Application Security Feature Guide for NFX Devices

Modified: 2018-07-05

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

Application Security Feature Guide for NFX Devices

END USER LICENSE AGREEMENT

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   ```

```
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/

- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

CHAPTER 1

Overview

Understanding Application Security on NFX Devices

Web-based applications are changing the dynamics of security. Previously, specific applications were associated with specific protocols and ports, making policy enforcement at the host level relatively straightforward. Web applications that can be accessed from anywhere create challenge for network administrators to effectively manage traffic flows and access to data while delivering the security and network services.

An individual can connect to the network using multiple devices simultaneously, making it impractical to identify a user, an application, or a device by a group of statically allocated IP addresses and port numbers.

Applications such as instant messaging, peer-to-peer file sharing, Webmail, social networking, and IP voice/video collaboration evade security mechanisms by changing communications ports and protocols, or by tunneling within other commonly used services (for example, HTTP or HTTPS). Organizations need control over the applications and traffic on their networks to protect their assets against attacks and manage bandwidth.

Juniper Networks' AppSecure is a suite of application-aware security services for the NFX Series devices that deliver security services to provide visibility and control over the types of applications traversing in the networks. AppSecure uses a sophisticated classification engine to accurately identify applications regardless of port or protocol, including nested applications that reside within trusted network services.

- Application identification (AppID)- Recognizes traffic at different network layers using characteristics other than port number. Once the application is determined, AppSecure service modules can be configured to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic.
- Application Tracking (AppTrack)—Tracks and reports applications passing through the device.
- Application Firewall (AppFW)—Implements an application firewall using application-based rules.

- Application Quality of Service (AppQoS)—Provides quality-of-service prioritization based on application awareness.
- Advanced policy-based routing (APBR)— Classifies session based on applications and applies the configured rules to reroute the traffic.

AppSecure works with additional content security on the device through integrated unified threat management (UTM), intrusion prevention systems (IPS), and Juniper Networks Sky Advanced Threat Prevention (Sky ATP) for deeper protection against malware, spam, phishing, and application exploits.

Benefits of Application Security

- Helps you identify application traffic traversing your network regardless of port, protocol, and encryption, thereby providing greater visibility to control network traffic.
- Enables you to control network traffic by setting and enforcing security policies based on accurate application information.
- Provides context and clarity to strengthen network protection.
- Provides protection against common evasion techniques.

Related Documentation

- *Understanding Application Identification TechniquesUnderstanding Application Identification Techniques*

CHAPTER 2

Application Identification

Application Identification for NFX Devices

Application Identification enables you to see the applications on your network and learn how they work, their behavioral characteristics, and their relative risk. Using different identification mechanisms, App ID detects the applications on your network regardless of the port, protocol, and encryption (TLS/SSL or SSH) or other evasive tactics used. For more information, see the following topics:

Understanding Application Identification Techniques

Historically, firewalls have used the IP address and port numbers as a way of enforcing policies. That strategy is based on the assumption that users connect to the network from fixed locations and access particular resources using specific port numbers.

Today, wireless networking and mobile devices require a different strategy. The way in which devices connect to the network changes rapidly. An individual can connect to the

network using multiple devices simultaneously. It is no longer practical to identify a user, application, or device by a group of statically allocated IP addresses and port numbers.

This topic includes the following section:

Junos OS Next-Generation Application Identification

Next-generation application identification builds on the legacy application identification functionality and provides more effective detection capabilities for evasive applications such as Skype, BitTorrent, and Tor.

Junos OS application identification recognizes Web-based and other applications and protocols at different network layers using characteristics other than port number. Applications are identified by using a protocol bundle containing application signatures and parsing information. The identification is based on protocol parsing and decoding and session management.

The detection mechanism has its own data feed and constructs to identify applications.

The following features are supported in application identification:

- Support for protocols and applications, including video streaming, peer-to-peer communication, social networking, and messaging
- Identification of services within applications
- Ability to distinguish actions launched within an application (such as login, browse, chat, and file transfer)
- Support for all versions of protocols and application decoders and dynamic updates of decoders
- Support for encrypted and compressed traffic and most complex tunneling protocols
- Ability to identify all protocols from Layer 3 to Layer 7 and above Layer 7

Benefits of Application Identification

- Provides granular control over applications, including video streaming, peer-to-peer communication, social networking, and messaging. It also identifies services, port usage, underlying technology, and behavioral characteristics within applications. This visibility enables you to block evasive applications inline at the NFX Series firewall.
- Identifies applications and allows, blocks, or limits applications—regardless of port or protocol, including applications known for using evasive techniques to avoid identification. This identification helps organizations control the types of traffic allowed to enter and exit the network.

Application Signature Mapping

Application signature mapping is a precise method of identifying the application that issued traffic on the network. Signature mapping operates at Layer 7 and inspects the actual content of the payload.

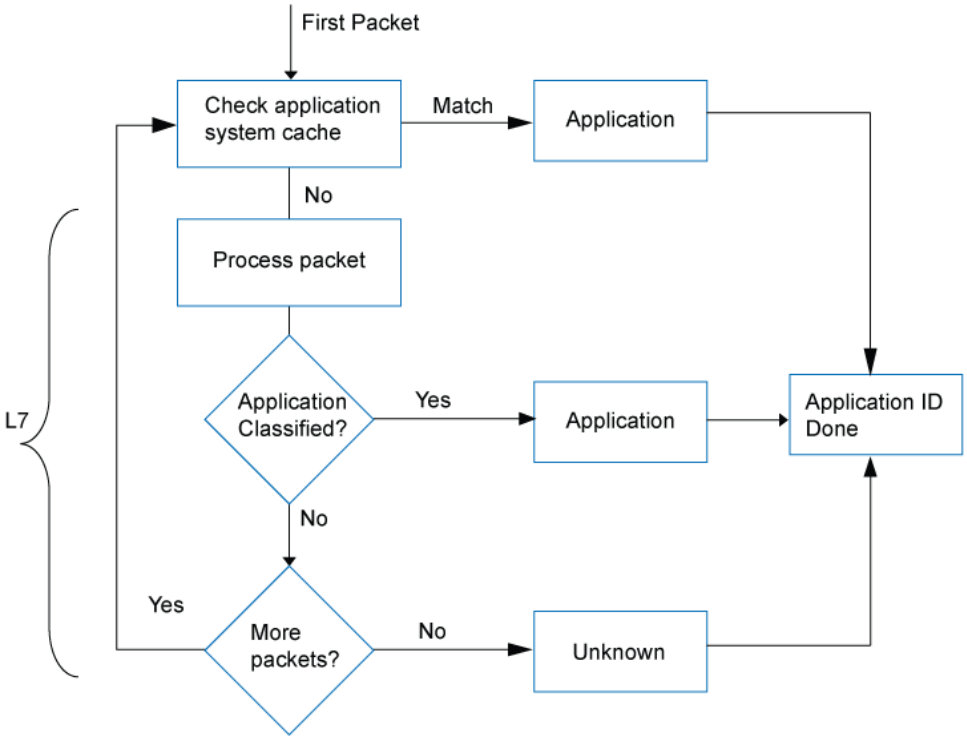
Applications are identified by using a downloadable protocol bundle. Application signatures and parsing information of the first few packets are compared to the content of the database. If the payload contains the same information as an entry in the database, the application of the traffic is identified as the application mapped to that database entry.

Juniper Networks provides a predefined application identification database that contains entries for a comprehensive set of known applications, such as FTP and DNS, and applications that operate over the HTTP protocol, such as Facebook, Kazaa, and many instant messaging programs. A signature subscription allows you to download the database from Juniper Networks and regularly update the content as new predefined signatures are added.

Application Identification Match Sequence

Figure 1 on page 23 shows the sequence in which mapping techniques are applied and how the application is determined.

Figure 1: Mapping Sequence



In application identification, every packet in the flow passes through the application identification engine for processing until the application is identified. Application bindings are saved in the application system cache (ASC) to expedite future identification process.

Application signatures identify an application based on protocol grammar analysis in the first few packets of a session. If the application identification engine has not yet identified the application, it passes the packets and waits for more data.

The application identification module matches applications for both client-to-server and server-to-client sessions.

Once the application is determined, AppSecure service modules can be configured to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic.

- AppTrack—Tracks and reports applications passing through the device.
- Intrusion Detection and Prevention (IDP)—Applies appropriate attack objects to applications running on nonstandard ports. Application identification improves IDP performance by narrowing the scope of attack signatures for applications without decoders.
- AppFW—Implements an application firewall using application-based rules.
- AppQoS—Provides quality-of-service prioritization based on application awareness.

See Also

- Application Tracking on NFX Devices on page 73
- Application Firewall on page 61
- Application QoS on page 84

Understanding the Junos OS Application Identification Database

A predefined signature database is available on the Juniper Networks Security Engineering website. This database includes a library of application signatures.

The predefined signature package provides identification criteria for known application signatures and is updated periodically.

Whenever new applications are added, the protocol bundle is updated and generated for all relevant platforms. It is packaged together with other application signature files. This package will be available for download through the security download website.

A subscription service allows you to regularly download the latest signatures for up-to-date coverage without having to create entries for your own use.

Application identification is enabled by default and is automatically turned on when you configure Intrusion Detection and Prevention (IDP), AppFW, AppQoS, or AppTrack.

NOTE: Updates to the Junos OS predefined application signature package are authorized by a separately licensed subscription service. You must install the application identification application signature update license key on your device to download and install the signature database updates provided by Juniper Networks. When your license key expires, you can continue to use the locally stored application signature package contents but you cannot update the package.

See Also

- *Understanding the Junos OS Application Package Installation*
- *Understanding IDP Application Identification*

Disabling and Reenabling Junos OS Application Identification

Application identification is enabled by default. You can disable application identification with the CLI.

To disable application identification:

```
user@host# set services application-identification no-application-identification
```

If you want to reenable application identification, delete the configuration statement that specifies disabling of application identification:

```
user@host# delete services application-identification no-application-identification
```

If you are finished configuring the device, commit the configuration.

To verify the configuration, enter the **show services application-identification** command.

See Also

- *Understanding Application Identification Techniques*
- *Understanding the Junos OS Application Identification Database*

Understanding the Application System Cache

Application system cache (ASC) saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. Once an application is identified, its information is saved in the ASC so that only a matching entry is required to identify an application running on a particular system, thereby expediting the identification process.

By default, the ASC saves the mapping information for 3600 seconds. However, you can configure the cache timeout value by using the CLI.

Refreshing all the ASC entries might have an impact on the performance of service. To eliminate the service degradation, entries in the ASC are only refreshed when Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) traffic triggers a cache lookup. Without a cache lookup, the entries in the ASC remain unchanged. For example, if you have configured the cache timeout value 4800 seconds and there are no new TCP or

UDP session for 6000 seconds, then the ASC entries are not refreshed even if the configured timeout value (4800 seconds) is already over.

You can use the **[edit services application-identification application-system-cache-timeout]** command to change the timeout value for the application system cache entries. The timeout value can be configured from 0 through 1,000,000 seconds. The ASC session might expire after 1000,000 seconds.

NOTE: When you configure a new custom application signature or modify an existing custom signature, all the existing application system cache entries for predefined and custom applications will be cleared.

NOTE: When you delete or disable a custom application signature, and the configuration commit fails, the application system cache (ASC) entry is not cleared completely; instead, a base application in the path of custom application will be reported in ASC.

See Also

- Enabling or Disabling Application Groups in Junos OS Application Identification on page 60

Enabling or Disabling Application System Cache for Application Services

Starting in Junos OS Release 18.2R1, the default behavior of the ASC is changed as follows:

- Security services such as security policies, AppFW, Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services such as APBR and AppTrack use the ASC for application identification by default.

NOTE: The change in the default behavior of the ASC affects the legacy AppFW functionality. With the ASC disabled by default for the security services starting in Junos OS Release 18.2 onward, AppFW will not use the entries present in the ASC.

You can revert to the ASC behavior as in Junos OS releases before Release 18.2 by using the **set services application-identification application-system-cache security-services** command.

CAUTION: The SRX Series device might become susceptible to application evasion techniques if the ASC is enabled for security services. We recommend that you enable the ASC only when the performance of the device in its default

configuration (disabled for security services) is not sufficient for your specific use case.

Use the following commands to enable or disable the ASC:

- Enable the ASC for security services:

  user@host# set services application-identification application-system-cache security-services

- Disable the ASC for miscellaneous services:

  user@host# set services application-identification application-system-cache no-miscellaneous-services

- Disable the enabled ASC for security services:

  user@host# delete services application-identification application-system-cache security-services

- Enable the disabled ASC for miscellaneous services:

  user@host# delete services application-identification application-system-cache no-miscellaneous-services

You can use the **show services application-identification application-system-cache** command to verify the status of the ASC.

The following sample output provides the status of the ASC:

```
user@host>show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
```

In releases before Junos OS Release 18.2R1, application caching is enabled by default. You can manually disable it by using the CLI.

user@host# set services application-identification no-application-system-cache

See Also

- *Understanding Application Identification Techniques*
- *Verifying Application System Cache Statistics*
- *Understanding the Junos OS Application Identification Database*

Verifying Application System Cache Statistics

Purpose Verify the application system cache (ASC) statistics.

NOTE: The application system cache will display the cache for application identification applications.

Action From CLI operation mode, enter the **show services application-identification application-system-cache** command.

Sample Output

```
user@host> show services application-identification application-system-cache
application-cache: on
  nested-application-cache: on
  cache-unknown-result: on
  cache-entry-timeout: 3600 seconds
```

Meaning The output shows a summary of the ASC statistics information. Verify the following information:

- IP address—Displays the destination address.
- Port—Displays the destination port on the server.
- Protocol—Displays the protocol type on the destination port.
- Application—Displays the name of the application identified on the destination port.

See Also
- Application Identification on page 21

Onbox Application Identification Statistics

Application Identification services provide statistical information per session. These statistics provide customers with an application usage profile. The Onbox Application Identification Statistics feature adds application-level statistics to the AppSecure suite. Application statistics allow an administrator to access cumulative statistics as well as statistics accumulated over user-defined intervals.

With this feature, the administrator can clear the statistics and configure the interval values while maintaining bytes and session count statistics. Because the statistics count occurs at session close event time, the byte and session counts are not updated until the session closes. Juniper Networks' devices support a history of eight intervals that an administrator can use to display application session and byte counts.

If application grouping is supported in your configuration of Junos OS, then the Onbox Application Identification Statistic feature supports onbox per-group matching statistics. The statistic*Onbox Application Identification Statistics*s are maintained for predefined groups only.

Reinstalling an application signature package will not clear the application statistics. If the application is disabled, there will not be any traffic for that application, but the application is still maintained in the statistics. It does not matter if you are reinstalling a predefined application, because applications are tracked according to application type. For predefined group statistics, reinstalling a security package will not clear the statistics. However, any changes to group memberships are updated. For example, junos:web might have 50 applications in the current release and 60 applications following an upgrade. Applications that are deleted and application groups that are renamed are handled in the same way as applications that are added.

The Application Identification module maintains a 64-bit session counters for each application on each Services Processing Unit (SPU). The counter increments when a session is identified as a particular application. Another set of 64-bit counters aggregates the total bytes per application on the SPU. Counters for unspecified applications are also maintained. Statistics from multiple SPUs for both sessions and bytes are aggregated on the Routing Engine and presented to the users.

Individual SPUs have interval timers to roll over statistics per *interval* time. To configure the interval for statistics collection, use the **set services application-identification statistics interval *time*** command. Whenever the Routing Engine queries for the required interval, the corresponding statistics are fetched from each SPU, aggregated in the Routing Engine and presented to the user.

Use the **clear services application-identification statistics** to clear all application statistics such as cumulative, interval, applications, and application groups.

Use the **clear services application-identification counter** command to reset the counters manually. Counters reset automatically when a device is upgraded or rebooted, when flowd restarts, or when there is a change in the interval timer.

Use the **set services application-identification application-system-cache-timeout value** to specify the timeout value in seconds for the application system cache entries.

Configuring IMAP Cache Size

Internet Message Access Protocol (IMAP) is an Internet standard protocol used by e-mail clients for e-mail storage and retrieval services. IMAP cache is used for protocol parsing and context generation. It stores parsing related information of an email.

You can configure to limit the maximum number of entries in the IMAP cache and specify the timeout value for the entries in the cache.

You can use the following commands to modify the settings for IMAP cache:

set services application-identification imap-cache imap-cache-size *size*

set services application-identification imap-cache imap-cache-timeout *time in seconds*

Example:

```
[edit]
user@host# set services application-identification imap-cache imap-cache-size 50000
```

In this example, the IMAP cache size is configured to store 50,000 entries.

```
[edit]
user@host# set services application-identification imap-cache-timeout 600
```

In this example, time out period is configured to 600 seconds during which a cache entry remains in IMAP cache.

See Also
- Application Identification on page 21

Understanding Jumbo Frames Support for Junos OS Application Identification Services

Application identification support the larger jumbo frame size of 9192 bytes. Although jumbo frames are enabled by default, you can adjust the maximum transmission unit (MTU) size by using the [**set interfaces**] command. CPU overhead can be reduced while processing jumbo frames.

See Also
- *Understanding Jumbo Frames Support for Ethernet Interfaces*

Improving the Application Traffic Throughput

The application traffic throughput can be improved by setting the deep packet inspection (DPI) in performance mode with default packet inspection limit as two packets, including both client-to-server and server-to-client directions. By default, performance mode is disabled on NFX Series devices.

To improve the application traffic throughput:

1. Enable the DPI performance mode.

   ```
   [edit]
   user@host# set services application-identification enable-performance-mode
   ```

2. (Optional) You can set the maximum packet threshold for DPI performance mode, including both client-to-server and server-to-client directions.

   You can set the packet inspection limit from 1 through 100.

   ```
   [edit]
   user@host# set services application-identification enable-performance-mode
     max-packet-threshold value
   ```

3. Commit the configuration.

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

Use the **show services application-identification status** command to display detailed information about application identification status.

show services application-identification status (DPI Performance Mode Enabled)

```
user@host> show services application-identification status
pic: 2/1

Application Identification
Status                          Enabled
Sessions under app detection    0
Engine Version                  4.18.2-24.006 (build date Jul 30 2014)
Max TCP session packet memory   30000
Force packet plugin             Disabled
Force stream plugin             Disabled
DPI Performance mode:           Enabled
Statistics collection interval  1 (in minutes)

Application System Cache
Status                          Enabled
Negative cache status           Disabled
Max Number of entries in cache  262144
Cache timeout                   3600 (in seconds)

Protocol Bundle
Download Server                 https://signatures.juniper.net/cgi-bin/index.cgi
AutoUpdate                      Disabled
Slot 1:
Application package version     2399
Status                          Active
Version                         1.40.0-26.006 (build date May 1 2014)
Sessions                        0
Slot 2
Application package version     0
Status                          Free
Version
Sessions                        0
```

The DPI Performance mode field displays whether the DPI performance mode is enabled or not. This field is displayed in the CLI command output only if the performance mode is enabled.

If you want to set DPI to default accuracy mode and disable the performance mode, delete the configuration statement that specifies enabling of the performance mode:

To disable the performance mode:

1. Delete the performance mode.

   ```
   [edit]
   user@host# delete services application-identification enable-performance-mode
   ```

2. Commit the configuration.

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

See Also

- enable-performance-mode on page 182

Related Documentation

- Application Identification on page 21
- Predefined Application Signatures for Application Identification on NFX Devices on page 32
- Custom Application Signatures for Application Identification on NFX Devices on page 47
- Predefined and Custom Application Groups for Application Identification on page 55

Predefined Application Signatures for Application Identification on NFX Devices

Predefined application signature package is a dynamically loadable module that provides application classification functionality and associated protocol attributes. It is hosted on an external server and can be downloaded as a package and installed on the device. For more information, see the following topics:

- Understanding the Junos OS Application Package Installation on page 32
- Installing and Verifying Licenses for an Application Signature Package on page 34
- Example: Downloading and Installing the Junos OS Application Signature Package Manually on NFX Devices on page 36
- Example: Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package on NFX Devices on page 39
- Example: Scheduling the Application Signature Package Updates on NFX Devices on page 42
- Scheduling the Application Signature Package Updates as Part of the IDP Security Package on page 44
- Verifying the Junos OS Application Identification Extracted Application Package on page 45
- Uninstalling the Junos OS Application Identification Application Package on page 46

Understanding the Junos OS Application Package Installation

Juniper Networks regularly updates the predefined application signature package database and makes it available to subscribers on the Juniper Networks website. This package includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, quality-of-service prioritization, and Intrusion Detection and Prevention (IDP). The database contains application objects such as FTP, DNS, Facebook, Kazaa, and many instant messenger programs.

You need to download and install the application signature package before configuring application services. The application signature package is included in the IDP installation directly and does not need to be downloaded separately.

- If you have IDP enabled and plan to use application identification, you can continue to run the IDP signature database download. To download the IDP signature database, run the following command: **request security idp security-package download**. The application package download can be performed manually or automatically. See *Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package*.

NOTE: If you have an IDP-enabled device and plan to use application identification, we recommend that you download only the IDP signature database. This will avoid having two versions of the application database, which could become out of sync.

- If you do not have IDP enabled and plan to use application identification, you can run the following commands: **request services application-identification download** and **request services application-identification install**. These commands will download the application signature database and install it on the device.

  You can perform the download manually or automatically. When you download the extracted package manually, you can change the download URL.

  After downloading and installing the application signature package, use CLI commands to download and install database updates, and view summary and detailed application information.

  See *Downloading and Installing the Junos OS Application Signature Package Manually* or *Example: Scheduling the Application Signature Package Updates*.

  NOTE: The Junos OS application signature package update is a separately licensed subscription service. You must install the application signature package update license key on your device to download and install the signature database updates provided by Juniper Networks. If your license key expires, you can continue to use the locally stored application signature package content but you cannot update the data.

  NOTE: When you upgrade or downgrade an application signature package, an error message is displayed if there is any mismatch of application IDs (unique ID number of an application signature) between proto bundles and these applications are configured in AppFW and AppQoS rules.

  Example:

  ```
  Please resolve following references and try it again
  [edit class-of-service application-traffic-control rule-sets RS8 rule
   1 match application junos:CCPROXY]
  ```

  As a workaround, disable the AppFW and AppQoS rules before upgrading or downgrading an application signature package. You can re-enable AppFW and AppQoS rules once the upgrade or downgrade procedure is complete.

  NOTE: We recommend using the CLI for configuration of AppSecure features on Juniper Networks' devices.

Upgrading to Next-Generation Application Identification

Next-generation application identification is supported on NFX devices.

Devices installed with Junos OS builds with legacy application identification include legacy application identification security packages. The next-generation application identification security package is installed along with the default protocol bundle. The device is automatically upgraded to next-generation application identification.

NOTE:

- The next-generation application identification security package introduces incremental updates to the legacy application identification package. You are not required to remove or uninstall any existing applications.
- Applications supported in previous releases (Junos OS Release 12.1X46 or prior) might have new aliases or alternative names in the new version. So existing configurations using such application work in Junos OS Release 12.1X47; however, related logs and other information will use the new name. You can use the **show services application-identification application detail** *new-application-name* command to get the details of the applications.
- When you upgrade Junos OS, you can include the **validate** or **no-validate** options with the **request system software add** command. Because the existing features, which are not part of next-generation application identification, are deprecated, incompatibility issues are not seen.
- Next-generation application identification eliminates the generation of new nested applications and treats existing nested applications as normal applications. In addition, next-generation application identification does not support custom applications or custom application groups. Existing configurations involving any nested applications, custom applications, or custom application groups are ignored with warning messages.

See Also

- *Understanding the Junos OS Application Identification Database*
- *Understanding the IDP Signature Database*
- *Downloading and Installing the Junos OS Application Signature Package Manually*
- *Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package*
- *Example: Scheduling the Application Signature Package Updates*

Installing and Verifying Licenses for an Application Signature Package

The Junos OS application signature package update is a separately licensed subscription service. You must install the application signature package update license key on your device to download and install the signature database updates provided by Juniper

Networks. If your license key expires, you can continue to use the locally stored application signature package content.

Licensing is usually ordered when the device is purchased, and this information is bound to the chassis serial number. These instructions assume that you already have the license. If you did not order the license during the purchase of the device, contact your account team or Juniper customer care for assistance. For more information, refer to the Knowledge Base article KB9731 at https://kb.juniper.net/InfoCenter/index?page=home.

NOTE: AppSecure is part of Juniper Networks Secure Edge software. A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

You can install the license on the NFX device using either the automatic method or manual method as follows:

- Install your license automatically on the device.

  To install or update your license automatically, your device must be connected to the Internet .

  user@host> **request system license update**

  ```
  Trying to update license keys from https://ae1.juniper.net, use 'show system
  license' to check status.
  ```

- Install the licenses manually on the device.

  user@host> **request system license add terminal**

  ```
  [Type ^D at a new line to end input,
   enter blank line between each license key]
  ```

  Paste the license key and press Enter to continue.

- Verify the license is installed on your device.

  Use the **show system license command** command to view license usage, as shown in the following example:

  ```
  License usage:
                                  Licenses     Licenses    Licenses    Expiry
    Feature name                      used    installed      needed
    logical-system                       4            1           3    permanent


   License identifier: JUNOSXXXXXX
    License version: 2
    Valid for device: AA4XXXX005
    Features:
      appid-sig        - APPID Signature
        date-based, 2014-02-17 08:00:00 GMT-8 - 2015-02-11 08:00:00 GMT-8
  ```

The output sample is truncated to display only license usage details.

See Also
- *Adding New Licenses (CLI Procedure)*

Example: Downloading and Installing the Junos OS Application Signature Package Manually on NFX Devices

This example shows how to download the application signature package, create a policy, and identify it as the active policy.

Requirements

Before you begin:

- Ensure that your device has a connection to the Internet to download security package updates.

  NOTE: DNS must be set up because you need to resolve the name of the update server.

- Ensure that you have installed the application identification feature license. See *Installing and Verifying Licenses for an Application Signature Package*.

Overview

Juniper Networks regularly updates the predefined application signature package database and makes it available on the Juniper Networks website. This package includes application objects that can be used in Intrusion Detection and Prevention (IDP), application firewall policy, and AppTrack to match traffic.

Configuration

CLI Quick Configuration

CLI quick configuration is not available for this example because manual intervention is required during the configuration.

Downloading and Installing Application Identification

Step-by-Step Procedure

1. Download the application package.

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

   ```
   Please use command "request services application-identification download
   status" to check status
   ```

Download retrieves the application package from the Juniper Networks security website https://signatures.juniper.net/cgi-bin/index.cgi.

You can also download a specific version of the application package or download the application package from the specific location by using the following options:

- To download a specific version of the application package:

  user@host>**request services application-identification download version** ***version-number***

- To change the download URL for the application package from configuration mode:

  [edit]
  user@host**# set services application-identification download url** ***URL or File Path***

NOTE: If you change the download URL and you want to keep that change, make sure you commit the configuration.

2. Check the download status.

   user@host>**request services application-identification download status**

```
Application package 2345 is downloaded successfully
```

NOTE: You can also use the system log to view the result of the download.

3. Install the application package.

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

```
Please use command "request services application-identification install
status" to check status and use command "request services
application-identification proto-bundle-status" to check protocol bundle
status
```

   The application package is installed in the application signature database on the device.

4. Check the installation status of the application package.

   The command output displays information about the downloaded and installed versions of the application package and protocol bundle.

   - To view the installation status:

     user@host>**request services application-identification install status**

```
Install application package 2345 succeed
```

- To view the protocol bundle status:

  user@host>**request services application-identification proto-bundle-status**

```
Protocol Bundle Version (1.30.4-22.005 (build date Jan 17 2014)) and
application secpack version (2345) is loaded and activated.
```

NOTE: It is possible that an application signature was removed from the newer version of an application signature database. If this signature is used in an existing application firewall policy on your device, the installation of the new database will fail. An installation status message identifies the signature that is no longer valid. To update the database successfully, remove all references to the deleted signature from your existing policies and groups, and rerun the install command.

Verification

Confirm that the configuration is working properly.

Verifying the Application Identification Status

Purpose Verify that the application identification configuration is working properly.

Action From operational mode, enter the **show services application-identification status** command.

```
pic: 1/0

Application Identification
 Status                          Enabled
 Sessions under app detection    0
 Engine Version                  4.18.1-20 (build date Jan 25 2014)
 Max TCP session packet memory   30000
 Max C2S bytes                   1024
 Max S2C bytes                   0
 Force packet plugin             Disabled
 Force stream plugin             Disabled
 Statistics collection interval  1 (in minutes)

Application System Cache
 Status                          Enabled
 Negative cache status           Disabled
 Max Number of entries in cache  131072
 Cache timeout in seconds        3600

Protocol Bundle
 Download Server              https://services.netscreen.com/cgi-bin/index.cgi

 AutoUpdate                      Enabled
Slot 1:
 Status                          Active
 Version                         1.30.4-22.005 (build date Jan 17 2014)
 Sessions                        0
Slot 2
 Status                          Free
```

Meaning The **Status: Enabled** field shows that application identification is enabled on the device.

See Also

- *Understanding the Junos OS Application Package Installation*
- *Installing and Verifying Licenses for an Application Signature Package*
- *Example: Scheduling the Application Signature Package Updates*
- *Verifying the Junos OS Application Identification Extracted Application Package*
- *Uninstalling the Junos OS Application Identification Application Package*

Example: Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package on NFX Devices

You can download and install application signatures through intrusion detection and prevention (IDP) security packages.

This example shows how to enhance security by downloading and installing the IDP signatures and application signature package. In this case, both IDP signature pack and application signature pack are downloaded with a single command.

Requirements

Before you begin:

- Ensure that your device has a connection to the Internet to download security package updates.

  NOTE: DNS must be set up because you need to resolve the name of the update server.

- Ensure that you have installed the application identification feature license. See *Installing and Verifying Licenses for an Application Signature Package*.

Overview

In this example, you download and install the signature database from the Juniper Networks website.

Configuration

Downloading and Installing the Signature Database

CLI Quick Configuration

CLI quick configuration is not available for this example because manual intervention is required during the configuration.

Step-by-Step Procedure

To download and install application signatures:

1. Download the signature database.

```
[edit]
user@host# run request security idp security-package download

Will be processed in async mode. Check the status using the status checking
 CLI
```

NOTE: Downloading the database might take some time depending on the database size and the speed of your Internet connection.

2. Check the security package download status.

```
[edit]
user@host# run request security idp security-package download status

Done;Successfully downloaded
from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:2230(Mon Feb  4 19:40:13 2013 GMT-8, Detector=12.6.160121210)
```

3. Install the attack database.

```
[edit]
user@host# run request security idp security-package install

Will be processed in async mode. Check the status using the status checking
 CLI
```

NOTE: Installing the attack database might take some time depending on the security database size.

4. Check the attack database install status. The command output displays information about the downloaded and installed versions of the attack database.

```
[edit]
user@host# run request security idp security-package install status

Done;Attack DB update : successful - [UpdateNumber=2230,ExportDate=Mon Feb
 4 19:40:13 2013 GMT-8,Detector=12.6.160121210]
Updating control-plane with new detector : successful
Updating data-plane with new attack or detector : successful
```

5. Confirm your IDP security package version.

```
[edit]
user@host# run show security idp security-package-version

Attack database version:2230(Mon Feb  4 19:40:13 2013 GMT-8)
  Detector version :12.6.160121210
  Policy template version :2230
```

6. Confirm your application identification package version.

```
[edit]
user@host# run show services application-identification version

Application package version: 1884
```

Verification

Confirm that the application signature package is being updated properly.

Verifying application signature package

Purpose Verify the services application identification version.

Action From operational mode, enter the **show services application-identification version** command.

```
user@host> show services application-identification version

Application package version: 1884
```

Meaning The sample output shows that the services application identification version is 1884.

See Also

- *request security idp security-package install*
- *request security idp security-package download*
- *Updating the IDP Signature Database Overview*
- *Understanding the IDP Signature Database*

Example: Scheduling the Application Signature Package Updates on NFX Devices

This example shows how to set up automatic updates of the predefined application signature package.

Requirements

Before you begin:

- Ensure that your device has a connection to the Internet to download security package updates.

  NOTE: DNS must be set up because you need to resolve the name of the update server.

- Ensure that you have installed the application identification feature license. See *Installing and Verifying Licenses for an Application Signature Package*.

Overview

In this example, you want to download the current version of the application signature package periodically. The download should start at 11:59 PM on December 10. To maintain the most current information, you want to update the package automatically every 2 days from your company's intranet site.

Configuration

Step-by-Step Procedure

To use the CLI to automatically update the Junos OS application signature package:

1. Specify the URL for the security package. The security package includes the detector and the latest attack objects and groups. The following statement specifies https://signatures.juniper.net/cgi-bin/index.cgi as the URL for downloading signature database updates:

   ```
   [edit]
   user@host# set services application-identification download url
     https://signatures.juniper.net/cgi-bin/index.cgi
   ```

2. Specify the time and interval for download. The following statement sets the interval as 48 hours and the start time as 11:59 pm on December 10:

   ```
   [edit]
   user@host# set services application-identification download automatic interval 48
     start-time 12-10.23:59
   ```

3. If you are done configuring the device, commit the configuration.

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

Verification

To verify that the application signature package is being updated properly, enter the **show services application-identification version** command. Review the version number and details for the latest update.

See Also

- *Understanding the Junos OS Application Package Installation*
- *Installing and Verifying Licenses for an Application Signature Package*
- *Downloading and Installing the Junos OS Application Signature Package Manually*
- *Verifying the Junos OS Application Identification Extracted Application Package*

Scheduling the Application Signature Package Updates as Part of the IDP Security Package

The following configuration procedure describes how to setup automatic updates of application identification signature package (part of IDP security package) at a specified date and time.

Requirements

Before you begin:

- Ensure that your device has a connection to the Internet to download security package updates.

  NOTE: DNS must be set up because you need to resolve the name of the update server.

- Ensure that you have installed the application identification feature license. See *Installing and Verifying Licenses for an Application Signature Package*.

Overview

In this procedure, you want to download the current version of the application signature package periodically. The download should start at 11:59 PM on December 10. To maintain the most current information, you want to update the package automatically every 2 days from your company's intranet site.

Configuration

Step-by-Step Procedure

To use the CLI to automatically update the Junos OS application signature package:

1. Specify the URL for the security package. The security package includes the detector and the latest attack objects and groups. The following statement specifies https://signatures.juniper.net/cgi-bin/index.cgi as the URL for downloading signature database updates:

   ```
   [edit]
   user@host# set security idp security-package url
     https://signatures.juniper.net/cgi-bin/index.cgi
   ```

2. Specify the time and interval for download. The following statement sets the interval as 48 hours and the start time as 11:55 pm on December 10, 2013:

   ```
   [edit]
   user@host# set security idp security-package automatic interval 48 start-time
     2013-12-10.23:55:55
   ```

3. Enable an automatic download and update of the security package.

```
[edit]
user@host# set security idp security-package automatic enable
```

4. If you are done configuring the device, commit the configuration.

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

Verification

Confirm that the application signature package is being updated properly.

Verifying application signature package

Purpose Verify services application identification version

Action From operational mode, enter the **show services application-identification version** command.

```
user@host> show services application-identification version

Application package version: 1884
```

Meaning The sample output shows that, the services application identification version is 1884.

See Also

- *Understanding the Junos OS Application Package Installation*
- *Installing and Verifying Licenses for an Application Signature Package*
- *Downloading and Installing the Junos OS Application Signature Package Manually*
- *Verifying the Junos OS Application Identification Extracted Application Package*

Verifying the Junos OS Application Identification Extracted Application Package

Purpose After successful download and installation of the application package, use the following commands to view the predefined application signature package content.

Action

- View the current version of the application package:

  show services application-identification version

  ```
  Application package version: 1608
  ```

- View the current status of the application package:

  show services application-identification status

```
pic: 1/0

Application Identification
 Status                            Enabled
 Sessions under app detection      0
 Engine Version                    4.18.1-20 (build date Jan 25 2014)
 Max TCP session packet memory     30000
 Max C2S bytes                     1024
 Max S2C bytes                     0
 Force packet plugin               Disabled
 Force stream plugin               Disabled
 Statistics collection interval    1 (in minutes)

Application System Cache
 Status                            Enabled
 Negative cache status             Disabled
 Max Number of entries in cache    131072
 Cache timeout in seconds          3600

Protocol Bundle
 Download Server
https://services.netscreen.com/cgi-bin/index.cgi
 AutoUpdate                        Enabled
Slot 1:
 Status                            Active
 Version                           1.30.4-22.005 (build date Jan 17 2014)
 Sessions                          0
Slot 2
 Status                            Free
```

See Also

- *Understanding the Junos OS Application Package Installation*
- *Downloading and Installing the Junos OS Application Signature Package Manually*

Uninstalling the Junos OS Application Identification Application Package

You can uninstall the predefined application package. The uninstall operation will fail if there are any active security policies referenced in the predefined application signatures in the Junos OS configuration

To uninstall application package:

1. Uninstall the application package:

   user@host> **request services application-identification uninstall**

   ```
   Please use command "request services application-identification uninstall
   status" to check status and use command "request services
   application-identification proto-bundle-status" to check protocol bundle status
   ```

2. Check the uninstall operation status of the application package. The command output displays information about the uninstall status of the application package and protocol bundle.

   - Check the uninstall status:

     user@host>**request services application-identification uninstall status**

```
Uninstall application package 2345 succeed
```

- Check the uninstall status of protocol bundle:

  user@host>**request services application-identification proto-bundle-status**

```
Protocol Bundle Version (1.30.4-22.005 (build date Jan 17 2014)) and
application secpack version (2345) is unloaded and deactivated
```

The application package and protocol bundle are uninstalled on the device. To reinstall application identification, you need to download application package and reinstall it again.

See Also

- request services application-identification uninstall on page 275
- request services application-identification uninstall status on page 276

Related Documentation

- *Application Identification*
- *Custom Application Signatures for Application Identification*
- Predefined and Custom Application Groups for Application Identification on page 55

Custom Application Signatures for Application Identification on NFX Devices

User-defined custom application signatures can also be used to identify the application regardless of the protocol and port being used. You can create custom signatures using hostnames, IP address ranges, and ports, which allows you to track traffic to specific destinations. For more information, see the following topics:

- Understanding Junos OS Application Identification Custom Application Signatures on page 47
- Example: Configuring Junos OS Application Identification Custom Application Signatures on page 50

Understanding Junos OS Application Identification Custom Application Signatures

Application identification supports user-defined custom application signatures and signature groups. Custom application signatures are unique to your environment and are not part of the predefined application package. You must install application signature package on your device to use custom signatures. When the custom signatures are configured, you cannot uninstall the application signature package.

Custom application signatures are required:

- To control traffic particular to an environment
- To bring visibility for unknown or unclassified applications by developing custom applications.

- To identify applications over Layer 7 and transiting or temporary applications, and to achieve further granularity of known applications
- To perform QoS for your specific application

You can create custom application signatures using CLI by specifying a name, protocol, port where the application runs, and match criteria. For more details, see *Example: Configuring Junos OS Application Identification Custom Application Signatures*.

CAUTION: We recommend that only advanced Junos OS users attempt to customize application signatures.

You can view application signatures and application signature groups by using the **show services application-identification application** and **show services application-identification group** commands.

NOTE: The following features are not supported:

- Prioritizing custom signatures over a specific predefined custom signature
- Complete Perl Compatible Regular Expressions (PCRE)-based character set, and unicode-based characters
- Enforcing of order among members in Layer 7-based signatures
- The wildcard address for address-based signatures (Layer 3 and Layer 4)

Unlike predefined signatures and groups, custom application signatures and groups are saved in the configuration hierarchy, not in the predefined application signature database. Custom application signatures and signature groups are located in the **[services application-identification]** hierarchy.

Juniper Networks' devices support the following types of custom signatures:

- ICMP-Based Mapping on page 48
- Address-Based Mapping on page 49
- IP Protocol-Based Mapping on page 49
- Layer 7-Based Signatures on page 49

ICMP-Based Mapping

The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. This mapping technique lets you differentiate between various types of ICMP messages.

NOTE: IDP works only with TCP or UDP traffic. ICMP mapping, therefore, does not apply to IDP and cannot support IDP features such as custom attacks.

NOTE: The ICMP mapping technique used for mapping standard ICMP message types and optional codes are not supported for ICMPv6 traffic.

Address-Based Mapping

Layer 3 and Layer 4 address mapping defines an application by the IP address and optional port range of the traffic.

To ensure adequate security, use address mapping when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy in handling traffic from a known application.

Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port. When both IP address and port are configured, both should match destination tuples (IP address and port range) of the packet.

Consider a Session Initiation Protocol (SIP) server that initiates sessions from its known port 5060. Because all traffic from this IP address and port is generated by only the SIP application, the SIP application can be mapped to the server's IP address and port 5060 for application identification. In this way, all traffic with this IP address and port is identified as SIP application traffic.

NOTE: When you configure an address-based application and a TCP/UDP stream-based application, and a session matches both applications, the TCP/UDP stream-based application is reported as application and address-based application is reported as extended application.

IP Protocol-Based Mapping

Standard IP protocol numbers can map an application to IP traffic. As with address mapping, to ensure adequate security, use IP protocol mapping only in your private network for trusted servers.

NOTE: IDP works only with TCP or UDP traffic. IP protocol mapping, therefore, does not apply to IDP and cannot support IDP features such as custom attacks.

Layer 7-Based Signatures

Layer 7 custom signatures define an application running over TCP or UDP or Layer 7 applications. Layer 7-based custom application signatures are required for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol.

Layer 7-based custom application signatures detect applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS). Application identification can also extract the server name information or the server certification from the TLS or SSL sessions. It can also detect patterns in TCP or UDP payload in Layer 7 applications.

Example: Configuring Junos OS Application Identification Custom Application Signatures

This example shows how to configure custom application signatures for Junos OS application identification.

CAUTION: **We recommend that only advanced Junos OS users attempt to customize application signatures.**

Requirements

Before you begin:

- Ensure that the application signature package is installed on your device. See *Downloading and Installing the Junos OS Application Signature Package Manually* or *Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package*.
- The device must be running Junos OS Release 15.1X49-D40 or later.

Overview

Application identification supports custom application signatures to detect applications as they pass through the device. When you configure custom signatures, make sure that your signatures are unique.

In this example, you create custom application signatures for applications based on ICMP, IP protocol, IP address, and Layer 7.

For information about specify context for matching application, see context (Application Identification).

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

HTTP Context-Based Custom Signatures

```
set services application-identification application mycustom-http over HTTP signature
  s1 member m01 context http-header-host
set services application-identification application mycustom-http over HTTP signature
  s1 member m01 pattern .*agent1.*
set services application-identification application mycustom-http over HTTP signature
  s1 member m01 direction client-to-server
```

SSL Context-Based Custom Signatures

```
set services application-identification application mycustom-ssl over SSL signature s1
  member m01 context ssl-server-name
set services application-identification application mycustom-ssl over SSL signature s1
  member m01 pattern "example\.com"
set services application-identification application mycustom-ssl over SSL signature s1
  member m01 direction client-to-server
```

TCP Stream-Based Custom Signatures

```
set services application-identification application mycustom-tcp over TCP signature s1
  member m01 context stream
set services application-identification application mycustom-tcp over TCP signature s1
  member m01 pattern "12345678901234567890123456789O"
set services application-identification application mycustom-tcp over TCP signature s1
  member m01 direction client-to-server
```

ICMP-Based

```
set services application-identification application MY-ICMP icmp-mapping type 100
set services application-identification application MY-ICMP icmp-mapping code 1
```

Layer 3/Layer 4 Address-Based

```
set services application-identification application My-ADDRESS address-mapping
  ADDR-SAMPLE filter ip 192.0.2.1/24
set services application-identification application My-ADDRESS address-mapping
  ADDR-SAMPLE filter port-range udp 5000-6000
```

IP Protocol-Based

```
set services application-identification application MY-IGMP ip-protocol-mapping protocol
  2
```

Step-by-Step Procedure

The following examples require you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *CLI User Guide*.

To configure HTTP context-based custom signatures:

1. Configure an application based on HTTP context. Define an application signature to match the pattern, a unique application signature identifier, application signature member identifier, and set the context to be matched.

   ```
   [edit services application-identification]
   user@host# set application mycustom-http over HTTP signature s1 member m01
     context http-header-host
   ```

2. Configure a pattern to match the context.

   ```
   [edit services application-identification]
   user@host# set application mycustom-http over HTTP signature s1 member m01
     pattern .*agent1.*
   ```

3. Configure the connection direction of the packets to apply pattern matching.

```
[edit services application-identification]
user@host# set application mycustom-http over HTTP signature s1 member m01
  direction client-to-server
```

Step-by-Step Procedure

To configure SSL context-based custom signatures:

1. Configure an application based on SSL. Define an application signature to match the pattern, a unique application signature identifier, application signature member identifier, and set the context to be matched.

```
[edit services application-identification]
user@host# set application mycustom-ssl over SSL signature s1 member m01
  context ssl-server-name
```

2. Configure a pattern to match the context.

```
[edit services application-identification]
user@host# set application mycustom-ssl over SSL signature s1 member m01
  pattern "example\.com"
```

3. Configure the connection direction of the packets to apply pattern matching.

```
[edit services application-identification]
user@host# set application mycustom-ssl over SSL signature s1 member m01
  direction client-to-server
```

Step-by-Step Procedure

To configure TCP stream-based custom signatures:

1. Configure an application based on TCP. Define an application signature to match the pattern, a unique application signature identifier, application signature member identifier, and set the context to be matched.

```
[edit services application-identification]
user@host# set application mycustom-tcp over TCP signature s1 member m01
  context stream
```

2. Configure a pattern to match the context.

```
[edit services application-identification]
user@host# set application mycustom-tcp over TCP signature s1 member m01
  pattern ""12345678901234567890123456789O"
```

3. Configure the connection direction of the packets to apply pattern matching.

```
[edit services application-identification]
user@host# set application mycustom-tcp over TCP signature s1 member m01
  direction client-to-server
```

Step-by-Step Procedure

To configure ICMP-based custom applications signatures:

1. Define the type of ICMP mapping. The type field identifies the ICMP message.

```
[edit services application-identification]
user@host# set application MY-ICMP icmp-mapping type 100
```

2. Define the code for ICMP mapping. The code field provides further information about the associated type field.

```
[edit services application-identification]
user@host# set application MY-ICMP icmp-mapping code 1
```

Step-by-Step Procedure

To configure Layer 3 or Layer 4 address-based custom applications signatures:

1. Configure the application to match the specified IP address.

```
[edit services application-identification]
user@host# set application My-ADDRESS address-mapping ADDR-SAMPLE filter
   ip 192.0.2.1/24
```

2. Configure the port range for TCP or UDP.

```
[edit services application-identification]
user@host# set application My-ADDRESS address-mapping ADDR-SAMPLE filter
   port-range udp 5000-6000
```

NOTE: You must provide the appropriate port range and specified IP address to configure address-based custom application signatures.

Step-by-Step Procedure

To configure IP protocol mapping-based custom application signatures:

- Specify the IP protocol value for an application to match.

```
[edit services application-identification]
user@host# set application MY-IGMP ip-protocol-mapping protocol 2
```

Results

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

```
[edit]
user@host# show services application-identification

download {
   url https://services.netscreen.com/cgi-bin/index.cgi;
}
application MY-ICMP {
```

```
    icmp-mapping {
      type 100;
      code 1;
    }
  }
  application MY-IGMP {
    ip-protocol-mapping {
      protocol 2;
    }
  }
  application My-ADDRESS {
    address-mapping ADDR-SAMPLE {
      filter {
        ip 192.0.2.1/24;
        port-range {
          udp 5000-6000;
        }
      }
    }
  }
  application mycustom-http {
    over HTTP {
      signature s1 {
        member m01 {
          context http-header-host;
          pattern ".*agent1.*;";
          direction client-to-server;
        }
      }
    }
  }
  application mycustom-ssl {
    over SSL {
      signature s1 {
        member m01 {
          context ssl-server-name;
          pattern "example\.com";
          direction client-to-server;
        }
      }
    }
  }
  application mycustom-tcp {
    over TCP {
      signature s1 {
        member m01 {
          context stream;
          pattern 12345678901234567890123901234567;
          direction client-to-server;
        }
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the Custom Application Definitions

Purpose Display predefined and custom application signatures and settings that are configured on your device. Note that predefined application signature names use the prefix "junos:"

Action From configuration mode, enter the **show services application-identification application detail *name*** command.

See show services application-identification application

See Also
- *Understanding the Junos OS Application Package Installation*
- Customizing Application Groups for Junos OS Application Identification on page 55

Related Documentation
- *Application Identification*
- *Predefined Application Signatures for Application Identification*
- Predefined and Custom Application Groups for Application Identification on page 55

Predefined and Custom Application Groups for Application Identification

You can define an application group for both predefined applications, as well as custom applications. An application group contains applications that need similar treatment when defining a security policy. For more information, see the following topics:

- Customizing Application Groups for Junos OS Application Identification on page 55
- Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management on page 56
- Enabling or Disabling Application Groups in Junos OS Application Identification on page 60

Customizing Application Groups for Junos OS Application Identification

In Junos OS, application identification allows you to group applications in policies. Applications can be grouped under predefined and custom application groups. The entire predefined application group can be downloaded as part of the IDP or application identification security package. You can create custom application groups with a set of similar applications for consistent reuse when defining policies.

Application group support associates related applications under a single name for simplified, consistent reuse when using any application services.

The hierarchy of application groups resembles a tree structure with associated applications as the leaf nodes. The group *any* refers to the root node. The group *unassigned* is always situated one level from the root and initially contains all applications. When a

group is defined, applications are assigned from the unassigned group to the new group. When a group is deleted, its applications are moved back to the unassigned group.

All predefined application groups have the prefix “junos“ in the application group name to prevent naming conflicts with custom application groups. You cannot modify the list of applications within a predefined application group. However, you can copy a predefined application group to use it as a template for creating a custom application group.

To customize a predefined application group, you must first disable the predefined group. Note that a disabled predefined application group remains disabled after an application database update. You can then use the operational command **request services application-identification group** to copy the disabled predefined application group. The copied group is placed in the configuration file, and the prefix “junos” is changed to “my”. At this point, you can modify the list of applications in “my” application group and rename the group with a unique name.

To reassign an application from one custom group to another, you must remove the application from its current custom application group, and then reassign it to the other.

See Also

- *Understanding the Junos OS Application Identification Database*

Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management

This example shows how to configure custom application groups for Junos OS application identification for consistent reuse when defining policies.

Requirements

Before you begin, install an entire signature database from an IDP or an application identification security package. See *Downloading and Installing the Junos OS Application Signature Package Manually* or *Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package*.

Overview

In this example, you define applications for an application group, delete an application from an application group, and include an application group within another application group.

In Junos OS, application identification allows you to group applications in policies. Applications can be grouped under predefined and custom application groups. The entire predefined application group can be downloaded as part of the IDP or application identification security package. You can create custom application groups with a set of similar applications for consistent reuse when defining policies.

NOTE: You cannot modify the applications defined in a predefined application group. However, you can copy a predefined application group using the operational command **request services application-identification group** *group-name* **copy** to create a custom application group and modify the list of applications. For more information, see request services application-identification group.

Configuration

Configuring Junos OS Application Identification User-Defined Application Groups

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set services application-identification application-group my_web
set services application-identification application-group my_web applications junos:HTTP
set services application-identification application-group my_web applications junos:FTP
set services application-identification application-group my_web applications
    junos:AMAZON
set services application-identification application-group my_web applications
    junos:GOPHER
set services application-identification application-group my_peer
set services application-identification application-group my_peer applications
    junos:BITTORRENT
set services application-identification application-group my_peer applications
    junos:BITTORRENT-APPLICATION
set services application-identification application-group my_peer applications
    junos:BITTORRENT-WEB-CLIENT
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure a custom application group for application identification:

1. Set the name of your custom application group.

   ```
   [edit services application-identification]
   user@host# set application-group my_web
   ```

2. Add the list of applications that you want to include in your custom application group.

   ```
   [edit services application-identification]
   ```

```
user@host# set application-group my_web applications junos:HTTP
user@host# set application-group my_web applications junos:FTP
user@host# set application-group my_web applications junos:GOPHER
user@host# set application-group my_web applications junos:AMAZON
```

3. Set the name of a second custom application group.

```
[edit services application-identification]
user@host# set application-group my_peer
```

4. Add the list of applications that you want to include in the group.

```
[edit services application-identification]
user@host# set application-group my_peer applications junos:BITTORRENT
user@host# set application-group my_peer applications
  junos:BITTORRENT-APPLICATION
user@host# set application-group my_peer applications
  junos:BITTORRENT-WEB-CLIENT
```

Results From configuration mode, confirm your configuration by entering the **show services application-identification group** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services application-identification application-group my_web
  applications {
    junos:HTTP;
    junos:FTP;
    junos:GOPHER;
    junos:AMAZON
  }
user@host# show services application-identification application-group my_peer
  applications {
    junos:BITTORRENT;
    junos:BITTORRENT-APPLICATION;
    junos:BITTORRENT-WEB-CLIENT;
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Deleting an Application from a User-Defined Application Group

CLI Quick Configuration To quickly configure this section of the example, copy the following command, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
delete services application-identification application-group my_web applications
  junos:AMAZON
```


Step-by-Step Procedure

To delete an application from a custom application group:

- Delete an application from a custom application group.

```
[edit services application-identification]
user@host# delete application-group my_web applications junos:AMAZON
```

Results

From configuration mode, confirm your configuration by entering the **show services application-identification application group detail** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services application-identification group detail
  application group my_web {
    junos:HTTP;
    junos:FTP;
    junos:GOPHER;
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Creating Child Application Groups for an Application Group

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set services application-identification application-group p2p
set services application-identification application-group p2p application-groups my_web
set services application-identification application-group p2p application-groups my_peer
```

Step-by-Step Procedure

To configure child application groups for a custom application group:

1. Set the name of the custom application group in which you are configuring the child application groups.

```
[edit services application-identification]
user@host# set application-group p2p
```

2. Add the child application groups.

```
[edit services application-identification]
user@host# set application-group p2p application-groups my_web
uer@host# set application-group p2p application-groups my_peer
```

Results

From configuration mode, confirm your configuration by entering the **show services application-identification application-group** ***application-group-name*** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services application-identification application-group p2p
  applications-groups {
    my_web;
    my_peer;
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

See Also

- *Understanding Junos OS Application Identification Custom Application Signatures*

Enabling or Disabling Application Groups in Junos OS Application Identification

All application groups are enabled by default. Predefined application groups are enabled at installation.

- For predefined application groups, you can disable and reenable a group using the **request services application-identification group** command. You cannot delete a predefined signature or signature group.
  - To disable a predefined application group:

    user@host> request services application-identification group disable *predefined-application-group-name*

    NOTE: Make sure to commit the configuration changes or roll back the configuration when you are attempting to enable a disabled application or an application group. Uncommitted changes might result in configuration failure.

  - To reenable a disabled predefined application group:

    user@host> request services application-identification group enable *predefined-application-group-name*

See Also

- *Understanding the Application System Cache*

Related Documentation

- *Application Identification*
- *Predefined Application Signatures for Application Identification*
- *Understanding Junos OS Application Identification Custom Application Signatures*

CHAPTER 3

Application Services Modules

Application Firewall on NFX Devices

Application Firewall (AppFW) refers to the ability to take the results from the App ID engine and leverage them to make an informed decision to permit, deny/ reject, or redirect the traffic. For more information, see the following topics:

Application Firewall Overview

Traditionally, applications like HTTP, SMTP, and DNS use well-known standard ports and are easily controlled by a stateful firewall. However, it is possible to run these applications on any port as long as the client and server are using the same protocol as the well-known ports.

Evasive applications could remain undetected with a standard firewall that functions at Layer 3 or Layer 4 by transmitting other protocols over these well-known ports that are usually open by a firewall. AppFW enforces protocol and policy control at Layer 7. It inspects the actual content of the payload and ensures that it conforms to the policy, rather than identifying the application based on Layer 3 and Layer 4 information.

Additionally, with the growing popularity of Web applications and the shift from traditional full client-based applications to the Web, more and more traffic is being transmitted over HTTP. An application firewall identifies not only HTTP but also any application running on top of it, letting you properly enforce policies. For example, an application firewall rule could block HTTP traffic from Facebook but allow Web access to HTTP traffic from MS Outlook.

A security administrator implements an application firewall by performing the following tasks:

- Define one or more application firewall rule sets.
- Create rules for each rule set that permit, reject, or deny traffic based on the application ID.
- Configure a security policy to invoke the application firewall service and specify the rule set to be applied to permitted traffic.

This topic includes the following sections:

Benefit of Application Firewall

- Controls access to high-risk applications based on user-defined policies.

Understanding Application Firewall Rule Sets

An application firewall permits, rejects, or denies traffic based on the application of the traffic. The firewall consists of one or more rule sets with rules that specify match criteria, including dynamic applications, and the action to be taken for matching traffic.

An application firewall rule set consists of:

- The name of the rule set
- One or more rules
- A single default rule

Each rule defines dynamic applications to permit, reject, or deny. Each rule consists of:

- The name of the rule
- A list of dynamic applications to be used as match criteria
- The action to take for any traffic that matches one of the specified applications
  - Reject—Notify the client, drop the traffic, close the session, and log the event.
  - Deny—Drop the traffic, close the session, and log the event.
  - Permit—Permit the traffic.

The default rule defines the action to be taken for any traffic that does not match one of the rules. An application firewall rule set must contain a default rule.

There is no limit to the number of dynamic applications in a rule or to the number of rules in a rule set. However, there is a limit to the overall number of rule sets and rules.

The junos:UNKNOWN keyword is reserved for unknown dynamic applications. In the following cases, the application ID is set to junos:UNKNOWN:

- The traffic does not match an application signature in the database.
- The system encounters an error when identifying the application.
- The session fails over to another device.

Traffic with an application ID of junos:UNKNOWN matches a rule with a dynamic application of junos:UNKNOWN. If there is no rule defined for junos:UNKNOWN, the default rule is applied.

Configuring an Application Firewall Within a Security Policy

An application firewall is invoked using the **then permit** statement of the security policy.

Any traffic denied or rejected by the security policy based on Layer 3 or Layer 4 criteria is dropped immediately. Traffic permitted by the security policy is further assessed by the application firewall at Layer 7 based on its application ID.

The following sample policy, outbound-traffic, permits matching HTTP traffic, and invokes application services and an application firewall. The rule set, unknown-traffic, permits, denies, or rejects, traffic based on its match criteria.

```
[edit security policies from-zone trust to-zone untrust outbound-traffic]
user@host# set match source-address 192.0.2.1
user@host# set match destination-address 198.51.100.1
user@host# set match application junos-http
user@host# set then permit application-services application-firewall rule-set
  unknown-traffic
```

Traffic is processed in the following sequence:

1. Match the zone pair specified in the policy.
2. When specified, match the source and destination IP addresses, ports, and application type.
3. Apply the security policy action to matching traffic.
   - Reject—Notify the client, drop the traffic, and log the event.
   - Deny—Drop the traffic, and log the event.
   - Permit—Open a session, log the event, and apply services as specified.
     - Invoke application services to retrieve the application ID for the traffic.
     - Apply the specified application firewall rule set.

NOTE: All IP fragmented packets received on the device must be reassembled before forwarding.

Application Group Support for Application Firewall

Application group support associates related applications under a single name for simplified, consistent reuse when using any application services. As the predefined signature database changes, the content of a predefined application group can be modified to include new signatures without affecting existing firewall rules. When you define application firewall rules, you can specify dynamic application groups as match criteria.

NOTE: An application group can contain applications and groups simultaneously. It is possible to assign one application to multiple groups. There is no limit to the number of dynamic application groups contained in one rule.

For information on creating or listing application groups, see "Customizing Application Groups for Junos OS Application Identification" on page 55.

NOTE: When ALG is enabled on the device, application identification includes the ALG result to identify the application of the control sessions. Application firewall permits ALG data sessions whenever control sessions are permitted. If the control session is denied, there will be no data sessions. When ALG is disabled, application identification relies on its signatures to identify the application of the control and data sessions. If a signature match is not found, the application is considered unknown. Application firewall handles applications based on the application identification result.

Redirecting Users

Although drop and reject actions are logged, application firewall does not notify clients when either action is taken. Clients are not aware that the webpage is not available and might keep trying to access the page. To provide an explanation for the action or to redirect the client to an informative webpage, use the **block-message** option with the **reject** or **deny** action in an application firewall rule.

```
...
then reject block-message
```

When traffic is rejected by the application firewall rule, a splash screen with the following default message is displayed to the user:

user-name, Application Firewall has blocked your request to application *application-name* at *dst-ip:dst-port* accessed from *src-ip:src-port*.

To help the user fully understand which request has been rejected or denied, the default message includes traffic-specific details, such as the username, application, and address information.

You can customize the redirect action by including additional text on the splash screen or by specifying a URL to which the user is redirected. To customize the block message, define the type and content in a block message profile defined in the rule set:

```
[edit security application-firewall profile deny-profile-1]
set block-message type custom-redirect-url content http://abc.company.com/information
```

The block message profile is identified for the rule set, and applied to one or more of the rules using the **block-message** option.

```
[edit security application-firewall rule-sets application-firewall-3]
set profile deny-profile-1
set rule redirect-on-deny
set match dynamic-application [junos:KAZAA junos:EDONKEY junos:YMSG]
set then deny block-message
```

In this example, any traffic matching one of the specified dynamic applications is denied, and the block message defined for rule set, deny-profile-1, is applied. Based on the profile for deny-profile-1, the user is redirected to the URL http://abc.company.com/information for further details.

Session Logging for Application Firewalls

With security policies, the permit action of the matched policy rule creates a session and logs a session create message. A reject or deny action logs a reject or deny message, but does not create a session.

When an application firewall is implemented, the permit action of the security policy creates a session before the application firewall rules are applied. If the dynamic application have been retrieved from the cache, this information is added to the session create message. If the application is in the process of being identified, the dynamic application fields specify UNKNOWN.

If traffic is rejected or denied by the application firewall, application firewall also closes the session. The reject or deny message actions are logged with the reason field containing one of the following phrases:

- **appfw deny** or **appfw deny redirect**
- **appfw reject** or **appfw reject redirect**
- **policy deny**
- **policy reject**

See Also

- *Understanding Security Policy Elements*
- *Security Policies Overview*
- *Understanding Security Policy Rules*

Example: Configuring Application Firewall Rule Sets Within a Security Policy

This example shows how to configure application firewall rule sets within the security policy.

Requirements

- Create zones. See *Example: Creating Security Zones*.
- Configure an address book with addresses for the policy. See *Example: Configuring Address Books and Address Sets*.

Overview

In Junos OS, the security policies provide firewall security functionality by enforcing rules for the traffic so that traffic passing through the device is permitted or denied based on the action defined in the rules. The application firewall support in the policies provides additional security control for dynamic applications.

The application firewall is defined by a collection of rule sets. These rule sets can be defined independently and shared across network security policies. A rule set defines the rules that match the application ID detected, based on the application signature.

This configuration example shows how to:

- Permit or deny selected traffic from the untrust zone to the trust zone, based on the application firewall rule sets defined with the rules matching the dynamic applications.

NOTE: We recommend using CLI for configuration of AppSecure features.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security policies from-zone untrust to-zone trust policy policy1 match source-address
    198.51.100.1
set security policies from-zone untrust to-zone trust policy policy1 match
    destination-address 192.0.2.1
set security policies from-zone untrust to-zone trust policy policy1 match application
    junos-http
set security policies from-zone untrust to-zone trust policy policy1 then permit
    application-services application-firewall rule-set rs1
```

```
set security policies from-zone untrust to-zone trust policy policy2 match source-address
  198.51.100.1
set security policies from-zone untrust to-zone trust policy policy2 match
  destination-address 192.0.2.1
set security policies from-zone untrust to-zone trust policy policy2 match application any
set security policies from-zone untrust to-zone trust policy policy2 then permit
  application-services application-firewall rule-set rs2
set security application-firewall rule-sets rs1 rule r1 match dynamic-application
  [junos:KAZAA junos:EDONKEY junos:YMSG]
set security application-firewall rule-sets rs1 rule r1 then deny
set security application-firewall rule-sets rs1 default-rule permit
set security application-firewall rule-sets rs2 rule r1 match dynamic-application
  [junos:FACEBOOK-ACCESS junos:GOOGLETALK junos:MEEBOME junos:UNKNOWN]
set security application-firewall rule-sets rs2 rule r1 then permit
set security application-firewall rule-sets rs2 default-rule deny
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *CLI User Guide*.

To configure two security policies with application firewall rule sets that permit or deny traffic from different dynamic applications:

1. Configure a policy to process the traffic that goes to the HTTP static ports with the application firewall rule set rs1.

   ```
   [edit security policies from-zone untrust to-zone trust policy policy1]
   user@host# set match source-address 198.51.100.1
   user@host# set match destination-address 192.0.2.1
   user@host# set match application junos-http
   user@host# set then permit application-services application-firewall rule-set rs1
   ```

2. Configure another policy to process any traffic that does not go to the HTTP static ports with the application firewall rule set rs2.

   ```
   [edit security policies from-zone untrust to-zone trust policy policy2]
   user@host# set match source-address 198.51.100.1
   user@host# set match destination-address 192.0.2.1
   user@host# set match application any
   user@host# set then permit application-services application-firewall rule-set rs2
   ```

3. Define the application firewall rule set rs1 to deny traffic from selected dynamic applications.

   ```
   [edit security application-firewall rule-sets rs1]
   user@host# set rule r1 match dynamic-application [junos:KAZAA junos:EDONKEY
     junos:YMSG]
   user@host# set rule r1 then deny
   user@host# set default-rule permit
   ```

4. Define the application firewall rule set rs2 to permit traffic from selected dynamic applications.

   ```
   [edit security application-firewall rule-sets rs2]
   ```

```
user@host# set rule r1 match dynamic-application [junos:FACEBOOK-ACCESS
  junos:GOOGLETALK junos:MEEBOME junos:UNKNOWN]
user@host# set rule r1 then permit
user@host# set default-rule deny
```

Results From configuration mode, confirm your configuration by entering the **show security policies** and **show security application-firewall** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
  from-zone untrust to-zone trust {
    policy 1 {
      match {
        source-address 198.51.100.1;
        destination-address 192.0.2.1;
        application junos-http;
      }
      then {
        permit {
          application-services {
            application-firewall {
              rule-set rs1;
            }
          }
        }
      }
    }
    policy 2 {
      match {
        source-address 198.51.100.1;
        destination-address 192.0.2.1;
        application any;
      }
      then {
        permit {
          application-services {
            application-firewall {
              rule-set rs2;
            }
          }
        }
      }
    }
  }
user@host# show security application-firewall
  rule-sets rs1 {
    rule r1 {
      match {
        dynamic-application [junos:KAZAA junos:EDONKEY junos:YMSG];
      }
      then {
        deny;
```

```
    }
  }
  default-rule {
    permit;
  }
}
rule-sets rs2 {
  rule r1 {
    match {
      dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLETALK
        junos:MEEBOME junos:UNKNOWN];
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Application Firewall Configuration on page 69

Verifying Application Firewall Configuration

Purpose Verify information about application firewall support enabled under the security policy.

Action To verify the security policy configuration enabled with application firewall, enter the **show security policies** and **show security policies detail** commands. To verify all the application firewall rule sets configured on the device, enter the **show security application-firewall rule-set all** command.

Meaning The output displays information about application firewall enabled policies configured on the system. Verify the following information.

- Rule set
- Rules
- Match criteria

See Also

- *Security Policies Configuration Overview*
- *Example: Configuring a Security Policy to Permit or Deny All Traffic*

Example: Configuring an Application Group for Application Firewall

With application identification, multiple applications can be configured in a dynamic application groups for consistent reuse. AppFW rules permit and deny traffic by specifying application names, dynamic application group names, or both. By using predefined application groups, AppFW rules require no updating when new applications are added to common groups.

NOTE: **The application group is managed by the application identification module.**

This example shows how to configure application groups within the application firewall rule set.

Requirements

Before you begin:

- Create zones. See *Example: Creating Security Zones*.

Overview

The following example configures network policies to control outbound traffic from the trust zone to the untrust zone. All traffic permitted by the policy is processed further with the specified application firewall. The application firewall denies outbound traffic from unknown applications. Outbound Google Talk traffic is allowed, but all other known social networking traffic is denied. All other traffic is permitted.

The junos:GOOGLETALK application is included in the predefined group junos:social-networking. To allow junos:GOOGLETALK traffic and deny the rest of the group, the rule permitting junos:GOOGLETALK traffic must come before the rule denying traffic from the rest of the applications in the group.

This configuration example shows how to:

- Configure dynamic application groups in an application firewall.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security application-firewall rule-sets social-network rule google-rule match
  dynamic-application junos:GOOGLETALK
set security application-firewall rule-sets social-network rule google-rule then permit
set security application-firewall rule-sets social-network rule denied-sites match
  dynamic-application-groups junos:social-networking
set security application-firewall rule-sets social-network rule denied-sites match
  dynamic-application junos:UNKNOWN
set security application-firewall rule-sets social-network rule denied-sites then deny
set security application-firewall rule-sets social-network default-rule permit
set security policies from-zone trust to-zone untrust policy outbound-traffic
set security policies from-zone trust to-zone untrust policy outbound-traffic match
  source-address any
set security policies from-zone trust to-zone untrust policy outbound-traffic match
  destination-address any
set security policies from-zone trust to-zone untrust policy outbound-traffic match
  application junos:HTTP
set security policies from-zone trust to-zone untrust policy outbound-traffic then permit
  application-services application-firewall rule-set social-network
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure application firewall rule-sets and security policies for outbound traffic:

1. Create the rule-set social-network.

   ```
   [edit]
   user@host# set security application-firewall rule-sets social-network
   ```

2. Define a rule to permit Google-Talk traffic.

   ```
   [edit security application-firewall rule-sets social-network]
   user@host# set rule google-rule match dynamic-application junos:GOOGLETALK
   user@host# set rule google-rule then permit
   ```

3. Define a second rule that denies all other social-networking traffic and traffic from an unknown application.

   ```
   [edit security application-firewall rule-sets social-network]
   user@host# set rule denied-sites match dynamic-application-groups
     junos:social-networking
   user@host# set rule denied-sites match dynamic-application junos:UNKNOWN
   user@host# set rule denied-sites then deny
   ```

   Note that rule sequence is important. If the rules google-rule and denied-sites are reversed, GOOGLETALK traffic would never be permitted. The denied-sites rule would shadow google-rule.

4. Define the default-rule that permits all other traffic.

   ```
   [edit security application-firewall rule-sets social-network]
   user@host# user@host# set default-rule permit
   ```

5. Configure the outbound-traffic policy to apply the social-network rule-set to all outbound traffic.

```
[edit security policies from-zone trust to-zone untrust policy outbound-traffic]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos:HTTP
user@host# set then permit application-services application-firewall rule-set
  social-network
```

Results From configuration mode, confirm your configuration by entering the **show security application-firewall** and **show security policies** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show security application-firewall
...
rule-sets social-network {
  rule google-rule {
    match {
      dynamic-application junos:GOOGLETALK;
    }
  }
    then {
      permit ;
    }
  rule denied-sites {
    match {
      dynamic-application-groups junos:social-networking
      dynamic-application junos:UNKNOWN;
    }
    then {
      deny ;
    }
  }
  default-rule {
    permit;
  }
}
...
```

```
[edit]
user@host# show security policies
from-zone untrust to-zone trust {
  ...
  policy outbound-traffic {
    match {
      source-address any;
      destination-address any;
      application junos-http;
    }
    then {
      permit {
```

```
            application-services {
              application-firewall {
                rule-set social-network
              }
            }
          }
        }
      }
      ...
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Application Firewall Configuration

Purpose Verify information about application grouping support under the application firewall policy.

Action

- To verify the application firewall policy configuration enabled with application grouping, from the operational mode, enter the **show security policies** and **show security policies detail** commands.
- To verify all the application firewall rule sets configured on the device, from the operational mode, enter the **show security application-firewall rule-set all** command.
- To verify the list of applications defined within the application group, from the operational mode, enter the **show services application-identification application-group *application-group-name*** command.

See Also

- *Security Policies Configuration Overview*
- Customizing Application Groups for Junos OS Application Identification on page 55

Related Documentation

- *Application Identification*
- *Application Tracking*
- *Application QoS*
- *Advanced Policy-Based Routing*

Application Tracking on NFX Devices

Application tracking (AppTrack) is a logging and reporting tool that can be used to share information for application visibility. AppTrack sends log messages through syslog

providing application activity update messages. For more information, see the following topics:

Understanding AppTrack

AppTrack, an application tracking tool, provides statistics for analyzing bandwidth usage of your network. When enabled, AppTrack collects byte, packet, and duration statistics for application flows in the specified zone. By default, when each session closes, AppTrack generates a message that provides the byte and packet counts and duration of the session, and sends it to the host device. Juniper Secure Analytics (formally known as STRM) retrieves the data and provides flow-based application visibility.

AppTrack messages are similar to session logs and use syslog or structured syslog formats. The message also includes an application field for the session. If AppTrack identifies a custom-defined application and returns an appropriate name, the custom application name is included in the log message. (If the application identification process fails or has not yet completed when an update message is triggered, the message specifies **none** in the application field.)

AppTrack supports both IPv4 and IPv6 addressing. Related messages display addresses in the appropriate IPv4 or IPv6 format.

User identity details such as user name and user role have been added to the AppTrack session create, session close, and volume update logs. These fields will contain the user name and role associated with the policy match. The logging of user name and roles is enabled only for security policies that provide UAC enforcement. For security policies without UAC enforcement, the user name and user role fields are displayed as N/A. The user name is displayed as unauthenticated user and user role is displayed as N/A, if the device cannot retrieve information for that session because there is no authentication table entry for that session or because logging of this information is disabled. The user role field in the log contains the list of all the roles performed by the user if match criteria is specific, authenticated user, or any, and the user name field in the log contains the correct user name. The user role field in the log will contain N/A if the match criteria and the user name field in the log contain unauthenticated user or unknown user.

If you enable AppTrack for a zone and specify a **session-update-interval** time, whenever a packet is received, AppTrack checks whether the time since the start of the session or since the last update is greater than the update interval. If so, AppTrack updates the counts and sends an update message to the host. If a short-lived session starts and ends within the update interval, AppTrack generates a message only at session close.

When you want the initial update message to be sent earlier than the specified update interval, use the **first-update-interval**. The **first-update-interval** lets you enter a shorter interval for the first update only. Alternatively, you can generate the initial update message at session start by using the **first-update** option.

The close message updates the statistics for the last time and provides an explanation for the session closure. The following codes are used:

TCP RST—RST received from either end.

TCP FIN—FIN received from either end.

Response received—Response received for a packet request (such as **icmp req-reply**).

ICMP error—ICMP error received (such as **dest unreachable**).

Aged out—Session aged out.

ALG—ALG closed the session.

IDP—IDP closed the session.

Parent closed—Parent session closed.

CLI—Session cleared by a CLI statement.

Policy delete—Policy marked for deletion.

- Benefits of Application Tracking on page 75
- Application Tracking Log Messages Fields on page 75

Benefits of Application Tracking

- Provides visibility into the types of applications traversing through a device.
- Enables you to gain insight into permitted applications and the risk they might pose.
- Assists in managing bandwidth, reports active users and applications.

Application Tracking Log Messages Fields

The AppTrack session create, session close, and volume update logs include a new field called *destination interface*. You can use the **destination interface** field to see which egress interface is selected for the session when a advanced policy-based routing (APBR) is applied to that session and AppTrack is enabled and configured within any logical system.

AppTrack log for route update includes APBR profile, rule, and routing instance details. When APBR is applied to a session, the new log is generated and the AppTrack session counter is updated to indicate the number of times a new route update log is generated. The AppTrack session close log is also updated to include APBR profile, rule, and routing instance details.

AppTrack session create, session close, and volume update logs include the new fields **category** and **subcategory**. These fields provide general information about the application attributes. For example, the **category** field specifies the technology of the application (web, infrastructure) and **subcategory** field specifies the subcategory of the application (for example, social networking, news, and advertisements).

Because category and subcategory are not applicable for a custom application, the AppTrack log messages present the category as **custom application** and the subcategory as **N/A**.

For unknown applications, both category and subcategories are logged as **N/A**.

Examples of the log messages in structured syslog format:

APPTRACK_SESSION_CREATE user@host.1.1.1.2.129 source-address="4.0.0.1" source-port="48873" destination-address="5.0.0.1" destination-port="80" service-name="junos-http" application="UNKNOWN" nested-application="UNKNOWN" nat-source-address="4.0.0.1" nat-source-port="48873" nat-destination-address="5.0.0.1" nat-destination-port="80" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="permit-all" source-zone-name="trust" destination-zone-name="untrust" session-id-32="32" username="user1" roles="DEPT1" encrypted="UNKNOWN" destination-interface-name=”ge-0/0/0” category=”N/A” sub-category=”N/A”]

APPTRACK_SESSION_CLOSE [junos@2636.1.1.1.2.129 reason="TCP CLIENT RST" source-address="4.0.0.1" source-port="48873" destination-address="5.0.0.1" destination-port="80" service-name="junos-http" application="HTTP" nested-application="UNKNOWN" nat-source-address="4.0.0.1" nat-source-port="48873" nat-destination-address="5.0.0.1" nat-destination-port="80" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="permit-all" source-zone-name="trust" destination-zone-name="untrust" session-id-32="32" packets-from-client="5" bytes-from-client="392" packets-from-server="3" bytes-from-server="646" elapsed-time="3" username="user1" roles="DEPT1" encrypted="No" routing-instance=“default” destination-interface-name=”st0.0” category=” Web” sub-category=”N/A”]

APPTRACK_SESSION_VOL_UPDATE [user@host.1.1.1.2.129 source-address="4.0.0.1" source-port="33040" destination-address="5.0.0.1" destination-port="80" service-name="junos-http" application="HTTP" nested-application="FACEBOOK-SOCIALRSS" nat-source-address="4.0.0.1" nat-source-port="33040" nat-destination-address="5.0.0.1" nat-destination-port="80" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="permit-all" source-zone-name="trust" destination-zone-name="untrust" session-id-32="28" packets-from-client="371" bytes-from-client="19592" packets-from-server="584" bytes-from-server="686432" elapsed-time="60" username="user1" roles="DEPT1" encrypted="No" destination-interface-name=”st0.0” category=” Web” sub-category=”Social-Networking”]

APPTRACK_SESSION_ROUTE_UPDATE [user@host.1.1.1.2.129 source-address="4.0.0.1" source-port="33040" destination-address="5.0.0.1" destination-port="80" service-name="junos-http" application="HTTP" nested-application="FACEBOOK-SOCIALRSS" nat-source-address="4.0.0.1" nat-source-port="33040" nat-destination-address="5.0.0.1" nat-destination-port="80" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="permit-all" source-zone-name="trust" destination-zone-name="untrust" session-id-32="28" username="user1" roles="DEPT1" encrypted="No" profile-name=”pf1”

rule-name="facebook1" routing-instance="instance1" destination-interface-name="st0.0" category="Web" sub-category="Social-Networking"]

See Also

- *Example: Configuring AppTrack*
- *Disabling AppTrack*
- *Understanding Application Identification Techniques*

Example: Configuring AppTrack

This example shows how to configure the AppTrack tracking tool so you can analyze the bandwidth usage of your network.

Requirements

Before you configure AppTrack, ensure that you have downloaded the application signature package, installed it, and verified that the application identification configuration is working properly. See *Downloading and Installing the Junos OS Application Signature Package Manually* or *Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package*. Use the **show services application-identification status** command to verify the status.

Overview

Application identification is enabled by default and is automatically turned on when you configure the AppTrack, AppFW, or IDP service. The Juniper Secure Analytics (JSA) retrieves the data and provides flow-based application visibility. STRM includes the support for AppTrack Reporting and includes several predefined search templates and reports.

Configuration

This example shows how to enable application tracking for the security zone named trust. The first log message is to be generated when the session starts, and update messages should be sent every 4 minutes after that. A final message should be sent at session end.

The example also shows how to add the remote syslog device configuration to receive AppTrack log messages in sd-syslog format. The source IP address that is used when exporting security logs is 192.0.2.1, and the security logs are sent to the host located at address 192.0.2.2.

NOTE: **We recommend using CLI for configuration of AppSecure features.**

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

NOTE: Changing the session-update-interval and the first-update-interval is not necessary in most situations. The commands are included in this example to demonstrate their use.

```
user@host# set security log mode stream
user@host# set security log format sd-syslog
user@host# set security log source-address 192.0.2.1
user@host# set security log stream app-track-logs host 192.0.2.2
user@host#set security zones security-zone trust application-tracking
user@host#set security application-tracking session-update-interval 4
user@host#set security application-tracking first-update
```

NOTE: If the syslog configuration does not specify a destination port, the default destination port will be the syslog port. If you specify a destination port in the syslog configuration, then that port will be used instead.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *CLI User Guide*.

To configure AppTrack:

1. Add the remote syslog device configuration to receive Apptrack messages in sd-syslog format.

   ```
   [edit]
   user@host# set security log mode stream
   user@host# set security log format sd-syslog
   user@host# set security log source-address 192.0.2.1
   user@host# set security log stream app-track-logs host 192.0.2.2
   ```

2. Enable AppTrack for the security zone trust.

   ```
   [edit]
   user@host# set security zones security-zone trust application-tracking
   ```

3. (Optional) For this example, generate update messages every 4 minutes.

   ```
   [edit]
   user@host# set security application-tracking session-update-interval 4
   ```

   The default interval between messages is 5 minutes. If a session starts and ends within this update interval, AppTrack generates one message at session close.

However, if the session is long-lived, an update message is sent every 5 minutes. The **session-update-interval** ***minutes*** is configurable as shown in this step.

4. (Optional) For this example, generate the first message when the session starts.

```
[edit]
user@host# set security application-tracking first-update
```

By default, the first message is generated after the first session update interval elapses. To generate the first message at a different time than this, use the **first-update** option (generate the first message at session start) or the **first-update-interval** ***minutes*** option (generate the first message after the specified minutes). For example, enter the following command to generate the first message one minute after session start.

```
[edit]
user@host# set security application-tracking first-update-interval 1
```

NOTE: The first-update option and the first-update-interval *minutes* option are mutually exclusive. If you specify both, the first-update-interval value is ignored.

Once the first message has been generated, an update message is generated each time the session update interval is reached.

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

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show security

...
application-tracking {
   first-update;
   session-update-interval 4;
}
log {
   mode stream;
   format sd-syslog;
   source-address192.0.2.2;
   stream app-track-logs {
      host {
         192.0.2.1;
      }
   }
```

```
}
...

[edit]
user@host# show security zones
...
security-zone trust {
   ...
   application-tracking;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Use the JSA product on the remote logging device to view the AppTrack log messages.

To confirm that the configuration is working properly, you can also perform these tasks on the device:

- Reviewing AppTrack Statistics on page 80
- Verifying AppTrack Counter Values on page 81
- Verifying Security Flow Session Statistics on page 81
- Verifying Application System Cache Statistics on page 81
- Verifying the Status of Application Identification Counter Values on page 82

Reviewing AppTrack Statistics

Purpose Review AppTrack statistics to view characteristics of the traffic being tracked.

Action From operational mode, enter the **show services application-identification statistics applications** command.

```
user@host> show services application-identification statistics applications

Last Reset: 2012-02-14 21:23:45 UTC

Application    Sessions              Bytes    Encrypted
HTTP                  1               2291          Yes
HTTP                  1                942           No
SSL                   1               2291          Yes
unknown               1                100           No
unknown               1                100          Yes
```

NOTE: For more information on the **show services application-identification statistics applications** command, see show services application-identification statistics applications.

Verifying AppTrack Counter Values

Purpose View the AppTrack counters periodically to monitor logging activity.

Action From operational mode, enter the **show security application-tracking counters** command.

```
user@host> show security application-tracking counters

AVT counters:                 Value
 Session create messages           1
 Session close messages            1
 Session volume updates            0
 Failed messages                   0
```

Verifying Security Flow Session Statistics

Purpose Compare byte and packet counts in logged messages with the session statistics from the **show security flow session** command output.

Action From operational mode, enter the **show security flow session** command.

```
user@host> show security flow session

Flow Sessions on FPC6 PIC0:

Session ID: 120000044, Policy name: policy-in-out/4, Timeout: 1796, Valid
In: 192.0.2.1/24 --> 198.51.100.0/21;tcp, If: ge-0/0/0.0, Pkts: 22, Bytes: 1032
Out: 198.51.100.0/24 --> 192.0.2.1//39075;tcp, If: ge-0/0/1.0, Pkts: 24, Bytes:
1442

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

Byte and packet totals in the session statistics should approximate the counts logged by AppTrack but might not be exactly the same. AppTrack counts only incoming bytes and packets. System-generated packets are not included in the total, and dropped packets are not deducted.

Verifying Application System Cache Statistics

Purpose Compare cache statistics such as IP address, port, protocol, and service for an application from the **show services application-identification application-system-cache** command output.

Action From operational mode, enter the **show services application-identification application-system-cache** command.

Verifying the Status of Application Identification Counter Values

Purpose Compare session statistics for application identification counter values from the **show services application-identification counter** command output.

Action From operational mode, enter the **show services application-identification counter** command.

See Also
- *Configuring Off-Box Binary Security Log Files*
- *Understanding On-Box Logging and Reporting*
- *log (Security Policies)*

Configuring AppTrack When SSL Proxy Is Enabled

This configuration procedure describes how AppTrack supports AppID functionality when SSL proxy is enabled.

Requirements

Before you begin:

- Create zones. See *Example: Creating Security Zones*.
- Create an SSL proxy profile that enables SSL proxy by means of a policy. See *Configuring SSL Forward Proxy*.

Overview

You can configure AppTrack either in the to or from zones. This example shows how to configure AppTrack in a to zone in a policy rule when SSL proxy is enabled.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone Z_1 application-tracking
set security policies from-zone Z_1 to-zone Z_2 policy policy1 match source-address any
set security policies from-zone Z_1 to-zone Z_2 policy policy1 match destination-address
  any
set security policies from-zone Z_1 to-zone Z_2 policy policy1 then permit
  application-services ssl-proxy profile-name ssl-profile-1
set security policies from-zone Z_1 to-zone Z_2 policy policy1 then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

In this example, you configure application tracking and permit application services in an SSL proxy profile configuration.

1. Configure application tracking in a to-zone (you can also configure using a from-zone).

```
[edit security policies]
user@host# set security zones security-zone Z_1 application-tracking
```

2. Configure SSL proxy profile.

```
[edit security policies from-zone Z_1 to-zone Z_2 policy policy1]
set match source-address any
set match destination-address any
set match application junos-https
set then permit application-services ssl-proxy profile-name ssl-profile-1
set then permit
```

Results

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

```
from-zone Z_1 to-zone Z_2 {
   policy policy1 {
      match {
         source-address any;
         destination-address any;
      }
      then {
         permit {
            application-services {
               ssl-proxy {
                  profile-name ssl-profile-1;
               }
            }
         }
      }
   }
}
```

NOTE: Verify that the configuration is working properly. Verification in AppTrack works similarly to verification in AppFW. See the verification section of *Example: Configuring Application Firewall When SSL Proxy Is Enabled*.

See Also

- *SSL Proxy Overview*

- *Application Firewall, IDP, and Application Tracking with SSL Proxy Overview*

Disabling AppTrack

Application tracking is enabled by default. You can disable application tracking without deleting the zone configuration.

To disable application tracking:

```
user@host# set security application-tracking disable
```

If application tracking has been previously disabled and you want to reenable it, delete the configuration statement that specifies disabling of application tracking:

```
user@host# delete security application-tracking disable
```

If you are finished configuring the device, commit the configuration.

To verify the configuration, enter the **show security application-tracking** command.

Related Documentation

- *Application Identification*
- *Application Firewall*
- *Application QoS*
- *Advanced Policy-Based Routing*

Application QoS on NFX Devices

Application quality of service (AppQoS) enables you to identify and control access to specific applications and provides the granularity of the stateful firewall rule base to match and enforce QoS at the application layer. For more information, see the following topics:

- Understanding Application QoS (AppQoS) on page 84
- Example: Configuring AppQoS on page 91

Understanding Application QoS (AppQoS)

The application quality of service (AppQoS) feature expands the capability of Junos OS class of service (CoS) to include marking DSCP values based on Layer-7 application types, honoring application-based traffic through loss priority settings, and controlling transfer rates on egress PICs based on Layer-7 application types.

There are four ways to mark DSCP values on a device:

- IDP attack action-based DSCP rewriters
- Layer 7 application-based DSCP rewriters
- ALG-based DSCP rewriters
- Firewall filter-based DSCP rewriters

IDP remarking is conducted at the ingress port based on IDP rules. Application remarking is conducted at the egress port based on application rules. Interface-based remarking also occurs at the egress port based on firewall filter rules. (See the *Class of Service Feature Guide for Security Devices* for a detailed description of Junos OS CoS features.)

The remarking decisions of these three rewriters can be different. If a packet triggers all three, the method that takes precedence is based on how deep into the packet content the match is conducted. IDP remarking has precedence over application remarking which has precedence over interface-based remarking.

If a packet triggers both AppQoS and ALG-based DSCP rewriters, then AppQoS takes precedence over ALG-based DSCP rewriters.

The AppQoS DSCP rewriter conveys a packet's quality of service through both the forwarding class and a loss priority. The AppQoS rate-limiting parameters control the transmission speed and volume for its associated queues.

Benefit of Application QoS

AppQoS provides the ability to prioritize and meter the application traffic to provide better service to business-critical or high-priority application traffic.

Unique Forwarding Classes and Queue Assignments

The forwarding class provides three functions:

- Groups packets with like characteristics
- Assigns output queues
- Resolves conflicts with existing Junos OS firewall filter-based rewriters

Unique forwarding class names protect AppQoS remarking from being overwritten by interface-based rewrite rules. A firewall filter-based rewriter remarks a packet's DSCP value if the packet's forwarding class matches a class defined specifically for this rewriter. If the packet's forwarding class does not match any of the firewall filter-based rewriter's classes, the DSCP value is not remarked. To protect AppQoS values from being overwritten, therefore, use forwarding class names that are unknown to the firewall filter-based rewriter.

Each forwarding class is assigned to an egress queue that provides the appropriate degree of enhanced or standard processing. Many forwarding classes can be assigned to a single queue. Therefore, any queues defined for the device can be used by IDP, AppQoS, and

firewall filter-based rewriters. It is the forwarding class name, not the queue, that distinguishes the transmission priority. (See the *Class of Service Feature Guide for Security Devices* for information about configuring queues and schedulers.)

The AppQoS forwarding class names and queue assignments are defined with the **class-of-service** CLI configuration command:

```
[edit class-of-service]
user@host# forwarding-classes class forwarding-class-name queue-num queue-number
```

Application-Aware DSCP Code-Point and Loss Priority Settings

For AppQoS, traffic is grouped based on rules that associate a defined forwarding class with selected applications. The match criteria for the rule includes one or more applications. When traffic from a matching application encounters the rule, the rule action sets the forwarding class, and remarks the DSCP value and loss priority to values appropriate for the application.

A Differentiated Services (DiffServ) code point (DSCP) value is specified in the rule either by a 6-bit bitmap value or by a user-defined or default alias. Table 3 on page 86 provides a list of Junos OS default DSCP alias names and bitmap values.

Table 3: Standard CoS Aliases and Bit Values

CoS Value Type	Alias	Bit Value
Expedited forwarding	ef	101110
Assured forwarding	af11	001010
Assured forwarding	af12	001100
Assured forwarding	af13	001110
Assured forwarding	af21	010010
Assured forwarding	af22	010100
Assured forwarding	af23	010110
Assured forwarding	af31	011010
Assured forwarding	af32	011100
Assured forwarding	af33	011110
Assured forwarding	af41	100010
Assured forwarding	af42	100100
Assured forwarding	af43	100110

Table 3: Standard CoS Aliases and Bit Values (continued)

CoS Value Type	Alias	Bit Value
Best effort	be	000000
	cs1	001000
	cs2	010000
	cs3	011000
	cs4	100000
	cs5	101000
Network control	nc1/cs6	110000
Network control	nc2/cs7	111000

The queue's scheduler uses the loss priority to control packet discard during periods of congestion by associating drop profiles with particular loss priority values. (See the *Class of Service Feature Guide for Security Devices* for information about configuring queues and schedulers.)

The rule applies a loss priority to the traffic groups. A high loss priority means a high probability that the packet could be dropped during a period of congestion. Four levels of loss priority are available:

- **high**
- **medium-high**
- **medium-low**
- **low**

The rule set is defined in the **class-of-service application-traffic-control** configuration command:

```
[edit class-of-service]
user@host# application-traffic-control rule-sets ruleset-name rule rule-name1 match
   application application-name application-name ...
user@host# application-traffic-control rule-sets ruleset-name rule rule-name1 match
   application-group application-group-name application-group-name ...
user@host# application-traffic-control rule-sets ruleset-name rule rule-name1 then
   forwarding-class fc-name
user@host# application-traffic-control rule-sets ruleset-name rule rule-name1 then
   dscp-code-point bitmap
user@host# application-traffic-control rule-sets ruleset-name rule rule-name1 then
   loss-priority loss-pri-value
```

Rate Limiters and Profiles

When congestion occurs, AppQoS implements rate limiting on all egress PICs on the device. If packets exceed the assigned limitations, they are dropped. *Rate limiters* maintain a consistent level of throughput and packet loss sensitivity for different classes of traffic. All egress PICs employ the same rate-limiting scheme.

The total bandwidth of a PIC is about 10 Gbps. Rate-limiter hardware for the PIC can provision up to 2 Gbps. Therefore, the upper bandwidth limit for rate limiting is 2^{31} bps.

A rate-limiter profile defines the limitations. It is a unique combination of **bandwidth-limit** and **burst-size-limit** specifications. The **bandwidth-limit** defines the maximum number of kilobits per second that can traverse the port. The **burst-size-limit** defines the maximum number of bytes that can traverse the port in a single burst. The **burst-size-limit** reduces starvation of lower priority traffic by ensuring a finite size for each burst.

AppQoS allows up to 16 profiles and up to 1000 rate limiters per device. Multiple rate limiters can use the same profile. In the following example, five rate limiters are defined using two profiles:

	Profile	
Rate Limiter Name	bandwidth-limit	burst-size-limit
limiter-1	200	26000
limiter-2	200	26000
limiter-3	200	26000
limiter-4	400	52000
limiter-5	400	52000

Rate limiters are defined with the **class-of-service application-traffic-control** configuration command.

```
[edit class-of-service]
user@host# application-traffic-control rate-limiters rate-limiter-name bandwidth-limit
   value-in-Kbps burst-rate-limit value-in-bytes
```

Rate-Limiter Assignment

Rate limiters are applied in rules based on the application of the traffic. Two rate limiters are applied for each session: **client-to-server** and **server-to-client**. This usage allows traffic in each direction to be provisioned separately.

Different AppQoS rules within the same rule set can share a rate limiter. In this case, the applications of those rules share the same bandwidth. There are no limitations on the number of rules in one rule set that can assign the same rate limiter.

The following examples show how the rate limiters defined in the preceding section could be assigned. For instance, a rule set could reuse a rate limiter in several rules and in one or both flow directions:

- rule-set-1
  - rule-1A
    - client-to-server limiter-1
    - server-to-client limiter-1
  - rule-1B
    - client-to-server limiter-1
    - server-to-client limiter-1

If the same profiles are needed in several rule sets, a sufficient number of rate limiters needs to be defined specifying the same **bandwidth-limit** and **burst-size-limit**. The two rule sets in the following example implement the same profiles by assigning different, but comparable, rate limiters.

- rule-set-2
  - rule-2A
    - client-to-server limiter-2
    - server-to-client limiter-2
  - rule-2B
    - client-to-server limiter-2
    - server-to-client limiter-4
- rule-set-3
  - rule-3A
    - client-to-server limiter-3
    - server-to-client limiter-3
  - rule-3B
    - client-to-server limiter-3
    - server-to-client limiter-5

A rate limiter is applied using the **class-of-service application-traffic-control rule-sets** command in the same way that a forwarding class, DSCP value, and loss priority are set.

```
[edit class-of-service]
user@host# application-traffic-control rule-sets rule-set-name rule rule-name1 then
   rate-limit client-to-server rate-limiter1 server-to-client rate-limiter2
```

If AppQoS and firewall filter-based rate limiting are both implemented on the egress PIC, both are taken into consideration. AppQoS rate limiting is considered first. Firewall filter-based rate limiting occurs after that.

NOTE: If packets are dropped from a PIC, the device does not send notifications to the client or the server. The upper-level applications on the client and the server devices are responsible for retransmission and error handling.

Rate-Limiter Action

Based on the type of the device, AppQoS rules can be configured with different rate-limiter actions:

- Discard
  - When this option is selected, the out-of-profile packets are just dropped.
  - This is the default action type and need not be configured.
  - This option is supported on all devices.
- Loss-priority-high
  - When this option is selected , it elevates the loss priority to maximum. In other words, it is a delayed drop; that is, the discard decision is taken at the egress output queue level. If there is no congestion, it allows the traffic even with maximum loss priority. But if congestion occurs, it drop these maximum loss priority packets first.
  - This option must be configured within the AppQoS rule (to override the default action) using the following command:

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets rset-01 rule r1
   then rate-limit loss-priority-high
```

AppQoS Security Policy Configuration

The AppQoS rule set can be implemented in an existing policy or a specific application policy.

```
[edit]
user@host# security policies from-zone zone-name to-zone zone-name
[edit security policies from-zone zone-name to-zone zone-name]
user@host# policy policy-name match source-address IP-address
user@host# policy policy-name match destination-address IP-address
user@host# policy policy-name match application application-name application-name
user@host# policy policy-name then permit application-services application-traffic-control
   rule-set app-rule-set-name
```

See Also

- *Understanding Class of Service*

Example: Configuring AppQoS

This example shows how to enable AppQoS prioritization and rate limiting within a policy.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, AppQoS is implemented so that FTP applications are restricted to a level below the specified throughput while other applications are transmitted at a more conventional speed and loss priority level.

NOTE: We recommend using CLI for configuration of AppSecure features.

Configuration

Step-by-Step Procedure

To configure an AppQoS implementation:

1. Define one or more forwarding classes dedicated to AppQoS marking. In this example, a single forwarding class, my-app-fc, is defined and assigned to queue 0.

   ```
   [edit]
   user@host# set class-of-service forwarding-classes queue-num 0 my-app-fc
   ```

2. Define rate limiters. In this example, two rate limiters are defined.

   NOTE: You can define up to 1000 rate limiters for a device, but only 16 profiles (unique bandwidth-limit and burst-size-limit combinations).

   - test-r1 with a bandwidth of 100 Kbps and a burst limit of 13,000 bytes
   - test-r2 with a bandwidth of 200 Kbps and a burst limit of 26,000 bytes

   ```
   [edit]
   user@host# set class-of-service application-traffic-control rate-limiters test-rl
     bandwidth-limit 100
   user@host# set class-of-service application-traffic-control rate-limiters test-rl
     burst-size-limit 13000
   user@host# set class-of-service application-traffic-control rate-limiters test-r2
     bandwidth-limit 200
   ```

```
user@host# set class-of-service application-traffic-control rate-limiters test-r2
  burst-size-limit 26000
```

3. Define AppQos rules and application match criteria. For this example, rule 0 in rule set ftp-test1 is applied to junos:FTP packets.

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 match application junos:FTP
```

4. Define the action for rule 0 when it encounters a junos:FTP packet. In this example, when a match is made, the packet is marked with the forwarding class my-app-fc, the DSCP value of af22, and a loss priority of low.

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then forwarding-class my-app-fc
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then dscp-code-point af22
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then loss-priority low
```

5. Assign rate limiters for rule 0 to traffic in each direction. In this case, the rate limiter test-r1 is set in both directions.

NOTE: Rate limiter test-r1 can be assigned to one or both traffic directions in rule 0. It could also be assigned in other rules within rule set ftp-test1. However, once test-r1 is assigned to rule set ftp-test1, it cannot be assigned in any other rule set.

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then rate-limit client-to-server test-r1
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then rate-limit server-to-client test-r1
```

6. Log the AppQoS event whenever this action is triggered:

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  0 then log
```

7. Define other rules to handle application packets that did not match the previous rule. In this example, a second and final rule applies to all remaining applications.

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 match application-any
```

8. Assign rate limiters for the second rule. In this example, any traffic that is not from FTP is assigned rate limiter test-r2 in both directions.

```
[edit]
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 then rate-limit client-to-server test-r2
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 then rate-limit server-to-client test-r2
user@host# set class-of-service application-traffic-control rule-sets ftp-test1 rule
  1 then log
```

9. Add the AppQoS implementation to a policy. In this example, policy p1 applies the rule set ftp-test1 to all traffic from the trust zone to the untrust zone.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy p1
[edit security policies from-zone trust to-zone untrust policy p1]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application any
user@host# set then permit application-services application-traffic-control rule-set
  ftp-test1
```

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

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
...
policy p1 {
  match {
    source-address any;
    destination-address any;
    application any;
  }
  then {
    permit {
      application-services {
        application-traffic-control {
          rule-set ftp-test1
        }
      }
    }
  }
}
...
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Flow Session Configuration

Purpose Verify that AppQoS is enabled.

Action From operational mode, enter the **show security flow session application-traffic-control extensive** command.

```
user@host> show security flow session application-traffic-control extensive
  Session ID: 3729, Status: Normal, State: Active
  Flag: 0x40
  Policy name: p1
  Source NAT pool: Null
  Dynamic application: junos:FTP
  Application traffic control rule-set: ftp-test1, Rule: rule0
  Maximum timeout: 300, Current timeout: 276
  Session State: Valid
  Start time: 18292, Duration: 603536
     In: 192.0.2.1/1 --> 203.0.113.0/1;pim,
      Interface: reth1.0,
      Session token: 0x1c0, Flag: 0x0x21
      Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
      Port sequence: 0, FIN sequence: 0,
      FIN state: 0,
      Pkts: 21043, Bytes: 1136322
     Out: 203.0.113.0/1 --> 192.0.2.0/1;pim,
      Interface: .local..0,
      Session token: 0x80, Flag: 0x0x30
      Route: 0xfffd0000, Gateway: 192.0.2.0, Tunnel: 0
      Port sequence: 0, FIN sequence: 0,
      FIN state: 0,
      Pkts: 0, Bytes: 0
```

Meaning The entry for application traffic control identifies the rule set and rule of the current session.

Verifying Session Statistics

Purpose Verify that AppQoS session statistics are being accumulated at each egress node.

Action From operational mode, enter the **show class-of-service application-traffic-control counter** command.

```
user@host> show class-of-service application-traffic-control counter
pic: 2/1
  Counter type                                          Value
  Sessions processed                                    300
  Sessions marked                                       200
  Sessions honored                                      0
  Sessions rate limited                                 100
  Client-to-server flows rate limited                   100
  Server-to-client flows rate limited                   100

pic: 2/0
  Counter type                                          Value
  Sessions processed                                    400
  Sessions marked                                       300
  Sessions honored                                      0
  Sessions rate limited                                 200
  Client-to-server flows rate limited                   200
  Server-to-client flows rate limited                   200
```

Meaning The AppQoS statistics are maintained only if application-traffic-control service is enabled. The number of sessions processed, marked, and honored show that sessions are being directed based on configured AppQoS features. The rate-limiting statistics count the number of directional session flows that have been rate limited.

Verifying Rate-Limiter Statistics

Purpose Verify that bandwidth is being limited as expected when the FTP application is encountered.

Action From operational mode, enter the **show class-of-service application-traffic-control statistics rate-limiter** command.

```
user@host> show class-of-service application-traffic-control statistics
rate-limiter
pic: 2/1
  Ruleset    Application  Client-to-server Rate(kbps)  Server-to-client Rate(kbps)

  ftp-test1     HTTP      test-r2           200       test-r2          200
  ftp-test1     HTTP      test-r2           200       test-r2          200
  ftp-test1     FTP       test-r1           100       test-r1          100
```

Meaning Real-time application bandwidth-limit information for each PIC is displayed by rule set. This command provides an indication of the applications being rate limited and the profile being applied.

Verifying Rule Statistics

Purpose Verify that the rule matches the rule statistics.

Action From operational mode, enter the **show class-of-service application-traffic-control statistics rule** command.

```
user@host>show class-of-service application-traffic-control statistics rule
pic: 2/1
  Ruleset          Rule           Hits
  ftp-test1        0              100
  ftp-test1        1              200
  ...

pic: 2/0
  Ruleset          Rule           Hits
  ftp-test1        0              100
  ftp-test1        1              200
```

Meaning This command provides information on the number of (session) hits for a rule under each rule set.

See Also
- *CoS Device Configuration Overview*

Related Documentation
- *Application Identification*
- *Application Firewall*
- *Application Tracking*
- *Advanced Policy-Based Routing*

Advanced Policy-Based Routing on NFX Devices

Advanced policy-based routing (APBR) also known as application-based routing, a new addition to Juniper Networks suite, provides the ability to forward traffic based on applications. For more information, see the following topics:

- Understanding Advanced Policy-Based Routing on page 96
- Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 103
- Configuring Advanced Policy-Based Routing Policies on page 110
- Example: Configuring Advanced Policy-Based Routing Policies on page 111

Understanding Advanced Policy-Based Routing

The relentless growth of voice, data, and video traffic and applications traversing on the network requires that networks recognize traffic types to effectively prioritize, segregate,

and route traffic without compromising performance or availability. Juniper devices support advanced policy-based routing (APBR) to address these challenges.

This topic includes the following sections:

Application Identification

Juniper devices support application identification (AppID) using deep packet inspection (DPI) technology. Junos OS application identification recognizes Web-based and other applications and protocols at different network layers using characteristics other than port number. Applications are identified by using a protocol bundle containing application signatures and parsing information. The identification is based on protocol parsing and decoding and session management. An application system cache (ASC) is maintained, where the applications identified are cached based on server (destination) IP address and port and logical system identification.

ASC saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. Once an application is identified, its information is saved in the ASC so that only one matching entry is required for an application running on a particular system. When the cache entry is present and it is valid, the identified application is picked from cache, thereby expediting the identification process.

Filter-Based Forwarding or Policy-Based Routing (PBR)

Juniper devices support filter-based forwarding, also known as policy-based routing (PBR), in which data packets are forwarded and routed based on the defined policies or filters. PBR includes a mechanism for selectively applying policies based on access list, packet size, or other criteria and routing the packets on user-defined routes.

When a device receives a packet, it routes the packets based on the information present in the packet header such as destination port, source IP address, and incoming interfaces. While processing an incoming packet, the device performs a routing table lookup to find the appropriate interface that leads to the destination address.

However, in some cases, you might need to forward the packet based on other criteria. In filter-based forwarding, you must create a filter that will match the type of traffic that you are going to direct to a different next hop. You can define matching criteria such as IP address, port, protocol, TCP flags, and much more. Once you have defined your term

to include the match criteria, the action will be to send the traffic to an appropriate route and corresponding interface.

For example, perhaps you want to offer services to your customers, and the services reside on different servers. You can use filter-based forwarding to send traffic to the servers by applying a match condition in the packet header such as destination port, source IP address, and incoming interfaces, and send the packets to a certain outgoing interface that is associated with the appropriate server.

Advanced Policy-Based Routing

Advanced policy-based routing is a type of session-based, application-aware routing. This mechanism combines the policy-based routing and application-aware traffic management solution. APBR implies classifying the flows based on applications' attributes and applying filters based on these attributes to redirect the traffic. The flow-classifying mechanism is based on packets representing the application in use.

APBR implements:

- Deep packet inspection and pattern-matching capabilities of AppID to identify application traffic or a user session within an application
- Lookup in ASC for application type and the corresponding destination IP address, destination port, protocol type, and service for a matching rule

If a matching rule is found, the traffic is directed to an appropriate route and the corresponding interface or device.

Benefits of APBR

- Enables you to define the routing behavior based on applications.
- Provides more flexible traffic-handling capabilities and offers granular control for forwarding packets based on application attributes.

Understanding How APBR Works

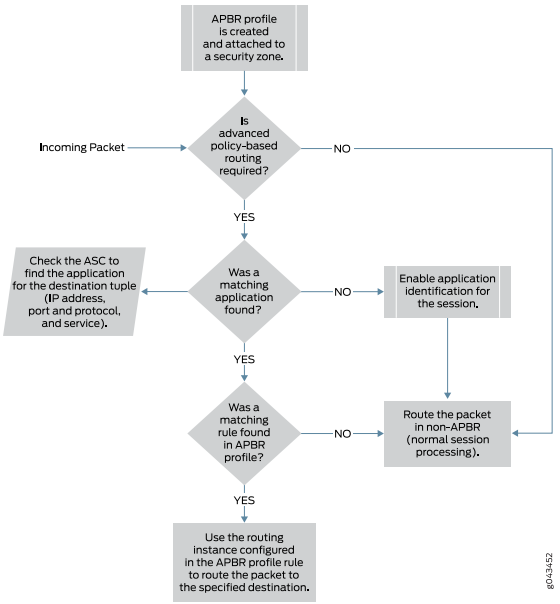
The following steps are involved in APBR:

- Create an APBR profile (also referred to as an application profile in this document) that will match the type of traffic that you are going to direct to a different next hop. The profile includes multiple rules. Each rule can contain multiple applications or application groups. If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered as a match.
- Associate a routing instance with the application profile rule. When the traffic on the ingress zone and interface matches an application profile, the associated static route and next hop defined in the routing instance is used to route the traffic for the particular session.
- Associate the application profile to the ingress traffic The application profile can be attached to a security zone or it can be attached to a specific logical or physical interface associated with the security zone. If the application profile is applied to a security zone,

then all interfaces belonging to that zone are attached to the application profile by default unless a specific configuration already exists for that interface.

Figure 2 on page 99 shows the sequence in which APBR techniques are applied.

Figure 2: APBR Flow Diagram



1. APBR evaluates the packets based on incoming interface to determine if the session is candidate for application-based routing. If the traffic has not been flagged for application-based routing, it undergoes normal processing (non-APBR route).
2. If the session needs application-based routing, APBR queries the application system cache (ASC) module to get the application attributes details (IP address, destination port, protocol type, and service).

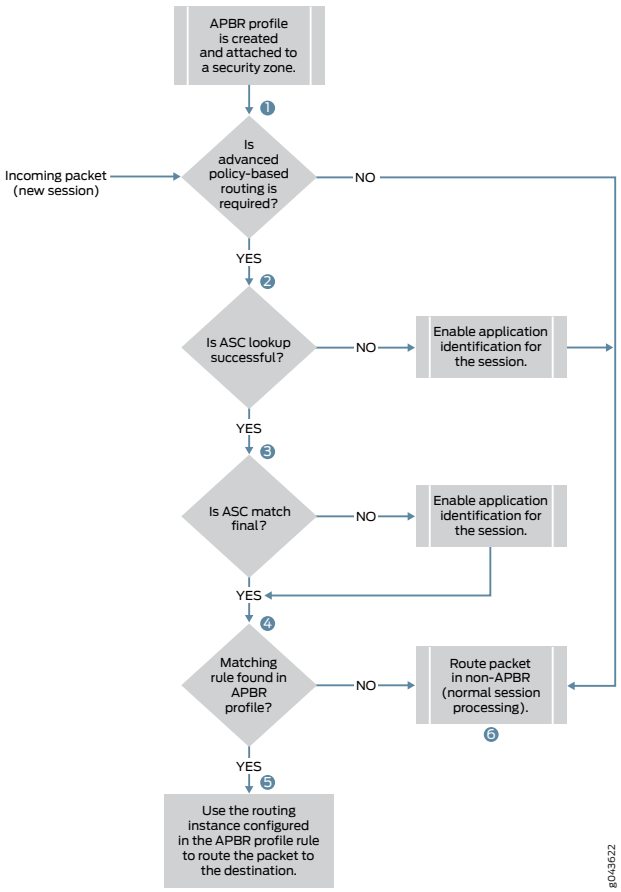
   If the ASC is found, it is further processed for a matching rule in the APBR profile (see Step 3). If the ASC is not found and the application signature is installed and ASC is enabled, application identification for the session is enabled so that ASC can be populated for use by subsequent sessions for the destination tuple.
3. APBR uses the application details to look for a matching rule in the APBR profile (application profile). If a matching rule is found, the traffic will be redirected to the specified routing instance for the route lookup.

Advanced Policy-Based Routing Midstream Support

Juniper devices support advanced policy-based routing (APBR) with an additional enhancement to apply the APBR in the middle of a session (which is also known as midstream support). With this enhancement, you can apply APBR for a non-cacheable application and also for the first session of the cacheable application. The enhancement provides more flexible traffic-handling capabilities that offer granular control for forwarding packets.

Figure 3 on page 100 shows the sequence in which APBR techniques with midstream support are applied.

Figure 3: APBR with Midstream Support Flow Diagram



Step 1: APBR evaluates the packets based on incoming security zone to determine if the session is candidate for application-based routing. If this is first packet of the new session and traffic is not flagged for application-based routing, it undergoes normal processing (non-APBR route) step 6.

Step 2: If the session needs application-based routing, APBR queries the application system cache (ASC) module to get the application attributes details (IP address, destination port, protocol type, and service). If the ASC is found, it is further processed to determine if the application match using ASC is final (see Step 3). APBR could also identify applications using ALG for the data sessions. If the application is matched using the ALG it is considered as final match. If the final application has not been identified, the DPI engine is engaged for the session to identify the application. The existing session undergoes normal processing (non-APBR route) step 6.

Step 3: If an application has been identified, it is further processed for a matching rule in the APBR profile (see Step 4).

Step 4: APBR uses the application details to look for a matching rule in the APBR profile (application profile). If a matching rule is found, the traffic will be redirected to the specified routing instance for the route lookup. If matching rule is not found, it undergoes normal processing (non-APBR route) (see step 6).

Step 5: Traffic is routed through the specified routing instance for the destination.
Step 6: Traffic traverses through a default route (non-APBR route) to the destination.

For a new session, when application cannot be identified based on first packet information the traffic traverses through a default route (non-APBR route) to the destination. At the same time, APBR is applied and the rest of the session packets passes through the route as per the rules defined in the APBR profile. This means that, APBR rules are applied as and when an application is identified by AppID. For first packet of session, always go through midstream re-routing case. That is, when the application is not yet identified, the traffic traverses through a default route (non-APBR route) to the destination. At the same time, application identification is enabled for that session. This continues still application signatures identify the application and APBR is applied and the rest of the session packets passes through the route as per the rules defined in the APBR profile. The traffic traverses through a non-APBR route till application signatures or ALG identify the application.

You can enable, AppTrack to inspect traffic and collect statistics for application flows in the specified zone. See *Understanding AppTrack* for more details.

Advanced Policy-Based Routing Options For Streamlining Traffic Handling

You can streamline the traffic handling with APBR by using the following options:

- **Limit route change**- Some sessions go through continuous classification in the middle of the session as application signatures identify the application. Whenever an application is identified by the application signatures, APBR is applied, and this results in a change in the route of the traffic. You can limit the number of times a route can change for a session by using the **max-route-change** option of the **tunables** statement.

  set security advance-policy-based-routing tunables max-route-change *value*

  Example:

  ```
  [edit]
  set security advance-policy-based-routing tunables max-route-change 5
  ```

  In this example, you want to limit the number of route changes per session to 5. When there is a change in the route in the middle of the session, this count is reduced to 4. This process continues until the count reaches 0. After that, APBR is not applied in the middle of the session.

  If an identified application has an entry in the ASC, then, the count is not reduced for that session, because the session started with the specified route according to the APBR configuration.

- **Terminate session if APBR is bypassed**—You can terminate the session if there is a mismatch between zones when APBR is being applied in the middle of the session. When you want to apply APBR in the middle of a session, both new egress interface and existing egress interface must be part of the same zone. If you change the zone

for an interface in the middle of a session, then, by default, APBR is not applied, and the traffic continues to traverse through the existing interface. To change this default behavior, you can terminate the session entirely, instead of allowing traffic to traverse through the same route bypassing APBR, by using the **drop-on-zone-mismatch** option of the **tunables** statement.

Example:

```
[edit]
set security advance-policy-based-routing tunables drop-on-zone-mismatch
```

- **Enable logging**—You can enable logging to record events that occur on the device, for instance, when APBR is bypassed because of a change in the zones for interfaces. You can use the **enable-logging** option of the **tunables** statement to configure the logging.

  Example:

  ```
  [edit]
  set security advance-policy-based-routing tunables enable-logging
  ```

- **Enable reverse reroute**—For deployments that require traffic symmetry for ECMP routes, and the incoming traffic needs to switch in the middle of session, the rerouting can be achieved using the option enable-reverse-reroute specific to a security zone as follows:

  Example:

  ```
  [edit]

  set security zones security-zone zone-name enable-reverse-reroute
  ```

  When the above configuration is enabled for a security zone, where an incoming packet arrives on an interface and has a different outgoing/return interface, a change in the interface is detected and triggers a reroute. A route lookup is performed for the reverse path, and the preference will be given to the interface on which the packet has arrived.

  Further processing stops for a particular session when a route lookup fails for the traffic on reverse path.

Use Case

- When multiple ISP links are used:
  - APBR can be used for selecting high-bandwidth, low-latency links for important applications, when more than one link is available.
  - APBR can be used for creating a fallback link for important traffic in case of link failure. When multiple links are available, and the main link carrying the important application traffic suffers an outage, then the other link configured as the fallback link can be used to carry traffic.
  - APBR can be used for segregating the traffic for deep inspection or analysis. With this feature, you can classify the traffic based on applications that are required to

go through deep inspection and audit. If required, such traffic can be routed to a different device.

Limitations

APBR has the following limitations:

- APBR does not work if an application signature package is not installed or application identification is not enabled.
- APBR does not work for Layer 3 and Layer 4 applications, because the Layer 3 and Layer 4 applications custom signatures are not maintained in the ASC.

APBR with midstream support has the following limitations:

- APBR works only for forward traffic.
- APBR does not work for data sessions initiated by an entity from the control session, such as active FTP.
- When using different NAT pools for source NAT and midstream APBR is applied, the source IP address of the session continues to be the same as the one with which the session has been using before applying the midstream APBR.
- APBR with midstream support works only when all egress interfaces are in the same zone. Because of this, only the forwarding and virtual routing and forwarding (VRF) routing instances can be used to avail APBR midstream support.

Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution

This example shows how to configure APBR on an NFX Series device.

Requirements

This example uses the following hardware and software components:

- Valid application identification feature license installed on an NFX Series device.
- NFX150 device with Junos OS Release 18.2 or later.

Overview

In this example, you want to forward HTTP, social networking, and Yahoo traffic arriving at the trust zone to a specific device or interface as specified by the next-hop IP address.

When traffic arrives at the trust zone, it is matched by the APBR profile, and if a matching rule is found, the packets are forwarded to the static route and next hop as specified in

the routing instance. The static route configured in the routing table is inserted into the forwarding table when the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit to a specific device or interface.

Figure 4 on page 104 shows the topology used in this configuration example.

Figure 4: Topology For Advanced Policy-Based Routing (APBR)

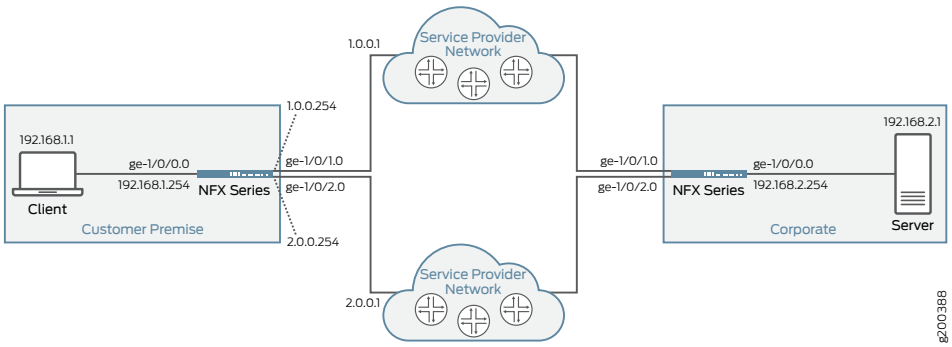


Table 4 on page 104 provides the details of the parameters used in this example.

Table 4: APBR Configuration Parameters

Parameter	Name	Description
Routing Instance	• Instance name—R1 • Instance type— forwarding • Static route— 1.0.0.254/8 • Next-hop— 1.0.0.1 • Instance name—R2 • Instance type— forwarding • Static route— 2.0.0.254/8 • Next-hop— 2.0.0.1	Routing instance of type forwarding is used for forwarding the traffic. All the qualified traffic destined for the static route (example: 5.0.0.0/8) is forwarded to the next-hop device (example: with 7.0.0.1 address on its interface).
RIB Group	apbr_group	Name of the routing information base (RIB) (also known as routing table) group. This RIB group is configured to import interface route entries from inet.0, RI1.inet.0, RI2.inet.0, and RI3.inet.0.
APBR Profile	profile-1	Name of the APBR profile. This profile matches applications and application groups and redirects the matching traffic to the specified routing instance (example: R1) for the route lookup. The profile includes multiple rules.

Table 4: APBR Configuration Parameters (continued)

Parameter	Name	Description
Rule	• Rule name—ruleApp1 • matching application—junos:HTTP • Associated routing instance—R1 • rule name—ruleApp2 • matching application—junos:web:social-networking • Routing instance— R2	Define the rules for the APBR profile. Associate the rule with one or more than one application (example: for HTTP) or application groups. If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered as a match and the traffic will be redirected to the routing instance (example: R1) for the route lookup.
Zone	trust	Specify the source zone to which the APBR profile can be applied.

NOTE:

To use the APBR for redirecting the traffic based on applications, importing interface routes might be required from one routing instance to another routing instance. You can use one of the following mechanisms:

- RIB groups to import interface routes
- Routing policy to import interface routes

When you use routing policy to import interface routes, it might cause management local routes (using fxp0) to leak to non-default routing instance, if the appropriate action is not used for the routing policy. When devices are in chassis cluster mode, such scenarios might result in RG0 failover due to limitations. We recommend not configure fxp0 local route in the routing table of non-default routing instance. Following sample depicts a sample configuration of policy options. Note that the reject action helps in eliminating the routes that are not required. You can use specific routes to reject the fxp0 routes.

```
policy-statement statement-name {
  term 1 {
    from {
      instance master;
      route-filter route-filter-ip-address exact;
    }
    then accept;
  }
  then reject;
}
```

NOTE: APBR is used for routing the packets in a forward path. For return traffic to arrive over the same path, we recommend to configure the remote NFX Series device with ECMP configuration along with load balance routing policy as shown in the following sample configuration:

```
user@host> set routing-options static route ip-address next-hop ip-address
user@host> set routing-options static route ip-address next-hop ip-address
user@host> set policy-options policy-statement load-balance-policy then
  load-balance per-packet
user@host> set routing-options forwarding-table export load-balance-policy
```

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set routing-instances R1 instance-type forwarding
set routing-instances R1 routing-options static route 1.0.0.254/8 next-hop 1.0.0.1
set routing-instances R2 instance-type forwarding
set routing-instances R2 routing-options static route 2.0.0.254/8 next-hop 2.0.0.1
set routing-options interface-routes rib-group inet apbr_group
set routing-options rib-groups apbr_group import-rib inet.0
set routing-options rib-groups apbr_group import-rib RI1.inet.0
set routing-options rib-groups apbr_group import-rib RI2.inet.0
set security advance-policy-based-routing profile profile1 rule rule-app1 match
  dynamic-application junos:HTTP
set security advance-policy-based-routing profile profile1 rule rule-app1 then
  routing-instance R1
set security advance-policy-based-routing profile profile1 rule rule-app2 match
  dynamic-application-group junos:web:social-networking
set security advance-policy-based-routing profile profile1 rule rule-app2 then
  routing-instance R2
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-1/0/1.0
set security zones security-zone trust interfaces ge-1/0/2.0
set security zones security-zone trust advance-policy-based-routing-profile profile1
```

Configuring Advanced Policy-Based Routing

Step-by-Step Procedure

To configure APBR:

1. Create routing instances.

```
[edit]
user@host# set routing-instances R1 instance-type forwarding
user@host# set routing-instances R1 routing-options static route 1.0.0.254/8
  next-hop 1.0.0.1
user@host# set routing-instances R2 instance-type forwarding
user@host# set routing-instances R2 routing-options static route 2.0.0.254/8
  next-hop 2.0.0.1
```

2. Group one or more routing tables to form a RIB group called apbr_group and import routes into the routing tables.

```
[edit]
set routing-options interface-routes rib-group inet apbr_group
set routing-options rib-groups apbr_group import-rib inet.0
set routing-options rib-groups apbr_group import-rib RI1.inet.0
set routing-options rib-groups apbr_group import-rib RI2.inet.0
```

3. Create the APBR profile and define the rules.

```
[edit]
user@host# set security advance-policy-based-routing profile profile1 rule rule-app1
  match dynamic-application junos:HTTP
user@host# set security advance-policy-based-routing profile profile1 rule rule-app1
  then routing-instance R1
user@host# set security advance-policy-based-routing profile profile1 rule rule-app2
  match dynamic-application-group junos:web:social-networking
user@host# set security advance-policy-based-routing profile profile1 rule rule-app2
  then routing-instance R2
```

4. Apply the APBR profile to the security zone.

```
[edit]
user@host# set security zones security-zone trust host-inbound-traffic
  system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols
  all
user@host# set security zones security-zone trust interfaces ge-1/0/1.0
user@host# set security zones security-zone trust interfaces ge-1/0/2.0
user@host# set security zones security-zone trust
  advance-policy-based-routing-profile profile1
```

Results

From configuration mode, confirm your configuration by entering the **show routing-instances** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
R1 {
   instance-type forwarding;
   routing-options {
      static {
         route 1.0.0.254/8 next-hop 1.0.0.1;
      }
   }
}
R2 {
   instance-type forwarding;
   routing-options {
      static {
```

```
        route 2.0.0.254/8 next-hop 2.0.0.1;
      }
    }
}

[edit]
user@host# show routing-options
interface-routes {
   rib-group inet apbr_group;
}
rib-groups {
   apbr_group {
      import-rib [ inet.0 RI1.inet.0 RI2.inet.0 ];
   }
}

[edit]
user@host# show security advance-policy-based-routing
profile profile1 {
   rule rule-app1 {
      match {
         dynamic-application junos:HTTP;
      }
      then {
         routing-instance R1;
      }
   }
   rule rule-app2 {
      match {
         dynamic-application-group junos:web:social-networking;
      }
      then {
         routing-instance R2;
      }
   }
}

[edit]
user@host# show security zones
security-zone trust {
   host-inbound-traffic {
      system-services {
         all;
      }
      protocols {
         all;
      }
   }
   interfaces {
      ge-1/0/1.0;
      ge-1/0/2.0;
   }
   advance-policy-based-routing-profile {
      profile1;
   }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Advanced Policy-Based Routing Statistics

Purpose Display the statistics for APBR such as the number of sessions processed for the application-based routing, number of times the APBR is applied for the session, and so on.

Action From configuration mode, enter the **show security advance-policy-based-routing statistics** command.

```
Advance Profile Based Routing statistics:
  Session Processed:                    5529
  ASC Success:                          3113
  Rule match success:                   107
  Route  modified:                      107
  AppID Requested:                      2416
```

Meaning The command output displays the following details:

- Sessions processed for the application-based routing.
- The number of times the application traffic matches the APBR profile and APBR is applied for the session.
- The number of times AppID was consulted to identify application traffic.

See show security advance-policy-based-routing statistics for more details.

Verifying Advanced Policy-Based Routing

Purpose Display information about the sessions and packet flows active on the device, including detailed information about specific sessions.

Action From configuration mode, enter the **show security flow session** command to display information about all currently active security sessions on the device.

```
Session ID: 12, Policy name: policy1/4, Timeout: 1798, Valid
  In: 4.0.0.1/38228 --> 5.0.0.1/80;tcp, Conn Tag: 0x0, If: ge-1/0/0.0, Pkts: 5,
Bytes: 388,
  Out: 5.0.0.1/80 --> 4.0.0.1/38228;tcp, Conn Tag: 0x0, If: ge-1/0/2.0, Pkts: 4,
 Bytes: 517,
Total sessions: 1
```

Meaning The command output displays the following details:

- All active sessions and packet flows on your device
- List of incoming and outgoing IP flows, including services
- Security attributes associated with a flow, for example, the policies that apply to traffic belonging to that flow
- Session timeout value, when the session became active, how long the session has been active, and if there is active traffic on the session

Configuring Advanced Policy-Based Routing Policies

You can configure advanced policy-based routing (APBR) policies by defining source addresses, destination addresses, and applications as match conditions; and after a successful match, the configured APBR profile is applied as an application services for the session. In the previous releases of Junos OS, an APBR profile could be attached to an incoming security zone of the ingress traffic, and the APBR was applied per security zone basis. Now, with support of APBR policies, you can apply different set of APBR rules on the traffic based on incoming security zone, source address, destination address and application

This enhancement provides more flexible traffic-handling capabilities that offer granular control for forwarding packets.

Supported match criteria includes source addresses, destination addresses, and applications. The applications can be used to support the matching condition based on protocol and Layer 4 ports.

If one or more APBR policy is configured for the security zone, then the policy is evaluated during session creating phase. The policy lookup is terminated once the policy, matching the session, is selected. After a successful match, the APBR profile configured with the APBR policy is used for the session.

How APBR Policy Works?

APBR policies are defined for a security zone. If there is one or more APBR policy associated with a zone, the session that is initiated from the security zone goes through the policy match.

The following sequences are involved in matching the traffic by an APBR policy and applying advanced policy-based routing to forward the traffic, based on the defined parameters/rules:

- When traffic arrives at the ingress zone, it is matched by the APBR policy rules. The policy match condition include the source address, destination address and application.
- When the traffic matches the security policy rules, the action of the APBR policy is applied to the traffic. You can enable APBR as an application service in the APBR policy action by specifying the APBR profile name.
- The APBR profile configuration incudes the set of rules that contains set of dynamic applications and dyamic application groups as match condition. The action part of

those rules contain the routing instance through which traffic needs to be forwarded. The routing instance can include configuration of static routs or dynamic learned routes.

- All traffic destined for the static route is transmitted to the next-hop address for transit to a specific device or interface.

APBR policy rules are terminal, which means that once the traffic is matched by a policy, it is not processed further by the other policies.

If an APBR policy has the matching traffic and APBR profile does not have any traffic matching the rule, then the traffic matching the APBR policy traverses through a default routing-instance [inet0] to the destination.

Legacy APBR Profile Support

Prior to the Junos OS Release 18.2R1, APBR profile was applied at security zone-level. With the support for APBR policy, APBR configuration at security-zone level is deprecated future, rather than being immediately removed in order to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

However, if you have configured a zone-based APBR, and you attempt to add an APBR policy for the particular security zone, commit might fail. You must delete the zone-based configuration in order to configure the APBR policy for the zone. Similarly if an APBR policy is configured for a security zone, and you attempt to configure zone-based APBR, results in commit error.

Limitation

- When using specific address or address set in the APBR policy rule, we recommend to use the global address book. Because, zone specific rules might not be applicable for destination address, as the destination zone is not known at time of policy evaluation.
- Configuring APBR policy for the security zone junos-host zone is not supported.

Example: Configuring Advanced Policy-Based Routing Policies

This example shows how configure an APBR policy and apply the APBR profile on the session that matches the APBR policy rules.

Requirements

This example uses the following hardware and software components:

- Valid application identification feature license installed on an NFX Series device.
- NFX Series device with Junos OS Release 18.2R1 or later. This configuration example is tested on Junos OS Release 18.2R1.

Overview

In this example, you want to forward HTTP traffic arriving at the trust zone to a specific device or interface as specified by the next-hop IP address.

When traffic arrives at the trust zone, it is matched by the APBR policy. When the traffic matches the policy, the configured APBR rule is applied on the permitted traffic as application services. The packets are forwarded based on the APBR rule to the static route and next hop as specified in the routing instance. The static route configured in the routing table is inserted into the forwarding table when the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit to a specific device or interface.

In this example, you must complete the following configurations:

- Define routing instance and RIB group.
- Create an ABPR profile.
- Create a security zone.
- Create an APBR policy and attach the APBR profile to it.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set routing-instances R1 instance-type forwarding
set routing-instances R1 routing-options static route 5.0.0.0/24 next-hop 3.0.0.2
set routing-options interface-routes rib-group inet fbf-group
set routing-options rib-groups fbf-group import-rib inet.0
set routing-options rib-groups fbf-group import-rib RI1.inet.0
set security advance-policy-based-routing profile profile1 rule rule-app1 match
  dynamic-application junos:HTTP
set security advance-policy-based-routing profile profile1 rule rule-app1 then
  routing-instance R1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-1/0/1.0
set security advance-policy-based-routing from-zone trust policy SLA1 match
  source-address any
set security advance-policy-based-routing from-zone trust policy SLA1 match
  destination-address any
set security advance-policy-based-routing from-zone trust policy SLA1 match application
  any
set security advance-policy-based-routing from-zone trust policy SLA1 then
  application-services advance-policy-based-routing-profile profile1
```

Configuring Advanced Policy-Based Routing

Step-by-Step Procedure

To apply APBR on the traffic matching the APBR policy:

1. Create routing instances.

```
[edit]
user@host# set routing-instances R1 instance-type forwarding
user@host# set routing-instances R1 routing-options static route 5.0.0.0/24
  next-hop 3.0.0.2
```

2. Group one or more routing tables to form a RIB group called apbr_group and import routes into the routing tables.

```
[edit]
user@host# set routing-options interface-routes rib-group inet fbf-group
user@host# set routing-options rib-groups fbf-group import-rib inet.0
user@host# set routing-options rib-groups fbf-group import-rib RI1.inet.0
```

3. Create the APBR profile and define the rules.

```
[edit]
user@host# set security advance-policy-based-routing profile profile1 rule rule-app1
  match dynamic-application junos:HTTP
user@host# set security advance-policy-based-routing profile profile1 rule rule-app1
  then routing-instance R1
```

4. Create a security zone.

```
[edit]
user@host# set security zones security-zone trust host-inbound-traffic
  system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols
  all
user@host# set security zones security-zone trust interfaces ge-1/0/1.0
```

5. Create an APBR policy and apply the APBR profile to the security zone.

```
[edit]
user@host# set security advance-policy-based-routing from-zone trust policy SLA1
  match source-address any
user@host# set security advance-policy-based-routing from-zone trust policy SLA1
  match destination-address any
user@host# set security advance-policy-based-routing from-zone trust policy SLA1
  match application any
user@host# set security advance-policy-based-routing from-zone trust policy SLA1
  then application-services advance-policy-based-routing-profile profile1
```

Results

From configuration mode, confirm your configuration by entering the **show routing-instances** and **show security zones** commands. If the output does not display the

intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
R1 {
    instance-type forwarding;
    routing-options {
        static {
            route 5.0.0.0/24 next-hop 3.0.0.2;
        }
    }
}

[edit]
user@host# show routing-options
interface-routes {
    rib-group inet fbf_group;
}
rib-groups {
    fbf_group {
        import-rib [ inet.0 RI1.inet.0];
    }
}

[edit]
user@host# show security advance-policy-based-routing
from-zone trust {
    policy SLA1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            application-services {
                advanced-policy-based-routing-profile profile1;
            }
        }
    }
}
profile profile1 {
    rule rule-app1 {
        match {
            dynamic-application junos:HTTP;
        }
        then {
            routing-instance R1;
        }
    }
}

[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
```

```
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-1/0/1.0;
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Advanced Policy-Based Routing Statistics

Purpose Display the statistics for APBR such as the number of sessions processed for the application-based routing, number of times the APBR is applied for the session, and so on.

Action From configuration mode, enter the **show security advance-policy-based-routing statistics** command.

```
Sessions Processed                    18994
  AppID cache hits                      18994
  AppID requested                       0
  Rule matches                          0
  Route changed on cache hits           0
  Route changed midstream               0
  Zone mismatch                         0
  Drop on zone mismatch                 0
  Next hop not found                    0
```

Meaning The command output displays the following details:

- Sessions processed for the application-based routing.
- The number of times the application traffic matches the APBR profile and APBR is applied for the session.
- The number of times AppID was consulted to identify application traffic.

See show security advance-policy-based-routing statistics for more details.

Verifying APBR Policy Configuration

Purpose Display information about the APBR policy, associated APBR profile and to display information about the APBR policy hit count.

Action From configuration mode, enter the **show security advanced-policy-based-routing** command.

```
user@host> show security advanced-policy-based-routing policy-name SLA1

From zone: trust
  Policy: SLA1, State: enabled, Index: 7, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    APBR profile: profile1
```

From configuration mode, enter the **show security advanced-policy-based-routing hit-count** command.

```
user@host>  show security advanced-policy-based-routing hit-count
Logical system: root-logical-system
 Index   From zone        Name           Hit count
 1       trust           SLA1          3
 2       trust           SLA2          0
 3       trust           SLA1          0

Number of policy: 3
```

Meaning The command output displays the following details:

- Details such as status of the policy, associated APBR profile.
- Display the utility rate of policies according to the number of hits they receive.

See Also
- *Understanding Advanced Policy-Based Routing*

Related Documentation
- Application Firewall on page 61
- Application Tracking on NFX Devices on page 73
- Application QoS on page 84

Application Quality of Experience on NFX Devices

- Application Quality of Experience (AppQoE) on page 116
- Example: Application Quality of Experience (AppQoE) on page 123

Application Quality of Experience (AppQoE)

This topic includes following sections:

- Introduction to AppQoE on page 117
- Benefits of AppQoE on page 117

Introduction to AppQoE

The relentless growth of cloud computing, mobility, and Web-based applications, requires that the network identify and control the traffic at the application level, and handle each application type separately to provide quality of experience (QoE) for users. To ensure application-specific QoE (AppQoE), you need to effectively prioritize, segregate, and route application traffic without compromising performance or availability.

AppQoE utilizes (or employs) the capabilities of two application security services - application identification (AppID) and advanced policy-based routing (APBR). It uses AppID to identify specific applications in your network and advanced policy-based routing (APBR) to specify a path for certain traffic by associating SLA profiles to a routing instance on which the application traffic is sent as per APBR rules.

AppQoE monitors the performance of business- critical applications, and based on the score, selects the best possible link for that application traffic in order to meet performance requirements specified as in SLA (service-level agreement).

The presence of an SLA rule in the APBR configuration triggers the AppQoE functionality; If there are no SLA profiles available, the APBR functions without triggering AppQoE.

Benefits of AppQoE

- Enables cost-effective QoE by providing real-time monitoring of application traffic to provide a consistent and predictable level of service.
- Increases customer retention and satisfaction by providing a guaranteed SLA for the delivery of the certain traffic (such as video traffic). AppQoE ensures that the approved traffic receives the appropriate priority, and bandwidth required to ensure the best quality of experience to the user.

Supported Use Cases

AppQoE finds use in the following network scenarios, among others:

- Networks with hub-and-spoke topology—In a hub-and-spoke configuration, the devices at the branch offices and remote offices connect directly to a specific device and do not form tunnels to other devices in the network. Communication between branch sites or remote offices is enabled through the configured VPN hubs.
- Mesh networks—In a mesh configuration, a device at the branch office or remote site is configured to connect directly to any other device in the network that is also part of mesh.

Limitations

Implementation of AppQoE on Juniper devices has the following limitations:

- All the different routes to the destination through different interfaces must have the same preference, weight, and metrics configured. All routes must be added as ECMP paths for the destination and must also be part of the same forwarding table.
- AppQoE SLA service only between two devices endpoints (book-ended) are supported. End-to-end AppQoE SLA service is not supported.
- AppQoE can be applied only if all interfaces are part of the same zone.
- AppQoE cannot be applied for reverse traffic.
- AppQoE does not influence in change in the destination for a session.
- AppQoE does not support IPv6/UDP probe encapsulation, GRES, chassis cluster (ISSU, high-availability, dual CPE high availability, Z-mode high availability), and logical systems.
- AppQoE is not supported in multihoming scenarios.
- AppQoE does not support preferred path selection and transit virtual routing and forwarding (VRF) are not supported.
- AppQoE does not support passive probing on IPv6 data packets.
- An input firewall filter is required at the non-WAN interfaces to discard UDP packets with UDP destination port 36000.

Understanding AppQoE Terminology

This section includes some of the terminologies used in understanding about how AppQoE works.

- SLA rule—An SLA rule includes all required information to measure SLA and to identify whether any SLA violation has occurred or not. It contains the complete probe profiles, period at which profile need to be sent, preferred SLA configuration and so on.
- SLA options—By using SLA options, you can specify that applications be seamlessly diverted to the alternate path if the performance of the primary link is below acceptable levels as specified by the SLA.
- SLA metrics profile — Defines the SLA metrics requirements parameters, which are used by AppQoE to evaluate the SLA of the link. The metric profile includes parameters such as jitter, jitter type, packet loss, round trip delay and so on.
- SLA violations—To accomplish an SLA, AppQoE monitors the network for sources of failures or congestion. If the performance of a link is below acceptable levels as specified by the SLA, the situation is considered as an SLA violation and an alternate path is determined to select the best link that satisfies the SLA.
- Active and passive probes—Active and passive probe measurements are used for an end-to-end analysis of the network. The data collected by active and passive probing is used for monitoring the network for sources of failures or congestion. If there is a

violation detected for any application, the synthetic probe metrics are evaluated to determine the best link that satisfies the SLA.

- Overlay path—an overlay path includes the overlay links that are used to send the application traffic. Application or application groups are assigned to a particular overlay link based on the SLA metrics of that overlay link.
- Destination groups—A destination group is a group of multiple overlay paths terminating at a destination.

How AppQoE Works?

AppQoE utilizes AppID and APBR capabilities to identify specific applications/application groups and specify a path for certain traffic by associating SLA profiles to a routing instance on which the application traffic is sent as per APBR rules.

AppQoE monitors the performance of applications, and based on the score, selects the best possible link for that application traffic in order to meet performance requirements specified as in SLA (service-level agreement).

Identifying Applications or Application Groups

Following steps are involved in identifying applications or application groups:

1. Junos OS application identification identifies applications and once an application is identified, its information is saved in the application system cache (ASC).
2. APBR evaluates the packets based to determine if the session is candidate for application-based routing (advance policy-based routing). If this is first packet of the new session and traffic is not flagged for application-based routing, it undergoes normal processing (non-APBR route) to destination.
3. If the session needs application-based routing, APBR queries the ASC module to get the application attributes (IP address, destination port, protocol type, and service).
4. - If the application in ASC is found, traffic is further processed for a matching rule in the APBR profile.
     - If a matching rule is found, the traffic is redirected to the specified routing instance for the route lookup.
       - AppQoE checks whether an SLA is enabled for a session. If the session is a candidate for an SLA measurement, AppQoE initiates active and passive probes for performance measurements.
       - If SLA is not enabled for the session in the APBR rule, the AppQoE ignores that session and the default behavior of APBR is applied to those sessions—that is, traffic is routed through the specified routing instance for the destination.
     - If a matching rule is not found, traffic traverses through a default route (non-APBR route) to the destination.
   - If the application in is not found in ASC, APBR requests for deep inspection of the flow. that is, application signature package is installed and application identification

for the session is enabled, so that ASC can be populated for use by subsequent sessions for APBR processing (see step 2).

Specifying Path for Applications or Application Groups

The following steps summarize how AppQoE specifies a path for the application traffic according to the SLA rules.

1. APBR uses the application details to look for a matching rule in the APBR profile (application profile). Traffic matching the applications and application groups, are forwarded to the static route and the next-hop address as specified in the routing instance.
2. An SLA rule attached to the APBR profile specifies parameters, that are required to measure the SLA and to identify whether any SLA violation has occurred or not.
3. The applications traffic is assigned to a particular overlay link based on the SLA metrics of that overlay link measured using active probing.
4. The SLA violation is determined through passive probing of live application/application group traffic. The best path/overlay link for the application/application group is determined through the path selection algorithm.

Application Traffic Path Selection

The following steps take place for routing data traffic from source to destination, specifically, to select the best path,

- For the first data packet of a flow (first path), if the application is already known (from the ASC lookup), then the best path for the application is searched in the database. If the application is not known or is new (from ASC lookup), then a random path or the default path is chosen. This path continues for the entire session. Later, after the application is detected by the DPI, the database is updated with the best path for the application.
- For the remaining data packet of a flow (fast path), if the application is not known initially, then the particular session continues on the same path. If the application is known initially, then AppQoE selects the best path for the application traffic.

When a new application is detected, the path selection mechanism attempts to find a path that satisfies all the SLA metrics. If no such path exists, then the next best path (based on number of metrics satisfied) is used. If there are more than one path that satisfies the metrics, a random path among the available paths is selected. The SLA violation is detected when any one of the metric is violated or none of the metrics meets the requirement, based on the profile configuration.

How AppQoE Measures Application Performance

Application performance is determined by the following indicators:

- Latency—The amount of time physically required for media to travel depending on media length and distance that need to be covered
- RTT— A round-trip time required to travel from source to destination and vice versa.

- Packet loss—Packet loss reflects the number of packets lost per 100 of packets sent by a host.
- Jitter—Jitter is the difference in the latency from packet to packet. Ingress jitter, egress jitter, and two-way jitter can be specified for evaluating the performance of the link.

AppQoE monitors RTT, jitter, and packet loss on each link, and based on the score, seamlessly diverts applications to the alternate path if performance of the primary link is below acceptable levels as specified by SLA. Measurement and monitoring of application performance is done using active and passive probes to detect SLA violations and to select an alternate path for that particular application.

AppQoE collects real-time data by continuously monitoring application traffic and identifying network or device issues by:

- Monitoring the performance on all configured overlay links.
- Using passive probes (inline with the application datapath) and active probes (synthetic probes for specific application) to monitor the traffic performance for application or application group.
- Sending all collected performance metrics or metadata for analysis to a log collector.
- Comparing specified application against a specific performance metric and changing the path for the application traffic dynamically in case of an SLA violation.
- Supporting flexible SLA metric configuration for a given application or application group.

AppQoE measures the application SLA across multiple WAN links, and maps the application traffic to a path among the available links, that is, to the path that best serves the SLA requirement.

Application Performance Measurement by Using Active and Passive Probes

Active and passive probe measurements are the two approaches used for end-to-end analysis of the network.

- Active probe—Active probes measure the service quality of the application to provide an end-to-end measurement of the network performance.

  In active probing, custom packets are sent between spoke and hub points on all the multiple routes and the RTT, latency, jitter, and packet-loss are measured between the installed probe points. The active probes are sent periodically on all the active and passive links. A configured number of samples is collected and a running average for each such application's probe path is measured. If there is a violation detected for any application traffic, the probe metrics are evaluated to determine the best link that satisfies the SLA.

- Passive probe—Passive probes are installed on links within the network, and they monitor all the traffic that flows through those links.

  Passive probing monitors links for SLA violations on live data traffic. In a passive probe, the actual data packets are encapsulated in an IP/UDP probe header in the live traffic

between the device book-ended points, and RTT, jitter and packet loss between the points of installation of the probes are measured to compute the service quality.

If there is a violation detected for any application, the synthetic probe metrics are evaluated to determine the best link that satisfies the SLA.

You can configure an SLA rule with active and passive probe parameters and associate the SLA rule with APBR profile. The APBR profile also includes a APBR rule. Rules are associated with one or more than one application or application groups and the traffic matching the rule is redirected to the routing instance

AppQoE triggers the probe requests to all probe paths of the application. Active and passive probes monitor the network for areas or points of failures or congestion.

AppQoE collects traffic class statistics for learned applications using active and passive probes and takes following actions:

1. Measure performance for SLA—The real-time metrics provided by probes are used to score service quality according to the SLA for an application and determine whether the application path does not meet SLA requirements. That is, if there is a violation detected for any application, the synthetic probe metrics are evaluated to determine the best alternate link for the application traffic that satisfies the SLA.
2. Reroute traffic—Switch the application traffic between the two links, that is, when one link has performance issues, the traffic is routed to the other link during the same session.

NOTE: **If the application's traffic can be reachable through multiple links, you must configure all the reachable paths as overlay paths and attach the overlay paths to application's SLA rule.**

Switching Application Traffic to An Alternate Path

You can enable or disable switching of the application traffic to another route (local to the device) during an SLA violation. When local route switching is enabled, switching of the application traffic to an alternate route is enabled and the SLA monitoring and reporting functionality is also available. Even when the option for switching of the application traffic to an alternate path is disabled in the SLA rule configuration, AppQoE resolves SLA violations---for example, by switching the application traffic to a new path

When local route switching is disabled, only SLA monitoring and reporting functionality is available and switching of the application traffic to the different route because of an SLA violation is tuned off.

When an application traffic switches to an alternative path, there will be a short time period during which the application traffic cannot be switched again to another path in case of SLA violation. This time period helps to avoid flapping of the traffic across links.

Example: Application Quality of Experience (AppQoE)

This example shows how to configure AppQoE to provide quality of experience (QoE) by enabling real- time monitoring of the application traffic according to the specified SLA..

This example provides step-by-step procedures required for Juniper devices to provide the quality-of-experience (QoE) service using AppQoE. In this configuration, devices in the network prioritize certain application traffic to enhance the user experience based on service-level agreement (SLA).

Requirements

- Valid application identification feature license installed on a Juniper device.
- Appropriate security policies to enforce rules for the transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on the traffic as it passes through the device.
- Enable application tracking support enabled for the zone. See Application Tracking.
- Supported NFX device with Junos OS Release 18.2R1 or later. This configuration example is tested for Junos OS Release 15.1X49-D130 on an SRX Series device.

Overview

AppQoE monitors the performance of business-critical applications, and based on the score, selects the best possible link for that application traffic in order to meet performance requirements that are specified as in the SLA. To achieve this goal, AppQoE creates application-specific SLA rules and associates the SLA rules to an APBR profile and to a routing instance on which the application traffic will be sent.

AppQoE measures the application performance across multiple links by collecting real-time data by continuously monitoring application traffic and identifying any network or device issues by active and passive probing. Measured application data is used to determine whether the application path meets SLA requirements and whether an alternate path can be used to reroute the traffic to meet the SLA requirements.

Figure 5 on page 124 shows the topology used in this configuration example.

Figure 5: Topology for AppQoE Configuration

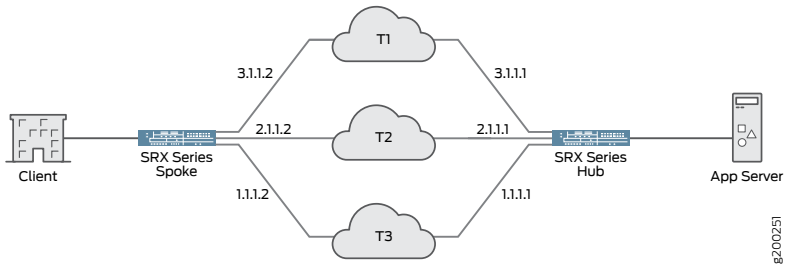


Table 5 on page 124 provides the details of the parameters used in this example.

Table 5: AppQoE Configuration Parameters

Parameter	Name	Description
APBR profile	apbr1	Name of the APBR profile. This profile matches applications and application groups and redirects the matching traffic to the specified routing instance for route lookup. The profile includes multiple rules.
APBR rule	rule-app1 rule-app2 rule-app2	Define the rules for the APBR profile. Associate the rule with one or more than one application (example: for HTTP, FTP, and SSH) or application groups.
Routing Instance	appqoe-vrf	Instance type as routing and forwarding (VRF) instance
RIB group	lanvrf	Name of the routing information base (RIB) (also known as routing table) group.
Define AppQoE as service	system-services=appqoe	Enable AppQoE as an individual service to allow host-inbound custom probe traffic that can reach the device for all the interfaces in a zone.
SLA rule	• sla1 • sla2	Individual applications and application group must have an SLA rule attached. The SLA rule includes all required information to measure the SLA and to identify whether any SLA violation has occurred or not. It contains the complete probe profiles, time period at which profile need to be sent, preferred SLA configuration and so on. An SLA rule is associated with an APBR rule, which is matched to the application or application group.

Table 5: AppQoE Configuration Parameters (continued)

Parameter	Name	Description
SLA options	local-route-switch = enabled	Specify local route switch option. This option enables switching of application traffic to an alternate path if an SLA violation occurs.
SLA metrics profile	• metric1 • metric 2	Defines the performance metrics for delay round trip, one-way jitter or two-way jitter, and packet loss. AppQoE uses metrics profile to evaluate the SLA of the link.
Active probes	• probe1 • probe2	An active probe parameter configures the probe data information such as probe's data size, intervals between individual probes, and so on. Active probe will be initiated from the spoke device to the hub device on each of the overlay path.

Table 5: AppQoE Configuration Parameters (continued)

Parameter	Name	Description
Overlay path	overlay-path1 Tunnel • Local IP addresses- 1.1.1.1 • Remote IP addresses- 2.1.1.1 Probe • Local IP addresses- 125.1.1.1 • Remote IP addresses- 125.1.1.10	Configuring an overlay path allows you to specify the destinations to which the active probe data needs to be sent. Overlay paths are configured for all overlay endpoints. Overlay path configuration includes two set of IP addresses: • Tunnel IP addresses–In this example, T1, T2, T3 are used as tunnels. Tunnel's start and end IP addresses must be mentioned. Tunnel IP addresses must be unique across individual overlay paths. end points • Probe IP addresses—Probe IP addresses are used as probes' start and end addresses to send over the corresponding tunnel paths. Probe IP addresses must be unique across individual overlay paths.
	path2 Tunnel • Local IP addresses- 100.0.0.1 • Remote IP addresses- 150.1.1.1 Probe • Local IP addresses- 25.1.1.1 • Remote IP addresses- 25.1.1.10	
	path3 Tunnel • Local IP addresses- 200.1.1.1 • Remote IP addresses- 250.1.1.1 Probe • Local IP addresses- 225.1.1.1 • Remote IP addresses-	
Destination Grouping	destination-path-group-1	You can group all the overlay paths terminating at the same destination under a destination group. In this example, you have a single destination—that is, hub device. So, all paths are configured under the same destination group and all the paths must be available in the routing instance specific for active probing.

Before you begin:

- When a traffic is identified for AppQoE, that traffic could be fragmented when the packet size exceeds the supported MTU value with the additional encapsulation of the probe header.

  To manage the fragmentation, we recommend you to configure the maximum segment size for TCP sessions for SRX Series devices using the following commands:

  ```
  [edit]
  user@hostset security flow tcp-mss ipsec-vpn mss 1200
  user@hostset security flow tcp-mss all-tcp mss 1350
  ```

- The passive probe packet carries actual source and destination IP address of the client packets. To allow the passive probe packets through the system, you must complete the following configuration:
  - Configure address-based custom applications signatures for UDP (port 36000). This configuration helps in identifying the application by AppID.

    ```
    [edit]
    user@hostset services application-identification application jun-appqoe priority high
    user@hostset services application-identification application jun-appqoe
      address-mapping addr1 filter port-range udp 36000
    ```

  - You must create an appropriate security policy and application firewall policy to support the above configuration.

NOTE: Passive probes generate application tracking log messages for session create and session delete. Once the custom signature identifies these packets, the message reports application as jun-appqoe.

Configuring AppQoE

Configure Advanced Policy-Based Routing (APBR)

Step-by-Step Procedure

Configure APBR profiles for HTTP, FTP, and SSH applications traffic.

1. Create routing instances.

   ```
   user@host# set routing-instances appqoe-vrf instance-type vrf
   user@host# set routing-instances appqoe-vrf routing-options static route 9.0.0.0/8
     next-hop [gr-0/0/0.0 gr-0/0/0.1 gr-0/0/0.2 ]
   user@host# set routing-instances appqoe-vrf routing-options static route 12.1.1.0/24
     next-hop 22.1.1.2
   user@host# set routing-instances appqoe-vrf routing-options static route 13.1.1.0/24
     next-hop 23.1.1.2
   user@host# set routing-instances appqoe-vrf routing-options static route 14.1.1.0/24
     next-hop 24.1.1.2
   ```

2. Group one or more routing tables to form a RIB group and import routes into the routing tables.

   ```
   user@host# set routing-options rib-groups lanvrf import-rib appqoe-vrf.inet.0 inet.0
   ```

3. Create the APBR profile and define the rules.

```
user@host# security advance-policy-based-routing profile apbr1 rule rule-app1
  match dynamic-application junos:HTTP

user@host# security advance-policy-based-routing profile apbr1 rule rule-app2
  match dynamic-application junos:FTP

user@host# security advance-policy-based-routing profile apbr1 rule rule-app2
  match dynamic-application junos:SSH

user@host# set security advance-policy-based-routing profile apbr1 rule rule-app1
  then routing-instance appqoe-vrf

user@host# set security advance-policy-based-routing profile apbr1 rule rule-app2
  then routing-instance appqoe-vrf

user@host# set security advance-policy-based-routing profile apbr1 rule rule-app3
  then routing-instance appqoe-vrf
```

4. Configure AppQoE as system service.

```
user@host# set security zones security-zone trust host-inbound-traffic
  system-services appqoe
```

5. Apply the APBR profile to the security zone.

```
user@host# set security zones security-zone trust host-inbound-traffic protocols
  all

user@host# set security zones security-zone trust
  advance-policy-based-routing-profile apbr1
```

Configuring Metrics Profile

Step-by-Step Procedure

1. Create the set of metrics which AppQoE uses to evaluate the SLA of the link.

```
user@host# set security advance-policy-based-routing metrics-profile metric1
  sla-threshold jitter 5000

user@host# set security advance-policy-based-routing metrics-profile metric1
  sla-threshold jitter-type two-way-jitter

user@host# set security advance-policy-based-routing metrics-profile metric1
  sla-threshold packet-loss 50

user@host# set security advance-policy-based-routing metrics-profile metric1
  sla-threshold match all

user@host# set security advance-policy-based-routing metrics-profile metric2
  sla-threshold delay-round-trip 4000
```

Configure Active Probe Parameters

Step-by-Step Procedure

Configure active probing to send custom packets between spoke device and hub device on all routes to measure RTT, jitter, and packet loss between the points.

1. Configure active probe parameter (probe1).

```
user@host# set security advance-policy-based-routing active-probe-params probe1
  settings data-fill deadbead
user@host# set security advance-policy-based-routing active-probe-params probe1
  settings data-size 100
user@host# set security advance-policy-based-routing active-probe-params probe1
  settings probe-interval 10
user@host# set security advance-policy-based-routing active-probe-params probe1
  settings probe-count 10
user@host# set security advance-policy-based-routing active-probe-params probe1
  settings burst-size 10
user@host# set security advance-policy-based-routing active-probe-params probe1
  settings enable-sla-export 600
```

2. Configuring active probe parameter (probe2).

```
user@host# set security advance-policy-based-routing active-probe-params probe2
  settings data-fill juniper
user@host# set security advance-policy-based-routing active-probe-params probe2
  settings data-size 256
user@host# set security advance-policy-based-routing active-probe-params probe2
  settings probe-interval 30
user@host# set security advance-policy-based-routing active-probe-params probe2
  settings probe-count 300
user@host# set security advance-policy-based-routing active-probe-params probe2
  settings enable-sla-export 600
```

Configuring Overlay and Probe Paths

Step-by-Step Procedure

Configure an overlay setup, which includes setting up both tunnel path and probe path, between local and remote endpoint on both ends of the overlay (spoke device and hub devices).

1. Create overlay paths for the tunnel and probe (overlay-path1).

```
user@host# set security advance-policy-based-routing overlay-path overlay-path1
  tunnel-path local ip-address 1.1.1.2

user@host# set security advance-policy-based-routing overlay-path overlay-path1
  tunnel-path remote ip-address 1.1.1.1

user@host# set security advance-policy-based-routing overlay-path overlay-path1
  probe-path local ip-address 1.1.1.2

user@host# set security advance-policy-based-routing overlay-path overlay-path1
  probe-path remote ip-address 1.1.1.1
```

2. Create overlay paths for the tunnel and probe (overlay-path2).

```
user@host# set security advance-policy-based-routing overlay-path overlay-path2
  tunnel-path local ip-address 2.1.1.2

user@host# set security advance-policy-based-routing overlay-path overlay-path2
  tunnel-path remote ip-address 2.1.1.1

user@host# set security advance-policy-based-routing overlay-path overlay-path2
  probe-path local ip-address 2.1.1.2
```

```
user@host# set security advance-policy-based-routing overlay-path overlay-path2
  probe-path remote ip-address 2.1.1.1
```

3. Create overlay paths for the tunnel and probe (overlay-path3).

```
user@host# set security advance-policy-based-routing overlay-path overlay-path3
  tunnel-path local ip-address 3.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path3
  tunnel-path remote ip-address 3.1.1.1
user@host# set security advance-policy-based-routing overlay-path overlay-path3
  probe-path local ip-address 3.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path3
  probe-path remote ip-address 3.1.1.1
```

4. Group all the overlay paths terminating at a destination. Because there is a single destination available—that is, the hub device— all paths must be configured under the same destination group. All paths must be available in the routing instance specific for active probing.

```
user@host# set security advance-policy-based-routing destination-path-group
  destination-path-group-1 probe-routing-instance R1-appqoe
user@host# set security advance-policy-based-routing destination-path-group
  destination-path-group-1 overlay-path overlay-path1
user@host# set security advance-policy-based-routing destination-path-group
  destination-path-group-1 overlay-path overlay-path2
user@host# set security advance-policy-based-routing destination-path-group
  destination-path-group-1 overlay-path overlay-path3
```

Configure SLA Rule

Step-by-Step Procedure

Configure an SLA rule to measure the SLA and to identify any SLA violation has occurred or not.

1. Configure the SLA rule, associate metrics profile, active probe parameter, and define passive probe parameters.

```
user@host# set security advance-policy-based-routing sla-rule sla1 switch-idle-time
  60
```

2. Define switch idle time for the SLA rule.

```
user@host# set security advance-policy-based-routing sla-rule sla1 metrics-profile
  metric1
```

3. Associate active probe parameter (probe1) to the SLA rule.

```
user@host# set security advance-policy-based-routing sla-rule sla1
  active-probe-params probe1
```

4. Define passive probe parameters.

```
user@host# set security advance-policy-based-routing sla-rule sla1
  passive-probe-params type book-ended
user@host# set security advance-policy-based-routing sla-rule sla1
  passive-probe-params violation-count 5
user@host# set security advance-policy-based-routing sla-rule sla1
  passive-probe-params sampling-percentage 25
user@host# set security advance-policy-based-routing sla-rule sla1
  passive-probe-params sampling-period 60000
user@host# set security advance-policy-based-routing sla-rule sla1
  passive-probe-params sla-export-factor 60
```

Configure SLA Rule Setting with APBR

Step-by-Step Procedure

Associate an SLA rule to with the APBR profile.

1. Enable local route switching. This option enables switching of application traffic to an alternate path if an SLA violation occurs.

```
user@host# set security advance-policy-based-routing sla-options
  local-route-switch enabled
```

2. Configure SLA rule setting with APBR.

```
user@host# set security advance-policy-based-routing profile apbr1 rule rule-app1
  then sla-rule sla1
user@host# set security advance-policy-based-routing profile apbr1 rule rule-app2
  then sla-rule sla2
user@host# set security advance-policy-based-routing profile apbr1 rule rule-app3
  then sla-rule sla1
```

Configure AppQoE on Device Acting as Hub

Step-by-Step Procedure

1. Configure AppQoE as service. You must configure AppQoE as service for host inbound traffic for a desired zone.

```
user@host# set security zones security-zone zone1 host-inbound-traffic
  system-services appqoe
```

2. Configure the percentage of sessions selected for book-ended measurement (passive probing).

```
user@host# set security advance-policy-based-routing sla-rule sla1
  passive-probe-setting session-sampling-percentage 25
```

Results

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

```
[edit security]
user@host# show advance-policy-based-routing
profile apbr1 {
  rule rule1 {
    match {
      dynamic-application [ junos:FTP junos:HTTP junos:SSH ];
    }
    then {
      routing-instance appqoe;
      sla-rule {
        sla_rule1;
      }
    }
  }
}
active-probe-params active_probes {
  settings {
    data-fill {
      deadbead;
    }
    data-size {
      100;
    }
    probe-interval {
      10;
    }
    probe-count {
      10;
    }
    burst-size {
      10;
    }
    enable-sla-export {
      600;
    }
  }
}
metrics-profile metrics_profile1 {
  sla-threshold {
    delay-round-trip {
      4000;
    }
    jitter {
      5000;
    }
    jitter-type {
      two-way-jitter;
    }
    packet-loss {
      50;
    }
    match {
      all;
    }
  }
}
```

```
overlay-path overlay-path1 {
  tunnel-path {
    local {
      ip-address {
        1.1.1.2;
      }
    }
    remote {
      ip-address {
        1.1.1.1;
      }
    }
  }
  probe-path {
    local {
      ip-address {
        1.1.1.2;
      }
    }
    remote {
      ip-address {
        1.1.1.1;
      }
    }
  }
}
overlay-path overlay-path2 {
  tunnel-path {
    local {
      ip-address {
        2.1.1.2;
      }
    }
    remote {
      ip-address {
        2.1.1.1;
      }
    }
  }
  probe-path {
    local {
      ip-address {
        2.1.1.2;
      }
    }
    remote {
      ip-address {
        2.1.1.1;
      }
    }
  }
}
overlay-path overlay-path3 {
  tunnel-path {
    local {
      ip-address {
```

```
            3.1.1.2;
          }
        }
        remote {
          ip-address {
            3.1.1.1;
          }
        }
      }
      probe-path {
        local {
          ip-address {
            3.1.1.2;
          }
        }
        remote {
          ip-address {
            3.1.1.1;
          }
        }
      }
    }
    destination-path-group destination-path-group-1 {
      probe-routing-instance {
        abc;
      }
      overlay-path overlay-path1;
      overlay-path overlay-path2;
      overlay-path overlay-path3;
    }
    sla-rule sla_rule1 {
      switch-idle-time {
        60;
      }
      metrics-profile {
        metrics_profile1;
      }
      active-probe-params {
        active_probes;
      }
      passive-probe-params {
        sampling-percentage {
          25;
        }
        violation-count {
          3;
        }
        sampling-period {
          60000;
        }
        sla-export-factor {
          60;
        }
        type {
          book-ended;
        }
```

```
  }
}
```

```
[edit routing-instances]
user@host# show appqoe-vrf
routing-options {
  static {
    route 9.0.0.0/8 next-hop [ gr-0/0/0.0 gr-0/0/0.1 gr-0/0/0.2 ];
    route 12.1.1.0/24 next-hop 22.1.1.2;
    route 13.1.1.0/24 next-hop 23.1.1.2;
    route 14.1.1.0/24 next-hop 24.1.1.2;
  }
}
```

```
[edit routing-options]
user@host# show
rib-groups {
  lanvrf {
    import-rib [ lan-vrf.inet.0 inet.0 ];
  }
}
forwarding-table {
  export load-balancing-policy;
}
```

```
[edit security advance-policy-based-routing profile apbr1}
user@host# show
rule rule1 {
  match {
    dynamic-application [ junos:FTP junos:HTTP junos:SSH ];
  }
  then {
    routing-instance appqoe-vrf;
    sla-rule {
      sla_rule1;
    }
  }
}
```

```
[edit security zones
user@host# show
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    ge-0/0/5.0;
  }
  application-tracking;
  advance-policy-based-routing-profile {
    apbr1
  }
```

```
}
```

Verify AppQoE Configuration

Verifying SLA Profile

Purpose Display the SLA version.

Action From operational mode, enter the **show security advance-policy-based-routing sla version** command.

```
user@host>show security advance-policy-based-routing sla version
SLA version: APPQOE.VERS.1.0.0.0
```

Meaning The command output displays the version of AppQoE. This information helps verify that the SLA version on both hub device and spoke device is same.

Verifying SLA Profile Status

Purpose Verify that the SLA is enabled on your device.

Action From operational mode, enter the **show security advance-policy-based-routing sla status** command.

```
user@host>show security advance-policy-based-routing sla status
Local Switching is enabled.
```

Meaning The command output confirms that local switching is enabled. That is, switching of the application traffic to another route (local to the device) during an SLA violations, is enabled.

When local route switching is enabled, switching of application traffic to other route is enabled and also SLA monitoring and reporting functionality is available. This configuration selects the best possible link for that application traffic in order to meet performance requirements as in the SLA.

Displaying SLA Statistics

Purpose Display the details of the SLA statistics based on APBR profile.

Action From operational mode, enter the **show security advance-policy-based-routing sla statistics** command.

```
user@host>show security advance-policy-based-routing sla statistics
Advance Profile Based Routing SLA statistics:
    Passive Probe Statistics
        Passive Probe Session Processed  7040
```

```
          Possible Passive Probe Sessions  0
          Passive Probe Sessions Sampled   0
          Passive Probe Ongoing Sessions   0
          SLA violations                   0
Active Probe Statistics
          Active Probe Paths               0
          Active Probe Session             3
          Active Probe Sents               18360
          Active Probe Paths down          3
```

Meaning The command output displays the session details subjected to passive probe and active probe.

Display SLA Statistics for An Application

Purpose Display the details of the application traffic.

Action From operational mode, enter the **show security advance-policy-based-routing sla** command.

```
user@host>  show security advance-policy-based-routing sla profile apbr-1
destination-group-name d1 status apbr1 application junos:HTTP
Application status:
  Num of SLA Violations       0
  Num of Path Switches        1
  Num of monitored sessions   0
  Num of sessions             0
```

```
user@host>  show security advance-policy-based-routing sla profile apbr-1 application junos:HTTP
destination-group-name d1
Application Details:
  Application Name            junos:HTTP
  Application ID              67
  APBR Profile Name           apbr1
  APBR Rule Name              rule1
  Application State           NO PATH SELECTED
  Path Switch Idle State      0
  Routing Instance Name       appqoe-vrf
  SLA Rule Name               sla1
  Active Probe Name           probe1
  Selected Tunnel Destination 0.0.0.0
SLA Metrics:
PKT-LOSS(%)     RTT(us)         2way-Jit(us)    Ing-Jit(us)     Egr-Jit(us)
  0               0               0               0               0
```

Meaning The command output samples help in understanding application details, APBR profile, SLA rule, application status, SLA violations occurred, number of times application traffic has switched route path, and monitored sessions.

Display Active Probe Statistics

Purpose Display active probe statistics.

Action From operational mode, enter the **show security advance-policy-based-routing sla active-probe-statistics** *active-probe-params-name* command.

```
user@host> show security advance-policy-based-routing sla active-probe-statistics
active-probe-params-name probe1
Active Probe Statistics:
Src-IP          Dst-IP          PKT-LOSS(%)     RTT(us)         2way-Jit(us)
Ing-Jit(us)     Egr-Jit(us)
  3.1.1.2         3.1.1.1         0               2633            119
  86              55
  2.1.1.2         2.1.1.1         0               3647            58
  67              56
  1.1.1.2         1.1.1.1         0               4101            42
  61              53
```

Meaning The output shows RTT, jitter and packet-loss measured between the installed probe points.

See Also
- *Advanced Policy-Based Routing*
- *Application Identification*

CHAPTER 4

Configuration Statements

address-mapping (Application Identification)

Syntax

```
address-mapping address-name {
  filter {
    ip ip-address-and-prefix-length;
    port-range {
      tcp [port];
      udp [port];
    }
  }
}
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Match the specified IP address.

Layer 3 and Layer 4 address mapping defines an application by the IP address and optional port range of the traffic. You can use the address mapping option to configure custom applications signatures when the configuration of your private network predicts application traffic to or from trusted servers.

Address mapping provides efficiency and accuracy in handling traffic from a known application.

Options **name**—Address mapping name.

filter—Specify the application matching criteria by the IP address of the application or the port range to match TCP or UDP destination port.

- ip—IP address and prefix-length.
- port-range—Port range to match a TCP or UDP destination port.
  - **tcp [*port*]**—Define the TCP port range for the application.
  - **udp [*port*]**—Define the UDP port range for the application.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Understanding Junos OS Application Identification Custom Application Signatures*

advance-policy-based-routing

Syntax

```
advance-policy-based-routing {
  active-probe-params probe-name {
    settings {
      burst-size {
        size;
      }
      data-fill {
        fill;
      }
      data-size {
        size;
      }
      dscp-code-points {
        dscp;
      }
      probe-count {
        count;
      }
      probe-interval {
        interval;
      }
      enable-sla-export {
        interval;
      }
    }
  }
  destination-path-group name {
    overlay-path {
      overlay-path-name;
    }
    probe-routing-instance {
      routing-instance-name;
    }
  }
  from-zone name {
    policy name {
      description description;
      match {
        source-address;
        destination-address;
        application;
        destination-address-excluded;
        source-address-excluded;
      }
      then {
        application-services {
          apbr-profile apbr-profile;
        }
      }
    }
  }
  metrics-profile metrics-name {
```

```
    sla-threshold {
      delay-round-trip {
        delay-value;
      }
      jitter {
        jitter-value;
      }
      jitter-type {
        egress-jitter ;
        ingress-jitter;
        two-way-jitter;
      }
      match {
        [all | any-one] ;
      }
      packet-loss {
        loss-value;
      }
    }
  overlay-path overlay-path-name {
    probe-path {
      local ip-address;
      remote ip-address
    }
    tunnel-path {
      local ip-address;
      remote ip-address
    }
  }
  profile profile-name {
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-group [system-application-group];
      }
      then {
        routing-instance name ;
      }
    }
  sla-options {
    local-route-switch {
      [enabled | disabled];
    }
    logging {
      syslog:
    }
  }
  sla-rule sla-rule-name {
    active-probe-params {
      probe-params-name;
    }
    metrics-profile {
      metric-profile-name;
    }
    passive-probe-params {
      sampling-percentage {
```

```
            percentage;
          }
          sampling-period {
            period;
          }
          sla-export-factor {
            value;
          }
          violation-count {
            count;
          }
        switch-idle-time {
          period;
        }
        type {
          book-ended;
        }
      }
      traceoptions {
        file {
          filename ;
          files number;
          match regular-expression;
          size maximum-file-size;
          (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
      }
      tunables {
        drop-on-zone-mismatch;
        max-route-change value;
        enable-logging;
      }
    }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 15.1X49-D60.

Description Configure an advanced policy-based routing.

You can create an advanced policy-based routing (APBR) profile (application profile) to match applications and application groups and redirect those matching traffic to the specified routing instance for the route lookup. The profile includes multiple rules. Each rule can contain multiple applications or application groups. If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered to be a match.

The APBR profile evaluates the application-aware traffic and permits or denies traffic based on the applications and application groups.

The application profile can be attached to a security zone or it can be attached to a specific logical or physical interface associated with the security zone.

Options

profile *profile-name*—Name of the profile. Must be a unique name with a maximum length of 63 characters.

from-zone—Specify a source zone to be associated with the APBR policy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Application Quality of Experience*
- *Understanding Advanced Policy-Based Routing*

advance-policy-based-routing (Security Zones)

Syntax advance-policy-based-routing;

Hierarchy Level [edit security zones security-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D60.

Description Enable or apply the advanced policy-based (APBR) routing profile (application profile) on the specified security zone.

To classify and redirect the traffic, the APBR profile matches applications and application groups and if the matching rule is found, the packets are routed to the routing instance that sends the traffic to a different interface as specified in the next-hop IP address. So, you must associate the application profile to the ingress traffic—that is, attach the application profile to a security zone.

When the application profile is applied to a security zone, then all interfaces belonging to that zone are attached to the application profile by default unless there is a specific configuration for an interface belonging to that zone.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*
- *Understanding Advanced Policy-Based Routing*

appfw-profile (System)

Syntax

```
appfw-profile {
  maximum amount;
  reserved amount;
}
```

Hierarchy Level [edit system security-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the application firewall profile quota of a logical system.

As a master administrator, you can create a security profile and specify the kinds and amounts of resources to allocate to a logical system to which the security profile is bound. A security profile is used for share the device's resources, including policies, zones, addresses and address books, flow sessions, and various forms of NAT, among all logical systems appropriately. You can dedicate various amounts of a resource to the logical systems and allow them to compete for use of the free resources.

Options

- **maximum *amount***—Specify the maximum allowed quota value.

  Range: 0 through 1024

- **reserved *amount***—Specify a reserved quota value that guarantees that the resource amount specified is always available to the logical system.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

appfw-rule

Syntax

```
appfw-rule {
  maximum amount;
  reserved amount;
}
```

Hierarchy Level [edit system security-profile *security-profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the number of application firewall rule configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.

The master administrator:

- Uses security profiles to provision logical systems with resources
- Binds security profiles to the master logical system and the user logical systems
- Can configure more than one security profile, allocating different numbers of resources in various profiles

Only the master administrator can create security profiles and bind them to logical systems.

Options

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can use resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

appfw-rule-set

Syntax

```
appfw-rule-set {
  maximum amount;
  reserved amount;
}
```

Hierarchy Level [edit system security-profile *security-profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the number of application firewall rule set configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.

The master administrator:

- Uses security profiles to provision logical systems with resources
- Binds security profiles to the master logical system and the user logical systems
- Can configure more than one security profile, allocating different numbers of resources in various profiles

Only the master administrator can create security profiles and bind them to logical systems.

Options

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can use resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

application-firewall

Syntax

```
application-firewall {
  profile profile-name {
    block-message type {
      custom-text content custom-html-text;
      custom-redirect-url content custom-redirect-url;
    }
  }
  rule-sets rule-set-name {
    default-rule {
      (deny [block-message] | permit | reject [block-message]);
    }
    profile profile-name;
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-groups [system-application-group];
        ssl-encryption (any | yes | no);
      }
      then {
        (deny [block-message] | permit | reject [block-message]);
      }
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (world-readable | no-world-readable);
      size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 11.1. Updated with the **ssl-encryption** and **reject** options in Junos OS Release 12.1X44-D10. Updated with the **block-message** option in Junos OS Release 12.1X45-D10.

Description Specify the profile options, rule set and rule specifications, and trace options to be used for application firewall implementations.

You can configure the application firewall by defining a collection of rule sets. These rule sets can be defined independently and shared across network security policies. A rule set defines the rules that match the application ID detected, based on the application signature.

The application firewall support in the security policies provides additional security control for dynamic applications.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Application Firewall Overview*

application (Application Identification)

Syntax

```
application application-name {
  address-mapping address-name {
    filter {
      ip ip-address-and-prefix-length;
      port-range {
        tcp [port];
        udp [port];
      }
    }
  }
  cacheable;
  description;
  icmp-mapping {
    code number;
    type number;
  }
  ip-protocol-mapping {
    protocol number;
  }
  order;
  over protocol-type  {
    signature name  {
      member name  {
        context {
          http-get-url-parsed-param-parsed;
          http-header-content-type;
          http-header-cookie;
          http-header-host;
          http-header-user-agent;
          http-post-url-parsed-param-parsed;
          http-post-variable-parsed ;
          http-url-parsed;
          http-url-parsed-param-parsed;
          ssl-server-name;
          stream;
        }
        direction {
          any;
          client-to-server;
          server-to-client;
        }
        pattern pattern;
      }
      port-range value;
  priority [high | low];
  type;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Configure application definition.

You can create custom application signatures by specifying a name, protocol, port where the application runs, and match criteria. You can create ICMP-based, address-based, IP protocol-based, and Layer 7-based custom application signatures. Custom applications are created to to identify applications over Layer 7 and transiting or temporary applications, and to achieve further granularity of known applications.

Custom application definitions can be used for applications that are not part of the Juniper Networks predefined application database.

Options **application *application-name***—Name of the custom application signature. Must be a unique name with a maximum length of 63 characters.

NOTE: **Application names are case insensitive.**

cacheable—Enable caching of application identification results. By enabling this option, you can cache the application detection result in an ASC table. If there is an entry in the ASC table, based on the destination IP address, protocol, and the port, we can identify AppID without again sending packet to engine. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.

description—Description of the application.

order *number*—Specify the order for the custom application. Lower order has higher priority. This option is used when multiple custom applications of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications.

priority [high | low]—Specify the priority over other signature applications.

type—Specify if application is a well-known application such as HTTP and FTP.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Junos OS Application Identification Custom Application Signatures*
- address-mapping (Application Identification) on page 142
- icmp-mapping (Application Identification) on page 193
- ip-protocol-mapping (Application Identification) on page 194
- over (Application Identification) on page 203

application-firewall (Application Services)

Syntax

```
application-firewall {
  rule-set rule-set-name;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Specify the rule sets configured as part of application firewall to be applied to permitted traffic in a security policy.

The application firewall is defined by a collection of rule sets. You can implement an application firewall by defining one or more application firewall rule sets and creating rules for each rule set that permit, reject, or deny traffic based on the application ID. These rule sets can be defined independently and shared across network security policies. Then you configure a security policy to invoke the application firewall service and specify the rule set to be applied to permitted traffic.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options

rule-set ***rule-set-name***—Name of the rule set that contains application firewall specification rules.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

  rule-sets (Security Application Firewall) on page 230

application-identification

Syntax

```
application-identification {
  application application-name {
    address-mapping address-name {
      filter {
        ip ip-address-and-prefix-length;
        port-range {
          tcp [port];
          udp [port];
        }
      }
    }
    cacheable;
    description;
    icmp-mapping {
      code number;
      type number;
    }
    ip-protocol-mapping {
      protocol number;
    }
    order;
    over protocol-type  {
      signature name  {
        member name  {
          context {
            http-get-url-parsed-param-parsed;
            http-header-content-type;
            http-header-cookie;
            http-header-host;
            http-header-user-agent;
            http-post-url-parsed-param-parsed;
            http-post-variable-parsed ;
            http-url-parsed;
            http-url-parsed-param-parsed;
            ssl-server-name;
            stream;
          }
          direction {
            any;
            client-to-server;
            server-to-client;
          }
          pattern pattern;
        }
        port-range value;
    priority [high | low];
    type;
  }
  application-group group-name {
    application-groups application-group-name;
    applications application-name;
  }
```

```
    application-system-cache-timeout value;
    download {
      automatic {
        interval hours;
        start-time  MM-DD.hh:mm;
      }
      url url;
    }
    enable-performance-mode max-packet-threshold number;
    imap-cache-size number;
    imap-cache-timeout number;
    no-application-identification;
    no-application-system-cache;
    statistics {
      interval minutes;
    }
    traceoptions {
      file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      level [all | error | info | notice | verbose | warning]
      no-remote-trace;
    }
}
```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 10.2. Custom application definition option introduced in Junos OS Release 15.1X49-D40.

Description Configure application identification to identify applications regardless of the application port or protocol that is used to transmit the application.

Configure application signatures, group applications under predefined and custom application groups, configuring and deactivating application system cache, application traffic throughput, and trace options to be used for application identification implementations.

Once the application is determined, other AppSecure service modules can be configured to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the application ID of the traffic.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Understanding Application Identification Techniques*

application-group (Services)

Syntax

```
application-group group-name {
  application-groups application-group-name;
  applications application-name;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure a custom application group for application identification.

Applications can be grouped under predefined and custom application groups. You can add number of applications or application groups that you want to include in your custom application group.

You can configure an application group to associates related applications under a single name for simplified, consistent reuse in configuring application-based policies.

Options

group-name—Name of the group. This name is used in policy configuration statements in place of multiple predefined applications, user-defined applications, or other groups.

application-groups *application-group-name*— Name of an application group to be assigned to this group. There is no maximum number of groups that can be assigned to a group. Use multiple commands to assign multiple groups.

applications *application-name*—Name of an application to be assigned to this group. An application can remain unassigned or be assigned to a group, but it cannot be assigned to more than one group. There is no maximum number of applications that can be assigned to a group. Use multiple commands to assign multiple groups.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management on page 55

application-services (Security Policies)

Syntax

```
application-services {
  advanced-anti-malware-policy advanced-anti-malware-policy;
  application-firewall {
    rule-set rule-set;
  }
  application-traffic-control {
    rule-set rule-set;
  }
  gprs-gtp-profile gprs-gtp-profile;
  gprs-sctp-profile gprs-sctp-profile;
  idp idp;
  (redirect-wx redirect-wx | reverse-redirect-wx reverse-redirect-wx);
  security-intelligence-policy security-intelligence-policy;
  ssl-proxy {
    profile-name profile-name;
  }
  uac-policy {
    captive-portal captive-portal;
  }
  utm-policy utm-policy;
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information Statement modified in Junos OS Release 11.1.

Description Enable application services within a security policy. You can enable service such as application firewall, IDP, UTM, SSL proxy, and so on by specifying them in a security policy permit action, when the traffic matches the policy rule.

Options

advanced-anti-malware-policy—Specify advanced-anti-malware policy name.

application-firewall—Specify the rule sets configured as part of application firewall to be applied to the permitted traffic.

application-traffic-control—Specify the rule sets configured as part of AppQoS, application-aware quality of service, to be applied to the permitted traffic.

gprs-gtp-profile—Specify GPRS tunneling protocol profile name.

gprs-sctp-profile—Specify GPRS stream control protocol profile name.

idp—Apply Intrusion detection and prevention (IDP) as application services.

redirect-wx—Specify the WX redirection needed for the packets that arrive from the LAN.

reverse-redirect-wx—Specify the WX redirection needed for the reverse flow of the packets that arrive from the WAN.

security-intelligence-policy—Specify security-intelligence policy name.

uac-policy —Enable Unified Access Control (UAC) for the security policy. This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a UAC deployment.

captive-portal *captive-portal*—Specify the preconfigured security policy for captive portal on the Junos OS Enforcer to enable the captive portal feature. The captive portal policy is configured as part of the UAC policy. By configuring the captive portal feature, you can redirect traffic destined for protected resources to the IC Series device or to the URL you configure on the Junos OS Enforcer.

utm-policy *utm-policy*—Specify UTM policy name. The UTM policy configured for antivirus, antispam, content-filtering, traffic-options, and Web-filtering protocols is attached to the security policy to be applied to the permitted traffic.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

application-system-cache

Syntax application-system-cache;

Hierarchy Level
```
application-system-cache {
  no-miscellaneous-services;
  security-services;
}
```

Release Information Statement introduced in Junos OS Release 9.2. The options **no-miscellaneous-services** and **security-services** are introduced in Junos OS Release 18.2R1.

Description Enable application system cache (ASC) to save the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service.

ASC is enabled by default when a session is created. You can manually turn this caching off using the **set services application-identification no-application-system-cache** command. You can re-enable the ASC by using the **delete services application-identification application-system-cache** command.

You can enable the ASC for faster application identification process and disable it for performance benefits and security.

Note the differences in the default behavior of ASC for services starting from Junos OS Release 18.2R1:

- Security services such as security policies, application firewall (AppFW), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services such as APBR and AppTrack use the ASC for application identification by default.

Options **no-miscellaneous-services**—Disable the ASC for miscellaneous services such as APBR and AppTrack.

security-services—Enable the ASC for security services such as security policies, application firewall (AppFW), Juniper Sky ATP, IDP, and UTM.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Understanding the Application System Cache*

application-system-cache-timeout (Services)

Syntax application-system-cache-timeout *value*;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 9.2. Support for application identification in the services hierarchy added in Junos OS Release 10.2.

Description Specify the timeout value in seconds for the application system cache (ASC) entries.

ASC saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. By default, the ASC saves the mapping information for 3600 seconds.

NOTE: On SRX Series devices, when you change the timeout value for the application system cache entries using the command **set services application-identification application-system-cache-timeout**, the cache entries need to be cleared to avoid inconsistency in timeout values of existing entries.

NOTE: ASC is not cleared when the IDP policy is loaded. Users need to manually clear or wait for the cache entries to expire.

Options *value*—Timeout value for the application system cache entries.

Range: 0 through 1,000,000 seconds

Default: 3600 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Understanding the Application System Cache*

application-tracking

Syntax

```
application-tracking {
  disable;
  (first-update | first-update-interval first-update-interval);
  session-update-interval session-update-interval;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 10.2. Support for **disable** added in Junos OS Release 11.4.

Description Enable application tracking (AppTrack).

After application identification identifies the application, AppTrack collects statistics for the application usage on the device, and when the session closes, AppTrack generates a message that provides the byte and packet counts and duration of the session, and sends details to the host device such as Security Threat Response Manager (STRM). STRM retrieves the data and provides flow-based application visibility details.

Options

first-update—Generate application tracking initial message when a session is created. This option overrides the **first-update-interval** option if both are specified.

first-update-interval—Interval when the first update message is sent (minutes).

NOTE: The first-update-interval setting is disregarded if the first-update option is set to log the first message at session start.

- ***minutes***—Maximum number of minutes after session start for the first update message to be sent. This value must be smaller than the **session-update-interval** setting.

  Default: 1

disable—Disable application tracking.

session-update-interval—Frequency in which application tracking update messages are generated (minutes).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppTrack*

application-tracking (Security Zones)

Syntax application-tracking;

Hierarchy Level [edit security zones security-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 10.2.

Description Enable application tracking support for the zone.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Example: Configuring AppTrack*

application-traffic-control

Syntax

```
application-traffic-control {
  rate-limiters {
    rate-limiter-name {
      bandwidth-limit value-in-kbps;
      burst-size-limit value-in-bytes;
    }
  }
  rule-sets ruleset-name{
    {
      rule rule-name {
        match {
          application application-name1;
          application-any;
          application-group application-group-name;
          application-known;
          application-unknown;
        }
        then {
          dscp-code-point dscp-value;
          forwarding-class forwarding-class-name;
          log;
          loss-priority [ high | medium-high | medium-low | low ];
          rate-limit {
            loss-priority-high;
            client-to-server rate-limiter-name;
            server-to-client rate-limiter-name;
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Junos OS Release 11.4.

Description Mark DSCP values for outgoing packets or apply rate limits based on the specified Layer 7 application types.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppTrack*

application-traffic-control (Application Services)

Syntax

```
application-traffic-control {
  rule-set rule-set-name;
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information Statement introduced in Junos OS Release 11.4.

Description Enables AppQoS, application-aware quality of service, as specified in the rules of the specified rule set.

Options

- **rule-set *rule-set-name***—Name of the rule set that contains application-aware traffic control specification rules.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppQoS*
- *Security Policies Overview*

block-message (Application Firewall)

Syntax

```
block-message type {
  custom-text content custom-html-text;
  custom-redirect-url content custom-redirect-url;
}
```

Hierarchy Level [edit security application-firewall profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Defines the profile of the notification to be sent to clients when HTTP or HTTPS traffic is blocked by a reject or deny action from an application firewall.

NOTE: The block message option is not supported for non-HTTP traffic such as FTP, SSH, Telnet, and so on. In these instances, if the action is drop or reject, the traffic is silently dropped or rejected. The user is not informed of the action and no redirection occurs. The associated system log message identifies the action taken for this traffic.

The reject or deny message actions are logged with the reason field containing one of the following phrases:

- appfw deny
- appfw reject

Following sample shows a system log message for SSH traffic, where the traffic was rejected:

```
RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.134 source-address="1.2.0.100"
 source-port="53540" destination-address="1.1.0.100"
destination-port="22" connection-tag="0" service-name="junos-ssh"
protocol-id="6" icmp-type="0" policy-name="p1" source-zone-name="untrust"
 destination-zone-name="trust" application="SSH"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="reth2.0" encrypted="No" reason="appfw reject"]
```

NOTE: You need to enable SSL forward proxy for the HTTPS traffic that needs to be blocked by a reject or a deny action from an application firewall.

When the **block-message** option is specified, a splash screen and message inform the client that the traffic has been blocked. The default message text is:

"*username*, Application Firewall has blocked your request to application *application-name* at *dest-ip:dest-port* accessed from *src-ip:source-port* "

The variables in the message are replaced with specific traffic values. For clarity, the prefix **junos:** is truncated from the application name.

NOTE: You need to enable SSL forward proxy for the HTTPS traffic,that needs to be blocked by a reject or a deny action from an application firewall.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options Use the following option pairs to customize the default message or to redirect the client to a custom webpage instead of the default splash screen.

NOTE: **Both the type and content fields must be used to add custom text or redirect the client to a URL.**

- **type**—(Optional) The message type to be displayed after a reject or deny action.
  - **custom-text**—Text message in HTML to be added to the default text. If **custom-text** is specified, the splash screen displays both the default block message and the custom-defined block message.

    When specified, the user is redirected when a reject or deny action is taken during one of the following HTTP methods: GET, POST, OPTIONS, HEAD, PUT, DELETE, TRACE, CONNECT, PROPFIND, PROPPATCH, LOCK, UNLOCK, COPY, MOVE, MKCOL, BCOPY, BDELETE, BCOPY, BMOVE, BPROPFIND, BPROPPATCH, POLL, SEARCH, SUBSCRIBE, and UNSUBSCRIBE. If the reject or deny action occurs during a different HTTP method, the traffic is silently dropped.
  - **custom-redirect-url**—URL redirection.
- **content**—(Optional) Message content for the selected message type.

NOTE: **The content value must match the type option selected: custom-text requires text, and custom-redirect-url requires a URL value.**

  - *custom-text*—Custom text to be added to the splash screen. Custom text is inserted below the default message. Add the characters \n to insert a line break in the displayed text.
  - *custom-redirect-url*—The URL of the webpage to which the client is directed. When traffic is rejected or denied, the client is redirected to the specified webpage for further action. The URL can be hosted on either the SRX Series device or an external server.

    Enter the redirect URL in quotation marks for an HTTP or HTTPS site, as shown in the following examples:

    "http://*custom-redirect-url*"
    "https://*custom-redirect-url*"

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Example: Configuring AppQoS*

context (Application Identification)

Syntax

```
context {
  http-get-url-parsed-param-parsed;
  http-header-content-type;
  http-header-cookie;
  http-header-host;
  http-header-user-agent;
  http-post-url-parsed-param-parsed;
  http-post-variable-parsed ;
  http-url-parsed;
  http-url-parsed-param-parsed;
  ssl-server-name;
  stream;
}
```

Hierarchy Level [edit services application-identification application *application-name* over *protocol-type* signature *name* member *name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify context for matching application running over TCP, UDP, or Layer 7.

Application identification supports custom application signatures to detect applications as they pass through the device. You can create custom application signatures for applications based on ICMP, IP protocol, IP address, and Layer 7. While configuring custom application signatures, you must specify context values that the device can use to match patterns in the application traffic.

Options

http-get-url-parsed-param-parsed—The decoded, normalized GET URL in an HTTP request along with the decoded CGI parameters (if any).

http-header-content-type —The content-type header in an HTTP transaction.

http-header-cookie—The cookie header in an HTTP transaction.

http-header-host —The host header in an HTTP transaction.

http-header-user-agent—The user-agent header in an HTTP transaction.

http-post-url-parsed-param-parsed —The decoded, normalized POST URL in an HTTP request along with the decoded CGI parameters (if any).

http-post-variable-parsed—The decoded POST URL or form data variables.

http-url-parsed—The decoded, normalized URL in an HTTP request.

http-url-parsed-param-parsed—The decoded, normalized URL in an HTTP request along with the decoded CGI parameters (if any).

ssl-server-name —Server name in the TLS server name extension or the SSL server certificate. This is also known as Server Name Indication (SNI).

stream —TCP or UDP stream data.

Starting from Junos OS release 15.1X49-D60 and Junos OS Release 17.3R1, when configuring custom application signatures, the context-direction combinations as mentioned in Table 6 on page 171 is supported. Any other combination other than this is not supported.

Table 6: Supported Context-Direction Combination for Custom Application Signatures

Context	Direction
http-get-url-parsed-param-parsed	client-to-server
http-header-host	client-to-server
http-header-user-agent	client-to-server
http-post-url-parsed-param-parsed	client-to-server
http-post-variable-parsed	client-to-server
http-url-parsed	client-to-server
http-url-parsed-param-parsed	client-to-server
ssl-server-name	client-to-server
stream	any/client-to-server/server-to-client
http-header-content-type	any/client-to-server/server-to-client
http-header-cookie	any/client-to-server/server-to-client

NOTE: If you are planning to upgrade the device to Junos OS release 15.1X49-D60 from the previous versions of the Junos OS, you must change the configuration to the valid combination of context-direction as mentioned in Table 6 on page 171 to avoid any commit failure and possible disabling of the secondary node.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Understanding Junos OS Application Identification Custom Application Signatures*

crl

Syntax

```
crl {
  disable disable;
  if-not-present (allow | drop);
  ignore-hold-instruction-code ignore-hold-instruction-code;
}
```

Hierarchy Level [edit services ssl initiation profile *name* actions]

Release Information Statement introduced in Junos OS Release 15.1X49-D30. This statement is supported in the SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances.

Description Specify certificate revocation actions.

CRL validation on SRX Series device involves checking for revoked certificates from servers. You can enable or disable the CRL validation to meet your specific security requirements. You can allow or drop the sessions when a CRL information is not available.

To enhance security, the certificate revocation checking feature has been enabled by default on SRX Series devices on any SSL proxy profile.

Options **disable**—Disable CRL validation.

if-not-present—Specify an action if CRL information is not present.

Values:

- **allow**—Allow session if CRL information is not present.
- **drop**—Drop session if CRL information is not present.

ignore-hold-instruction-code—Allow the sessions when a certificate is revoked and the revocation reason is on hold.

Required Privilege Level system

Related Documentation

- *Working with the Certificate Revocation Lists for SSL Proxy*

custom-ciphers

Syntax custom-ciphers [ecdhe-rsa-with-3des-ede-cbc-sha | ecdhe-rsa-with-aes-128-cbc-sha | ecdhe-rsa-with-aes-128-cbc-sha256 | ecdhe-rsa-with-aes-128-gcm-sha256 | ecdhe-rsa-with-aes-256-cbc-sha | ecdhe-rsa-with-aes-256-cbc-sha384 | ecdhe-rsa-with-aes-256-gcm-sha384 | rsa-with-aes-128-cbc-sha256 RSA | rsa-with-aes-128-gcm-sha256 RSA | rsa-with-aes-256-cbc-sha256 RSA | rsa-with-aes-256-gcm-sha384 RSA | rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash rsa-with-aes-128-cbc-sha RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no symmetric cipher | sha hash];

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.
This statement is supported in the SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances.

Description Configure custom cipher, which SSH server can use to perform encryption and decryption functions.

Custom ciphers allow you to define your own cipher list. If you do not want to use one of the three categories, you can select ciphers from each of the categories to form a custom cipher set.

To configure custom ciphers, you must set preferred-ciphers to custom. See preferred-ciphers for more details.

Options **ecdhe-rsa-with-3des-ede-cbc-sha**—ECDHE/RSA, 3 DES EDE/CBC, SHA hash

ecdhe-rsa-with-aes-128-cbc-sha—ECDHE/RSA, 128-bit AES/CBC, SHA hash

ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE/RSA, 128-bit AES/CBC, SHA256 hash

ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE/RSA, 128-bit AES/GCM, SHA256 hash

ecdhe-rsa-with-aes-256-cbc-sha—ECDHE/RSA, 256-bit AES/CBC, SHA hash

ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE/RSA, 256-bit AES/CBC, SHA384 hash

ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE/RSA, 256-bit AES/GCM, SHA384 hash

rsa-export-with-des40-cbc-sha—RSA-export, 40-bit DES/CBC, SHA hash

rsa-export-with-rc4-40-md5—RSA-export, 40-bit RC4, MD5 hash

rsa-export1024-with-des-cbc-sha—RSA 1024-bit export, DES/CBC, SHA hash

rsa-export1024-with-rc4-56-md5—RSA 1024-bit export, 56 bit RC4, MD5 hash

rsa-export1024-with-rc4-56-sha—RSA 1024-bit export, 56 bit RC4, SHA hash

rsa-with-3des-ede-cbc-sha—RSA, 3DES EDE/CBC, SHA hash

rsa-with-aes-128-cbc-sha—RSA, 128-bit AES/CBC, SHA hash

rsa-with-aes-128-cbc-sha256—RSA, 128-bit AES/CBC, SHA256 hash

rsa-with-aes-128-gcm-sha256—RSA, 128-bit AES/GCM, SHA256 hash

rsa-with-aes-256-cbc-sha—RSA, 256-bit AES/CBC, SHA hash

rsa-with-aes-256-cbc-sha256—RSA, 256-bit AES/CBC, SHA256 hash

rsa-with-aes-256-gcm-sha384—RSA, 256-bit AES/GCM, SHA384 hash

rsa-with-des-cbc-sha—RSA, DES CBC, SHA hash

rsa-with-null-md5—RSA, no symmetric cipher, MD5 hash

rsa-with-null-sha—RSA, no symmetric cipher, SHA hash

rsa-with-rc4-128-md5—RSA, 128-bit RC4, MD5 hash

rsa-with-rc4-128-sha—RSA, 128-bit RC4, SHA hash

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *Enabling Debugging and Tracing for SSL Proxy*

default-rule

Syntax

```
default-rule {
  (deny [block-message] | permit | reject [block-message]);
}
```

Hierarchy Level [edit security application-firewall rule-sets *rule-set-name*]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 with the **reject** option. The **block-message** option added in Junos OS Release 12.1X45-D10.

Description Configure the default rule that defines the actions to be performed on a packet that does not match any defined rule.

An application firewall permits, rejects, or denies traffic based on the application of the traffic. The firewall consists of one or more rule sets with rules that specify match criteria, including dynamic applications, and the action to be taken for matching traffic. The application firewall rule set must contain a single default rule. The default rule defines the action to be taken for any traffic that does not match one of the rules.

Starting in Junos OS Release 18.2R1 application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options

- **deny**—Block the traffic at the firewall. The device drops the packet. No message is returned to the sender.
  - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for denied HTTP or HTTPS traffic. All other traffic is dropped silently.
- **permit**—Permit traffic at the firewall.
- **reject**—Block the traffic at the firewall. For TCP traffic, by default the device drops the packet and returns a TCP reset (RST) message to the source host and to the server in some cases. For UDP and other protocol traffic, by default the device drops the packet and returns an ICMP “destination unreachable, port unreachable” message to both the client and the server.
  - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for rejected HTTP or HTTPS traffic. All other traffic is dropped as specified in the default action for the **reject** option.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Example: Configuring Application Firewall Rule Sets Within a Security Policy*

direction (Application Identification)

Syntax

```
direction {
  any;
  client-to-server;
  server-to-client;
}
```

Hierarchy Level
[edit services application-identification application *application-name* over *protocol-type* signature *name* member *name*]

Release Information
Statement introduced in Junos OS Release 15.1X49-D40.

Description
The connection direction of the packets to apply pattern matching. You can specify match patterns on both client to server and server to client while configuring custom application signatures.

Options
any—The directions of packets are either from client-side to server-side or from server-side to client-side.

client-to-server—The direction of packets is from client-side to server-side.

server-to-client—The direction of packets is from server-side to client-side.

Required Privilege Level
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Understanding Junos OS Application Identification Custom Application Signatures*

disable (Application Tracking)

Syntax disable;

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Junos OS Release 11.4.

Description Disable application tracking on a device without deleting the zone configuration.

Application tracking is enabled by default. If application tracking has been previously disabled and you want to reenable it, delete the configuration statement that specifies disabling of application tracking as shown in the following statement:

```
[edit]
user@host# delete security application-tracking disable
```

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppTrack*

download (Services)

Syntax

```
download {
  automatic {
    interval hours;
    start-time MM-DD.hh:mm;
  }
url url;
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure automatic download for the application identification services application package.

The application package contains definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP. The application package is extracted from the IDP signature database located at **https://signatures.juniper.net**. If you do not have access to the default download site from your device, you can use the URL option to download from a different location.

NOTE: You need to download the application package before configuring application identification services.

Options

- automatic—Download the application package automatically at a certain time of day or at intervals.
- *interval*—Download the application package at intervals.

  Range: 6 through 720 hours

- *start-time*—Start time in which the application package will be download. Format is MM-DD.hh:mm. Example: 04-15.09:00 will start the download on April 15 at 9 AM.
- *url*—Use this option to change the default download location of the application package.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Scheduling the Application Signature Package Updates*

dynamic-application

Syntax dynamic-application [*system-application*];

Hierarchy Level [edit security application-firewall rule-sets *rule-set-name* rule *rule-name* match]

Release Information Statement introduced in Junos OS Release 11.1.

Description Specify the dynamic application names for match criteria in application firewall rule set.

An application firewall configuration permits, rejects, or denies traffic based on the application of the traffic. The AppFW consists of one or more rule sets with rules that specify match criteria, including dynamic applications, and the action to be taken for matching traffic.

The junos:UNKNOWN keyword is reserved for unknown dynamic applications. In the following cases, the application ID is set to junos:UNKNOWN:

- The traffic does not match an application signature in the database.
- The system encounters an error when identifying the application.
- The session fails over to another device.

Traffic with an application ID of junos:UNKNOWN matches a rule with a dynamic application of junos:UNKNOWN. If there is no rule defined for junos:UNKNOWN, the default rule is applied.

Starting in Junos OS Release 18.2R1 application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options ***system-application***—Set of system applications for match criteria.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Application Firewall Overview*

dynamic-application-group

Syntax dynamic-application-group [*system-application-group*];

Hierarchy Level [edit security application-firewall rule-sets *rule-set-name* rule *rule-name* match]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the dynamic application group to match. When you define application firewall rules, you can specify dynamic application groups as match criteria.

With application identification, multiple applications can be configured in a dynamic application groups for consistent reuse. AppFW rules permit and deny traffic by specifying application names, dynamic application group names, or both. By using predefined application groups, AppFW rules require no updating when new applications are added to common groups.

Starting in Junos OS Release 18.2R1 application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options ***system-application-group***—Set of groups defining one or more system applications for match criteria.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Application Firewall Overview*

enable-flow-tracing (Services)

Syntax enable-flow-tracing;

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. This statement is supported on the SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

Description Enable flow tracing for the profile.

When you configure **enable-flow-tracing** for SSL profiles, the debug tracing will be enabled on that profile when the flag is set as **selected-profile**.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *Enabling Debugging and Tracing for SSL Proxy*

enable-performance-mode

Syntax enable-performance-mode max-packet-threshold *number*;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 12.1X47-D10.

Description Set the deep packet inspection (DPI) in performance mode for application identification.

The application traffic throughput can be improved by setting the DPI in performance mode with default packet inspection limit as two packets, including both client-to-server and server-to-client directions. By default, performance mode is disabled on SRX Series devices.

If you want to set DPI to default accuracy mode and disable the performance mode, delete the configuration statement that specifies enabling of the performance mode by using the **delete services application-identification enable-performance-mode** command.

Options **max-packet-threshold *number***—Set the maximum packet threshold for DPI performance mode.

Range: 1 through 100

Default: 2

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Improving the Application Traffic Throughput*
- show services application-identification status on page 347

enable-reverse-reroute

Syntax enable-reverse-reroute;

Hierarchy Level [edit security zones security-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D123.

Description Reroute the reverse traffic when there is a link switch for the incoming traffic.

When you configure the **enable-reverse-reroute** option for a security zone, then the packets of each session that has been initiated from the zone are checked for the change in the incoming interface. When an incoming packet arrives on an interface that is different from the one cached in session, the route lookup is performed for the reverse path, and the preference is given to the interface on which the packet has arrived when there are ECMP routes available to the source. Ensure that when you configure enable-reverse-reroute option, the new interface on which packets arrive must be part of the same zone as the earlier interface.

You can enable reverse rerouting in hub-and-spoke deployments, where a spoke device uses APBR to re-route the traffic based on the dynamic applications. In such cases reverse re-route can be used on hub device to correctly re-route the reverse traffic.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Understanding Advanced Policy-Based Routing*

enable-session-cache

Syntax enable-session-cache;

Hierarchy Level [edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. This statement is supported on the SRX550M, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

Description Enable SSL session cache.

You can enable session caching to cache session information, such as the pre-master secret key and agreed-upon ciphers, for both the client and server.

The cached information is identified by a session ID. In subsequent connections both parties agree to use the session ID to retrieve the information rather than create a new pre-master secret key. Session resumption shortens the handshake process and accelerates SSL transactions there by improves the throughput and maintains an appropriate level of security at the same time.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *Enabling Debugging and Tracing for SSL Proxy*

file (System Logging)

Syntax

```
file filename {
  allow-duplicates;
  any (alert | any | critical | emergency | error | info | none | notice | warning);
  archive {
    archive-sites {
      url password;
    }
    (binary-data | no-binary-data);
    files number;
    size size;
    start-time start-time;
    transfer-interval transfer-interval;
    (world-readable | no-world-readable);
  }
  authorization (alert | any | critical | emergency | error | info | none | notice | warning);
  change-log (alert | any | critical | emergency | error | info | none | notice | warning);
  conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);
  daemon (alert | any | critical | emergency | error | info | none | notice | warning);
  dfc (alert | any | critical | emergency | error | info | none | notice | warning);
  explicit-priority;
  external (alert | any | critical | emergency | error | info | none | notice | warning);
  firewall (alert | any | critical | emergency | error | info | none | notice | warning);
  ftp (alert | any | critical | emergency | error | info | none | notice | warning);
  interactive-commands (alert | any | critical | emergency | error | info | none | notice | warning);
  kernel (alert | any | critical | emergency | error | info | none | notice | warning);
  match "regular-expression";
  ntp (alert | any | critical | emergency | error | info | none | notice | warning);
  pfe (alert | any | critical | emergency | error | info | none | notice | warning);
  security (alert | any | critical | emergency | error | info | none | notice | warning);
  structured-data {
    brief;
  }
  user (alert | any | critical | emergency | error | info | none | notice | warning);
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description Specify the file in which to log data.

Options

- *filename*—Specify the name of the file in which to log data.
- *allow-duplicates*—Do not suppress the repeated messages.
- *any*—Specify all facilities information.
  - *alert*—Specify the conditions that should be corrected immediately.
  - *critical*—Specify the critical conditions.

    - *emergency*—Specify the conditions that cause security functions to stop.
    - *error*—Specify the general error conditions.
    - *info*—Specify the information about normal security operations.
    - *none*—Do not specify any messages.
    - *notice*—Specify the conditions that should be handled specifically.
    - *warning*—Specify the general warning conditions.
- *archive*—Specify the archive file information.
    - *archive-sites*—Specify a list of destination URLs for the archived log files.
        - *url*—Specify the primary and failover URLs to receive archive files.
    - *binary-data*—Mark file such that it contains binary data.
    - *no-binary-data*—Do not mark the file such that it contains binary data.
    - *files*—Specify the number of files to be archived. Range: 1 through 1000 files.
    - *size*—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
    - *world-readable*—Allow any user to read the log file.
    - *no-world-readable*—Do not allow any user to read the log file.
    - *start-time*—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
    - *transfer-interval*—Specify the frequency at which to transfer the files to archive sites.
- *authorization*—Specify the authorization system.
- *change-log*—Specify the configuration change log.
- *conflict-log*—Specify the configuration conflict log.
- *daemon*—Specify the various system processes.
- *dfc*—Specify the dynamic flow capture.
- *explicit-priority*—Include the priority and facility in messages.
- *external*—Specify the local external applications.
- *firewall*—Specify the firewall filtering system.
- *ftp*—Specify the FTP process.
- *interactive-commands*—Specify the commands executed by the UI.
- *kernel*—Specify the kernel information.
- *match*—Specify the regular expression for lines to be logged.
- *ntp*—Specify the NTP process.
- *pfe*—Specify the Packet Forwarding Engine.

- *security*—Specify the security-related information.
- *structured-data*—Log the messages in structured log format.
  - *brief*—Omit English language text from the end of the logged message.
- *user*—Specify the user processes.
  - *info*—Specify the informational messages.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

flag (Services)

Syntax
flag (*all* | *cli-configuration* | *initiation* | *proxy* | *selected-profile* | *termination*);

Hierarchy Level
[edit services ssl traceoptions]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10. This statement is supported on the SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX.

Description
Specify the tracing flag parameters.

Options
- *all*—Trace all the parameters.
- *cli-configuration*—Trace CLI configuration events.
- *initiation*—Trace initiation service events.
- *proxy*—Trace proxy service events.
- *selected-profile*—Trace events for profiles with **enable-flow-tracing** set.
- *termination*—Trace termination service events.

Required Privilege Level
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Configuring SSL Forward Proxy*

format (Security Log)

Syntax format (binary | sd-syslog | syslog)

Hierarchy Level [edit security log]

Release Information Statement introduced prior to Junos OS Release 10.0. Statement updated in Junos OS Release 12.1.

Description Set the default log format for event mode security logging on the device.

Options

- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.

Default: syslog.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- log (Security) on page 197

forwarding-classes (CoS)

Syntax

```
forwarding-classes {
  class class-name {
    priority (high | low);
    queue-num number;
    spu-priority (high | low | medium-high | medium-low);
  }
  queue queue-number {
    class-name {
      priority (high | low);
    }
  }
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Junos OS Release 8.5. Statement updated in Junos OS Release 11.4. The **spu-priority** option introduced in Junos OS Release 11.4R2.

Description Configure forwarding classes and assign queue numbers.

Options

- **class class-name**—Display the forwarding class name assigned to the internal queue number.

  NOTE: This option is supported only on SRX1500, SRX5400, SRX5600, and SRX5800.

  NOTE: AppQoS forwarding classes must be different from those defined for interface-based rewriters.

- **priority**—Fabric priority value:
  - **high**—Forwarding class' fabric queuing has high priority.
  - **low**—Forwarding class' fabric queuing has low priority.

  The default **priority** is **low**.
- **queue queue-number**—Specify the internal queue number to which a forwarding class is assigned.
- **spu-priority**—Services Processing Unit (SPU) priority queue, **high**, **medium-high**, **medium-low**, or **low**. The default **spu-priority** is **low**.

NOTE: The **spu-priority** option is only supported on SRX1500 devices and SRX5000 line devices.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppQoS*

global-config (Services)

Syntax

```
global-config {
  disable-cert-cache;
  certificate-cache-timeout;
  invalidate-cache-on-crl-update;
  session-cache-timeout seconds;
}
```

Hierarchy Level [edit services ssl proxy]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. **disable-cert-cache**, **certificate-cache-timeout**, and **Invalidate-cache-on-crl-update** options are introduced in Junos OS Release 18.1R1.

Description Specify the global proxy configuration. When SSL proxy is configured at a global level (within "services ssl proxy"), it is visible across the system configurations on the device.

Options

certificate-cache-timeout—Regulates the certificate cache timeout.

Default: 600 seconds

disable-cert-cache—Disable the certificate cache. By default certificate cache is enabled.

invalidate-cache-on-crl-update—Invalidate the existing certificate cache. By default, this option is disabled.

session-cache-timeout—Specify the session cache timeout.

Range: 300 to 3600 seconds

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *Enabling Debugging and Tracing for SSL Proxy*

icap-redirect

Syntax

```
icap-redirect {
  profile name {
    fallback-option {
      connectivity (block | log-permit | permit);
      default-action (block | log-permit | permit);
      timeout (block | log-permit | permit);
    }
    http {
      redirect-request redirect-request;
      redirect-response redirect-response;
    }
    server name {
      authorization {
        authorization-type authorization-type;
        credentials (ascii ascii | base64 base64);
      }
      host host;
      port port;
      reqmod-uri reqmod-uri;
      respmod-uri respmod-uri;
      routing-instance ri-name;
      sockets sockets;
      tls-profile tls-profile;
    }
    timeout timeout;
  }
  traceoptions {
    file <filename> <files files>< match match><size size> (world-readable |
      no-world-readable)>;
    flag name;
    no-remote-trace no-remote-trace;
  }
}
```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 18.1 R1.

Description Configure the ICAP redirection service.

The SRX Series device acts as an SSL proxy, decrypts HTTP or HTTPS traffic, and redirects the HTTP message to a third-party, on-premise DLP server through the Internet Content Adaptation Protocol (ICAP) channel. To enable ICAP redirection service, you must configure an ICAP redirect profile.

The ICAP server profile allows the ICAP server to process request messages, response messages, fallback options, and so on, to the permitted traffic. This profile is applied as an application service in the security policy.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

icmp-mapping (Application Identification)

Syntax

```
icmp-mapping {
  code number;
  type number;
}
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify the Internet Control Message Protocol (ICMP) value for an application to match while configuring custom application signatures for Junos OS application identification.

The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. The ICMP code and type provide additional specification, for packet matching in an application definition.

Options

code *number*—Numeric value of an ICMP code. The code field provides further information about the associated type field.

Range: 0-254

type *number*—Numeric value of an ICMP type. The type field identifies the ICMP message.

Range: 0-254

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Understanding Junos OS Application Identification Custom Application Signatures*

ip-protocol-mapping (Application Identification)

Syntax

```
ip-protocol-mapping {
  protocol number;
}
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify the IP protocol value for an application to match. This parameter is used to identify an application based on IP and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.

Options

protocol *number*—Industry-standard numeric protocol value.

Range: 0 through 254.

You can find a complete list of industry standard protocol numbers at the IANA website.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Understanding Junos OS Application Identification Custom Application Signatures*

initiation (Services)

Syntax

```
initiation{
  profile name {
    actions {
      crl {
        disable disable;
        if-not-present (allow | drop);
        ignore-hold-instruction-code ignore-hold-instruction-code;
      }
      ignore-server-auth-failure ignore-server-auth-failure;
    }
    client-certificate client-certificate;
    custom-ciphers (ecdhe-rsa-with-3des-ede-cbc-sha | ecdhe-rsa-with-aes-128-cbc-sha
      | ecdhe-rsa-with-aes-128-cbc-sha256 | ecdhe-rsa-with-aes-128-gcm-sha256 |
      ecdhe-rsa-with-aes-256-cbc-sha | ecdhe-rsa-with-aes-256-cbc-sha384 |
      ecdhe-rsa-with-aes-256-gcm-sha384 | rsa-export-with-des40-cbc-sha |
      rsa-export-with-rc4-40-md5 | rsa-export1024-with-des-cbc-sha |
      rsa-export1024-with-rc4-56-md5 | rsa-export1024-with-rc4-56-sha |
      rsa-with-3des-ede-cbc-sha | rsa-with-aes-128-cbc-sha | rsa-with-aes-128-cbc-sha256
      | rsa-with-aes-128-gcm-sha256 | rsa-with-aes-256-cbc-sha |
      rsa-with-aes-256-cbc-sha256 | rsa-with-aes-256-gcm-sha384 | rsa-with-des-cbc-sha
      | rsa-with-null-md5 | rsa-with-null-sha | rsa-with-rc4-128-md5 | rsa-with-rc4-128-sha);
    enable-flow-tracing enable-flow-tracing;
    enable-session-cache enable-session-cache;
    preferred-ciphers (custom | medium | strong | weak);
    protocol-version (all | ssl3 | tls1 | tls11 | tls12);
    trusted-ca ;
  }
}
```

Hierarchy Level [edit services ssl]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The **protocol-version** statement is updated to include **tls11** and **tls12** from Junos OS Release 15.1X49-D30.

Description Specify the configuration for Secure Socket Layer (SSL) initiation support service. The SRX Series device, acting as an SSL proxy client, initiates and maintains SSL sessions between itself and an SSL server. SRX device receives un-encrypted data from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server.

Options

- **client-certificate**—Local certificate.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Configuring SSL Forward Proxy*

- *Firewall User Authentication Overview*

level (Services)

Syntax level [*brief* | *detail* | *extensive* | *verbose]*];

Hierarchy Level [edit services ssl traceoptions]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the level of debugging the output. This statement is supported on the SRX550M, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

Options

- *brief*—Specify brief debugging output.
- *detail*—Specify detailed debugging output.
- *extensive*—Specify extensive debugging output.
- *verbose*—Specify verbose debugging output.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Configuring SSL Forward Proxy*

log (Security)

Syntax

```
log {
  cache {
    exclude exclude-name {
      destination-address destination-address;
      destination-port destination-port;
      event-id event-id;
      failure;
      interface-name interface-name;
      policy-name policy-name;
      process process-name;
      protocol protocol;
      source-address source-address;
      source-port source-port;
      success;
      user-name user-name;
    }
    limit value;
  }
  disable;
  event-rate rate;
  facility-override (authorization | daemon | ftp | kernel | local | user);
  file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
  }
  format (binary | sd-syslog | syslog);
  max-database-record <max-database-record>;
  mode (event | stream);
  rate-cap <rate-cap-value>;
  report;
  (source-address source-address | source-interface interface-name);
  stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp
      | rtlog |pst-ds-lite | appqos |secintel);
    file {
      name file-name;
      size file-size;
      rotation max-rotation-number;
    }
    filter {
      threat-attack;
      }
    format (binary | sd-syslog | syslog | welf);
    host {
      ip-address;
      port port-number;
    }
    rate-limit {
      log-rate;
    }
```

```
    severity (alert | critical | debug | emergency | error | info | notice | warning);
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | hpl | report | source);
    no-remote-trace;
  }
  transport {
    protocol (udp | tcp | tls);
    tcp-connections tcp-connections;
    tls-profile tls-profile-name;
  }
  utc-timestamp;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

Options

cache—Cache security log events in the audit log buffer.

disable—Disable the security logging for the device.

event-rate *rate*—Limit the rate at which logs are streamed per second.

Range: 0 through 1500

Default: 1500

facility-override—Alternate facility for logging to remote host.

file—Specify the security log file options for logs in binary format.

Values:

- ***max-file-number***—Maximum number of binary log files.
  - The range is 2 through 10 and the default value is 10.
- ***file-name***—Name of binary log file.
- ***binary-log-file-path***—Path to binary log files.
- ***maximum-file-size***—Maximum size of binary log file in megabytes.
  - The range is 1 through 10 and the default value is 10.

format—Set the security log format for the device.

max-database-record—The following are the disk usage range limits for the database:

Range:

- SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
- vSRX: 0 through 1,000,000

Default:

- SRX1500, SRX4100, and SRX4200: 15,000,000
- vSRX: 1,000,000

NOTE: Be sure there is enough free space in /var/log/hostlogs/, otherwise logs might be dropped when written into the database.

mode—Control how security logs are processed and exported.

rate-cap *rate-cap-value*—Work with event mode only. This option limits the rate at which data plane logs are generated per second.

Range: 0 through 5000 logs per second

Default: 5000 logs per second

source-address *source-address*—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface *interface-name*—Specify a source interface name, which is mandatory to configure *stream host*.

NOTE: The source-address and source-interface are alternate values. Using one of the options is mandatory.

stream—Every stream can configure file or host.

- ***category***— Type of events that might be logged.
- ***file name***—Specify the filename.
- ***file size***—Specify the file size.
  - SRX1500, SRX4100, and SRX4200—The default value is 25 MB and the range is 10 MB through 50 MB.
  - vSRX - The default value is 2 MB and the range is 1 MB through 3 MB.
- ***rotation***—Configure the maximum file number for rotation.
  - The default value is 10 and the range is 2 through 19.
- ***rate-limit***—Rate-limit for security logs.
  - The range is 1 through 65,535 logs per second and the default value is 65,535 .
- ***filter***—Selects the filter to filter the logs to be logged.
- ***format***—Specify the log stream format.
- ***host***—Destination to send security logs.
- ***severity***—Severity threshold for security logs.

traceoptions—Specify security log daemon trace options.

transport—Set security log transport settings.

utc-timestamp—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

log (Services)

Syntax

```
log {
  all;
  errors;
  info;
  sessions-allowed;
  sessions-dropped;
  sessions-ignored;
  sessions-whitelisted;
  warning;
}
```

Hierarchy Level [edit services ssl proxy profile *profile-name* actions]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the logging actions. When configuring SSL proxy, you can choose to set the option to receive some or all of the logs.

SSL proxy logs contain the logical system name, SSL proxy whitelists, policy information, SSL proxy information, and other information that helps you troubleshoot when there is an error.

You can configure logging of all or specific events, such as error, warning, and information events. You can also configure logging of sessions that are whitelisted, dropped, ignored, or allowed after an error occurs.

Options

- **all**—Log all events.
- **errors**—Log all error events.
- **info**—Log all information events.
- **sessions-allowed**—Log SSL session allowed events after an error.
- **sessions-dropped**—Log only SSL session dropped events.
- **sessions-ignored**—Log session ignored events.
- **sessions-whitelisted**—Log SSL session whitelisted events.
- **warning**—Log all warning events.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Configuring SSL Forward Proxy*

no-application-identification (Services)

Syntax no-application-identification;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 10.2.

Description Disable the application identification of applications running on nonstandard ports. By default, application identification is enabled on the device. You can disable application identification by using the following command:

user@host# set services application-identification no-application-identification

If you want to reenable application identification, delete the configuration statement that specifies disabling of application identification by using the following command:

user@host# delete services application-identification no-application-identification

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Disabling and Reenabling Junos OS Application Identification*

no-application-system-cache (Services)

Syntax no-application-system-cache;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 10.2.

Description Application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the **no-application-system-cache** statement to turn it off.

ASC is enabled by default when a session is created. You can manually turn this caching off using the **set services application-identification no-application-system-cache** command. You can re-enable the ASC by using the **set services application-identification application-system-cache** command.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Deactivating Application System Cache Information for Application Identification (CLI Procedure)*

over (Application Identification)

Syntax

```
over protocol-type  {
  signature name  {
    member name  {
      context {
        http-get-url-parsed-param-parsed;
        http-header-content-type;
        http-header-cookie;
        http-header-host;
        http-header-user-agent;
        http-post-url-parsed-param-parsed;
        http-post-variable-parsed ;
        http-url-parsed;
        http-url-parsed-param-parsed;
        ssl-server-name;
        stream;
      }
      direction {
        any;
        client-to-server;
        server-to-client;
      }
      pattern pattern;
    }
    port-range value;
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify set of L4/L7 application that carries given application

Configure a custom signature based on Layer 4/Layer 7 applications. You create Layer 7-based custom application signatures for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol.

Options ***protocol-type***—Application protocol

signature *name* —Name of the custom application signature. Must be a unique name with a maximum length of 63 characters.

member *name* —Member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01 through m15.)

context—Service-specific context, such as http-header-content-type.

direction—Connection direction of the packets to match pattern

patterns—(Optional) Deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature. Maximum length is 128.

port-range—Port range. This option is applicable for TCP or UDP-based applications only.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Understanding Junos OS Application Identification Custom Application Signatures*

policies

Syntax

```
policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-identity {
          [role-name];
          any;
          authenticated-user;
          unauthenticated-user;
          unknown-user;
        }
      }
      scheduler-name scheduler-name;
      then {
        count {
          alarm {
            per-minute-threshold number;
            per-second-threshold number;
          }
        }
        deny;
        log {
          session-close;
          session-init;
        }
        permit {
          application-services {
            application-firewall {
              rule-set rule-set-name;
            }
            application-traffic-control {
              rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
```

```
            gprs-sctp-profile profile-name;
            idp;
            idp-policy idp-policy;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            user-firewall {
              access-profile profile-name;
              domain domain-name
              ssl-termination-profile profile-name;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
  }
  global {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
```

```
    destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
    }
    from-zone {
        [zone-name];
        any;
    }
    source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
    }
    source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
    }
    to-zone {
        [zone-name];
        any;
    }
}
scheduler-name scheduler-name;
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            idp-policy idp-policy;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
                profile-name profile-name;
```

```
                    }
                    uac-policy {
                        captive-portal captive-portal;
                    }
                    utm-policy policy-name;
                }
                destination-address {
                    drop-translated;
                    drop-untranslated;
                }
                firewall-authentication {
                    pass-through {
                        access-profile profile-name;
                        client-match user-or-group-name;
                        ssl-termination-profile profile-name;
                        web-redirect;
                        web-redirect-to-https;
                    }
                    web-authentication {
                        client-match user-or-group-name;
                    }
                }
                services-offload;
                tcp-options {
                    initial-tcp-mss mss-value;
                    reverse-tcp-mss mss-value;
                    sequence-check-required;
                    syn-check-required;
                }
            }
            reject;
        }
    }
}
policy-rematch;
policy-stats {
    system-wide (disable | enable) ;
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
```

Hierarchy Level [edit security]

Release Information

Statement introduced in Junos OS Release 8.5.
Support for the **services-offload** option added in Junos OS Release 11.4.
Support for the **source-identitiy** option added in Junos OS Release 12.1.
Support for the **description** option added in Junos OS Release 12.1.
Support for the **ssl-termination-profile** and **web-redirect-to-https** options added on SRX5400, SRX5600, and SRX5800 devices starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40.
Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.
Support for the **domain** option, and for the **from-zone** and **to-zone** global policy match options, added in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Support for the **extensive** option for **policy-rematch** added in Junos OS Release 15.1X49-D20.
Starting in Junos OS Release 18.2R1, IDP policy is available within unified security policy. IDP policy is simplified and made available under the unified policy as one of the policy. When IDP policy is available within the unified security policy, configuring source or destination address, source and destination-except, from and to zone, or application is not required, as the match happens in the security policy itself.

Description

Configure network security policies.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*

policy (Security Policies)

Syntax

```
policy policy-name {
  description description;
  match {
    application {
      [application];
      any;
      junos-twamp;
    }
    destination-address {
      [address];
      any;
      any-ipv4;
      any-ipv6;
    }
    source-address {
      [address];
      any;
      any-ipv4;
      any-ipv6;
    }
    source-identity {
      [role-name];
      any;
      authenticated-user;
      unauthenticated-user;
      unknown-user;
    }
  }
  scheduler-name scheduler-name;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number;
      }
    }
    deny;
    log {
      session-close;
      session-init;
    }
    permit {
      application-services {
        application-firewall {
          rule-set rule-set-name;
        }
        application-traffic-control {
          rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
```

```
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
          profile-name profile-name;
        }
        uac-policy {
          captive-portal captive-portal;
        }
        utm-policy policy-name;
      }
      destination-address {
        drop-translated;
        drop-untranslated;
      }
      firewall-authentication {
        pass-through {
          access-profile profile-name;
          client-match user-or-group-name;
          web-redirect;
        }
        user-firewall {
          access-profile profile-name;
          domain domain-name
          ssl-termination-profile profile-name;
        }
        web-authentication {
          client-match user-or-group-name;
        }
      }
      services-offload;
      tcp-options {
        initial-tcp-mss mss-value;
        reverse-tcp-mss mss-value;
        sequence-check-required;
        syn-check-required;
      }
      tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
        pair-policy pair-policy;
      }
    }
    reject;
  }
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 8.5. The **services-offload** option added in Junos OS Release 11.4. Statement updated with the **source-identity** option and the **description** option added in Junos OS Release 12.1. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.
The **junos-twamp** application is introduced in Junos OS Release 18.2R1.

Description Define a security policy.

Options ***policy-name***—Name of the security policy.

—

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Configuring SSL Forward Proxy*
- *Security Policies Overview*

port-range (Application Identification)

Syntax
```
port-range {
  tcp [port];
  udp [port];
}
```

Hierarchy Level [edit services application-identification application *application-name* address-mapping *address-name* filter]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify a port to match a TCP or UDP destination port for Layer 3 and Layer 4 address-based custom applications.

.

Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port. When both IP address and port are configured, both should match destination tuples (IP address and port range) of the packet. The format for numeric port ranges is in the format *minimum-value–maximum-value*.

Options
- **tcp [*port*]**—Define the TCP port range for the application.
- **udp [*port*]**—Define the UDP port range for the application.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Understanding Junos OS Application Identification Custom Application Signatures*

preferred-ciphers

Syntax preferred-ciphers (custom | medium | strong | weak);

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Select preferred ciphers. Preferred ciphers allow you to define an SSL cipher that can be used with acceptable key strength. Ciphers are divided in three categories depending on their key strength: strong, medium, or weak.

Custom ciphers allow you to define your own cipher list. If you do not want to use one of the three categories, you can select ciphers from each of the categories to form a custom cipher set. To configure custom ciphers, you must set **preferred-ciphers** to **custom**.

Options

- **custom**—Configure custom cipher suite and order of preference.
- **medium**—Use ciphers with key strength of 128 bits or greater.
- **strong**—Use ciphers with key strength of 168 bits or greater.
- **weak**—Use ciphers with key strength of 40 bits or greater.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Firewall User Authentication Overview*
- *SSL Proxy Overview*

profile (Application Firewall)

Syntax

```
profile profile-name {
  block-message {
    type {
      custom-redirect-url {
        content content;
      }
      custom-text {
        content content;
      }
    }
  }
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Define the profile of the response to be issued when an application firewall rule set blocks HTTP or HTTPS traffic with a **deny** or **reject** action.

Although drop and reject actions are logged, application firewall does not notify users when either action is taken. To provide an explanation for the action or to redirect the users to an informative webpage, you can use the **block-message** option with the reject or deny action in an application firewall rule.

You can customize the redirect action by including additional text on the splash screen or by specifying a URL to which the user is redirected. To customize the block message, define the **type** and **content** in a block message profile defined in the rule set.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options **name**—Profile name.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

profile (Rule Sets)

Syntax profile *profile-name*;

Hierarchy Level [edit security application-firewall rule-sets *rule-set-name*]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Specifies the profile of the block message to be used for any deny or reject action in the rule set that specifies the **block-message** option.

The block-message option enables you to provide an explanation for the action or to redirect the client to an informative webpage. You can configure the block-message in **set security application-firewall profile** hierarchy.

Options *profile-name*—Name of the block-message profile to be used for this rule set.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

profile (SSL Proxy)

Syntax

```
profile name {
  ( root-ca root-ca | server-certificate [ server-certificate ... ]);
  actions {
    crl {
      disable disable;
      if-not-present (allow | drop);
      ignore-hold-instruction-code ignore-hold-instruction-code;
    }
    disable-session-resumption disable-session-resumption;
    ignore-server-auth-failure ignore-server-auth-failure;
    log {
      all all;
      errors errors;
      info info;
      sessions-allowed sessions-allowed;
      sessions-dropped sessions-dropped;
      sessions-ignored sessions-ignored;
      sessions-whitelisted sessions-whitelisted;
      warning warning;
    }
    renegotiation (allow | allow-secure | drop);
  }
  custom-ciphers (ecdhe-rsa-with-3des-ede-cbc-sha | ecdhe-rsa-with-aes-128-cbc-sha |
    ecdhe-rsa-with-aes-128-cbc-sha256 | ecdhe-rsa-with-aes-128-gcm-sha256 |
    ecdhe-rsa-with-aes-256-cbc-sha | ecdhe-rsa-with-aes-256-cbc-sha384 |
    ecdhe-rsa-with-aes-256-gcm-sha384 | rsa-export-with-des40-cbc-sha |
    rsa-export-with-rc4-40-md5 | rsa-export1024-with-des-cbc-sha |
    rsa-export1024-with-rc4-56-md5 | rsa-export1024-with-rc4-56-sha |
    rsa-with-3des-ede-cbc-sha | rsa-with-aes-128-cbc-sha | rsa-with-aes-128-cbc-sha256
    | rsa-with-aes-128-gcm-sha256 | rsa-with-aes-256-cbc-sha |
    rsa-with-aes-256-cbc-sha256 | rsa-with-aes-256-gcm-sha384 | rsa-with-des-cbc-sha
    | rsa-with-null-md5 | rsa-with-null-sha | rsa-with-rc4-128-md5 | rsa-with-rc4-128-sha);
  enable-flow-tracing enable-flow-tracing;
  preferred-ciphers (custom | medium | strong | weak);
  trusted-ca ;
  whitelist [ whitelist ... ];
  whitelist-url-categories [ whitelist-url-categories ... ];
}
```

Hierarchy Level [edit services ssl proxy]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The **crl** statement is supported from 15.1X49-D30.

Description Specify the SSL server profile. An SSL proxy profile defines SSL behavior for the SRX Series device.

The SSL proxy profile will be applied to the security policy as application services.

Options ***profile-name***—Profile identifier.

root-ca—Root certificate for interdicting server certificates in proxy mode.

server-certificate—Local certificate identifier.

custom-ciphers—Custom cipher list.

Values:

- **ecdhe-rsa-with-3des-ede-cbc-sha**—ECDHE/RSA, 3DES EDE/CBC, SHA hash
- **ecdhe-rsa-with-aes-128-cbc-sha**—ECDHE/RSA, 128-bit AES/CBC, SHA hash
- **ecdhe-rsa-with-aes-128-cbc-sha256**—ECDHE/RSA, 128-bit AES/CBC, SHA256 hash
- **ecdhe-rsa-with-aes-128-gcm-sha256**—ECDHE/RSA, 128-bit AES/GCM, SHA256 hash
- **ecdhe-rsa-with-aes-256-cbc-sha**—ECDHE/RSA, 256-bit AES/CBC, SHA hash
- **ecdhe-rsa-with-aes-256-cbc-sha384**—ECDHE/RSA, 256-bit AES/CBC, SHA384 hash
- **ecdhe-rsa-with-aes-256-gcm-sha384**—ECDHE/RSA, 256-bit AES/gcm, SHA384 hash
- **rsa-export-with-des40-cbc-sha**—RSA-export, 40-bit DES/CBC, SHA hash
- **rsa-export-with-rc4-40-md5**—RSA-export, 40-bit RC4, MD5 hash
- **rsa-export1024-with-des-cbc-sha**—RSA 1024-bit export, DES/CBC, SHA hash
- **rsa-export1024-with-rc4-56-md5**—RSA 1024-bit export, 56 bit RC4, MD5 hash
- **rsa-export1024-with-rc4-56-sha**—RSA 1024-bit export, 56 bit RC4, SHA hash
- **rsa-with-3des-ede-cbc-sha**—RSA, 3DES EDE/CBC, SHA hash
- **rsa-with-aes-128-cbc-sha**—RSA, 128-bit AES/CBC, SHA hash
- **rsa-with-aes-128-cbc-sha256**—RSA, 128-bit AES/CBC, SHA256 hash
- **rsa-with-aes-128-gcm-sha256**—RSA, 128-bit AES/gcm, SHA256 hash
- **rsa-with-aes-256-cbc-sha**—RSA, 256-bit AES/CBC, SHA hash
- **rsa-with-aes-256-cbc-sha256**—RSA, 256-bit AES/CBC, SHA256 hash
- **rsa-with-aes-256-gcm-sha384**—RSA, 256-bit AES/gcm, SHA384 hash
- **rsa-with-des-cbc-sha**—RSA, DES CBC, SHA hash
- **rsa-with-null-md5**—RSA, no symmetric cipher, MD5 hash
- **rsa-with-null-sha**—RSA, no symmetric cipher, SHA hash
- **rsa-with-rc4-128-md5**—RSA, 128-bit RC4, MD5 hash
- **rsa-with-rc4-128-sha**—RSA, 128-bit RC4, SHA hash

enable-flow-tracing—Enable flow tracing for the profile.

preferred-ciphers—Select preferred ciphers.

Values:

- **custom**—Configure custom cipher suite and order of preference.
- **medium**—Use ciphers with key strength of 128-bits or greater.
- **strong**—Use ciphers with key strength of 168-bits or greater.
- **weak**—Use ciphers with key strength of 40-bits or greater.

trusted-ca—List of trusted certificate authority profiles.

whitelist—Addresses exempted from SSL proxy.

whitelist-url-categories—URL categories exempted from SSL proxy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *Enabling Debugging and Tracing for SSL Proxy*

protocol-version

Syntax protocol-version (all | tls1 | tls11 | tls12);

Hierarchy Level [edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The **tls11** and **tls12** options are introduced in 15.1X49-D30.

Description Specify the accepted SSL protocol version.

You can specify the SSL/TLS protocol version the SRX Series device uses to negotiate in SSL connections.

Options

- **all**—Accept all versions of TLS.
- **TLS version 1.0**—Accept TLS version 1.0. It provides secure communication over networks by providing privacy and data integrity between communicating applications
- **TLS version 1.1**—Accept TLS version 1.1. This enhanced version of TLS provides protection against cipher-block chaining (CBC) attacks.
- **TLS version 1.2** —Accept TLS version 1.2. This enhanced version of TLS provides improved flexibility for negotiation of cryptographic algorithms.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Firewall User Authentication Overview*
- *SSL Proxy Overview*

proxy (Services)

Syntax

```
proxy {
  global-config {
    session-cache-timeout seconds;
  }
  profile profile-name {
    actions {
      crl {
        disable;
        if-not-present (allow | drop);
        ignore-hold-instruction-code;
      }
      disable-session-resumption;
      ignore-server-auth-failure;
      logs {
        all;
        errors;
        info;
        sessions-allowed;
        sessions-dropped;
        sessions-ignored;
        sessions-whitelisted;
        warning;
      }
      renegotiation {
        (allow | allow-secure | drop);
      }
    }
    custom-ciphers [cipher];
    enable-flow-tracing;
    preferred-ciphers (custom | medium | strong | weak);
    root-ca root-certificate;
    trusted-ca (all | [ca-profile] );
    whitelist [global-address-book-addresses];
  }
}
```

Hierarchy Level [edit services ssl]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The **crl** statement is supported from 15.1X49-D30.

Description Specify the configuration for Secure Socket Layer (SSL) proxy support service.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *Enabling Debugging and Tracing for SSL Proxy*

rate-limiters

Syntax

```
rate-limiters {
  rate-limiter-name {
    bandwidth-limit value-in-kbps;
    burst-size-limit value-in-bytes;
  }
}
```

Hierarchy Level [edit class-of-service application-traffic-control]

Release Information Statement introduced in Junos OS Release 11.4.

Description Share the available bandwidth and burst size of a device's PICs by defining rate limiter profiles and applying them in AppQoS rules.

Options

- ***rate-limiter-name***—Name of the rate limiter. It is applied in AppQoS rules to share device resources based on quality-of-service requirements.

  The combination of rate limiting parameters, namely bandwidth- limit and burst-size-limit rate limit, make up the rate limiter profile. A maximum of 16 profiles are allowed per device. The same profile can be used by multiple rate limiters. For example, a profile with a bandwidth-limit of 200 Kbps and a burst-limit of 130,000 bytes, could be used in several rate limiters.

  A maximum of 1000 rate limiters can be created. Rate limiters are defined for the device, and are assigned in rules in a rule set. A single rate limiter can be used multiple times within the same rule set. However, the rate limiter cannot be used in another rule set.

- **bandwidth-limit *value-in-Kbps***—Maximum number of kilobits to be transmitted per second for this rate limiter. Up to 2 GB of bandwidth can be provisioned among multiple rate limiters to share the resource proportionally.

- **burst-size-limit *value-in-bytes***—Maximum number of bytes to be transferred in a single burst or time-slice. This limit ensures that a high-priority transmission does not keep a lower priority transmission from transmitting.

NOTE: The number of **bandwidth-limit** and **burst-size-limit** combinations cannot exceed 16.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppQoS*

renegotiation (Services)

Syntax renegotiation (allow | allow-secure | drop);

Hierarchy Level [edit services ssl proxy profile *profile-name* actions]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the renegotiation options.

Options
- **allow**—Allow secure and nonsecure renegotiation.
- **allow-secure**—Allow secure negotiation only.
- **drop**—Drop session on renegotiation request.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Configuring SSL Forward Proxy*

root-ca (Services)

Syntax root-ca *root-certificate*;

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Root certificate for interdicting server certificates in proxy mode. This statement is supported on the SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX.

Options *root-ca-name*—Specify root certificate for interdicting server certificates in proxy mode.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Configuring SSL Forward Proxy*
- *Firewall User Authentication Overview*

routing-instance (Advanced Policy-Based Routing)

Syntax routing-instance *name* ;

Hierarchy Level [edit security advance-policy-based-routing profile *profile-name* rule *rule-name* then]

Description Specify a specific routing instance to which the device sends the matched packets.

When traffic arrives at the specified zone or interface, it is matched by the advanced policy-based routing (APBR) profile (application profile). The application profile matches applications and application groups and if the matching rule is found, the packets are routed to the routing instance that sends the traffic to a different interface as specified in the next-hop IP address.

The routing instances specify the routing table and the destination to which a packet is forwarded. The following types of routing instances are supported:

- Forwarding—Use this routing instance type for filter-based forwarding applications.
- Virtual router—Similar to the forwarding instance type, but used for non-VPN-related applications.

Options **name**—Specify the name of the routing instance.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*
- *Understanding Advanced Policy-Based Routing*

rule (Advanced Policy-Based Routing)

Syntax

```
rule rule-name {
  match {
    dynamic-application [system-application];
    dynamic-application-group [system-application-group];
  }
  then {
    routing-instance name ;
  }
}
```

Hierarchy Level [edit security advance-policy-based-routing profile *profile-name*]

Description Configure rules for the advanced policy-based routing (APBR) profile (application profile). Associate the rule with one or more than one applications (example: for HTTP) or application groups.

The deep packet inspection and pattern matching capabilities of AppID to identify application traffic and application system cache (ASC) is consulted to get application type for matching the rule condition.

If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered as a match and the traffic will be redirected to the defined routing instance for the route lookup.

Options

match—Define an APBR term as dynamic application or dynamic application group for match criteria.

then—Define the action for matching condition by specifying the name of the routing instance for redirecting traffic.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*
- *Understanding Advanced Policy-Based Routing*

rule (Application Firewall)

Syntax

```
rule rule-name {
  match {
    dynamic-application [system-application];
    dynamic-application-groups [system-application-group];
    ssl-encryption (any | yes | no);
  }
  then {
    deny {
      block-message block-message;
    }
    permit permit;
    reject {
      block-message block-message;
    }
  }
}
```

Hierarchy Level [edit security application-firewall rule-sets *name*]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 to include the **ssl-encryption** and **reject** options. The **block-message** options added in Junos OS Release 12.1X45-D10.

Description Specify rules for application firewall.

You need to create rules to permit, reject, or deny traffic for dynamic applications to configure application firewall rule sets within the security policy. The application firewall support in the policies provides additional security control for dynamic applications.

Starting in Junos OS Release 18.2R1 application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options **match**—Specify security rule match-criteria

dynamic-application—Select dynamic applications as match criteria.

dynamic-application-group—Select dynamic applications group as match criteria.

ssl-encryption—Select SSL encryption rules as match criteria.

Values:

- **any**—Encrypted and non-encrypted rule.
- **no**—Non-encrypted rule.
- **yes**—Encrypted rule.

then—Specify the action to be performed when traffic matches the associated match criteria.

deny—Block the traffic at the firewall. The device drops the packet. By default, no message is returned to the sender.

block-message ***block-message***—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for denied HTTP or HTTPS traffic. All other traffic is dropped silently.

reject—Block the traffic at the firewall. For TCP traffic, by default the device drops the packet and returns a TCP reset (RST) message to the source host. For UDP and other protocol traffic, by default the device drops the packet and returns an ICMP "destination unreachable, port unreachable" message to both the client and the server.

block-message ***block-message***—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for denied HTTP or HTTPS traffic. All other traffic is dropped silently.

permit—Permit traffic at the firewall.

Required Privilege Level

security

Related Documentation

- *Application Firewall Overview*
- rule-sets (Security Application Firewall) on page 230
- application-firewall (Application Services) on page 155

rule-sets (CoS AppQoS)

Syntax

```
rule-sets {
  rule-set-name {
    rule rule-name {
      match {
        application application-name;
        application-any;
        application-group application-group-name;
        application-known;
        application-unknown;
      }
      then {
        dscp-code-point dscp-value ;
        forwarding-class forwarding-class-name;
        log;
        loss-priority [ high | medium-high | medium-low | low ];
        rate-limit {
          loss-priority-high;
          client-to-server rate-limiter-name;
          server-to-client rate-limiter-name;
        }
      }
    }
  }
}
```

Hierarchy Level [edit class-of-service application-traffic-control]

Release Information Statement introduced in Junos OS Release 11.4.

Description Defines AppQoS rule sets and the rules that establish priorities based on quality-of-service requirements for the associated applications. AppQoS rules can be included in policy statements to implement application-aware quality of service control.

Options

- ***rule-set-name***—Name used to refer to a collection of AppQoS rules.
- **rule *rule-name***—Name applied to the match criteria and resulting actions that control the quality-of-service provided to any matching applications.
- **application *application-name***—Name of the application to be used as match criteria for the rule.
- **application-any** —Any application encountering this rule. Note that when you use this specification, all application matching ends. Any application rule following this one will never be encountered.
- **application-group *application-group-name***—Group of applications to be used as match criteria for the rule. Both applications and application groups can be match criteria for a single rule.

- **application-known**—Match criteria specifying any session that is identified, but its corresponding application is not specified.
- **application-unknown**—Match criteria specifying any session that is not identified.
- **forwarding-class *forwarding-class-name***—The AppQoS class with which matching applications will be marked. This field identifies the rewriter that has marked the DSCP value . Therefore, the AppQoS forwarding class must be different from those used by IDP or firewall filters. With this class specified, firewall filter class will not overwrite the existing DSCP value.
- **dscp-code-point**—DSCP alias or bit map with which matching applications will be marked to establish the output queue. This value can be marked by rewriters from IDP, AppQoS, or a firewall filter. The forwarding-class value identifies which rewriter has re-marked the packet with the current DSCP value. If a packet triggers all three rewriters, IDP takes precedence over AppQoS, which takes precedence over a firewall filter.
- **loss-priority**—Loss priority with which matching applications will be marked. This value is used to determine the likelihood that a packet would be dropped when encountering congestion. A high loss priority means that there is an 80% chance of packet loss in congestion. Possible values are high, medium-high, medium-low and low.
- **rate-limit**—Rate limiters to be associated with client-to-server and with server-to-client traffic for this application. The rate limiter profile defines maximum speed and volume limits for matching applications.
- **log**—AppQoS event logging.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppQoS*

rule-sets (Security Application Firewall)

Syntax

```
rule-sets rule-set-name {
  default-rule {
    (deny [block-message] | permit | reject [block-message]);
  }
  profile profile-name;
  rule rule-name {
    match {
      dynamic-application [system-application];
      dynamic-application-groups [system-application-group];
      ssl-encryption (any | yes | no);
    }
    then {
      deny {
        block-message block-message;
      }
      permit permit;
      reject {
        block-message block-message;
      }
    }
  }
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 to include the **ssl-encryption** and **reject** options. The **block-message** options added in Junos OS Release 12.1X45-D10.

Description Configure the set of rules for the application firewall.

The application firewall is defined by a collection of rule sets. These rule sets can be defined independently and shared across network security policies. A rule set defines the rules that specify match criteria, including dynamic applications, and the action to be taken for matching traffic.

To implement an application firewall, you need to:

- Define one or more application firewall rule sets.
- Create rules for each rule set that permit, reject, or deny traffic based on the application ID.
- Configure a security policy to invoke the application firewall service and specify the rule set to be applied to permitted traffic.

The application firewall support in the policies provides additional security control for dynamic applications.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options

rule-set-name—Name of the rule set.

profile *profile-name*—Profile for block message.

default-rule—Specify default rule.

rule—Specify security rule match-criteria

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring an Application Group for Application Firewall*

security-zone

Syntax

```
security-zone zone-name {
  address-book {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
      range-address lower-limit to upper-limit;
      wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
      address address-name;
      address-set address-set-name;
      description text;
    }
  }
  advance-policy-based-routing;
  application-tracking;
  description text;
  enable-reverse-reroute;
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
  interfaces interface-name {
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
      system-services service-name {
        except;
      }
    }
  }
  screen screen-name;
  tcp-rst;
}
```

Hierarchy Level [edit security zones]

Release Information Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description Define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.

Options ***zone-name*** —Name of the security zone.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Security Zones and Interfaces Overview*
- *Example: Configuring Application Firewall Rule Sets Within a Security Policy*

server-certificate (Services)

Syntax server-certificate *server-certificate*;

Hierarchy Level [edit services ssl termination profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. This statement is supported on the SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX.

Description Specify the local certificate identifier.

Options **server-certificate**—Specify the name of the local certificate identifier.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

session-update-interval

Syntax session-update-interval *session-update-interval*;

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure the interval between session update messages for long-lived sessions being monitored by AppTrack. Byte count, packet count, and start and end times are updated and logged when the amount of time between session start or the previous update and the current time exceeds the interval.

Options ***session-update-interval***—Minutes between updates.

Default: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring AppTrack*

signature

Syntax

```
signature name {
  member name {
    context context;
    direction (any | client-to-server | server-to-client);
    pattern pattern;
  }
  port-range [ port-range ... ];
}
```

Hierarchy Level [edit services application-identification application *application-name* over *protocol-type*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Application signature for pattern matching. A unique application signature identifier. Must be a unique name with a maximum length of 63 characters.

You need to define an application signature to match the pattern by defining a unique application signature identifier, application signature member identifier, connection direction of the packets, and set the context to be matched. You also need to specify port range for TCP or UDP.

Options

member—Member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01 through m15.)

port-range—Port range. This option is applicable for TCP-based or UDP-based applications only.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level system

Related Documentation

- *Custom Application Signatures for Application Identification*

size (Services)

Syntax size *size*;

Hierarchy Level [edit services ssl traceoptions file *file-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the maximum trace file size. This statement is supported on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

Options **size**—Specify the maximum trace file size.

Range: 10,240 to 1,073,741,824.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Configuring SSL Forward Proxy*
- *Firewall User Authentication Overview*

statistics (Services)

Syntax

```
statistics {
  interval interval-number;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the interval, in minutes, for statistics collection.

Options

interval *interval-number*—Length of time, in minutes, that application statistics are collected.

Range: 1 through 1440 minutes

Default: 1 minute

NOTE: For SRX Series devices, the maximum number of interval periods for which statistics are stored is 8.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Onbox Application Identification Statistics*

termination (Services)

Syntax

```
termination {
  profile profile-name {
    custom-ciphers [cipher];
    enable-flow-tracing;
    enable-session-cache;
    preferred-ciphers (custom | medium | strong | weak);
    protocol-version (all | tls1 | tls11 | tls12);
    server-certificate certificate-identifier;
  }
}
```

Hierarchy Level [edit services ssl]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The **protocol-version** statement is updated to include **tls11** and **tls12** from Junos OS Release 15.1X49-D30.

Description Specify the configuration for Secure Socket Layer (SSL) termination support service.

Following types of SSL profiles are supported on SRX Series to secure connections based on the role of the SRX Series device:

- SSL initiation: The SRX Series device, acting as an SSL proxy client, initiates and maintains SSL sessions between itself and an SSL server. SRX device receives unencrypted data from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server.
- SSL termination: The SRX Series device, actings as an SSL proxy server, terminates the SSL session from the client and then establishing a new SSL connection to the server. The SRX Series device decrypts the data and then sends the data as un-encrypted request to the other servers (HTTP server).

The SSL proxy profile will be applied to the security policy as application services.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

then (Security Application Firewall)

Syntax

```
then {
   (deny [block-message] | permit | reject [block-message]);
}
```

Hierarchy Level [edit security application-firewall rule-set *rule-set-name* rule *rule-name*]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 with the **reject** option. The **block-message** option added in Junos OS Release 12.1X45-D10.

Description Specify the action to be performed when traffic matches the associated match criteria.

Note that an application firewall is applied after a session has already been created by the security firewall. When traffic is rejected or denied by an application firewall, therefore, logs contain a session open message, a session reject or deny message, and a session close message.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options

- **deny**—Block the traffic at the firewall. The device drops the packet. By default, no message is returned to the sender.
  - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for denied HTTP or HTTPS traffic. All other traffic is dropped silently.
- **permit**—Permit traffic at the firewall.
- **reject**—Block the traffic at the firewall. For TCP traffic, by default the device drops the packet and returns a TCP reset (RST) message to the source host. For UDP and other protocol traffic, by default the device drops the packet and returns an ICMP “destination unreachable, port unreachable” message to both the client and the server.
  - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for rejected HTTP or HTTPS traffic. All other traffic is dropped as specified in the default action for the **reject** option.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring an Application Group for Application Firewall*

traceoptions (advanced policy-based routing)

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security advance-policy-based-routing]

Release Information Statement introduced in Junos OS Release 15.1X49-D60.

Description Configure tracing operations for advanced policy-based routing.

Options

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **compilation**—Trace rule set compilation events
  - **configuration**—Trace configuration events
  - **ipc**—Trace process inter communication events
  - **lookup**—Trace rule set lookup events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*
- *Understanding Advanced Policy-Based Routing*

traceoptions (Security Application Firewall)

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure trace options for the application firewall.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme

continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: ***x*** **K** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **compilation**—Trace rule set compilation events
  - **configuration**—Trace configuration events
  - **ipc**—Trace process inter communication events
  - **lookup**—Trace rule set lookup events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Application Firewall Overview*

traceoptions (Services Application Identification)

Syntax

```
traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag all;
  level (all | error | info | notice | verbose | warning)
  no-remote-trace;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure tracing operations for application identification services.

Options

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

  all—Trace with all flags enabled.

- **level**—Set the level of debugging the output option.
  - **all**—Match all levels.
  - **error**—Match error conditions.
  - **info**—Match informational messages.
  - **notice**—Match conditions that should be handled specially
  - **verbose**—Match verbose messages.
  - **warning**—Match warning messages.
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Understanding Application Identification Techniques*

trusted-ca (Services)

Syntax trusted-ca (all | [*ca-profile*]);

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the list of trusted certificate authority profiles. This statement is supported on the SRX1500, SRX5400, SRX5600, and SRX5800 devices, and vSRX.

Options
- *trusted-ca-name*—Specify the certificate authority profile name.
- **all**—Select all certificate authority profiles.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Configuring SSL Forward Proxy*
- *Firewall User Authentication Overview*

tunables

Syntax

```
tunables {
  drop-on-zone-mismatch;
  enable-logging;
  max-route-change value;
}
```

Hierarchy Level [edit security advance-policy-based-routing]

Release Information Statement introduced in Junos OS Release 15.1X49-D110.

Description Configure the advanced policy-based (APBR) routing options to streamline the traffic handling.

You can streamline the traffic handling with APBR such as limiting the number of times a route can change for a session, terminating the session if there is a mismatch between zones when APBR is being applied in the middle of the session, and enabling logging to record events that occur on the device.

Fine-tuning the APBR configuration is required to avoid the possible issues such as excessive transitions due to route changes.

Options

drop-on-zone-mismatch—Terminate the session instead of instead of allowing traffic to traverse through the same route bypassing APBR.

enable-logging—Enable logging to record events that occur on the device for APBR-related operations.

max-route-change *value*—Configure the threshold for limiting the number of times a route can change for a session.

Range: 0-5

Default: 1

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*
- *Understanding Advanced Policy-Based Routing*

whitelist (Services)

Syntax whitelist [global-address-book-addresses];

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the addresses exempted from the SSL proxy. This statement is supported on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

You can selectively bypass SSL proxy processing for some sessions by configuring a whitelist. Typically, you might configure the whitelist to include trusted servers or domains with which you are very familiar. Whitelists include addresses that you want to exempt from undergoing SSL proxy processing.

To configure the whiltelist, you need to specify the domain that you want to exempt in an address book and then configure the address in the SSL proxy profile.

Options

- *whitelist-address*—Specify address from the global address book.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Configuring SSL Forward Proxy*
- *Firewall User Authentication Overview*

whitelist-url-categories

Syntax whitelist-url-categories *url-category-list*;

Hierarchy Level [edit services ssl proxy profile *profile-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D80.

Description Specify the enhanced Web filtering URL categories to be whitelisted.

Whitelist URL categories include URL categories supported by UTM in the whitelist configuration of SSL forward proxy.

The predefined URL categories depends on UTM. To enable the URL-based whitelisting in SSL proxy, the following basic configurations are required:

```
[edit]
user@host# set security utm feature-profile web-filtering type juniper-enhanced
user@host# set security utm utm-policy policy-name web-filtering http-profile
  junos-wf-enhanced-default
```

NOTE: Starting with Junos OS Release 17.4R1, the whitelisting feature is extended to support custom URL categories.

Options ***url-category-list***— List of custom URLs along with URL categories defined by enhanced Web filtering that need to be whitelisted.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *SSL Proxy Overview*
- *Configuring SSL Forward Proxy*
- *show services ssl proxy statistics*

zones

Syntax

```
zones {
  functional-zone {
    management {
      description text;
      host-inbound-traffic {
        protocols protocol-name {
          except;
        }
        system-services service-name {
          except;
        }
      }
      interfaces interface-name  {
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
      }
      screen screen-name;
    }
  }
  security-zone zone-name {
    address-book {
      address address-name {
        ip-prefix {
          description text;
        }
        description text;
        dns-name domain-name {
          ipv4-only;
          ipv6-only;
        }
        range-address lower-limit to upper-limit;
        wildcard-address ipv4-address/wildcard-mask;
      }
      address-set address-set-name {
        address address-name;
        address-set address-set-name;
        description text;
      }
    }
    advance-policy-based-routing;
    application-tracking;
    description text;
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
```

```
        system-services service-name {
          except;
        }
      }
      interfaces interface-name {
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
      }
      screen screen-name;
      tcp-rst;
    }
  }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:

- Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.
- Security zone—Most common type of zone that is used as a building block in policies.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Zones and Interfaces Overview*
- *Supported System Services for Host Inbound Traffic*

CHAPTER 5

Operational Commands

- clear security application-firewall rule-set statistics
- clear security application-firewall rule-set statistics logical-system
- clear services application-identification application-statistics
- clear services application-identification application-statistics cumulative
- clear services application-identification application-statistics interval
- clear services application-identification application-system-cache (Junos OS)
- clear services application-identification counter (Values)
- request security pki ca-certificate ca-profile-group load
- request security pki local-certificate export
- request security pki local-certificate generate-self-signed
- request security pki local-certificate load
- request services application-identification application
- request services application-identification download
- request services application-identification download status
- request services application-identification group
- request services application-identification install
- request services application-identification install status
- request services application-identification proto-bundle-status
- request services application-identification uninstall
- request services application-identification uninstall status
- show class-of-service application-traffic-control counter
- show class-of-service application-traffic-control statistics rate-limiter
- show class-of-service application-traffic-control statistics rule
- show security advance-policy-based-routing statistics
- show security advance-policy-based-routing status
- show security advance-policy-based-routing profile
- show security application-firewall rule-set
- show security application-firewall rule-set logical-system

- show security application-tracking counters
- show security flow session
- show security flow session application-firewall
- show security pki ca-certificate
- show security pki local-certificate (View)
- show security policies
- show services application-identification application
- show services application-identification application-system-cache (View)
- show services application-identification commit-status
- show services application-identification counter (AppSecure)
- show services application-identification group
- show services application-identification statistics applications
- show services application-identification statistics application-groups
- show services application-identification status
- show services application-identification version
- show services icap-redirect server status
- show services service-redirect statistic

clear security application-firewall rule-set statistics

Syntax **clear security application-firewall rule-set statistics**

Release Information Command introduced in Junos OS Release 11.1.

Description Clear all the security application firewall rule set statistics information.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Required Privilege Level clear

Related Documentation

- show security application-firewall rule-set on page 287

Output Fields This command produces no output.

clear security application-firewall rule-set statistics logical-system

Syntax The master, or root, administrator can issue the following statements:

clear security application-firewall rule-set statistics [logical-system *logical-system-name* | all | root-logical-system]

The user logical system administrator can issue the following statement:

clear security application-firewall rule-set statistics all

Release Information Command introduced in Junos OS Release 11.4.

Description Clear all security application firewall rule set statistics.

NOTE: User logical system administrators can clear statistics only for the logical systems they can access. For information about master and user administrator roles in logical systems, see *Understanding the Master Logical System and the Master Administrator Role*.

Starting in Junos OS Release 18.2R1 application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options ***logical-system-name***—Name of a specific logical system.

all—(default) Clear all rule set statistics for a specific logical system or all logical systems.

root-logical-system—Clear application firewall rule set statistics on the root logical system (master administrator only).

Required Privilege Level clear

Related Documentation

- show security application-firewall rule-set logical-system on page 290

Output Fields This command produces no output.

clear services application-identification application-statistics

Syntax clear services application-identification application-statistics

Release Information Statement introduced in Junos OS Release 11.4.

Description Clears all Junos OS application statistics such as cumulative, interval, applications, and application groups.

Required Privilege Level clear

Related Documentation

- show services application-identification statistics applications on page 343
- show services application-identification statistics application-groups on page 345
- clear services application-identification application-statistics interval on page 259
- clear services application-identification application-statistics cumulative on page 258

Output Fields This command produces no output.

clear services application-identification application-statistics cumulative

Syntax clear services application-identification application-statistics cumulative

Release Information Statement introduced in Junos OS Release 11.4.

Description Clear all Junos OS application cumulative statistics.

Required Privilege Level clear

Related Documentation

- show services application-identification statistics applications on page 343
- show services application-identification statistics application-groups on page 345
- clear services application-identification application-statistics on page 257
- clear services application-identification application-statistics interval on page 259

Output Fields This command produces no output.

clear services application-identification application-statistics interval

Syntax clear services application-identification application-statistics interval

Release Information Statement introduced in Junos OS Release 11.4.

Description Clear all Junos OS application interval statistics.

Required Privilege Level clear

Related Documentation

- show services application-identification statistics applications on page 343
- show services application-identification statistics application-groups on page 345
- clear services application-identification application-statistics on page 257
- clear services application-identification application-statistics cumulative on page 258

Output Fields This command produces no output.

clear services application-identification application-system-cache (Junos OS)

Syntax

clear services application-identification application-system-cache
<node (*node-id* | all | local | primary) >

Release Information

Command introduced in Junos OS Release 10.2. Command syntax updated in Junos OS Release 12.1.

Description

Clear Junos OS application identification application system cache.

Options

- none—Clear the application system cache on the device.
- **node**—(Optional) For chassis cluster configurations, clear application system cache on the specified nodes.
  - ***node-id***—Specific node number
  - **all**—All nodes
  - **local**—Local node
  - **primary**—Primary node

Required Privilege Level

clear

Related Documentation

- show services application-identification application-system-cache (View) on page 333

Output Fields

This command produces no output.

clear services application-identification counter (Values)

Syntax clear services application-identification counter <ssl-encrypted-sessions>

Release Information Command introduced in Junos OS Release 10.2. Command updated in Junos OS Release 12.1-X47-D15.

Description Reset all the Junos OS application identification counter values.

Options **ssl-encrypted-sessions**—Reset application identification counter values for SSL encrypted sessions.

Required Privilege Level clear

Related Documentation
- show services application-identification counter (AppSecure) on page 337

List of Sample Output clear services application-identification counter on page 261

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services application-identification counter

```
user@host> clear services application-identification counter
clear_counter_class: counters cleared, status = 0
```

request security pki ca-certificate ca-profile-group load

Syntax request security pki ca-certificate ca-profile-group load ca-group-name *ca-group-name* filename [*path/filename* | default]

Release Information Command introduced in Junos OS Release 12.1; **default** option added in Junos OS Release 12.1X47-D10.

Description For SSL forward proxy, you need to load trusted CA certificates on your system. By default, Junos OS provides a list of trusted CA certificates that include default certificates used by common browsers. Alternatively, you can define your own list of trusted CA certificates and import them on to your system.

Use this command to load the default certificates or to specify a path and filename of trusted CA certificates that you define.

Options **ca-group-name *ca-group-name***—Load the specified CA group profile.

filename *path/filename*—Directory location and filename of the trusted CA certificates defined by you.

filename default—Load the trusted CA certificates available by default.

Required Privilege Level maintenance

Related Documentation
- show security pki ca-certificate on page 307
- *Understanding Certificates and PKI*

List of Sample Output
request security pki ca-certificate ca-profile-group load (default) on page 262
request security pki ca-certificate ca-profile-group load (path/filename) on page 263

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate ca-profile-group load (default)

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name ca-default
filename default

Do you want to load this CA certificate ? [yes,no] (no) yes
Loading 157 certificates for group 'ca-default'.
ca-default_1: Loading done.
ca-default_2: Loading done.
ca-default_3: Loading done.
.....
```

Sample Output

request security pki ca-certificate ca-profile-group load (path/filename)

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name ca-manual
filename /var/tmp/firefox-all.pem

Do you want to load this CA certificate ? [yes,no] (no) yes

Loading 196 certificates for group 'ca-manual'.
ca-manual_1_sysgen: Loading done.
ca-manual_2_sysgen: Loading done.
ca-manual_3_sysgen: Loading done.
ca-manual_4_sysgen: Loading done.
ca-manual_5_sysgen: Loading done.
ca-manual_6_sysgen: Loading done.

...
ca-manual_195_sysgen: Loading done.
ca-manual_196_sysgen: Loading done.
ca-profile-group 'ca-manual' successfully loaded. Success[193] Skipped[3]
```

request security pki local-certificate export

Syntax request security pki local-certificate export

Release Information Command introduced in Junos OS Release 12.1.

Description Export a generated self-signed certificate from the default location (var/db/certs/common/local) to a specific location within the device.

Options

certificate id *certificate-id-name*—Name of the local digital certificate.

filename *path/filename*—Target directory location and filename of the CA digital certificate.

type (der | pem)—Certificate format: DER (distinguished encoding rules) or PEM (privacy-enhanced mail).

Required Privilege Level maintenance

Related Documentation

- *Understanding Certificates and PKI*

List of Sample Output request security pki local-certificate export on page 264

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate export

```
user@host> request security pki local-certificate export filename /var/tmp/my-cert.pem
certificate-id nss-cert type pem
certificate exported successfully
```

request security pki local-certificate generate-self-signed

Syntax request security pki local-certificate generate-self-signed certificate-id *certificate-id-name* domain-name *domain-name* ip-address *ip-address* email *email-address* subject *subject-distinguished-name*

Release Information Command introduced in Junos OS Release 9.1.

Description Manually generate a self-signed certificate for the given distinguished name.

Options

certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

domain-name *domain-name*—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

email *email-address*—E-mail address of the certificate holder.

ip-address *ip-address*—IP address of the router.

subject *subject-distinguished-name*—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

Required Privilege Level maintenance
security

Related Documentation

- *Requesting for and Installing a Digital Certificates on Your Router*

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name example.net email user1@example.net
Self-signed certificate generated and loaded successfully
```

request security pki local-certificate load

Syntax request security pki local-certificate load certificate-id *certificate-id-name* filename *path*

Release Information Command introduced in Junos OS Release 7.5.

Description Manually load a local digital certificate from a specified location.

Options

certificate-id *certificate-id-name*—Name of the public/private key pair mapped to the local digital certificate.

filename *path/filename*—Directory location and filename of the local digital certificate provided by the CA.

Required Privilege Level maintenance

List of Sample Output request security pki local-certificate load on page 266

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate load

```
user@host> request security pki local-certificate load filename /tmp/router2-cert certificate-id
local-entrust2
Local certificate local-entrust2 loaded successfully
```

request services application-identification application

Syntax request services application-identification application [disable | enable] *predefined-application-name*

Release Information Command introduced in Junos OS Release 11.4.

Description Disable, or enable a predefined application signature.

Options **disable**—(Optional) Disable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration.

The following conditions apply:

- You cannot disable a predefined application signature that is referenced by an active security policy or custom application signature. First modify or deactivate the policy or custom application signature.
- If you disable an application signature, for example, junos:HTTP, that has nested applications, the nested applications are not recognized.

enable—(Optional) Enable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration.

Required Privilege Level maintenance

Related Documentation
- show services application-identification application on page 327

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification application disable

```
user@host> request services application-identification application disable junos:163
 Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
 Disable application junos:163 succeed.
```

request services application-identification download

Syntax request services application-identification download <*version*>;

Release Information Statement introduced in Junos OS Release 10.2.
Statement modified in Junos OS Release 11.4.

Description Manually download the application package for Junos OS application identification. The application package is extracted from the IDP signature database and contains signature definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP.

Options ***version***—(Optional) Download a specific version of the application package from the Juniper Networks security website. If you do not enter a version, the most recent version is downloaded.

Required Privilege Level maintenance

Related Documentation
- request services application-identification download status on page 269
- request services application-identification install on page 272

List of Sample Output request services application-identification download on page 268

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services application-identification download

```
user@host> request services application-identifications download
Please use command "request services application-identification download status"
 to check status
```

request services application-identification download status

Syntax request services application-identification download status

Release Information Statement introduced in Junos OS Release 10.2.
Statement modified in Junos OS Release 11.4.

Description Check the download status of the application signature package. The downloaded application package is saved under **/var/db/appid/sec-download/**.

Required Privilege Level maintenance

Related Documentation
- request services application-identification download on page 268

List of Sample Output request services application-identification download status on page 269

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification download status

```
user@host> request services application-identifications download status
Application package 1608 is downloaded successfully.
```

request services application-identification group

Syntax request services application-identification group [copy | disable | enable] *predefined-application-group-name*

Release Information Command introduced in Junos OS Release 11.4.

Description Copy, disable, or enable a predefined application signature group.

Options **copy**—(Optional) Copy a predefined application signature group from the database to the configuration and change the name (for example, my:FTP). The ID and order are generated automatically. Do not name your custom application signature group with the **junos** prefix; this prefix is reserved for predefined application signature groups. You can copy the same predefined application signature group only once; duplicate custom signature groups are not allowed.

NOTE: In configuration mode, if an uncommitted action is pending, the **request services application-identification group copy** command fails.

disable—(Optional) Disable a predefined application signature group.

NOTE: You cannot disable a predefined application signature group that is referenced by an active security policy or custom application signature group. First modify or deactivate the policy or custom application signature group.

enable—(Optional) Enable a predefined application signature group.

predefined-application-group-name—Name of the predefined application signature group.

Required Privilege Level maintenance

Related Documentation

- show services application-identification group on page 341

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification group

```
user@host> request services application-identification group disable
junos:infrastructure:networking
Disable application group junos:infrastructure:networking succeed.
```

request services application-identification group

```
user@host> request services application-identification group enable
junos:infrastructure:networking
Enable application group junos:infrastructure:networking succeed.
```

request services application-identification group

```
user@host> request services application-identification group copy junos:infrastructure:networking
Please wait while we are copying group ...
Copy application group junos:infrastructure:networking succeed.
```

request services application-identification install

Syntax request services application-identification install

Release Information Statement introduced in Junos OS Release 11.4.

Description Install the downloaded predefined application signature package.

Required Privilege Level maintenance

Related Documentation

- request services application-identification install status on page 273
- request services application-identification download on page 268

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

```
user@host> request services application-identification install
Please use command "request services application-identification install status"
to check status and use command "request services application-identification
proto-bundle-status" to check protocol bundle status
```

request services application-identification install status

Syntax request services application-identification install status

Release Information Statement introduced in Junos OS Release 11.4.

Description Display the status of the install operation.

Required Privilege Level maintenance

Related Documentation
- request services application-identification install on page 272

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

```
user@host> request services application-identification install status
Install application package version (1776) succeed.
```

request services application-identification proto-bundle-status

Syntax request services application-identification proto-bundle-status

Release Information Statement introduced in Junos OS Release 12.1X47-D10.

Description Display the status of the install operation of the protocol bundle.

Required Privilege Level maintenance

Related Documentation
- request services application-identification install on page 272

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

```
user@host> request services application-identification proto-bundle-status
Protocol Bundle Version (1.30.4-22.005 (build date Jan 17 2014)) and application
 secpack version (2345) is loaded and activated.
```

request services application-identification uninstall

Syntax request services application-identification uninstall

Release Information Statement introduced in Junos OS Release 10.2. Statement modified in Junos OS Release 10.4. Statement modified in Junos OS Release 11.4.

Description Uninstall the predefined application package.

The uninstall operation will fail if any active security policies reference predefined application signatures or predefined application signature groups in the Junos OS configuration.

Required Privilege Level maintenance

Related Documentation

- request services application-identification install on page 272

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

```
user@host> request services application-identification uninstall
Please use command "request services application-identification uninstall status"
 to check status and use command "request services application-identification
proto-bundle-status" to check protocol bundle status
```

request services application-identification uninstall status

Syntax request services application-identification uninstall status

Release Information Statement introduced in Junos OS Release 11.4.

Description Display the status of the uninstall operation.

Required Privilege Level maintenance

Related Documentation
- request services application-identification uninstall on page 275

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

```
user@host> request services application-identification uninstall status
Uninstall application package version (1776) succeed.
```

show class-of-service application-traffic-control counter

Syntax show class-of-service application-traffic-control counter

Release Information Command introduced in Junos OS Release 11.4.

Description Display AppQoS DSCP marking and honoring statistics based on Layer 7 application classifiers.

Required Privilege Level view

Related Documentation
- *Example: Configuring AppQoS*

List of Sample Output
show class-of-service application-traffic-control counter on page 277
show class-of-service application-traffic-control counter (Unified Policies) on page 278

Output Fields Table 7 on page 277 lists the output fields for the **show class-of-service application-traffic-control counter** command. Output fields are listed in the approximate order in which they appear.

Table 7: show class-of-service application-traffic-control counter Output Fields

Field Name	Field Description
pic	PIC number of the accumulated statistics. NOTE: The PIC number is always displayed as **0** for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Sessions processed	The number of sessions where the class of service was checked.
Sessions marked	The number of sessions marked based on application-aware DSCP marking.
Sessions honored	The number of sessions honored based on application-aware traffic honoring.
Sessions rate limited	The number of sessions that have been rate limited.
Client-to-server flows rate limited	The number of client-to-server flows that have been rate limited.
Server-to-client flows rate limited	The number of server-to-client flows that have been rate limited.

Sample Output

show class-of-service application-traffic-control counter

```
user@host> show class-of-service application-traffic-control counter
```

```
pic: 2/1
  Counter type                                          Value
  Sessions processed                                    300
  Sessions marked                                       200
  Sessions honored                                      0
  Sessions rate limited                                 100
  Client-to-server flows rate limited                   100
  Server-to-client flows rate limited                   70

pic: 2/0
  Counter type                                          Value
  Sessions processed                                    400
  Sessions marked                                       300
  Sessions honored                                      0
  Sessions rate limited                                 200
  Client-to-server flows rate limited                   200
  Server-to-client flows rate limited                   100
```

show class-of-service application-traffic-control counter (Unified Policies)

```
user@host> show class-of-service application-traffic-control counter
pic: 0/0
  Counter type                                                Value
 Sessions processed                                           2
 Sessions marked                                              1
 Sessions honored                                             1
 Sessions rate limited                                        1
 Client-to-server flows rate limited                          0
 Server-to-client flows rate limited                          1
 Session default ruleset hit                    1
 Session ignored no default ruleset                           1
```

show class-of-service application-traffic-control statistics rate-limiter

Syntax show class-of-service application-traffic-control statistics rate-limiter

Release Information Command introduced in Junos OS Release 11.4.

Description Display AppQoS real-time run information about application rate limiting of current or recent sessions.

Required Privilege Level view

Related Documentation
- *Example: Configuring AppQoS*

List of Sample Output show class-of-service application-traffic-control statistics rate-limiter on page 279

Output Fields Table 8 on page 279 lists the output fields for the **show class-of-service application-traffic-control statistics rate-limiter** command. Output fields are listed in the approximate order in which they appear.

Table 8: show class-of-service application-traffic-control statistics rate-limiter Output Fields

Field Name	Field Description
pic	PIC number. NOTE: The PIC number is always displayed as **0** for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Ruleset	The rule set applied on the session.
Application	The application match for applying the rule set.
Client-to-server	The rate limiter applied from client to server.
Rate(kbps)	The rate in the client-to-server direction
Server-to-client	The rate limiter applied from server to client.
Rate(kbps)	The rate in the server-to-client direction.

Sample Output

show class-of-service application-traffic-control statistics rate-limiter

```
user@host> show class-of-service application-traffic-control statistics rate-limiter
pic: 2/1
  Ruleset       Application  Client-to-server   Rate(kbps)   Server-to-client
```

```
Rate(kbps)
  my-ruleset-1  HTTP         my-http-c2s-rl     10000000    my-http-s2c-rl
20000000
  my-ruleset-2  HTTP         my-http-c2s-rl-2   20000000    my-http-s2c-rl-2
30000000
  my-ruleset-2  FTP          my-ftp-c2s-rl      50000       my-ftp-s2c-rl
50000
  ...

pic: 2/0
  Ruleset       Application  Client-to-server   Rate(kbps)   Server-to-client
Rate(kbps)
  my-ruleset-1  HTTP         my-http-c2s-rl     10000000    my-http-s2c-rl
20000000
  my-ruleset-2  HTTP         my-http-c2s-rl-2   20000000    my-http-s2c-rl-2
30000000
  my-ruleset-2  FTP          my-ftp-c2s-rl      50000       my-ftp-s2c-rl
50000
```

show class-of-service application-traffic-control statistics rule

Syntax show class-of-service application-traffic-control statistics rule

Release Information Command introduced in Junos OS Release 11.4.

Description Display AppQoS counters identifying rule hits.

Required Privilege Level view

Related Documentation
- *Example: Configuring AppQoS*

List of Sample Output show class-of-service application-traffic-control statistics rule on page 281

Output Fields Table 9 on page 281 lists the output fields for the **show class-of-service application-traffic-control statistics rule** command. Output fields are listed in the approximate order in which they appear.

Table 9: show class-of-service application-traffic-control statistics rule Output Fields

Field Name	Field Description
pic	PIC number where the rule is applied. NOTE: The PIC number is always displayed as **0** for for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Ruleset	The rule set containing the rule.
Rule	The rule to which the statistic applies.
Hits	The number of times a match for the rule was encountered.

Sample Output

show class-of-service application-traffic-control statistics rule

```
user@host> show class-of-service application-traffic-control statistics rule
pic: 2/0
  Ruleset          Rule           Hits
  my-ruleset-1     ftp-rule       100
  my-ruleset-1     httpp-rule     100
  my-ruleset-2     telnet-rule    300
  my-ruleset-2     smtp-rule      300
  ...

pic: 2/1
  Ruleset          Rule           Hits
  my-ruleset-1     ftp-rule       200
```

```
my-ruleset-1     httpp-rule     300
my-ruleset-2     telnet-rule    400
my-ruleset-2     smtp-rule      500
```

show security advance-policy-based-routing statistics

Syntax show security advance-policy-based-routing statistics

Release Information Command introduced in Junos OS Release 15.1X49-D60. Support for Advanced Policy-Based Routing Midstream is introduced in Junos OS Release 15.1X49-D110.

Description Display the statistics counter for APBR.

You can use this command to understand the details on traffic handling with APBR such as:

- Sessions processed for the application-based routing.
- The number of times the application traffic matches the APBR profile and APBR is applied for the session.
- The number of times AppID was consulted to identify application traffic.

Required Privilege Level view

Related Documentation
- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*

Output Fields Table 10 on page 283 lists the output fields for the **show security advance-policy-based-routing statistics** command. Output fields are listed in the approximate order in which they appear.

Table 10: show security advance-policy-based-routing statistics

Field Name	Field Description
Session Processed	The number of sessions processed for the application-based routing.
ASC Success	The number of times the presence of an entry in the application system cache (ASC) is found.
Rule match success	The number of times the application traffic matches the APBR profile.
Route modified	The number of times the APBR is applied for the session.
AppID Requested	The number of times AppID was consulted to identify application traffic.

Table 11 on page 284 lists the output fields for the **show security advance-policy-based-routing statistics** command for midstream support. Output fields are listed in the approximate order in which they appear.

Table 11: show security advance-policy-based-routing statistics (Advanced Policy-Based Routing Midstream Support)

Field Name	Field Description
Session Processed	The number of sessions processed for the application-based routing.
AppID cache hits	The number of times the presence of an entry in the application system cache (ASC) is found.
AppID Requested	The number of times AppID was consulted to identify application traffic.
Rule matches	The number of times the application traffic matches the APBR profile.
Route changed on cache hits	The number of times the APBR is applied for the session.
Route changed midstream	Number of times a route is changed for a session.
Zone mismatch	No of times a zone for an interface is changed in the middle of a session.
Drop on zone mismatch	Number of times a session is terminated because of change of zone in the middle of the session.

Sample Output

show security advance-policy-based-routing statistics

```
user@host> show security advance-policy-based-routing statistics
Advance Profile Based Routing statistics:
  Session Processed:                    5529
  ASC Success:                          3113
  Rule match success:                   107
  Route  modified:                      107
  AppID Requested:                      2416
```

show security advance-policy-based-routing statistics (Midstream Support)

```
user@host> show security advance-policy-based-routing statistics
Advance Profile Based Routing statistics:
  Sessions Processed                    0
  AppID cache hits                      0
  AppID requested                       0
  Rule matches                          0
  Route changed on cache hits           0
  Route changed midstream               0
  Zone mismatch                         0
  Drop on zone mismatch                 0
```

show security advance-policy-based-routing status

Syntax show security advance-policy-based-routing status

Release Information Command introduced in Junos OS Release 15.1X49-D60.

Description Check if the advanced policy-based routing (APBR) is enabled.

You can create an advanced policy-based routing (APBR) profile (application profile) to match applications and application groups and redirect those matching traffic to the specified routing instance for the route lookup. The application profile is attached to a security zone or it can be attached to a specific logical or physical interface associated with the security zone.

Required Privilege Level view

Related Documentation

- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*

Sample Output

show security advance-policy-based-routing status

```
user@host> show security advance-policy-based-routing status
Advance Policy Based Routing is enabled.
```

show security advance-policy-based-routing profile

Syntax show security advance-policy-based-routing profile

Release Information Command introduced in Junos OS Release 15.1X49-D60.

Description Display the advanced policy-based routing (APBR) profile-to-zone mapping.

Required Privilege Level view

Related Documentation
- *Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution*

Output Fields Table 12 on page 286 lists the output fields for the **show security advance-policy-based-routing profile** command. Output fields are listed in the approximate order in which they appear.

Table 12: show security advance-policy-based-routing profile

Field Name	Field Description
pic	PIC number of the accumulated statistics. NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Profile	The name of the advanced policy-based (APBR) routing profile.
Zone	The zone on which APBR profile is applied to.

Sample Output

show security advance-policy-based-routing profile

```
user@host> show security advance-policy-based-routing profile

pic: 0/0
Profile    Zone
Profile1  trust
```

show security application-firewall rule-set

Syntax show security application-firewall rule-set (*<rule-set-name>* | all)

Release Information Command introduced in Junos OS Release 11.1. Updated in Junos OS Release 12.1X44-D10 with output format changes. Updated in Junos OS Release 12.1X45-D10 with redirection counters.

Description Display information about the specified rule set defined in the application firewall.

The application firewall is defined by a collection of rule sets. A rule set defines the rules that specify match criteria, including dynamic applications, and the action to be taken for matching traffic.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options ***rule-set-name***—Name of the rule set.

all—Display information about all the application firewall rule sets.

Required Privilege Level view

Related Documentation
- clear security application-firewall rule-set statistics on page 255

List of Sample Output
show security application-firewall rule-set my_ruleset1 on page 288
show security application-firewall rule-set all on page 288

Output Fields Table 13 on page 287 lists the output fields for the **show security application-firewall rule-set** command. Output fields are listed in the approximate order in which they appear.

Table 13: show security application-firewall rule-set Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.
Logical system	Name of the logical system of the rule set.
Profile	The redirect profile to be used for rules requiring redirection for reject or deny actions.

Table 13: show security application-firewall rule-set Output Fields (continued)

Field Name	Field Description

Rule	Name of the rule
	• **Dynamic applications**—Name of the applications.
	• **Dynamic application groups**—Name of the application groups.
	• **SSL-Encryption**—Setting for SSL traffic.
	• **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  ◦ **permit**
	  ◦ **deny**
	  ◦ **reject**
	  ◦ **redirect**
	• **Number of sessions matched**—Number of sessions matched with the application firewall rule.
	• **Number of sessions redirected**—Number of sessions redirected by the application firewall rule.

Default rule	The default rule applied when the identified application is not specified in any rules of the rule set. • **Number of sessions matched**—Number of sessions matched with the application firewall default rule. • **Number of sessions redirected**—Number of sessions redirected by the application firewall rule.
Number of sessions with appid pending	Number of sessions that are pending application identification processing

Sample Output

show security application-firewall rule-set my_ruleset1

```
user@host>show security application-firewall rule-set my_ruleset1
Rule-set: my_ruleset1
     Rule: rule1
         Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
         Dynamic Application Groups: junos:web, junos:chat
         SSL-Encryption: any
         Action: deny or redirect
         Number of sessions matched: 10
         Number of sessions redirected: 10
     Default rule: permit
         Number of sessions matched: 200
         Number of sessions redirected: 0
     Number of sessions with appid pending: 2
```

Sample Output

show security application-firewall rule-set all

```
user@host> show security application-firewall rule-set all
```

```
Rule-set: appfw
    Logical system: root-logical-system
    Profile: lsy2_pf555
    Rule: 2
        Dynamic Applications: junos:HTTP
        SSL-Encryption: any
        Action:deny or redirect
        Number of sessions matched: 2
        Number of sessions redirected: 2
    Rule: 1
        Dynamic Applications: junos:FTP
        SSL-Encryption: any
        Action:permit
        Number of sessions matched: 0
        Number of sessions redirected: 0
    Default rule:permit
        Number of sessions matched: 0
        Number of sessions redirected: 0
    Number of sessions with appid pending: 0
```

show security application-firewall rule-set logical-system

Syntax The master, or root, administrator can issue the following statements:

show security application-firewall rule-set all
show security application-firewall rule-set *rule-set-name* | all | logical-system *logical-system-name* | all | root-logical-system [*logical-system-name* | all]

The user logical system administrator can issue the following statement:

show security application-firewall rule-set all

Release Information Command introduced in Junos OS Release 11.4.

Description Display information about application firewall rule set(s) associated with a specific logical system, all logical systems, or the root logical system configured on a device.

NOTE: The master administrator can configure and view application firewall rule sets for the root logical system and all user logical systems configured on the device. User logical system administrators can configure and view application firewall rule set information only for the user logical systems for which they have access. For information about master and user administrator roles in logical systems, see *Understanding Logical Systems for SRX Series Services Gateways*.

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options ***rule-set-name***—Name of a specific rule set.

logical-system-name—Name of a specific logical system.

all—(default) Display all rule sets for all logical systems. The user logical system administrator can display all rule sets only for the logical system they can access.

root-logical-system—Display application firewall rule set information for the root logical system (master administrator only).

Required Privilege Level view

Related Documentation

- clear security application-firewall rule-set statistics logical-system on page 256

List of Sample Output show security application-firewall rule-set logical-system all on page 291
show security application-firewall rule-set all on page 292

Output Fields Table 14 on page 291 lists the output fields for the **show security application-firewall rule-set logical-system** command. Output fields are listed in the approximate order in which they appear.

Table 14: show security application-firewall rule-set logical-system Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.
Logical system	Name of the logical system.

Rule	Name of the rule.
	• **Dynamic applications**—Name of the applications.
	• **Dynamic application groups**—Name of the application groups.
	• **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  ◦ **permit**
	  ◦ **deny**
	• **Number of sessions matched**—Number of sessions matched with the application firewall rule.

Default rule	The default rule applied when the identified application is not specified in any rules of the rule set. • **Number of sessions matched**—Number of sessions matched with the application firewall default rule.
Number of sessions with appid pending	Number of sessions that are pending with the application ID processing.

Sample Output

show security application-firewall rule-set logical-system all

```
root@host> show security application-firewall rule-set logical-system all

Rule-set: root_rs1
    Logical system: root-logical-system
    Rule: r1
        Dynamic Applications: junos:FTP
        Action:permit
        Number of sessions matched: 10
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 4

Rule-set: root-rs2
    Logical system: root-logical-system
    Rule: r1
        Dynamic Application Groups: junos:web
```

```
        Action:permit
        Number of sessions matched: 20
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 10
```

show security application-firewall rule-set all

```
root@host> show security application-firewall rule-set all

Rule-set: ls-product-design-rs1
    Logical system: ls-product-design
    Rule: r1
        Dynamic Applications: junos:TELNET
        Action:permit
        Number of sessions matched: 10
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 2

Rule-set: ls-product-design-rs1
    Logical system: ls-product-design
    Rule: r2
        Dynamic Application Groups: junos:web
        Action:permit
        Number of sessions matched: 20
Default rule:deny
        Number of sessions matched: 200
Number of sessions with appid pending: 4

Rule-set: ls-product-design-rs2
    Logical system: ls-product-design
    Rule: r1
        Dynamic Applications: junos:FACEBOOK-ACCESS
        Action:deny
        Number of sessions matched: 40
Default rule:permit
        Number of sessions matched: 400
Number of sessions with appid pending: 10
```

show security application-tracking counters

Syntax show security application-tracking counters

Release Information Command introduced in Junos OS Release 10.2.

Description Display the status of AppTrack counters.

Required Privilege Level view

Related Documentation
- *Understanding AppTrack*
- *Example: Configuring AppTrack*

Output Fields Table 15 on page 293 lists the output fields for the **show security application-tracking counters** command. Output fields are listed in the approximate order in which they appear.

Table 15: show security application-tracking counters

Field Name	Field Description
Session create messages	The number of log messages generated when a session was created.
Session close messages	The number of log messages generated when a session was closed.
Session volume updates	The number of log messages generated when an update interval was exceeded.
Session route updates	The number of log messages generated when an egress interface was selected based on application carried in the session by APBR.
Failed messages	The number of messages that were not generated due to memory or session constraints.

Sample Output

show security application-tracking counters

```
user@host> show security application-tracking counters

Application tracking counters:

    AppTrack counter type                          Value
 Session create messages                             1
 Session close messages                              1
 Session volume updates                              0
 Session route updates                               1
 Failed messages                                     0
```

show security flow session

Syntax **show security flow session [<filter>] [brief | extensive | summary]**
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Junos OS Release 8.5. Support for filter and view options added in Junos OS Release 10.2.
Application firewall, dynamic application, and logical system filters added in Junos OS Release 11.2.
Policy ID filter added in Junos OS Release 12.3X48-D10.
Support for connection tag added in Junos OS Release 15.1X49-D40.

Description Display information about all currently active security sessions on the device.

NOTE: For the normal flow sessions, the **show security flow session** command displays byte counters based on IP header length. However, for sessions in Express Path mode, the statistics are collected from the IOC2 and IOC3 ASIC hardware engines and include full packet length with L2 headers. Because of this, the output displays slightly larger byte counters for sessions in Express Path mode than for the normal flow session.

Options

- *filter*—Filter the display by the specified criteria.

  The following filters reduce the display to those sessions that match the criteria specified by the filter. Refer to the specific **show** command for examples of the filtered output.

  advanced-anti-malware—Show advanced-anti-malware sessions. For details on the **advanced-anti-malware** option, see the Sky Advanced Threat Prevention CLI Reference Guide.

  application—Predefined application name.

  application-firewall—Application firewall enabled.

  application-firewall-rule-set—Application firewall enabled with the specified rule set.

  application-traffic-control—Application traffic control session.

  application-traffic-control-rule-set—Application traffic control rule set name and rule name.

  conn-tag—Session connection tag (0..4294967295).

  destination-port—Destination port.

  destination-prefix—Destination IP prefix or address.

dynamic-application—Dynamic application.

dynamic-application-group—Dynamic application.

encrypted—Encrypted traffic.

family—Display session by family.

idp—IDP-enabled sessions.

interface—Name of incoming or outgoing interface.

logical-system (all | *logical-system-name*)—Name of a specific logical system or **all** to display all logical systems.

nat—Display sessions with network address translation.

node—(Optional) For chassis cluster configurations, display security flow session information on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Display information about all nodes.
- **local** —Display information about the local node.
- **primary**—Display information about the primary node.

policy-id—Display session information based on policy ID; the range is 1 through 4,294,967,295.

protocol—IP protocol number.

resource-manager—Resource manager.

root-logical-system—Display root logical system as default.

security-intelligence—Display security intelligence sessions.

services-offload—Display services offload sessions.

session-identifier—Display session with specified session identifier.

source-port—Source port.

source-prefix—Source IP prefix.

tunnel—Tunnel sessions.

- brief | extensive | summary—Display the specified level of output.
- none—Display information about all active sessions.

Required Privilege Level view

Related Documentation

- *Juniper Networks Devices Processing Overview*
- *clear security flow session all*

List of Sample Output

Output Fields

Table 16 on page 296 lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 16: show security flow session Output Fields

Field Name	Field Description	Level of Output
Session ID	Number that identifies the session. Use this ID to get more information about the session.	brief extensive none
If	Interface name.	brief none
State	Status of security flow session.	brief extensive none
Conn Tag	A 32-bit connection tag that uniquely identifies the GPRS tunneling protocol, user plane (GTP-U) and the Stream Control Transmission Protocol (STCP) sessions. The connection tag for GTP-U is the tunnel endpoint identifier (TEID) and for SCTP is the vTag. The connection ID remains 0 if the connection tag is not used by the sessions.	brief extensive none
CP Session ID	Number that identifies the central point session. Use this ID to get more information about the central point session.	brief extensive none
Policy name	Name and ID of the policy that the first packet of the session matched.	brief extensive none

Table 16: show security flow session Output Fields (continued)

Field Name	Field Description	Level of Output
Timeout	Idle timeout after which the session expires.	brief extensive none
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).	brief extensive none
Bytes	Number of received and transmitted bytes.	brief extensive none
Pkts	Number of received and transmitted packets.	brief extensive none
Total sessions	Total number of sessions.	brief extensive none
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).	brief extensive none
Status	Session status.	extensive
Flag	Internal flag depicting the state of the session, used for debugging purposes.	extensive
Source NAT pool	The name of the source pool where NAT is used.	extensive
Dynamic application	Name of the application.	extensive
Application traffic control rule-set	AppQoS rule set for this session.	extensive
Rule	AppQoS rule for this session.	extensive
Maximum timeout	Maximum session timeout.	extensive

Table 16: show security flow session Output Fields (continued)

Field Name	Field Description	Level of Output
Current timeout	Remaining time for the session unless traffic exists in the session.	extensive
Session State	Session state.	extensive
Start time	Time when the session was created, offset from the system start time.	extensive
Unicast-sessions	Number of unicast sessions.	Summary
Multicast-sessions	Number of multicast sessions.	Summary
Services-offload-sessions	Number of services-offload sessions.	Summary
Failed-sessions	Number of failed sessions.	Summary
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states	Summary
Maximum-sessions	Maximum number of sessions permitted.	Summary

Sample Output

show security flow session

```
root> show security flow session
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 56, Valid
  In: 203.0.113.1/1000 --> 203.0.113.11/2000;udp, Conn Tag: 0x0, If: reth1.0,
Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.11/2000 --> 203.0.113.1/1000;udp, Conn Tag: 0x0, If: reth0.0,
Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1
```

show security flow session (with default policy)

```
root> show security flow session
Session ID: 36, Policy name: pre-id-default-policy/n, Timeout: 2, Valid
  In: 10.10.10.2/61606 --> 10.10.10.1/179;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
Pkts: 1, Bytes: 64,
  Out: 10.10.10.1/179 --> 10.10.10.2/61606;tcp, Conn Tag: 0x0, If: .local..0,
Pkts: 1, Bytes: 40,
```

show security flow session brief

```
root> show security flow session brief
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 62, Valid
  In: 203.0.113.11/1000 --> 203.0.113.1/2000;udp, Conn Tag: 0x0, If: reth1.0,
Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp, Conn Tag: 0x0, If: reth0.0,
Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1
```

show security flow session extensive

```
root> show security flow session extensive
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Status: Normal, State: Active
Flags: 0x8000040/0x18000000/0x12000003
Policy name: SG/4
Source NAT pool: Null, Application: junos-gprs-gtp-v0-udp/76
Dynamic application: junos:UNKNOWN,
Encryption:  Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 90, Current timeout: 54
Session State: Valid
Start time: 6704, Duration: 35
   In: 203.0.113.11/1000 --> 201.11.0.100/2000;udp,
    Conn Tag: 0x0, Interface: reth1.0,
    Session token: 0x6, Flag: 0x40000021
    Route: 0x86053c2, Gateway: 201.10.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 86
    CP Session ID: 10320276
   Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp,
    Conn Tag: 0x0, Interface: reth0.0,
    Session token: 0x7, Flag: 0x50000000
    Route: 0x86143c2, Gateway: 203.0.113.11, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
    CP Session ID: 10320276
Total sessions: 1
```

show security flow session summary

```
root> show security flow session summary
Flow Sessions on FPC10 PIC1:
Unicast-sessions: 1
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456
```

```
Flow Sessions on FPC10 PIC2:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456

Flow Sessions on FPC10 PIC3:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456
```

show security flow session application-firewall

Syntax

show security flow session application-firewall
< dynamic-application (*dyn-app-name* | junos:UNKNOWN) >
< dynamic-application-group (*dyn-app-group* | junos:UNASSIGNED) >
< application-firewall-rule-set *rule-set-name* >
< rule *rule-name* >
< brief | extensive | summary >

Release Information

Command introduced in Junos OS Release 11.2.

Description

Display all sessions where application firewall is enabled.

Include options to filter the output and display only those enabled sessions with the specified features.

Options

- **dynamic-application (*dyn-app-name* | junos:UNKNOWN)**—Display only those enabled sessions with the specified dynamic application. Enter **junos:UNKNOWN** to display all enabled sessions where no dynamic application can be determined.
- **dynamic-application-group (*dyn-app-group* | junos:UNASSIGNED)**— Display only those enabled session with the specified dynamic application group. Enter **junos:UNASSIGNED** to display all enabled sessions where no dynamic application group can be determined.
- **application-firewall-rule-set *rule-set-name***—Display only those enabled sessions that match the specified rule set.
- **rule *rule-name***—Display only those enabled sessions that match the specified rule.
- **brief | extensive | summary**—Specify the level of detail for the display.

  The output fields for the **brief** and **summary** options are the same as those of the **show security flow session** command. Only the **extensive** display is different and is shown in the following output table and examples.

Required Privilege Level

view

Related Documentation

- *Example: Configuring an Application Group for Application Firewall*
- show security flow session on page 294

List of Sample Output

show security flow session application-firewall extensive on page 303
show security flow session application-firewall dynamic-application junos:FTP extensive on page 303
show security flow session application-firewall dynamic-application junos:UNKNOWN extensive on page 304
show security flow session application-firewall dynamic-application-group junos:WEB extensive on page 305

show security flow session application-firewall application-firewall-rule-set rule-set1 extensive on page 305

Output Fields Table 17 on page 302 lists the output fields for the **show security flow session application-firewall extensive** command. Output fields are listed in the approximate order in which they appear in the extensive display.

Table 17: show security flow session application-firewall extensive Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to display more information about a session.
Status	Session status.
State	Current state of the session: Active, Pending, Closed, Unknown.
Flag	Internal flag depicting the state of the session. It is used for debugging purposes.
Policy name	The name of the policy that permitted the traffic.
Source NAT pool	The name of the source pool where NAT is used.
Dynamic application	Name of the dynamic application of the session. If the dynamic application has yet to be determined, the output indicates Pending. If the dynamic application cannot be determined, the output indicates junos:UNKNOWN.
Dynamic application group	Name of the dynamic application group of the session. If the dynamic application cannot be determined, the output indicates junos:UNASSIGNED.
Dynamic nested application	Name of the dynamic nested application of the session if one exists. If the dynamic nested application is yet to be determined, the output indicates Pending. If the dynamic nested application cannot be determined, the output indicates junos:UNKNOWN.
Application firewall rule-set	Name of the rule set that the session matched.
Rule	Name of the rule that the session matched. If the match has not yet been made, the output indicates Pending. If the rule has been deleted since the match was made, the output indicates the rule is invalid.
Maximum timeout	Maximum amount of idle time allowed for the session.
Current timeout	Number of seconds that the current session has been idle.
Session State	Session state.
Start time	Time when the session was created. Start time is indicated as an offset from the system start time.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets, and bytes).

Table 17: show security flow session application-firewall extensive Output Fields (continued)

Field Name	Field Description
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions per PIC that fit the display criteria.

Sample Output

show security flow session application-firewall extensive

The displayed information is similar to the **show security flow session** output but includes dynamic application and application firewall details for the session.

```
user@host> show security flow session application-firewall extensive
Flow Sessions on FPC9 PIC0:

     Session ID: 3729, Status: Normal, State: Active
      Policy name: self-traffic-policy/1
      Source NAT pool: Null
      Dynamic application: junos:HTTP, Dynamic nested application:
junos:FACEBOOK-ACCESS
      Application firewall rule-set: rule-set1, Rule: rule2
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 192.0.2.1/1 --> 203.0.113.1/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 203.0.113.1/1 --> 192.0.2.1/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

     Total sessions: 1
```

show security flow session application-firewall dynamic-application junos:FTP extensive

Entering a specific dynamic application in the command line filters the output and displays only those sessions with the specified application.

```
user@host> show security flow session application-firewall dynamic-application junos:FTP
extensive
Flow Sessions on FPC3 PIC0:

     Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
      Dynamic application: junos:FTP
```

```
Application firewall rule-set: rule-set1, Rule: rule1
Maximum timeout: 300, Current timeout: 276
Session State: Valid
Start time: 18292, Duration: 603536
   In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
   Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Total sessions: 1
```

show security flow session application-firewall dynamic-application junos:UNKNOWN extensive

Using the keyword **junos:UNKNOWN** displays those enabled sessions where the dynamic application cannot be determined.

```
user@host> show security flow session application-firewall dynamic-application junos:UNKNOWN
extensive
Flow Sessions on FPC9 PIC0:

Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
 Dynamic application: junos:UNKNOWN
 Application firewall rule-set: rule-set1, Rule:rule1
 Maximum timeout: 300, Current timeout: 276
 Session State: Valid
 Start time: 18292, Duration: 603536
    In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
     Interface: reth1.0,
     Session token: 0x1c0, Flag: 0x0x21
     Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
     Port sequence: 0, FIN sequence: 0,
     FIN state: 0,
     Pkts: 21043, Bytes: 1136322
    Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
     Interface: .local..0,
     Session token: 0x80, Flag: 0x0x30
     Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
     Port sequence: 0, FIN sequence: 0,
     FIN state: 0,
     Pkts: 0, Bytes: 0

 Session ID: 180013339, Policy name: policy1/4, Timeout: 1776, Valid
Dynamic application: junos:HTTP, Dynamic nested application: junos:UNKNOWN

 Application firewall rule-set: rule-set1, Rule:rule1
 Maximum timeout: 300, Current timeout: 276
 Session State: Valid
 Start time: 18292, Duration: 603536
    In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
     Interface: reth1.0,
```

```
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
   Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Total sessions: 2
```

show security flow session application-firewall dynamic-application-group junos:WEB extensive

Entering a specific dynamic application group in the command line filters the output and displays only those sessions with the specified application group.

```
user@host> show security flow session application-firewall dynamic-application-group junos:WEB
extensive
Flow Sessions on FPC9 PIC0:

Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
 Dynamic application: junos:HOTMAIL
 Application firewall rule-set: rule-set1, Rule: rule1
 Maximum timeout: 300, Current timeout: 276
 Session State: Valid
 Start time: 18292, Duration: 603536
   In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
   Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

 Total sessions: 1
```

show security flow session application-firewall application-firewall-rule-set rule-set1 extensive

Specifying a rule set name reduces the display to only those sessions matching the specified rule set.

```
user@host> show security flow session application-firewall application-firewall-rule-set rule-set1
extensive
Flow Sessions on FPC9 PIC0:

Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
 Dynamic application: junos:FTP
 Application firewall rule-set: rule-set1, Rule: rule1
```

```
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

     Session ID: 180013339, Policy name: policy1/4, Timeout: 1776, Valid
      Dynamic application: junos:HTTP, Dynamic nested application:
junos:FACEBOOK-ACCESS
      Application firewall rule-set: rule-set1, Rule: rule2
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 203.0.113.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0


      Total sessions: 2
```

show security pki ca-certificate

Syntax show security pki ca-certificate
<brief | detail>
<ca-profile *ca-profile-name*>

Release Information Command introduced in Junos OS Release 7.5.

Description Display information about certificate authority (CA) digital certificates installed in the router.

Options **none**—(Same as brief) Display information about all CA digital certificates.

brief | detail—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*—(Optional) Display information about only the specified CA profile.

Required Privilege Level view

List of Sample Output show security pki ca-certificate on page 308
show security pki ca-certificate detail on page 309

Output Fields Table 18 on page 307 lists the output fields for the **show security pki ca-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 18: show security pki ca-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Issued by	Authority that issued the digital certificate.	**none brief**
Issued to	Device that was issued the digital certificate.	**none brief**
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**

Table 18: show security pki ca-certificate Output Fields (continued)

Field Name	Field Description	Level of Output
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the requestor. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption(1024 bits)**.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki ca-certificate

```
user@host> show security pki ca-certificate
Certificate identifier: abc
  Issued to: example, Issued by: exmple
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier: entrust
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier:abe
  Issued to: First Officer, Issued by: example
  Validity:
```

```
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
```

show security pki ca-certificate detail

```
user@host> show security pki ca-certificate detail
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
    ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
    42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
    da:eb:10:27:bd:46:34:33
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
    23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: Key encipherment
Certificate identifier: entrust
  Certificate version: 3
```

```
Serial number: 4355 925b
Issuer:
  Organization: example, Country: us
Subject:
  Organization: example, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
  ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
  d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
  00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
  e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
  90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
  b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
  af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
  ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
  C=us, O=example, CN=CRL1
  http://CA-1/CRL/example_us_crlfile.crl
Use for key: Digital signature
```

show security pki local-certificate (View)

Syntax

show security pki local-certificate
< **brief** | **detail** >
< certificate-id ***certificate-id-name*** >
<system-generated>

Release Information

Command modified in Junos OS Release 9.1. Subject string output field added in Junos OS Release 12.1X44-D10.

Description

Display information about the local digital certificates, corresponding public keys, and the automatically generated self-signed certificate configured on the device.

Options

- none—Display basic information about all configured local digital certificates, corresponding public keys, and the automatically generated self-signed certificate.
- **brief** | **detail**—(Optional) Display the specified level of output.
- certificate-id ***certificate-id-name*** —(Optional) Display information about only the specified local digital certificates and corresponding public keys.
- **system-generated**—Display information about the automatically generated self-signed certificate.

Required Privilege Level

view

Related Documentation

- *clear security pki local-certificate (Device)*
- *request security pki local-certificate generate-self-signed (Security)*

List of Sample Output

show security pki local-certificate certificate-id hello on page 313
show security pki local-certificate certificate-id hello detail on page 313
show security pki local-certificate system-generated on page 314
show security pki local-certificate system-generated detail on page 314
show security pki local-certificate certificate-id mycert - (local certificate enrolled online using SCEP) on page 315
show security pki local-certificate certificate-id mycert detail - (local certificate enrolled online using SCEP) on page 315

Output Fields

Table 19 on page 311 lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 19: show security pki local-certificate Output Fields

Field Name	Field Description
Certificate identifier	Name of the digital certificate.

Table 19: show security pki local-certificate Output Fields (continued)

Field Name	Field Description
Certificate version	Revision number of the digital certificate.
Serial number	Unique serial number of the digital certificate.
Issued to	Device that was issued the digital certificate.
Issued by	Authority that issued the digital certificate.
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority.
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority. • **Serial number**—Serial number of the device. If the certificate contains multiple subfield entries, all entries are displayed.
Subject string	Subject field as it appears in the certificate.
Alternate subject	Domain name or IP address of the device related to the digital certificate.
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**).
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.
Fingerprint	Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate.

Table 19: show security pki local-certificate Output Fields (continued)

Field Name	Field Description
Distribution CRL	Distinguished name information and URL for the certificate revocation list (**CRL**) server.
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**.

Sample Output

show security pki local-certificate certificate-id hello

```
user@host> show security pki local-certificate certificate-id hello
Certificate identifier: hello
  Issued to: cn1, Issued by: DC = local, DC = demo, CN = domain-example-WIN-CA
  Validity:
    Not before: 08- 8-2012 17:02
    Not after: 08- 8-2014 17:02
  Public key algorithm: rsaEncryption(1024 bits)
```

Sample Output

show security pki local-certificate certificate-id hello detail

```
user@host> show security pki local-certificate certificate-id hello detail
Certificate identifier: hello
  Certificate version: 3
  Serial number: 61ba9da000000000d72e
  Issuer:
    Common name: Example-CA,
    Domain component: local, Domain component: demo
  Subject:
    Organization: o1, Organization: o2,
    Organizational unit: ou1, Organizational unit: ou2, Country: US, State: CA,
    Locality: Sunnyvale, Common name: cn1, Common name: cn2,
    Domain component: dc1, Domain component: dc2
  Subject string:
    C=Example, DC=dc1, DC=dc2, ST=CA, L=Sunnyvale, O=o1, O=o2, OU=ou1, OU=ou2,
CN=cn1, CN=cn2
  Alternate subject: "user@example.net", user.example.net, 192.0.2.1
  Validity:
    Not before: 08- 8-2012 17:02
    Not after: 08- 8-2014 17:02
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:b4:14:01:d5:4f:79:87:d5:bb:e6:5e:c1:14
    97:da:b4:40:ad:1a:77:3e:ec:2e:68:8e:e4:93:a3:fe:7c:0b:58:af
    e1:20:27:82:ca:8d:6f:f0:97:d1:ad:fe:df:6c:cb:3c:b0:4f:cc:dd
    ac:d8:69:3f:3c:59:b5:2a:c6:83:e8:b3:94:5e:0a:2d:cd:e2:b0:15
    3e:97:a7:8a:4e:fb:59:f7:20:4c:ba:a8:80:3e:ba:be:69:ef:2b:32
    e4:1a:1c:24:53:1b:d5:c3:aa:d4:25:73:96:76:ea:49:d4:da:7e:3e
    0c:c6:6b:22:43:cb:04:84:0d:25:33:07:6b:49:41:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Distribution CRL:
    ldap:///Example-CA,CN=cn-win,CN=CDP,CN=Public%20Key
%20Services,CN=Services,CN=Configuration,DC=demo,DC=local?certificateRevocationList?base?
objectClass=cRLDistributionPoint
    http://example.example.net/CertEnroll/Example-CA.crl
```

```
  Use for key: Key encipherment, Digital signature, 1.3.6.1.5.5.8.2.2,
  1.3.6.1.5.5.8.2.2
  Fingerprint:
    76:a8:5f:65:b4:bf:bd:10:d8:56:82:65:ff:0d:04:3a:a5:e9:41:dd (sha1)
    8f:99:a4:15:98:10:4b:b6:1a:3d:81:13:93:2a:ac:e7 (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```

Sample Output

show security pki local-certificate system-generated

```
user@host> show security pki local-certificate system-generated
Certificate identifier: system-generated
  Issued to: JN10B9390AGB, Issued by: CN = JN10B9390AGB, CN = system generated,
CN = self-signed
  Validity:
    Not before: 10-30-2009 23:02
    Not after: 10-29-2014 23:02
  Public key algorithm: rsaEncryption(1024 bits)
```

Sample Output

show security pki local-certificate system-generated detail

```
user@host> show security pki local-certificate system-generated detail
Certificate identifier: system-generated
  Certificate version: 3
  Serial number: e90d42ebd14ef954b3e48c2eed5b30fb
  Issuer:
    Common name: JN10B9390AGB, Common name: system generated, Common name:
self-signed
  Subject:
    Common name: JN10B9390AGB, Common name: system generated, Common name:
self-signed
  Subject string:
    CN=JN10B9390AGB, CN=system generated, CN=self-signed
  Validity:
    Not before: 10-30-2009 23:02
    Not after: 10-29-2014 23:02
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:cb:c8:3f:e6:d3:e5:ca:9d:dc:2d:e9:ca:c7
    5f:b1:f5:3a:f0:1c:a7:55:43:0f:ef:fd:1c:fe:29:09:d5:37:d0:fa
    d6:ee:bc:b8:3f:58:d4:31:fb:96:4f:4f:cc:a9:1a:8f:2e:1b:50:6f
    2b:88:34:74:b2:6d:ad:94:b5:dd:3d:80:87:56:d0:42:50:4d:ac:d7
    8c:21:06:2d:07:1e:f4:d0:c7:85:2e:25:60:ad:1b:b5:b2:d2:1d:c8
    79:67:8c:56:06:04:75:6e:be:4e:99:b8:07:e6:9a:11:fe:b5:ec:c0
    1e:68:da:47:99:1b:b2:c8:07:ab:cd:6e:fe:c1:fd:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    be:1f:21:13:71:cd:9d:de:7a:41:d7:4c:52:8d:3e:d6:ba:db:75:96 (sha1)
    ba:fc:90:4b:5f:a8:66:a3:b9:64:89:9f:e2:45:b5:84 (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```

Sample Output

show security pki local-certificate certificate-id mycert - (local certificate enrolled online using SCEP)

```
user@host> show security pki local-certificate certificate-id mycert
Certificate identifier: mycert
  Issued to: bubba, Issued by: DC = local, DC = demo, CN = domain-example-WIN-CA

  Validity:
    Not before: 11-15-2012 18:58
    Not after: 11-15-2014 18:58
  Public key algorithm: rsaEncryption(1024 bits)
```

Sample Output

show security pki local-certificate certificate-id mycert detail - (local certificate enrolled online using SCEP)

```
user@host> show security pki local-certificate certificate-id mycert detail
Certificate identifier: mycert
  Certificate version: 3
  Serial number: 1f00b50a000000013ad2
  Issuer:
    Common name: Example-CA,
    Domain component: local, Domain component: demo
  Subject:
    Organization: example, Organizational unit: SSD, Country: US,
    Common name: host1, Serial number: SRX240-11152012
  Subject string:
    serialNumber=SRX240-11152012, C=US, O=example, OU=SSD, CN=host1
  Alternate subject: "user@example.net", user.example.net, 192.0.2.1
  Validity:
    Not before: 11-15-2012 18:58
    Not after: 11-15-2014 18:58
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:e3:e5:ae:c0:82:af:db:94:01:2f:56:46:50
    7d:3d:0b:0c:f0:1f:1d:7d:c3:aa:d4:4c:a0:cd:23:8b:3f:47:05:ee
    7b:65:42:a0:dc:c4:ac:a7:b6:a6:9f:5c:ea:d8:22:b0:bf:03:75:09
    be:fa:77:cb:d6:67:19:e6:80:fa:a5:7c:93:af:96:66:9f:cc:45:d5
    eb:ab:c1:f0:32:a6:d9:27:1b:80:bb:57:ec:31:a2:e0:2b:e1:42:c0
    92:8a:9b:ed:a6:d2:ec:7c:84:5a:8a:d9:96:a7:7e:40:c3:80:0e:f4
    d6:a2:5d:78:93:3b:7d:d5:8a:f5:de:fb:bc:0d:6d:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Distribution CRL:
    ldap:///Example-CA,CN=cn-win,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=demo,DC=local?certificateRevocationList?
base?objectClass=cRLDistributionPoint
    http://example.example.net/CertEnroll/Example-CA.crl
  Use for key: Key encipherment, Digital signature, 1.3.6.1.5.5.8.2.2,
  1.3.6.1.5.5.8.2.2
  Fingerprint:
    1f:2f:a9:22:a8:d5:a9:36:cc:c4:bd:81:59:9d:9c:58:bb:40:15:72 (sha1)
    51:27:e4:d5:29:90:f7:85:9e:67:84:a1:75:d1:5b:16 (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```

show security policies

Syntax

show security policies
none
<detail>
policy-name *policy-name*
<global>

Release Information

Command modified in Junos OS release 9.2. Support for IPv6 addresses added in Junos OS release 10.2. Support for wildcard addresses added in Junos OS release 11.1. Support for global policy added in Junos OS release 11.4. Support for services offloading added in Junos OS release 11.4. Support for source-identities added in Junos OS release 12.1. The **Description** output field added in Junos OS release 12.1. Support for negated address added in Junos OS release 12.1X45-D10. The output fields for Policy Statistics expanded, and the output fields for the **global** and **policy-name** options expanded to include from-zone and to-zone global match criteria in Junos OS release 12.1X47-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS release 12.3X48-D20. Output field and description for **source-end-user-profile** option added in Junos OS release 15.1x49-D70. Output field and description for **dynamic-applications** option added in Junos OS release 15.1x49-D100. Output field and description for **dynapp-redir-profile** option added in Junos OS release 18.2R1.

Description

Display a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy.

Options

- **none**—Display basic information about all configured policies.
- **detail**—(Optional) Display a detailed view of all of the policies configured on the device.
- **policy-name *policy-name***—(Optional) Display information about a specified policy.
- **global**—(Optional) Display information about global policies.

Required Privilege Level

view

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*
- *Unified Policies Configuration Overview*

List of Sample Output

show security policies on page 320
show security policies (Dynamic Applications) on page 320
show security policies policy-name detail on page 321
show security policies (Services-Offload) on page 322
show security policies (Device Identity) on page 322

show security policies detail on page 323
show security policies detail (TCP Options) on page 325
show security policies policy-name (Negated Address) on page 325
show security policies policy-name detail (Negated Address) on page 325
show security policies global on page 326

Output Fields Table 20 on page 317 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 20: show security policies Output Fields

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
Description	Description of the applicable policy.
State	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	Internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
source-end-user-profile	Name of the device identity profile (referred to as **end-user-profile** in the CLI) that contains attributes, or characteristics of a device. Specification of the device identity profile in the **source-end-user-profile** field is part of the device identity feature. If a device matches the attributes specified in the profile and other security policy parameters, then the security policy's action is applied to traffic issuing from the device.
Source addresses (excluded)	Name of the source address excluded from the policy.

Table 20: show security policies Output Fields (continued)

Field Name	Field Description
Destination addresses (excluded)	Name of the destination address excluded from the policy.
Source identities	One or more user roles specified for a policy.
Applications	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time. • **IP protocol**: The Internet protocol used by the application—for example, TCP, UDP, ICMP. • **ALG**: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If **application-protocol ignore** is configured, **ignore** is displayed. Otherwise, **0** is displayed. However, even if this command shows **ALG: 0**, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when **application-protocol ignore** is not configured for custom applications. • **Inactivity timeout**: Elapsed time without activity after which the application is terminated. • **Source port range**: The low-high source port range for the session application.
Dynamic Applications	Application identification based layer 7 dynamic applications.
Destination Address Translation	Status of the destination address translation traffic: • **drop translated**—Drop the packets with translated destination addresses. • **drop untranslated**—Drop the packets without translated destination addresses.
Application Firewall	An application firewall includes the following: • **Rule-set**—Name of the rule set. • **Rule**—Name of the rule. ◦ **Dynamic applications**—Name of the applications. ◦ **Dynamic application groups**—Name of the application groups. ◦ **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following: ▪ **permit** ▪ **deny** • **Default rule**—The default rule applied when the identified application is not specified in any rules of the rule set.

Table 20: show security policies Output Fields (continued)

Field Name	Field Description
Action or Action-type	• The action taken for a packet that matches the policy's tuples. Actions include the following: ◦ **permit** ◦ **firewall-authentication** ◦ **tunnel ipsec-vpn** *vpn-name* ◦ **pair-policy** *pair-policy-name* ◦ **source-nat pool** *pool-name* ◦ **pool-set** *pool-set-name* ◦ **interface** ◦ **destination-nat** *name* ◦ **deny** ◦ **reject** ◦ **services-offload**
Session log	Session log entry that indicates whether the **at-create** and **at-close** flags were set at configuration time to log session information.
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.
Policy statistics	• **Input bytes**—The total number of bytes presented for processing by the device. ◦ **Initial direction**—The number of bytes presented for processing by the device from the initial direction. ◦ **Reply direction**—The number of bytes presented for processing by the device from the reply direction. • **Output bytes**—The total number of bytes actually processed by the device. ◦ **Initial direction**—The number of bytes from the initial direction actually processed by the device. ◦ **Reply direction**—The number of bytes from the reply direction actually processed by the device. • **Input packets**—The total number of packets presented for processing by the device. ◦ **Initial direction**—The number of packets presented for processing by the device from the initial direction. ◦ **Reply direction**—The number of packets presented for processing by the device from the reply direction. • **Output packets**—The total number of packets actually processed by the device. ◦ **Initial direction**—The number of packets actually processed by the device from the initial direction. ◦ **Reply direction**—The number of packets actually processed by the device from the reply direction. • **Session rate**—The total number of active and deleted sessions. • **Active sessions**—The number of sessions currently present because of access control lookups that used this policy. • **Session deletions**—The number of sessions deleted since system startup. • **Policy lookups**—The number of times the policy was accessed to check for a match.

Table 20: show security policies Output Fields (continued)

Field Name	Field Description
dynapp-redir-profile	Displays application-firewall profile. See redirect profile(dynamic-application)
Per policy TCP Options	Configured syn and sequence checks, and the configured TCP MSS value for the initial direction, the reverse direction or, both.

Sample Output

show security policies

```
user@host> show security policies

  From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Sequence number: 1
    Source addresses:
    sa-1-ipv4: 198.51.100.11/24
    sa-2-ipv6: 2001:db8:a0b:12f0::1/32
    sa-3-ipv6: 2001:db8:a0b:12f0::22/32
    sa-4-wc:   203.0.113.1/255.255.0.255
    Destination addresses:
    da-1-ipv4: 2.2.2.2/24
    da-2-ipv6: 2001:db8:a0b:12f0::8/32
    da-3-ipv6: 2001:db8:a0b:12f0::9/32
    da-4-wc:   192.168.22.11/255.255.0.255
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, application services, log, scheduled
    Application firewall : my_ruleset1
  Policy: p2, State: enabled, Index: 5, Sequence number: 2
    Source addresses:
    sa-1-ipv4:  198.51.100.11/24
    sa-2-ipv6:  2001:db8:a0b:12f0::1/32
    sa-3-ipv6:  2001:db8:a0b:12f0::22/32
    Destination addresses:
    da-1-ipv4:  2.2.2.2/24
    da-2-ipv6:  2001:db8:a0b:12f0::1/32
    da-3-ipv6:  2001:db8:a0b:12f0::9/32
    Source identities: role1, role4
    Applications: any
    Action: deny, scheduled
```

show security policies (Dynamic Applications)

```
user@host>show security policies

  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:YAHOO
    Action: deny, log
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source addresses: any
    Destination addresses: any
    Applications: any
```

```
    Dynamic Applications: junos:web, junos:web:social-networking:facebook,
    junos:TFTP, junos:QQ
    Action: permit, log
  Policy: p3, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 3
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:HTTP, junos:SSL
    Action: permit, application services, log
```

The following example displays the output with unified policies configured.

```
user@host> show security policies

Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
  Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
    dynapp-redir-profile: profile1
```

show security policies policy-name detail

```
user@host> show security policies policy-name p1 detail

  Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    sa-1-ipv4:  198.51.100.11/24
    sa-2-ipv6:  2001:db8:a0b:12f0::1/32
    sa-3-ipv6:  2001:db8:a0b:12f0::9/32
    sa-4-wc:    203.0.113.1/255.255.0.255
  Destination addresses:
    da-1-ipv4: 192.0.2.0/24
    da-2-ipv6: 2001:db8:a0b:12f0::1/32
    da-3-ipv6: 2001:db8:a0b:12f0::9/32
    da-4-wc:   192.168.22.11/255.255.0.255
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Destination Address Translation: drop translated
  Application firewall :
  Rule-set: my_ruleset1
    Rule: rule1
      Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
      Dynamic Application groups: junos:web, junos:chat
      Action: deny
    Default rule: permit
  Session log: at-create, at-close
  Scheduler name: sch20
  Per policy TCP Options: SYN check: No, SEQ check: No
```

```
  Policy statistics:
    Input  bytes       :               18144                 545 bps
      Initial direction:                9072                272 bps
      Reply direction  :                9072                272 bps
    Output bytes       :               18144                 545 bps
      Initial direction:                9072                272 bps
      Reply direction  :                9072                272 bps
    Input  packets     :                 216                   6 pps
      Initial direction:                 108                   3 bps
      Reply direction  :                 108                   3 bps
    Output packets     :                 216                   6 pps
      Initial direction:                 108                   3 bps
      Reply direction  :                 108                   3 bps
    Session rate       :                 108                   3 sps
    Active sessions    :                  93
    Session deletions  :                  15
    Policy lookups     :                 108
```

The following example displays the output with unified policies configured.

```
user@host> show security policies policy-name p1 detail

Default policy: permit-all
Pre ID default policy: permit-all
From zone: trust, To zone: trust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: reject
    dynapp-redir-profile: profile1
```

show security policies (Services-Offload)

```
user@host> show security policies

  Policy: p1, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies (Device Identity)

```
user@host> show security policies
From zone: trust, To zone: untrust
       Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0,
Sequence number: 1
         Source addresses: any
         Destination addresses: any
```

```
        source-end-user-profile: marketing-profile
        Applications: any
        Action: permit
```

show security policies detail

```
user@host> show security policies detail

Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
 4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input  bytes       :                18144                 545 bps
      Initial direction:                 9072                272 bps
      Reply direction  :                 9072                 272 bps
    Output bytes       :                18144                 545 bps
      Initial direction:                 9072                 272 bps
      Reply direction  :                 9072                 272 bps
    Input  packets     :                  216                   6 pps
      Initial direction:                  108                   3 bps
      Reply direction  :                  108                   3 bps
    Output packets     :                  216                   6 pps
      Initial direction:                  108                   3 bps
      Reply direction  :                  108                   3 bps
    Session rate       :                  108                   3 sps
    Active sessions    :                   93
    Session deletions  :                   15
    Policy lookups     :                  108
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
 5, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p2 is for the sales team
  Sequence number: 1
  From zone: untrust, To zone: trust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
```

```
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

The following example displays the output with unified policies configured.

```
user@host> show security policies detail

Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
```

```
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
  Dynamic Application:
    junos:FACEBOOK-CHAT: 10704
    junos:GMAIL: 51
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies detail (TCP Options)

```
user@host> show security policies policy-name p2 detail
node0:
--------------------------------------------------------------------------
Policy:p2, action-type:permit, State: enabled,Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: tcp, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
 Destination port range: [80-80]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Dynamic-application: junos:HTTP
```

show security policies policy-name (Negated Address)

```
user@host> show security policies policy-name p1
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses(excluded): as1
    Destination addresses(excluded): as2
    Applications: any
    Action: permit
```

show security policies policy-name detail (Negated Address)

```
user@host> show security policies policy-name p1 detail
node0:
--------------------------------------------------------------------------
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses(excluded):
    ad1(ad): 255.255.255.255/32
    ad2(ad):  198.51.100.1/24
    ad3(ad):  198.51.100.6  ~ 198.51.100.56
    ad4(ad):  192.0.2.8/24
```

```
    ad5(ad):  198.51.100.99 ~ 198.51.100.199
    ad6(ad):  203.0.113.9/24
    ad7(ad):  203.0.113.23/24
  Destination addresses(excluded):
    ad13(ad2): 198.51.100.76/24
    ad12(ad2): 198.51.100.88/24
    ad11(ad2): 192.0.2.23 ~ 192.0.2.66
    ad10(ad2): 192.0.2.93
    ad9(ad2):  203.0.113.76 ~ 203.0.113.106
    ad8(ad2):  203.0.113.199
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

show security policies global

```
user@host> show security policies global policy-name Pa
node0:
--------------------------------------------------------------------------
  Global policies:
  Policy: Pa, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source addresses: H0
    Destination addresses: H1
    Applications: junos-http
    Action: permit
```

show services application-identification application

Syntax show services application-identification application (detail | summary)

Release Information Command introduced in Junos OS Release 11.4. Starting in Junos OS Release 15.1X49-D100, the options **Cacheable**, **Activation Date**, and **Last modified** are introduced for **show services application-identification application detail** command. The **Underlying consolidated Protocols/ports application is dependent on** and **Layer-7 Immediate Protocol(s)** options are introduced in Junos OS Release 18.2R1.

Description Display detailed information about a specified application signature, detailed information about all application signatures, or a summary of the existing application signatures.

Options **detail** —Display detailed information for all application signatures.

summary—Display summary information for all application signatures.

Required Privilege Level view

Related Documentation
- request services application-identification application on page 267

List of Sample Output
show services application-identification application summary on page 329
show services application-identification application detail on page 330
show services application-identification application detail (Custom Applications) on page 330
show services application-identification application detail (Unified Policies) on page 331

Output Fields Table 21 on page 327 lists shows the output details for the **show services application-identification application detail** command.

Table 21: show services application-identification application summary Output Fields

Field Name	Field Description
Application(s)	The number of applications present.
Application	Name of the custom application.
Disabled	The status of the application and whether the mapping method is currently used to identify this application.
ID	The unique ID number of an application. ID numbers 1 through 32,767 are automatically generated for applications; these IDs do not change. ID numbers for custom applications use 16,777,216 to 33,554,431.
Order	Number used to specify priority when multiple applications match the traffic. The lowest order number takes the highest priority.

Table 22 on page 328 lists the output fields for the **show services application-identification application** command. Output fields are listed in the approximate order in which they appear.

Table 22: show services application-identification application Output Fields

Field Name	Field Description
Application Name	Name of the application.
Application Type	The basic application type, such as HTTP.
Description	A description of the application.
Application ID	The unique ID number of an application signature. ID numbers 1 through 32,767 are automatically generated for application; these IDs do not change. ID numbers for custom applications use 16,777,216 to 33,554,431.
Priority	Priority over other signature applications.
Disabled	The status of the application and whether the mapping method is currently used to identify this application.
Cacheable	The status whether the application identification results caching is enabled or not for the application. When this option is enabled, you can cache the application detection result in an ASC table.
Activation Date	Date when the application was activated for the first time.
Last Modified	Date when the application was last updated.
Number of Parent Group(s)	Total number of parent groups in this application signature group or cluster.
Application Group	Name of the application signature group associated with this application signature. Must be a unique name with a maximum length of 32 characters.
Application Tags	General information about this application type, for example, associated risk factors, technology, type of traffic, and so on. Support of application signature tags is dependent on the version of the loaded signature database (Juniper Networks security website).
Underlying consolidated Protocols/ports application is dependent on	List of default protocols and ports for dependent applications of the specified application.
Layer-7 Immediate Protocol(s)	List of applications over which that dynamic application can be identified.
Application Specific Ports:	The default port for this application type.

Table 22: show services application-identification application Output Fields (continued)

Field Name	Field Description
Signature:	Signature mapping criteria for application identification: Port range, Client-to-server, and Order.
Alias List:	An alternative name for an application.

Sample Output

show services application-identification application summary

```
user@host> show services application-identification application summary
Application(s): 3616
  Applications                                Disabled         ID      Order
  junos:SLACKER                               No               1179    1

  junos:GOOGLE-TRUSTED-STORE                  No               2819    5

  junos:AMJILT                                No               2272    4

  junos:DSI                                   No               2644    3

  junos:HLN                                   No               2096    2

  junos:ETSI-LI                               No               537     1

  junos:CRAZYSALOON                           No               1720    5

  junos:EKSISOZLUK                            No               2436    4

  junos:SABAH                                 No               2574    3

  junos:AFREECA                               No               2373    2

  junos:SENEWEB                               No               2068    1

  junos:DIINO                                 No               776     5

  junos:CARE2                                 No               376     4

  junos:MOBAGE                                No               1456    3

  junos:CARTOONNETWORK                        No               982     2

  junos:AVATARS-UNITED                        No               363     1

  junos:CONVIVA                               No               2015    5

  junos:DREAMORA                              No               1725    4

  junos:ELWATANNEWS                           No               2381    3

  junos:REUTERS                               No               1044    2

  junos:BABYCENTER                            No               364     1

  junos:SOUTHWEST                             No               289     5
```

```
  junos:ONEDIO                                    No              2517    4


........
........
```

show services application-identification application detail

```
user@host> show services application-identification application detail junos:FTP

Application Name: junos:FTP
Application type: FTP
Description: This signature detects the File Transfer Protocol (FTP), which
provides facilities for transferring files to and from remote computer systems.
It usually runs on TCP port 21.
Application ID: 45
Priority: high
Order: 0
Disabled: Yes
Cacheable: Yes
Activation Date: 2003-05-05
Last Modified: 2016-04-11
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:file-servers
Application Tags:
    characteristic        : Supports File Transfer
    characteristic        : Known Vulnerabilities
    characteristic        : Capable of Tunneling
    risk                  : 3
    subcategory           : File-Servers
    category              : Infrastructure
Layer-7 Protocol(s):
    Protocol: TCP         / 205
    Protocol: SPDY        / 1469
    Protocol: SOCKS5      / 193
    Protocol: SOCKS4      / 192
    Protocol: HTTPS       / 68
    Protocol: HTTP2       / 2553
    Protocol: HTTP        / 67
Port Mapping:
    Default ports: TCP/21
```

show services application-identification application detail (Custom Applications)

```
user@host> show services application-identification application detail my-custom-app

Application Name: my-custom-app
Application type: MY-CUSTOM-APP
Description: custom App
Application ID: 16777216
Priority: high
Order: 65500
Disabled: No
Cacheable: No
Activation Date: N/A
Last Modified: N/A
Layer-7 Protocol(s):
```

```
    Protocol: http        / http
    Port range: N/A
    Member(s): 1
        Member m01
            Context: http-header-host
            Pattern: MY-SERVER.COM
            Direction: CTS
```

Sample Output

show services application-identification application detail (Unified Policies)

```
user@host> show services application-identification application detail


Application Name: junos:GOOGLE
Application type: GOOGLE
Description: This signature detects SSL connections to Google.com. Google is a
             company best known for their search engine but offers many cloud
             based services.
Application ID: 54
Priority: high
Order: 0
Disabled: No
Cacheable: No
Activation Date: 2003-05-05
Last Modified: 2017-06-28
Number of Parent Group(s): 2
Application Groups:
    junos:web:applications
    junos:web:portal
Application Tags:
    characteristic        : Can Leak Information
    characteristic        : Loss of Productivity
    characteristic        : Supports File Transfer
    risk                  : 3
    subcategory           : Applications
    category              : Web
Underlying consolidated Protocols/ports application is dependent on:
    Protocols:
        Protocol: junos:GOOGLE-GEN / 943
        Protocol: junos:STUN  / 201
        Protocol: junos:UDP   / 216
        Protocol: junos:TCP   / 205
        Protocol: junos:HTTP-PROXY / 2956
        Protocol: junos:SSL   / 199
        Protocol: junos:SPDY  / 1469
        Protocol: junos:POSTGRESQL / 150
        Protocol: junos:HTTPS / 68
        Protocol: junos:HTTP  / 67
        Protocol: junos:NET-PROXY / 2629
        Protocol: junos:HTTP2 / 2553
        Protocol: junos:HTTP-TUNNEL / 750
        Protocol: junos:COTP  / 22
        Protocol: junos:RTSP  / 176
        Protocol: junos:RTP   / 175
        Protocol: junos:DTLS  / 1291
        Protocol: junos:RTMP  / 337
        Protocol: junos:QUIC  / 2521
        Protocol: junos:JABBER / 94
```

```
    TCP Ports:
        Port: 443
        Port: 554
        Port: 80
    UDP Ports:
        Port: 554
Layer-7 Immediate Protocol(s):
    Protocol: GOOGLE-GEN  / 943
Alias List:
    junos:GOOGLE-SSL
Application Specific Ports:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 1
```

show services application-identification application-system-cache (View)

Syntax show services application-identification application-system-cache

Release Information Command introduced in Junos OS Release 10.2. Command updated in Junos OS Release 12.1X47-D10. Output updated in Junos OS Release 12.1X47-D15. The **Cache lookup for security-services** and the **Cache lookup for miscellaneous-services** are introduced in Junos OS Release 18.2R1.

Description Display application ID from default port/protocol binding or from the application system cache.

Required Privilege Level view

Related Documentation
- clear services application-identification application-system-cache (Junos OS) on page 260

List of Sample Output
show services application-identification application-system-cache on page 334
show services application-identification application-system-cache (Application System Cache Changes with Unified Policy Support) on page 334

Output Fields Table 23 on page 333 and Table 24 on page 334 list the output fields for the **show services application-identification application-system-cache** command. Output fields are listed in the approximate order in which they appear.

Table 23: show services application-identification application-system-cache Output Fields

Field Name	Field Description
application-cache	On or Off status of the application cache.
nested-application-cache	On or Off status of the nested application cache.
cache-unknown-result	On or Off status for caching unknown results.
cache-entry-timeout	The number of seconds the mapping information is saved.
pic	PIC number of the accumulated statistics.
Logical system name	Name of a specific logical system.
IP address	IP address.
Port	Port number.
Protocol	Type of protocol.

Table 23: show services application-identification application-system-cache Output Fields (continued)

Field Name	Field Description
Application	Name of the application.
Encrypted	Yes or No to identify the traffic as encrypted or not.

Table 24: show services application-identification application-system-cache Output Fields (For Unified Policies)

Field Name	Field Description
application-cache	On or Off status of the application cache.
Cache lookup for security-services	On or Off status of the application cache for security services such as security policies, application firewall (AppFW), Juniper Sky ATP, IDP, and UTM. By default, the ASC is disabled for the security services.
Cache lookup for miscellaneous-services	On or Off status of the application cache for miscellaneous services such as APBR and AppTrack. By default, the ASC is enabled for the miscellaneous services.
cache-entry-timeout	The number of seconds the mapping information is saved.

Sample Output

show services application-identification application-system-cache

```
user@host> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
  nested-application-cache: on
  cache-unknown-result: on
  cache-entry-timeout: 3600 seconds
  pic: 1/0
  Logical system name: root-logical-system
  IP address: 192.0.2.1                                  Port: 443    Protocol:
TCP
  Application: SSL                                     Encrypted: Yes

  pic: 1/1
  Logical system name: root-logical-system
  IP address: 192.0.2.2                                  Port: 80     Protocol:
TCP
  Application: HTTP                                    Encrypted: No
```

Sample Output

show services application-identification application-system-cache (Application System Cache Changes with Unified Policy Support)

```
user@host> show services application-identification application-system-cache

Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
```

```
  Cache lookup for miscellaneous-services: on
cache-entry-timeout: 3600 seconds
```

show services application-identification commit-status

Syntax show services application-identification commit-status]

Release Information Command introduced in Junos OS Release 15.1X49-D40.

Description Display information about the commit status. Because the custom signatures commit is performed asynchronously, the command output shows the current status of your configuration commit.

Required Privilege Level view

Related Documentation
- request services application-identification application on page 267

List of Sample Output
show services application-identification commit-status on page 336
show services application-identification commit-status on page 336
show services application-identification commit-status on page 336

Sample Output

show services application-identification commit-status

```
user@host> show services application-identification commit-status
Custom signatures commit is in progress
```

show services application-identification commit-status

```
user@host> show services application-identification commit-status
Custom signatures committed successfully
```

show services application-identification commit-status

```
user@host> show services application-identification commit-status
Custom signatures serialization failed
```

show services application-identification counter (AppSecure)

Syntax show services application-identification counter <ssl-encrypted-sessions>

Release Information Command introduced in Junos OS Release 10.2. Output updated in Junos OS Release 12.1X47-D10. Command and output updated in Junos OS Release 12.1X47-D15.

Description Display the status of all Junos OS application identification counter values per SPU.

Options **ssl-encrypted-sessions**—Display counters for SSL encrypted sessions.

Required Privilege Level view

Related Documentation
- clear services application-identification counter (Values) on page 261

List of Sample Output
show services application-identification counter on page 338
show services application-identification counter ssl-encrypted-sessions on page 339

Output Fields Table 25 on page 337 lists the output fields for the **show services application-identification counter** command. Output fields are listed in an approximate order in which they appear.

Table 25: show services application-identification counter Output Fields

Field Name	Field Description
PIC	PIC number of the accumulated statistics. NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, and SRX345 devices.
Unknown applications	Number of unknown applications.
Encrypted unknown applications	Number of encrypted unknown applications.
Cache hits	Number of sessions that matched the application in the AI cache.
Cache misses	Number of sessions that did not find the application in the AI cache.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.

Table 25: show services application-identification counter Output Fields (continued)

Field Name	Field Description
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.
Client-to-server encrypted packets processed	Number of client-to-server encrypted packets processed.
Server-to-client encrypted packets processed	Number of server-to-client encrypted packets processed.
Client-to-server encrypted bytes processed	Number of client-to-server encrypted payload bytes processed.
Server-to-client layer encrypted bytes processed	Number of server-to-client encrypted payload bytes processed.
Sessions bypassed due to resource allocation failure	Number of sessions bypassed due to resource allocation failure.
Segment case 1 - New segment to left	TCP segments contained before the previous segment.
Segment case 2 - New segment overlap right	TCP segments that start before the previous segment and are contained in it.
Segment case 3 - Old segment overlapped	TCP segments that start before the previous segment and extend beyond it.
Segment case 4 - New segment overlapped	TCP segments that start and end within the previous segment.
Segment case 5 - New segment overlap left	TCP segments that start within the previous segments and extend beyond it.
Segment case 6 - New segment overlap left	TCP segments that start after the previous segment. This is the normal case.

Sample Output

show services application-identification counter

```
user@host> show services application-identification counter

 pic: 6/0
  Counter type                                                    Value
```

```
Unknown applications                                          5
Encrpted unknown applications                                 0
Cache hits                                                    0
Cache misses                                                  8
Client-to-server packets processed                            678
Server-to-client packets processed                            0
Client-to-server bytes processed                              83577
Server-to-client bytes processed                              0
Client-to-server encrypted packets processed                  0
Server-to-client encrypted packets processed                  0
Client-to-server encrypted bytes processed                    0
Server-to-client encrypted bytes processed                    0
Sessions bypassed due to resource allocation failure          0
Segment case 1 - New segment to left                          0
Segment case 2 - New segment overlap right                    0
Segment case 3 - Old segment overlapped                       0
Segment case 4 - New segment overlapped                       0
Segment case 5 - New segment overlap left                     0
Segment case 6 - New segment to right                         0
```

Sample Output

show services application-identification counter ssl-encrypted-sessions

```
user@host> show services application-identification counter ssl-encrypted-sessions

 pic: 1/0
Counter type                                                Value
AI cache hits                                                 0
AI cache hits by nested application                           0
AI cache misses                                               0
AI matches                                                    0
AI uni-matches                                                0
AI no-matches                                                 0
AI partial matches                                            0
AI no-partial matches                                         0
Sessions that triggered Appid create session API              0
Sessions that do not incur signature match or decoding        0
Sessions that incur signature match or decoding               0
Client-to-server packets processed                            0
Server-to-client packets processed                            0
Client-to-server layer-7 bytes processed                      0
Server-to-client layer-7 bytes processed                      0
Terminal first data packets on both direction                 0
pic: 1/1
Counter type                                              Value
AI cache hits                                                 0
AI cache hits by nested application                           0
AI cache misses                                               0
AI matches                                                    0
AI uni-matches                                                0
AI no-matches                                                 0
AI partial matches                                            0
AI no-partial matches                                         0
Sessions that triggered Appid create session API              0
Sessions that do not incur signature match or decoding        0
Sessions that incur signature match or decoding               0
Client-to-server packets processed                            0
Server-to-client packets processed                            0
Client-to-server layer-7 bytes processed                      0
```

```
Server-to-client layer-7 bytes processed                        0
Terminal first data packets on both direction                   0
```

show services application-identification group

Syntax show services application-identification group [detail *application-group name* | summary]

Release Information Command introduced in Junos OS Release 11.4.

Description Display detailed or summary information about a specified application signature group or all application signature groups. Both custom and predefined application signature groups can be displayed.

Options **detail *application-group name*—**(Optional) Display detailed information for the specified application signature group.

summary—(Optional) Display summary information for all application signature groups.

Required Privilege Level view

Related Documentation
- request services application-identification group on page 270

List of Sample Output
show services application-identification group summary on page 342
show services application-identification group detail on page 342

Output Fields Table 26 on page 341 lists the output fields for the **show services application-identification group** command. Output fields are listed in the approximate order in which they appear.

Table 26: show services application-identification group Output Fields

Field Name	Field Description
Description	Description of the specified application in the detailed display.
Group ID or **ID**	The unique ID number of an application signature or application signature group. ID numbers 1 through 32,767 are automatically generated for predefined application signatures and application signature groups; these IDs do not change. ID numbers for custom application signatures and application signature groups use ID numbers 32,768 to 65,534.
Disabled	The status of the application signature group and whether the signature method is currently used to identify this application. The default is No.
Application Group(s)	The application signature groups present.
Applications	The application signatures associated with this application signature group.

Sample Output

show services application-identification group summary

```
user@host> show services application-identification group summary
Application Group(s): 24
Application Groups                                  Disabled  ID
  my:enterprise                                      No        32770
  junos:enterprise:voip                              No        25
  junos:peer-to-peer:voip                            No        24
  junos:peer-to-peer:chat                            No        23
  junos:peer-to-peer:file-sharing                    No        22
...
```

show services application-identification group detail

```
user@host> show services application-identification group detail junos:social-networking
Group Name: junos:social-networking
Group ID: 36
Description: N/A
Disabled: No
Number of Applications: 0
Number of Sub-Groups: 2
Number of Parent-Groups: 1
Sub Groups:
    junos:social-networking:applications
    junos:social-networking:business
```

show services application-identification statistics applications

Syntax show services application-identification statistics applications <interval *interval-number*>

Release Information Command introduced in Junos OS Release 11.4. Command updated in Junos OS Release 12.1.

Description Display application usage statistics.

Options

- none—Display cumulative session and byte statistics per application. Statistics are displayed in alphabetical order.
- **interval *interval-number***—(Optional) Display interval statistics per application. Interval statistics are displayed in Top-N format, such that the first application displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval. The previous interval is 2, and the least current (oldest) is 8.

Required Privilege Level view

Related Documentation

- statistics (Services) on page 237
- clear services application-identification application-statistics on page 257

List of Sample Output

show services application-identification statistics applications on page 344
show services application-identification statistics applications interval 3 on page 344

Output Fields Table 27 on page 343 lists the output fields for the **show services application-identification statistics applications** command. Output fields are listed in the approximate order in which they appear.

Table 27: show services application-identification statistics applications Output Fields

Field Name	Field Description
Application	Name of the application.
Sessions	Number of sessions for the application.
Bytes	Size of the application in bytes. NOTE: When an SRX Series device is operating in chassis cluster mode (Active/Active mode - Z mode), the **show services application-identification statistics applications** command output does not provide complete statistics for bytes count for the session in application/application group statistics. This is because, ingress and egress traffic byte counts are updated separately on the primary and secondary nodes in the chassis cluster setup for a given application.
Encrypted	Yes or No identifying the traffic as encrypted or not.

Sample Output

show services application-identification statistics applications

```
user@host> show services application-identification statistics applications

Last Reset: 2014-02-19 00:38:01 PST
                        Application           Sessions              Bytes
Encrypted
                             SYSLOG                  2              18610
  No
```

show services application-identification statistics applications interval 3

```
user@host> show services application-identification statistics applications interval 8

Interval Start: 2014-02-19 21:10:29 PST
Elapsed time: 00:07:14
```

show services application-identification statistics application-groups

Syntax show services application-identification statistics application-groups <interval *interval-number*>

Release Information Command introduced in Junos OS Release 11.4.

Description Display application group usage statistics.

Options

- none—Display cumulative session and byte statistics per application group. Statistics are displayed in alphabetical order.
- **interval** ***interval-number***— (Optional) Display interval statistics per application group. Interval statistics are displayed in Top-N format, such that the first application group displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval. The previous interval is 2, and the least current (oldest) is 8.

Required Privilege Level view

Related Documentation

- statistics (Services) on page 237
- clear services application-identification application-statistics on page 257

List of Sample Output show services application-identification statistics application-groups on page 346
show services application-identification statistics application-groups interval 8 on page 346

Output Fields Table 28 on page 345 lists the output fields for the **show services application-identification statistics application-groups** command. Output fields are listed in the approximate order in which they appear.

Table 28: show services application-identification statistics application-groups Output Fields

Field Name	Field Description
Application Group	Displays the name of the application group.
Sessions	Displays the number of sessions for the application group.
Kilo Bytes	Displays the size of the application group in kilobytes. NOTE: When an SRX Series device is operating in Chassis Cluster mode (Active/Active mode - Z mode), the **show services application-identification statistics application-groups** command output does not provide complete statistics for bytes count for the session in application/application group statistics. This is because, ingress and egress traffic byte counts are updated separately on the primary and secondary nodes in the chassis cluster setup for a given application.

Sample Output

show services application-identification statistics application-groups

```
user@host> show services application-identification statistics application-groups

Last Reset: 2014-02-19 00:38:01 PST
                Application Group           Sessions         Kilo Bytes
             junos:infrastructure                  2                 18
             junos:encryption                      1                  2
  junos:infrastructure:monitoring                  2                 18
```

show services application-identification statistics application-groups interval 8

```
user@host> show services application-identification statistics application-groups interval 8

Interval Start: 2014-02-19 21:07:29 PST
Elapsed time: 00:07:15
```

show services application-identification status

Syntax show services application-identification status

Release Information Command introduced in Junos OS Release 12.1X47-D10.

Description Display detailed information about application identification status.

Required Privilege Level view

Related Documentation
- request services application-identification application on page 267

List of Sample Output
show services application-identification status on page 348
show services application-identification status (DPI Performance Mode Enabled) on page 349

Output Fields Table 29 on page 347 lists the output fields for the **show services application-identification status** command. Output fields are listed in the approximate order in which they appear.

Table 29: show services application-identification status Output Fields

Field Name	Field Description
Status	Status of application identification: **Enabled** or **Disabled**.
Sessions under app detection	Sessions undergoing application identification detection.
Engine Version	Application identification detector engine version.
Max TCP session packet memory	Maximum number of TCP sessions that application identification maintains.
Force packet plugin	Force packet plugin status: **Enabled** or **Disabled**.
Force stream plugin	Force stream plugin status: **Enabled** or **Disabled**.
DPI Performance mode	DPI performance mode status. This field is displayed only if the DPI performance mode is enabled.
Statistics collection interval	Frequency (in minutes) for collecting statistics.
Status	Status of application system cache: **Enabled** or **Disabled**.
Negative cache status	Status on the number of sessions that reach the Unknown cache entry: **Enabled** or **Disabled**.

Table 29: show services application-identification status Output Fields (continued)

Field Name	Field Description
Max Number of entries in cache	Maximum number of cache entries.
Cache timeout	Idle timeout after which the cache entries expires.
Download Server CGI	Name of the server from where protocol bundle was downloaded.
Auto Update	Status of auto update to receive protocol bundle updates from the server: **Enabled** or **Disabled**.
Status	Status of protocol bundle: **Active** or **Free**.
Version Or **PB Version**	Version of protocol bundle. NOTE: Starting from Junos OS Release 17.4R1, the field **PB Version** is used for displaying version of the protocol bundle.
Session	The number of active sessions.

Starting from Junos OS Release 17.4R1, Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) engine, is packaged along with the application signature package version 534 that includes protobundle version 1.270.0.48.005. When you upgrade to Junos OS Release 17.4R1 or later from the earlier versions of Junos OS, the application identification security package installed is of version 534.

However, if you require latest versions of the protocol bundle, you must download and install the application signature package separately.

Sample Output

show services application-identification status

```
user@host> show services application-identification status
pic: 5/0

Application Identification
 Status                          Enabled
 Sessions under app detection    0
 Engine Version                  4.18.1-20 (build date Feb 15 2014)
 Max TCP session packet memory   30000
 Force packet plugin             Disabled
 Force stream plugin             Disabled
 Statistics collection interval  1 (in minutes)

Application System Cache
 Status                          Enabled
 Negative cache status           Disabled
 Max Number of entries in cache  131072
 Cache timeout                   3600 (in seconds)
```

```
Protocol Bundle
 Download Server                https://services.netscreen.com/cgi-bin/index.cgi

 AutoUpdate                        Disabled
Slot 1:
 Status                            Active
 Version                           1.30.4-22.005 (build date Jan 17 2014)
 Sessions                          0
Slot 2
 Status                            Free
```

Sample Output

show services application-identification status (DPI Performance Mode Enabled)

```
user@host> show services application-identification status
pic: 2/1

Application Identification
Status                             Enabled
Sessions under app detection       0
Engine Version                     4.18.2-24.006 (build date Jul 30 2014)
Max TCP session packet memory      30000
Force packet plugin                Disabled
Force stream plugin                Disabled
DPI Performance mode:              Enabled
Statistics collection interval     1 (in minutes)

Application System Cache
Status                             Enabled
Negative cache status              Disabled
Max Number of entries in cache     262144
Cache timeout                      3600 (in seconds)

Protocol Bundle
Download Server                 https://services.netscreen.com/cgi-bin/index.cgi
AutoUpdate                         Disabled
Slot 1:
Application package version        2399
Status                             Active
Version                            1.40.0-26.006 (build date May 1 2014)
Sessions                           0
Slot 2
Application package version        0
Status                             Free
Version
Sessions                           0
```

show services application-identification status (Application Identification Detector Engine Version)

```
Application Identification
 Status                            Enabled
 Sessions under app detection      0
 Max TCP session packet memory     0
 Force packet plugin               Disabled
 Force stream plugin               Disabled
 Statistics collection interval    1 (in minutes)
```

```
Application System Cache
 Status                            Enabled
 Max Number of entries in cache    131072
 Cache timeout                     3600 (in seconds)

Protocol Bundle
 Download Server
https://indiavm-sigdb2.englab.juniper.net/cgi-bin/index.cgi
 AutoUpdate                        Disabled
Slot 1:
 Application package version       534
 Status                            Active
 PB Version                        1.270.0-48.005 (build date May 22 2017)
 Engine version                    4.20.0-49.005 (build date May 22 2017)
 Sessions                          0
```

show services application-identification version

Syntax show services application-identification version

Release Information Command introduced in Junos OS Release 10.2.

Description Display the Junos OS application package version.

Required Privilege Level view

Related Documentation
- request services application-identification download on page 268

List of Sample Output show services application-identification version on page 351

Sample Output

show services application-identification version

The following output shows that the application package version is 1608.

```
user@host> show services application-identification version
Application package version: 1608
```

show services icap-redirect server status

Syntax show services icap-redirect server status

Release Information Command introduced in Junos OS Release 18.1R1.

Description Display the status of On-Premises in DLP.

Required Privilege Level view

Sample Output

show services icap-redirect server status

```
user@host> show services icap-redirect server status
 ICAP Status :
         Spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
         Spu-1 Profile: icap-pf1 Server: icap-svr2 : UP
ICAP Status :
         Spu-2 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
         Spu-2 Profile: icap-pf1 Server: icap-svr2 : UP
ICAP Status :
         Spu-3 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
         Spu-3 Profile: icap-pf1 Server: icap-svr2 : UP
```

show services service-redirect statistic

Syntax show services service-redirect statistic

Release Information Command introduced in Junos OS Release 18.1R1.

Description Display the Service Redirect statistic.

Required Privilege Level view

Sample Output

show services service-redirect statistic

```
user@host> show services service-redirect statistic
ICAP Redirect statistic:
  Message Redirected                 : 4
      Message REQMOD Redirected      : 2
      Message RESPMOD Redirected     : 2
  Message Received                   : 4
      Message REQMOD Received        : 2
      Message RESPMOD Received       : 2
Fallback:      permit           log-permit       reject
  Timeout         0                0                0
  Connectivity    0                0                0
  Default         0                0                0
```