At the top of the **Details** page, click the **Download PDF Report** link.

April, 2018 Release

IN THIS SECTION

New and Changed Features: April, 2018

IPv6 support

IPv6 addresses are now supported for all Juniper Sky ATP features including Command and Control, Blacklist, Whitelist, IP filtering, and GeoIP feeds. Note that references to “IPv4” in open API calls have changed to “IP.” This may impact your current API configurations.

Office365 feed

Push Microsoft Office 365 services endpoint information to the SRX Series Firewall for use in security policies. The office365 feed works differently from other third-party feeds and requires specific configuration parameters, including a pre-defined name of “ipfilter_office365.” Enable the Office365 feed on Juniper Sky ATP through **Configure > Third Party Feeds**.

User Notification of Infected Hosts

This is configured using the CLI on the SRX Series Firewall (support starting in Junos OS 18.1R1). During the processing of a session IP address, if the IP address is on the infected hosts list and HTTP traffic is using ports 80 or 8080, infected hosts HTTP redirection to a specified URL can be configured.

[See Juniper Advanced Threat Prevention Cloud CLI Reference Guide.]

March, 2018 Release

IN THIS SECTION

New and Changed Features: March, 2018

Support added for APAC and Canada Web Portal locations.

Host names vary by location as described in the following table:

Table 4: Support for APAC and Canada Web Portal locations

Location	Juniper Sky ATP URL
United States	Customer Portal: https://amer.sky.junipersecurity.net Open API (infected hosts, whitelist/blacklist, sample submission): https://api.sky.junipersecurity.net Open API (threat intelligence): https://threat-api.sky.junipersecurity.net
European Union	Customer Portal: https://euapac.sky.junipersecurity.net Open API (infected hosts, whitelist/blacklist, sample submission): https://api-eu.sky.junipersecurity.net Open API (threat intelligence): https://threat-api.sky.junipersecurity.net
APAC	Customer Portal: https://apac.sky.junipersecurity.net Open API (infected hosts, whitelist/blacklist, sample submission): https://api-apac.sky.junipersecurity.net Open API (threat intelligence): https://threat-api-apac.sky.junipersecurity.net

Table 4: Support for APAC and Canada Web Portal locations *(Continued)*

Location	Juniper Sky ATP URL
Canada	Customer Portal: https://canada.sky.junipersecurity.net Open API (infected hosts, whitelist/blacklist, sample submission): https://api-canada.sky.junipersecurity.net Open API (threat intelligence): https://threat-api-canada.sky.junipersecurity.net

Hash File Support

Hash files are now supported for blacklist and whitelist file scanning. A hash is a unique signature for a file generated by an algorithm. You can add custom whitelist and blacklist hashes for filtering by listing them in a text file, with each entry on a single line, and uploading the file. Configure this through **Configure > File Inspection Management > Whitelists or Blacklists**. Click the **Hash File** tab.

Telemetry Data

(Support starting in Junos OS 17.4R1) The Telemetry page, located under **Monitor > Telemetry > Web Protocols or Email Protocols**, provides comprehensive monitoring information of devices for a variety of activities, including the number of web and email files scanned or blocked on a per protocol basis.

Role-Based Access Control

When you create or edit users on the Web Portal, you can assign a role to each user to determine his or her level of access to configurations. Available roles are System Administrator, Operator, and Observer. Access the **Role Assignment** pulldown field from **Administration > Users**. Then select a user to edit or click + to add a new user and select the role from the available pulldown field.

Release 2017

IN THIS SECTION

December, 2017 Release

IN THIS SECTION

New and Changed Feature: December, 2017

Trusted Proxy Servers

Juniper Sky ATP now supports the addition of a list of trusted proxy server IP addresses. (support starting in Junos OS 17.4R1). When you add trusted proxy servers IP addresses to the list in Juniper Sky ATP, by matching this list with the IP addresses in the HTTP header (X-Forwarded- For field) for requests sent from the SRX Series Firewalls, Juniper Sky ATP can determine the originating IP address. Configure this through the **Configure > Global Configuration > Proxy Servers** window.

November, 2017 Release

IN THIS SECTION

New and Changed Feature: November, 2017

IMAP Email Scanning

Juniper Sky ATP now supports IMAP email management. Enrolled SRX devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Juniper Sky ATP assigns the file a threat score between 0-10 with 10 being the most malicious. Configure this through the **Configure > Email Management > IMAP** window.

October, 2017 Release

IN THIS SECTION

New and Changed Feature: October, 2017

External threat feeds

You can now enable external feeds for integration with Juniper Sky ATP through the **Configure > Threat Intelligence Feeds** window. For each feed, click the Details link to view information, including the contents of the feed. For more information, see the GUI online help.

Download malware files

A Download Zipped File option lets you download quarantined malware (as a password-protected zip file) for analysis. You can access this option from both the Email attachment scanning details page and the HTTP file download details page. For more information, see the GUI online help.

September, 2017 Release

IN THIS SECTION

New and Changed Features: September, 2017

Password reset

If you forget your password to login to the Juniper Sky ATP dashboard, you can reset it when you click **Forgot Password** from the Juniper Sky ATP login screen. An email with a link for resetting your password is sent to the address associated with your account. For more information, see the GUI online help.

Feed-based URL redirection

The set services security-intelligence profile CLI command now has a feed- name option that lets you perform an action based on feeds, such as URL redirection.

[See security-intelligence(services).]

May, 2017 Release

IN THIS SECTION

New and Changed Features: May, 2017

Basic (threat feeds only) license

A basic service level is available and adds filters using the following threat feed types: Command and Control, GeoIP, custom filtering and threat intel feeds. With the basic license, there is no file processing or advanced malware protection.

Customer feedback

An option is available on the toolbar for providing feedback to improve the product usability.

IP Filter Open APIs

APIs to update the IP Filter feeds.

[See Threat Intelligence Open API Setup Guide.]

Infected Host Open APIs

APIs to update the infected host feeds.

[See Threat Intelligence Open API Setup Guide.]

MAC address

For use by Policy Enforcer customers, this field (in the Host Details page) displays the host MAC address.

Editable host identifier

Juniper Sky ATP will generate and assign an identifier to the host that is editable in the Host Details pages. Any change to the host identifier will be reflected in the C&C Server Details page, Host details page, and File Scanning Details page.

April, 2017 Release

IN THIS SECTION

New and Changed Features: April, 2017

Logging

Logging options are now available in the Global Configuration window (**Configure > Global Configuration**) to configure syslog event types.

License expiration

A column is added to the Enrolled Devices table that displays the license expiration date for that device.

C&C Blocked by

A Blocked Via column is added to the C&C Servers window (**Monitor > C&C Servers**) that displays the feed name that blocked that server.

March, 2017 Release

IN THIS SECTION

New and Changed Features: March, 2017

SMTP E-Mail attachments

An E-Mail Management window is added to the Configure menu to inspect and management e-mail attachments sent over SMTP.

See the Juniper Sky Advanced Threat Prevention Supported Platforms Guide for information on supported platforms.

File Scan details

The Behavior Analysis tab now shows a Behaviors by Severity illustration to provide a quick overview of what the malware is targeting.

File Scan details

A Behavior Details tab is added to the File Scan details page, providing information on what the file did when it was opened in the sandbox.

Printable View

A Printable View link is added to the File Scan details page, allowing you to print the general and network activity information to a PDF file or to a local or network printer.

February, 2017 Release

IN THIS SECTION

New and Changed Feature: February, 2017

Windows 10 support

Sandboxing now supports the Windows 10 operating system.

See the Juniper Sky Advanced Threat Prevention Supported Platforms Guide for information on supported OS versions.

January, 2017 Release

IN THIS SECTION

New and Changed Feature: January, 2017

File Scan details

Enhancements have been made to the file scan details page, providing more details on the threat and network activity.

Release 2016

IN THIS SECTION

December, 2016 Release

IN THIS SECTION

New and Changed Features: December, 2016

SYSLOG support

Malware and host status SYSLOG messages are now created.

See the Juniper Sky Advanced Threat Prevention Supported Platforms Guide for information on supported versions of JSA and QRadar SIEM.

URL-based lists

Support for both URL-based and IP-based C&C, blacklist and whitelists.

Security Director 16.1 support

Juniper Sky ATP now supports SD 16.1 and later releases. For more information on using Juniper Sky ATP in SD, see the SD online help.

November, 2016 Release

IN THIS SECTION

New and Changed Feature: November, 2016

Android file types

Android operating system, and the APK (Android application package) file type are now supported.

October, 2016 Release

IN THIS SECTION

New and Changed Features: October, 2016

C&C server details

Click an IP address in the C&C servers table (**Monitor > C&C Servers**) to view more information about that C&C server, such as hosts that have contacted that server, associated domains, etc.

New platform support

Junos OS Release 15.1X49-D65 now supports Juniper Sky ATP running on SRX4100 and SRX4200. See the Supported Platforms Guide for a complete list of supported platforms.

September, 2016 Release

IN THIS SECTION

New and Changed Features: September, 2016

New platform support

Junos OS Release 15.1X49-D60 and later releases support Juniper Sky ATP running on the SRX340, SRX345 and SRX550M devices and vSRX instances, in addition to existing support for SRX1500, SRX5400, SRX5600 and SRX5800 devices.

Reporting false positives

An option to report false positives and false negatives is added to the file scanning details page and to the C&C page.

RESTful APIs

RESTful APIs are now available to provide:

- Custom feed support for C&C
- Custom whitelists and blacklists for malware detection.
- Hash submission and file submission

July, 2016 Release

IN THIS SECTION

New and Changed Features: July, 2016

Hide number of rows

Tables (for example, File Scanning and Hosts) no longer display the number of returned rows at the bottom of the table.

File scanning table updates

Select **Monitor > File Scanning**. The following changes have been made:

- Threat level legend—A color-coded threat level legend is added to the top of the file scanning table to easily identify the threat levels of files listed in the table.
- Hide scans with lower threat level—By default, only files with a threat level of 4 or higher are now displayed in the file scanning table. To view all files, click **Clear All** located in the upper-right corner of the table or click the close icon (x) next to threat_level ge 4. To return to the default view, click **File Scanning** in the left pane to refresh the window.
- Rename Device Serial Number—Click a file signature to view file scanning details. In the Hosts That Have Downloaded File table, the *Device Serial Number* column is changed to *Device Name*. Clicking a device name in the table continues to show details of that particular device.
- Filter by threat level—A numeric filter has been added to allow you to display rows by threat level. This option is also available in the Hosts table (Select **Monitor > Hosts**) for the Threat Level, C&C Hits, and Malware Hits columns.

Policy override for this host menu

Select **Monitor > Hosts** and then click a host in the table to view detailed host information. The *Blocking setting for this host* pulldown menu is changed to *Policy override for this host*, and the new options are:

- Use configured policy (included in infected host feeds)
- Always include host in infected host feeds
- Never include host in infected host feeds

Reorder host details page

When you view detailed host information (select **Monitor > Hosts** and then click a host in the table), the current threat table is now reordered to show the most recent event at the top of the table.

June, 2016 Release

IN THIS SECTION

New and Changed Features: June, 2016

Manually upload files for inspection

You can now manually upload suspicious files to the cloud for malware inspection. For more information, see the Web GUI tooltips (click the question marks (?) to view the tooltips) and online Help.

Download file scanning activity

A report of scanned files and their results can be downloaded to an Excel spreadsheet. For more information, see the Web GUI tooltips (click the question marks (?) to view the tooltips) and online Help.

Support for SRX5400, SRX5600, and SRX5800

Junos OS Release 15.1X49-D50 and later releases support Juniper Sky Advanced Threat Prevention running on SRX5400, SRX5600 and SRX5800 devices.

Full support for IDP and Juniper Sky Advanced Threat Prevention

Full support for Juniper Sky Advanced Threat Protection inline blocking and IDP configured together in the same security policy is provided in Junos OS Release 15.1X49-D50 and later releases.

Additional command & control information

The Web GUI C&C page now lists the external server hostname and the category for which the server is classified as a C&C server.

Efficacy improvements

Resolved Issues

June 2020

- SATP-473 – Since Ransomware Tracker is deprecated, ransomware tracker IP feeds are not supported on Juniper Sky ATP. The option to enable these feeds has been removed from Juniper Sky ATP UI. If you had enabled the Ransomware Tracker feed earlier, you might stop receiving this feed.
- SATP-117 – Unable to search devices on Realm Management page.

September 2019

- PR 1457400 and PR 1456736 – Host in infected hosts feed was being auto-resolved and removed from feed with no manual intervention.

July 2019

- PR1352313 – The Juniper Sky ATP Web Portal does not display the OS version and device name for vSRX

December 2018

- PR1402190 – IPv6 addresses were not being correctly added to blacklist feeds.
- PR1351544 – Tool tips for third party feeds were not appearing when clicking on the “?” in the Sky ATP Web UI.
- PR1356443 – The modify profile screen contained errors in the file categories description.
- PR1380649 – The command and control server details page duplicated the threat summary, total hits, protocols & ports fields when clicking on the time range links.

November 2018

- PR1383886 – In some instances, malicious SMTP attachments were not detected correctly.
- PR1367466 – With X-Forwarded-For (XFF) enabled on the proxy server, Sky ATP populated the portal with the proxy IP address instead of the host IP address.

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 22.2R1 for Juniper ATP Cloud.

- Starting with Junos OS Release 18.2R2 onwards, if advanced-anti-malware configuration is enabled in a security policy in Block mode, the SMB network traffic throughput can decrease significantly. To avoid this, we recommend that you configure the policy application as HTTP, HTTPS, SMTP, SMTPS, IMAP, or IMAPS. [PR1515053]

- After you change the revocation configuration of a CA profile, the change cannot be populated to the revocation check of the SSL. Change the SSL configuration to enable or disable CRL checking instead of using a ca-profile configuration. [PR1143462]

- For an SRX1500 device in chassis cluster mode, if you disable and re-enable certificate revocation list (CRL) checking of certificate validity, the system does not re-enable CRL checking. You must reboot the SRX1500 Services Gateway before to re-enable CRL checking. [PR1144280]

- If you select the Permit action in the Configure > Email Management > SMTP window, e-mails with attachments are sent directly to the recipients while the attachments are sent to the cloud for analysis. If system constraints such as memory issues and cloud connectivity issues occur while the attachment is sent to the cloud, the fallback condition is supposed to be used. However, the Permit action overrides the fallback action. For example, if your fallback condition is Block, the Permit action as configured in the Web GUI is used. [PR1239650]

- A file submission timeout can occur on the SRX Series Firewall when the following conditions are present:

  - The advanced anti-malware (AAMW) service is enabled.
  - SMTP or SMTPS is configured in the AAMW policy.
  - The fallback action is Permit.
  - Long network latency exists between the SRX Series Firewall and the Juniper ATP Cloud service.

  Under these circumstances, the e-mail remains in the sender's outbox and the recipient never receives the e-mail.

  As a workaround, try to resolve the long latency issue between the SRX Series Firewall and the Juniper ATP Cloud service. If this is not possible, increase the server timeout setting in the recipient's Outlook. [PR1254088]

- When the AAMW service is enabled and SMTP inspection is configured in the AAMW policy, SMTP e-mails that are encoded with the uuencode mechanism cannot be decoded or identified, and are not inspected for malware by the Juniper ATP Cloud service. [PR1236721]

- AAMW sessions always use the AAMW parameters that were configured when the session was established. Configuration changes do not retroactively affect sessions that are already established. For example, a session that is established when the verdict threshold is 5 will always have 5 as the threshold even if the verdict threshold changes to other values during that session's lifetime. [PR1270751]

- When you select the Deliver malicious messages with warning headers added option, Juniper ATP Cloud adds headers to e-mails that most mail servers will recognize and filter into spam or junk folders. However, some SMTP servers do not recognize the added headers and might reject these e-mails. [PR1281987]

- If UTM IMAP and AAMW IMAP are configured in the same policy, AAMW does not inspect the e-mail attachment. [PR1275002]

- If you are upgrading from Junos 15.1X4 9-D110 or earlier, and you select the `no validate` option, the Network Security Daemon (NSD) might not function properly. This could result in other issues. For instance, If you configure a `block close http` *`file`* in a security intelligence policy the system software validation might fail. For example:

  ```
  set services security-intelligence profile CC_SERVER rule Rule-2 then action block close http file
  secintel_default_page.html
  ```

  As a workaround, you deactivate the SecIntel service redirect configuration before upgrading from Junos 15.1X4 9-D110 or earlier:

  ```
  deactivate services security-intelligence profile CC_SERVER rule Rule-2 then action block close http
  ```

  [PR1315593]

- For certain actions for inspection profiles, the eicar.exe file is permitted instead of taking the configured actions. This applies to HTTP and SMTP. The inspection profile eicar.exe file is permitted instead of being blocked for HTTP and tag-and-deliver for SMTP. [PR1317897]