Release Notes

Juniper Secure Edge

SOFTWARE HIGHLIGHTS

- Delivers full-stack Security Service Edge (SSE) features such as Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Application Visibility and Control, Advanced Threat Prevention, and Intrusion Prevention System from the cloud, providing users anywhere with fast, reliable, secure access to their applications and resources on the Internet.

- Provides a cloud-delivered explicit proxy service.

- Supports IPsec and GRE tunneling from customer premises equipment including SD-WAN devices.

- Integrates with customer's identity sources through SAML and LDAP protocols.

- Enables administrators to manage all their security deployments such as cloud delivered security, cloud-based security, and on premises security from a single user interface.

- Quick Start: Use this new setup guide to get your Juniper Security Edge up and running in three quick steps.

JUNIPer NETWORKS | Engineering Simplicity

Table of Contents

Introduction

Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by Juniper Security Director Cloud.

Juniper Secure Edge empowers organizations to secure their workforce wherever they are. With consistent security policies that follow the user, device, and application without having to copy over or re-create rule sets, Juniper Secure Edge makes it easy to deploy cloud-delivered application control, intrusion prevention, content and Web filtering, and effective threat prevention without breaking the visibility or security enforcement.

Before You Begin

IN THIS SECTION

- Supported Browsers | **1**
- Supported Operating Systems | **1**

Supported Browsers

You can view Juniper Secure Edge best on the following browsers:

- Google Chrome version 88 and later

- Mozilla Firefox version 83 and later

- Safari version 14 and later

- Microsoft Edge

Supported Operating Systems

Juniper Secure Edge supports the following operating systems:

- Microsoft Windows

- macOS

- iOS

- Android Clients

Release 2024

October 23, 2024 Release

Secure Edge New Features: October 23, 2024

Identity

Authentication settings—You can now set the authentication frequency for a specific number of hours for users to authenticate their access to . [See Configure the Authentication Frequency.]

Security Policy

Session initiate logs—You can enable session initiate logs while creating security policy rules to log events when sessions are created.

[See Add a Secure Edge Policy Rule.]

Security Subscriptions

CASB inline cloud application—You can configure rules to control activities on the cloud applications for a Cloud Access Security Broker (CASB) profile. Juniper Secure Edge supports the following newly added cloud applications and features:

- Microsoft Outlook—Login, Read, Compose, Send, UploadAttachment, and DownloadAttachment

- Google Chat—Login, Chat, Audio/Video, and FileTransfer

[See Add Rules to a CASB Profile and Create an Application Instance.]

Administration

Subscription notifications—You will now receive daily notifications starting from 10 days before the expiry of your Secure Edge trial subscription. See Subscription Notifications.

July 17, 2024 Release

IN THIS SECTION

- Secure Edge New Features: July 17, 2024 | 3

Secure Edge New Features: July 17, 2024

Monitor

Secure Edge reports—You can see information about the logs that are sent to an external security information and event management (SIEM) server, such as how many log streaming licenses are assigned

and used and how much data is streamed in logs, in the Secure Edge reports. [See About the Secure Edge Reports Page.]

Identity

Authentication frequency settings—You can now decide when users' web browser cookies expire by configuring how frequently users must authenticate their access to Juniper Secure Edge. This configuration gives you control over users' access to the portal. [See About the Authentication Settings Page.]

Security Subscriptions

CASB inline cloud application—You can configure rules to control activities on the cloud applications for a Cloud Access Security Broker (CASB) profile. Juniper Secure Edge supports the following newly added cloud applications and features:

- Amazon EFS—Login, Upload, Download, Create, Delete, and Edit

- Amazon S3—Login, Upload, Download, Create, and Delete

- GitHub—Login, Upload, Download, Create, View, and CreateRepo

- Microsoft OneDrive Personal—Login, Upload, Download, and Share

- Microsoft Teams—Chat, Audio/Video, and File Transfer

[See Add Rules to a CASB Profile.]

CASB profile rules—You can now:

- Click the application/application group name, activities, or application instances on the CASB Rules page to view the details on the configured activities and application instances.

- Select either **Cloud application group** or **Cloud applications** under Cloud Applications on the CASB Rules page.

[See About the CASB Rules Page and Add Rules to a CASB Profile.]

Service Management

Protected networks using address groups in sites—You can now give access to groups of IP addresses as protected networks while creating a new site, in addition to specifying IP address ranges. You can also create new address groups to include them in the new site. This new option enables you to add protected networks based on address groups rather than manually adding IP addresses or IP address ranges. [See Create a Site.]

Integrating Mist with Juniper Security Director Cloud —Customer administrators can now configure tunnel keepalives between customer-premises equipment (CPE) and Juniper Secure Edge from the Mist console. After you enable an external probe for a site, Juniper Secure Edge automatically creates a shared address object and a security firewall policy that allows the probes to pass through. [See About the External Probe Page.]

Administration

Log compression before streaming—You can now choose to compress logs using GZip before streaming the logs to Microsoft Azure. To use this feature, you must select the Azure Logic App SIEM server connection type in a log stream. [See Add a Log Stream.]

Back up logs at a cloud-based location—You can now configure a cloud-based location where your SRX Series Firewall and Secure Edge logs are backed up. Only paid subscribers with a Juniper Security Director Cloud, a Juniper Secure Edge, or a storage license can use this backup option. [See About the Organization Page.]

API security—Customer administrators can now allow specified users to access protected services or resources using access tokens. Log in to the Juniper Security Director Cloud portal, navigate to **Administration** > **API Security**, and configure API security. We currently support the API key and OAuth token security mechanisms.

Juniper Secure Edge supports Swagger 2.0 REST API specifications in JSON format. To access the Swagger API specification, open a web browser and enter **https://base-url/sd-swagger/**, where *base-url* is the root address of the website or application. You can access APIs for the following functions:

- Identity and access management (IAM)

- PAC Manager

- Service Location

- Sites

While IAM APIs are available to both Juniper Secure Edge customers and SRX Series firewall customers, PAC Manager, Service location, and Sites APIs are available only to the Juniper Secure Edge customers.

[See About the API Security Page.]

February 26, 2024 Release

Secure Edge New Features: February 26, 2024

Security Subscriptions

CASB inline cloud application activity controls—You can configure rules to control activities on the cloud applications for a Cloud Access Security Broker (CASB) profile. Juniper Secure Edge now supports the following newly added cloud applications and features:

- Gmail—Login, Read, Compose, Send, Upload Attachment, and Download Attachment

- SharePoint—Login, Upload, Download, and Share

- Slack—Login, Chat, Audio/Video, and File Transfer

[See Add Rules to a CASB Profile.]

Service Management

Sites—You can now see a hierarchy-based structure on the Sites page (**Secure Edge** > **Service Management** > **Sites**). You can also perform the following tasks:

- Expand the specific site name to view details about the customer premises equipment (CPE) devices on the Sites page.

- Enable external probe settings when creating a site.

- Configure the following Traffic Forwarding settings:

  - Two or more CPE devices for a single site

  - External interfaces to CPE devices

  - One or more tunnels to a CPE device depending on the number of users per site

- Tunnel type as either IPsec or GRE to forward the traffic

- Configure CPE routing settings such as the primary service location.

[See About the Sites Page.]

External Probe

External Probe—You can now configure the probe settings to enable external probe for a site. With this configuration, customer premises equipment (CPE) devices can monitor the tunnel health status. To navigate to the External Probe page, select **Secure Edge** > **Service Management** > **External Probe**.

[See About the External Probe Page.]

Administration

Log streaming—With log streaming, you can now forward audit logs, session logs, and security events from Juniper Secure Edge Cloud to an external security information and event management (SIEM) system via webhook, such as Microsoft Sentinel. On the Log Streaming page, you can configure the type of log to forward to the external SIEM system. [See About the Log Streaming Page.]

Additionally, you can create a log stream report. You can create a report for the current or previous month or the entire period of data transfer to the SIEM system. [See Create Log Streaming Report Definitions.]

Identity Management

User group retrieval from Microsoft Entra ID and Okta—You can now configure the identity provider (IdP) settings in Juniper Secure Edge to retrieve user group information from Microsoft Entra ID (previously known as Azure Active Directory) and Okta. Prior to this release, you had to deploy on-premises Juniper® Identity Management Service (JIMS) collector to retrieve user group information from Active Directory.

To retrieve user group information, log in to the Juniper Security Director Cloud portal, navigate to **Secure Edge > Identity > User Authentication > SAML**, and enter the required information to configure IdP. Juniper Secure Edge receives user group information from Microsoft Entra ID or Okta. You can use the user groups to manage security policies.

[See About the End User Authentication Page.]

Secure Edge Bug Fixes: February 26, 2024

There are no bug fixes in this release.

Release 2023

IN THIS SECTION

- October 07, 2023 Release | **8**
- April 25, 2023 Release | **11**

October 07, 2023 Release

IN THIS SECTION

- Secure Edge New Features: October 07, 2023 | **8**
- Secure Edge Bug Fixes: October 07, 2023 | **11**

Secure Edge New Features: October 07, 2023

Service Management

Enhancements on the Service Locations page—We've made the following enhancements:

- You get at least one pair of service locations to ensure maximum service availability.

- You can add more pairs of service locations as needed.

- You can add more users to any pair of service locations as needed.

[See About the Service Locations Page.]

Monitor

View CASB logs—When associated with a Secure Edge policy, a Cloud Access Security Broker (CASB) profile collects logs from the configured cloud applications. You can view and monitor these activity-based and action-based application logs on **Monitor** > **Logs** > **CASB**. [See Monitor CASB Logs.]

View CASB application visibility logs—On the new CASB Application Visibility page (**Monitor** > **Maps & Charts** > **CASB Applications**), you can view the following information related to CASB-supported cloud applications:

- Volume (network traffic) that each application uses

- Volume (bandwidth) that each category of the application consumes

- Number of events or sessions received, grouped by risk as defined by the applications

[See About the CASB Application Visibility Page.]

Tunnel status alerts—You can use the Tunnel Status Alerts page (**Monitor** > **Alerts** > **Tunnel Status Alerts**) to view the tunnel status alerts for the configured tunnels between sites and service locations.

[see About the Tunnel Status Alerts

Security Subscriptions

Manage CASB profiles—You can create, modify, clone, and delete Cloud Access Security Broker (CASB) profiles. The CASB functionality provides visibility into the security of your cloud applications. You can also create CASB profile rules to control specific actions on each cloud application to secure your data. After you assign the CASB profile to a Secure Edge policy, the profiles ensure that the traffic flows between cloud providers and on-premises devices comply with the Secure Edge policy. [See About the CASB Profiles Page, About the CASB Rules Page, and Add a Secure Edge Policy Rule.]

CASB inline cloud application activity controls—You can configure rules to control activities on the cloud applications for a CASB profile. The supported activities are login, upload, download, and share. The supported cloud applications are Box, Dropbox, Salesforce, Google Docs, and OneDrive. [See About the CASB Rules Page.]

Application instance for CASB—You can configure an application instance for the CASB profile. Use instance names to define which particular instances of the same cloud application you want to take a policy action on. [See About the CASB Rules Page.]

Application tagging for CASB—You can tag an application instance as **Untagged**, **Sanctioned**, or **Unsanctioned** for a CASB profile to reflect whether or not your organization approves the cloud application. By default, all the application instances are tagged as **None**. This type of tagging is not the same as the application instance tagging for the CASB rules. [See About the Application Tagging Page.]

Custom URL categories—You can create custom URL categories and add them to Web filtering profiles. You can also assign one of the following actions to the URL categories:

- Log and permit the URLs.

- Block the URLs.

- Permit the URLs.

- Quarantine the URLs.

[See About the Web Filtering Profiles Page.]

Security Policy

Captive portal support for unauthenticated on-premises users—You can now use captive portal to authenticate on-premises users that request access to a network service. In earlier releases, you could use captive portal to authenticate only roaming users. By default, captive portal is enabled for roaming users and disabled for on-premises site users. You can enable the captive portal support for on-premises users from the Secure Edge Policy page. [See About the Secure Edge Policy Page, and Add a Secure Edge Policy Rule.]

Identity

Supported JIMS Collector version—Secure Edge now supports JIMS Collector Release 1.7.0 and later. [See Juniper Identity Management Service Overview.]

Shared Services

Import URL patterns from a CSV file—Import multiple allowed or blocked URL patterns from a CSV file. You can use these URL patterns to validate inbound and outbound URL requests and allow or block the requests.

[See Import URL Patterns from a CSV File.]

DAG filter—You can filter and view the dynamic address group (DAG) feeds from the Amazon Web Services (AWS) regions and services that you select. Use a DAG filter to add the feeds. You can configure a maximum of 10 DAG filters for the selected AWS regions and services. [See Configure DAG Filter.]

Webhook for audit log notifications—You can use an audit log webhook to send Juniper Advanced Threat Prevention Cloud (ATP Cloud) audit log notifications to a remote server. A webhook is an automated message or a real-time notification that any application receives from another application that triggers an event. You can enable the webhook and configure the remote server URL to receive

these notifications in a chat application that can process JavaScript Object Notation (JSON) responses. [See Configure Webhook.]

Secure Edge Bug Fixes: October 07, 2023

There are no bug fixes in this release.

April 25, 2023 Release

IN THIS SECTION

- Secure Edge New Features: April 25, 2023 | **11**
- Secure Edge Bug Fixes: April 25, 2023 | **12**

Secure Edge New Features: April 25, 2023

Service Management

Multiregion deployment support—You can now deploy Juniper Secure Edge across multiple global regions. While creating a point of presence (POP), you can select the following regions and locations:

- North America—Virginia, Ohio, Oregon

- Asia Pacific—Singapore, Tokyo

- Europe—Frankfurt, London

- Canada—Toronto

[See Create a Service Location.]

Administration

Service Updates page—You can view all the scheduled update activities with update descriptions and status of the past, present, and future updates on the **Service Updates** page. The **Service Updates** page

contains a record of scheduled maintenance activities that are planned for updating Security Director Cloud and its features. You can also subscribe to receive e-mail notifications about the scheduled maintenance activities.

[See About the Service Updates Page.]

Secure Edge Bug Fixes: April 25, 2023

There are no bug fixes in this release for Secure Edge.

Release 2022

IN THIS SECTION

December 22, 2022 Release

IN THIS SECTION

Secure Edge New Features: December 22, 2022

Monitor

Download Secure Edge report—You can download the Secure Edge report for the required month and year from the Secure Edge Reports page. You can also update the report recipients using the **Update Report Recipients** option.

[See About the Secure Edge Reports Page.]

Secure Edge

Enhancements on the Sites page—We have made the following enhancements on the **Sites** page:

* You can see the lists of deployed sites and undeployed sites in two different tabs.

* You can import multiple sites by uploading a Microsoft Excel file to the Create Bulk Sites page. You can download the sample file template, enter the site details, and upload the filled-in template to create bulk sites.

  [See About the Sites Page.]

Service Administration

Enhancement in the PAC Files interface—You can now use the new PAC file builder to customize cloned proxy auto-configuration files. You can add domains and IP addresses and designate servers as on-premises. Juniper Secure Edge excludes these network components from the proxy auto-configuration file processing, and the traffic that reaches these network components bypasses Juniper Secure Edge. The wizard contains two tabs—Basic and Advanced. You can use the Advanced tab to directly configure the XML code. You can now also generate new recommended proxy auto-configuration files and delete existing recommended proxy auto-configuration files.

[See About the PAC Page.]

Secure Edge Bug Fixes: December 22, 2022

There are no bug fixes in this release for Secure Edge.

November 17, 2022 Release

Secure Edge New Features: November 17, 2022

Monitor

View Secure Edge Report—To view the Secure Edge Reports, navigate to Monitor > Reports > Secure Edge Reports page. Creating and downloading Secure Edge Reports is disabled from Report Definitions page. [See About the Secure Edge Reports Page].

Secure Edge Bug Fixes: November 17, 2022

There are no bug fixes in this release for Secure Edge.

October 07, 2022 Release

Secure Edge New Features: October 07, 2022

Monitor

- **View Secure Edge Report**—You can view the Secure Edge report consisting of data transfer details such as monthly data allocation and usage at various regions. You can view the total outbound data transfer by region for the current month in comparison to the previous 11 months. [See About the Secure Edge Reports Page].

- **Generate and download Secure Edge report**—You can generate the Secure Edge report and run the report on-demand or at scheduled intervals. You can E-mail the generated report or download it in the PDF format. [See Create Secure Edge Report Definitions].

Security Policy

- **Add SRX Policy Rules to Secure Edge Policy**—You can now migrate your on-premises security policies to Secure Edge by converting the security policy rules to Secure Edge policy. [See Add SRX Policy Rules to Secure Edge Policy (From SRX Policy Page) and Add SRX Policy Rules to Secure Edge Policy (From Secure Edge Policy Page)].

Secure Edge

- **Enhancements in the Create Site page**—

  - The selection of primary and secondary service locations is moved as a first step in creating a site.

  - In the Site Configuration page, a new field **Devices Type** is introduced. In this field, you can select if the site configuration is for the Juniper device or for the Non-Juniper device. [See Create a Site].

- **JIMS Collector**—Juniper Secure Edge now supports JIMS Collector Release 1.6.0. [See About the JIMS Page.]

Secure Edge Bug Fixes: October 07, 2022

There are no bug fixes in this release for Secure Edge.

August 16, 2022 Release

Secure Edge New Features: August 16, 2022

Secure Edge

- **Enhancement in the JIMS interface**—You can now delete JIMS Collectors. The delete option helps in removing JIMS Collectors that are no longer needed. [See About the JIMS Page.]

- **Enhancement in the PAC file management to exclude domains from the files**—You can now update the proxy auto configuration file with a list of domains to be excluded from PAC file-based forwarding. This UI-based function can be used to update any PAC file hosted on Juniper Security Director Cloud. [See About the PAC Page.]

- **Enhancement in the LDAP profile**—

  - The LDAP profile now mandates SSL encryption.

  - The LDAP profile tab now displays the source IP address or prefix for Juniper Secure Edge. You will need the Secure Edge IP address or prefix to make the inbound LDAP queries to the LDAP servers and update the firewall rules. [See About the End User Authentication Page].

- **Enhancement in the SAML profile**—

  - The SSL option is now removed from the SAML Profile tab. You must upload a certificate to indicate an SSL connection.

  - Name and Domain name fields are removed. You must now configure only Identity Provider (IdP) and Service Provider (SP) settings. [See About the End User Authentication Page].

Secure Edge Bug Fixes: August 16, 2022

- SAML Profile: Users were unable to edit the existing SAML settings. This issue is now resolved.

- Hosted Database: Earlier when you tried to add a user to a group, you could add the user to multiple groups belonging to multiple domains. Now, you can add users to multiple groups but belonging to a single domain.

July 8, 2022 Release

IN THIS SECTION

- New Features: July 08, 2022 | **17**

New Features: July 08, 2022

Dashboard

Secure Edge dashboard—You can use the following Secure Edge widgets in the user-configurable Security Director Cloud dashboard to get a customized view of the status of network services:

- C&C Server and Malware Source Locations

- Top Infected File Categories

- Top Scanned File Categories

- Top Malware Identified

- Top Compromised Hosts

- VPN Tunnel Status

- Devices Connection Status

- Devices by OS Version

- Devices by Platforms

- Device Subscriptions Status

- Device Management Entitlements

- Overall Storage

- Threat Map: IPS

- Threat Map: Virus

- Firewall: Top Denials

- Firewall: Top Events

- IP: Top Sources

- IP: Top Destinations

- NAT: Top Source Translations

- NAT: Top Destination Translations

- Top Source IPs by Volume

- Virus: Top Blocked

- Web Filtering: Top Blocked

- Applications: Most Sessions

- Top Applications by Volume

- Top Spam by Source

- IPS: Top Attacks

- Top 5 Users by Bandwidth

- Top 5 Service Locations by Users

- Top 3 Sites by Bandwidth

- Top 3 Service Locations by Bandwidth

- Top 5 Sites by Users

- Overview

- Monitored Tunnels Up/Down

- Total Service Locations

[See About the Dashboard.]

Monitor

- **View site tunnel status**—You can view the status of the configured tunnels between sites and service locations. [See About the Site Tunnel Status Page].

- **View service location status**—You can view the status of all the service locations, the users in a location, the bandwidth consumed by the users, and the available storage. [See About the Service Locations Monitor Page].

- **View ATP status**—You can monitor the status of compromised hosts, malicious threat sources, suspicious file downloads, Domain Name System (DNS) Domain Generation Algorithm (DGA) detections, tunnel detections, encrypted traffic insights, quarantined e-mail, blocked e-mail, and telemetry of blocked Web and e-mail files in Juniper Advanced Threat Prevention Cloud (ATP Cloud).

  [See Hosts Overview, DNS DGA and Tunneling Detection Details, Encrypted Traffic Insights Details, and Telemetry Overview.]

- **Generate, view, and download ATP reports**—You can generate ATP Cloud threat assessment reports in PDF format and run the report on-demand or at scheduled intervals. The report consists of a list of malware, C&C Server destinations, hosts with malicious activities, suspicious domains and URLs, high-risk user data, and actions taken on scanned e-mail.

  [See About the ATP Report Definition Page and About the ATP Generated Reports Page.]

- **View end user authentication logs**—You can view the details of the logs that are generated while authenticating on-premises and roaming users.

  [See Monitor End User Authentication Logs.]

Secure Edge

- **Service locations**—You can create, edit, and delete a point of presence (POP) location for a Juniper Secure Edge instance. The service location is the connection (access) point for both on-premises and roaming users. The number of users specified for a service location indicates Secure Edge the capacity that it needs to provision for. [See About the Service Locations Page.]

- **Sites**—You can create, edit, and delete sites. You can also view and manage the configuration of existing sites. A site is a customer location such as a branch or office. Some or all of the Internet-bound traffic from customer sites may be forwarded to the Juniper Secure Edge cloud through GRE or IPsec tunnels from CPE devices at the site. You can create the following types of sites:

  - GRE

  - IPsec Static

  - IPsec Dynamic

[See About the Sites Page.]

- **IPsec profiles**—You can view, create, edit, and delete IPsec profiles. IPsec profiles define the parameters with which an IPsec tunnel is established when the CPE devices start communicating with your Secure Edge solution in the cloud. [See About the IPsec Profiles Page.]

- **Manage Secure Edge policies**—You can specify what actions to take for specific sets of traffic by using a Secure Edge policy. You can view and manage the policy rules associated with the tenants. [See About the Secure Edge Policy Page].

- **Web filtering profiles**—You can view, create, edit, and delete Web filtering profiles. Web filtering enables you to manage Internet usage by preventing access to inappropriate Web content over HTTP. [See About the Web Filtering Profiles Page.]

- **Content filtering policies**—You can view, edit, and delete content filtering policies. Content filtering policies block or permit certain types of traffic over several protocols, such as HTTP, FTP upload and download, IMAP, SMTP, and POP3, based on the MIME type, file extension, protocol command, and embedded object type. [See About the Content Filtering Policies page.]

- **DNS security profiles**—You can configure a DNS security profile for Domain Generation Algorithm (DGA) detection and tunnel detection. DNS DGA generates random domain names that are used as rendezvous points with potential command and control servers. Tunnel detection detects DNS tunneling which is a cyberattack method that encodes the data of other programs or protocols in DNS queries and responses. Tunnel detection indicates that DNS traffic is likely to be subverted to transmit malware beaconing data or data of another protocol. [See Create a DNS Security Profile.]

- **Encrypted traffic insights profiles**—You can configure an encrypted traffic insights profile that detects malicious threats hidden in encrypted traffic without intercepting and decrypting the traffic. [See Create an Encrypted Traffic Insights Profile.]

- **PAC files**—You can download the proxy auto configuration (PAC) files, clone the configuration files, and edit the cloned files. A web browser uses information from the PAC file to know where to direct the traffic for a URL. Depending on the PAC file configuration, the traffic destination can be a proxy server or a real content server. [See About the PAC Page.]

- **Explicit proxy profiles**—You can configure an explicit proxy profile that Juniper Secure Edge can use to determine which port to listen to for the client-side traffic and which traffic to decrypt or bypass. [See Configure an Explicity Proxy Profile.]

- **Decrypt profiles**—You can configure decrypt profiles. The configuration enables a decrypt profile to function as an application service within a security policy. [See About the Decrypt Profiles Page.]

- **JIMS Collector**—You can onboard JIMS Collector in Juniper Secure Edge. Juniper Identity Management Service (JIMS) is a standalone service application that runs on Microsoft Windows. JIMS Collector collects and maintains a large database of user, device, and group information from

Active Directory domains or system log services. Juniper Secure Edge supports JIMS Collector Release 1.5 or later. [See Juniper Identity Management Service Overview.]

- **IPS profiles**—You can configure an intrusion prevention system (IPS) profile that enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through a device. You can create IPS rules or exempt rules for customized IPS profiles.

  [See About IPS Policies.]

- **SecIntel profiles**—You can configure Security Intelligence (SecIntel) profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. SecIntel provides carefully curated and verified threat intelligent feeds that's continuously collected from Juniper Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, dynamic address groups (DAGs), and industry-leading threat feeds to the Juniper Networks MX Series, SRX Series, EX Series, QFX Series, and NFX Series devices and Juniper's wireless access points (WAPs). SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

  [See About SecIntel Profiles.]

- **Antimalware profiles**—You can configure anti-malware profiles that define the content to scan for any malware and the action to be taken when a malware is detected.

  [See About Anti-malware Profiles.]

- **Certificate management**—You can configure TLS/SSL certificates that are used to establish secure communications between Juniper Secure Edge and user endpoints. The certificates may be signed by your own Certificate Authority (CA) or by Juniper's CA. You can create a new certificate signing request (CSR) to generate a new certificate or you can have Juniper create a new certificate.

  [See About the Certificate Management Page.]

- **End-user authentication**—You can configure various authentication methods to authenticate end users. If you are a roaming user, you can configure:

  - Hosted DB—User database hosted on Secure Edge

  - SAML—Identity provider (IdP) through the Security Assertion Markup Language (SAML) 2.0 protocol

  - LDAP—Lightweight Directory Access Protocol (LDAP) servers

  Roaming users are authenticated in the following order: hosted DB, SAML, LDAP.

  If you are an on-premises user, you can use Juniper Identity Management System (JIMS) for authentication.

  [See About the End User Authentication Page.]

Shared Services

- **Juniper Advanced Threat Prevention Cloud**—You can configure the following ATP features:

  - File inspection profiles—You can define which files to send to the cloud for inspection. You can group types of files to be scanned together (such as <file>.tar, <file>.exe, and <file>.java) under a common name and create multiple profiles based on the content you want scanned.
    [See File Inspection Profiles Overview.]

  - Allowlists—You can configure an allowlist that contains known trusted IP addresses, hash, e-mail addresses, and URLs. Content downloaded from locations on the allowlist does not need to be inspected for malware.
    [See Create Allowlists and Blocklists.]

  - Blocklists—You can configure a blocklist that contains known untrusted IP addresses and URLs. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
    [See Create Allowlists and Blocklists.]

  - SecIntel feeds—You can configure SecIntel feeds for domains, IP addresses and URLs that are known to be connected to malicious activities. SecIntel provides carefully curated and verified threat intelligent feeds that's continuously collected from Juniper Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, dynamic address groups (DAGs), and industry-leading threat feeds.
    [See SecIntel Feeds Overview.]

  - Miscellaneous features—You can configure these additional Juniper ATP Cloud features:

    - Infected hosts—You can set the global threat level to block infected hosts. You can configure Juniper ATP Cloud to send e-mails when certain threat levels are reached for infected hosts.
      [See Global Configuration for Infected Hosts.]

    - Logging—You can select the event types that you want to log for the devices in your realm. The devices in your realm use the event logs to generate system logs (syslogs).
      [See Enable Logging.]

    - Threat intelligence sharing—You can enable Trusted Automated eXchange of Intelligence Information (TAXII) to report and share threat intelligence. You can configure the threshold for threat intelligence sharing. TAXII uses only those files that meet or exceed the set threshold.
      [See Configure Threat Intelligence Sharing.]

    - Proxy servers—You can add trusted proxy server IP addresses to Juniper ATP Cloud. If there is a proxy server between users on the network and a firewall, the firewall might see the proxy server IP address as the source of an HTTP or HTTPS request instead of the actual address of the user making the request.

[See Configure Trusted Proxy Servers.]

Administration

- **Subscriptions**—You can add and manage subscriptions for SRX Series Firewalls, Juniper Secure Edge, and storage space. [See Subscriptions.]

- **ATP Mapping**—You can map a security realm in Juniper ATP Cloud to Juniper Secure Edge in order to access all features from Juniper ATP Cloud.

  [See About the ATP Mapping Page.]

- **ATP Audit Log**—You can use the ATP Audit Logs page to view information about the login activity and specific tasks that were completed successfully using the Juniper 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 and filter for audit logs, and export audit logs in comma-separated values (CSV) format.

  [See About the ATP Audit Logs Page.]

Known Issues

- We do not support the use of third-party authenticators for access to certain SaaS applications. For example, the Box application allows you to log in using your Google credentials, but Juniper Secure Edge recognizes the activity as a Google login rather than a Box login.

  Workaround: Use the SaaS application's built-in authentication system.

- Box upload activity is not detected in roaming traffic.

- If you use the CASB-supported Microsoft Teams application, you must edit the decrypt profile to identify the activities. By default, the decrypt profile (exempt list) includes the following Microsoft URLs:

  - *.delivery.mp.microsoft.com

  - *.teams.microsoft.com

  - *.update.microsoft.com

  - *.vortex-win.data.microsoft.com

  - activation.sls.microsoft.com

- update.microsoft.com

- windowsupdate.microsoft.com

- *.windowsupdate.microsoft.com

You must remove ***.teams.microsoft.com** from the exempt list to identify Microsoft Teams activities.

- If a non-administrator user launches the Juniper® Identity Management Service (JIMS) Collector GUI, the status of the Enforcement Points is not updated. The status always shows `Inactive` in the **Monitor** > **Enforcement Points** page in the JIMS Collector UI.

- When authenticated by Hosted DB, end users with disabled accounts are not notified that their account has been disabled. The end-user account was either disabled by the administrator or automatically disabled after five consecutive failed authentication attempts.

  Workaround: End users can contact their administrator to unlock their account.

- When you create an IPsec tunnel from a site to Secure Edge, the tunnel configuration status on the UI displays a "tunnel_status_undefined" message instead of an "in progress" message.

  Workaround: The status updates when the tunnel creation process is complete – typically in about <10> minutes.

- The LDAP configuration may display a blank error screen when incorrect information is entered.

  Workaround: The administrator will need to reenter the correct LDAP values.

- A few CASB applications and activities are not identified by the browser.

  Workaround: Disable the HTTP over QUIC in your browser settings to use the SSL proxy.

  - Steps to disable HTTP over QUIC in Firefox:

    1. In the address bar, enter **about:config**.

    2. In the **Search preference name** box, enter **network.http.http3.enable** and change the toggle to **False**.

    3. Repeat the above step for **network.http.http3.enable** and change the toggle to **False**.

    4. Clear the browser cookies and restart the browser.

  - Steps to disable HTTP over QUIC in Chrome:

    1. In the address bar, enter **chrome://flags/**.

    2. In the **Search flags** box, enter **Experimental QUIC protocol** and select **Disabled** from the drop-down menu.

3. Clear the browser cookies and restart the browser.