Juniper Advanced Threat Prevention Cloud New Features

This document describes the new features introduced in Juniper Advanced Threat Prevention Cloud.

Please refer to the Supported Platforms Guide for feature support details on various SRX Series devices.

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 Request Filtering for Disallowed Domains, dns-filtering, security-intelligence, 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.

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

- 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 Add Threat Feed for Adaptive Threat Profiling.]
- 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 Add Threat Feed for Adaptive Threat Profiling.]
- 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 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 SecIntel 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

- Adaptive Threat Profiling—Adaptive threat profiling enables SRX Series devices 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 Add Threat Feed for Adaptive Threat Profiling.]
- 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 Analysis Overview and Encrypted Traffic Analysis 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 Enabling Third Party Threat Feeds.]

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

- 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 VRF Routing Instance in SRX Series Devices, 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 the Juniper Sky Advanced Threat Prevention Administration Guide.
- 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.

November 2019

- Enhanced Email Alerts— These alerts now include more detailed information and improved formatting.

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 the Administration Guide for details.
- 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 device 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 the Administration Guide for details.
- 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 the CLI Reference Guide for details.
- Resolved Issues

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 the Administration Guide for details.
- Security Intelligence HTTPS and SNI Support— Starting in Junos OS Release 19.2R1, SRX Series devices 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.
- Resolved Issues

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 the Administration Guide for details.

January 2019

- Tenant System (TSYS) Support—Starting in Junos OS Release 18.4R1, SRX Series devices 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 device will then perform policy enforcement based on tenant system and the associated Juniper Sky ATP realm. See the Administration Guide for details.
- 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 device enrolls to Sky ATP, all associated tenant systems are also enrolled. The SRX Series device can then perform policy enforcement based on tenant system and an associated Juniper Sky ATP realm. See the Administration Guide for details.

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 device 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 the Administration Guide for details.
- Resolved issues

November 2018

- 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.
- Resolved issues

September 2018

- Added Platform Support—Junos OS 18.3R1 adds support for the following SRX Series Devices: SRX320 and SRX300. Please refer to the Supported Platforms Guide for details.
- 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

- 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 device 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 device. 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 devices to Sky ATP using a slightly different process. See the Administration Guide for details.
- 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

- 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 device 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 device (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 the ‘set services security-intelligence’ command in the Juniper Sky ATP CLI Reference Guide.

March 2018

- Support added for APAC and Canada Web Portal locations. Host names vary by location as described in the following table:

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
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.

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 devices, Juniper Sky ATP can determine the originating IP address. Configure this through the **Configure > Global Configuration > Proxy Servers** window.

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

- 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

- 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. For more information, see set services security-intelligence.

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 for more information.
- Infected Host Open APIs—APIs to update the infected host feeds. See Threat Intelligence Open API Setup Guide for more information.
- 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

- 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

- 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 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

- Windows 10 support—Sandboxing now supports the Windows 10 operating system. See the Supported Platforms Guide for information on supported OS versions.

January 2017

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

December 2016

- SYSLOG support—Malware and host status SYSLOG messages are now created. See the 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

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

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.

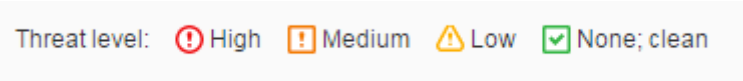
- New platform support—Junos OS Release 15.1X49-D65 now supports Juniper Sky ATP running on SRX4100 and SRX4200. See the Supported Platforms Guide for a complete list of supported platforms.

September 2016

- 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

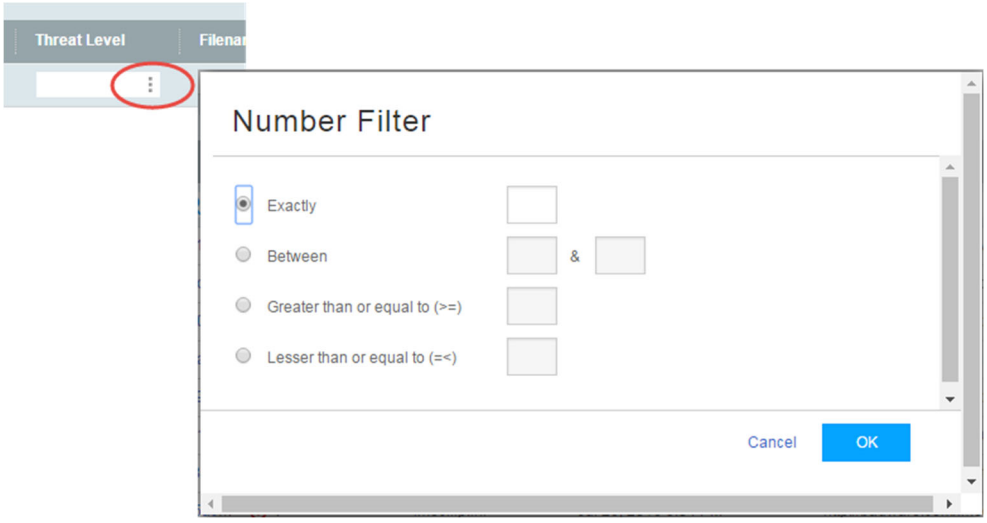
- Hide number of rows—Tables (for example, File Scanning and Hosts) no longer display the number of returned rows at the bottom of the table.
- File scanning table updates—Select **Monitor > File Scanning**. The following changes have been made:
  - Threat level legend—A color-coded threat level legend 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

- 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.