Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

**About the Documentation** | xxi

- Documentation and Release Notes | xxi
- Using the Examples in This Manual | xxi
  - Merging a Full Example | xxii
  - Merging a Snippet | xxiii
- Documentation Conventions | xxiii
- Documentation Feedback | xxvi
- Requesting Technical Support | xxvi
  - Self-Help Online Tools and Resources | xxvii
  - Creating a Service Request with JTAC | xxvii

## Overview

**Understanding Application Security** | 29
- Benefits of Application Security | 30

## Application Identification

**Application Identification** | 32

- Understanding Application Identification Techniques | 32
  - Junos OS Next-Generation Application Identification | 33
  - Benefits of Application Identification | 33
  - Application Signature Mapping | 34
  - Application Identification Match Sequence | 34
- Understanding the Junos OS Application Identification Database | 36
- Disabling and Reenabling Junos OS Application Identification | 37
- Understanding the Application System Cache | 37
- Enabling or Disabling Application System Cache for Application Services | 38
- Verifying Application System Cache Statistics | 40
- Onbox Application Identification Statistics | 41
  - Configuring IMAP Cache Size | 42
- Understanding Jumbo Frames Support for Junos OS Application Identification Services | 43
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined and Custom Application Groups for Application Identification</td>
<td>98</td>
</tr>
<tr>
<td>Customizing Application Groups for Junos OS Application Identification</td>
<td>99</td>
</tr>
<tr>
<td>Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management</td>
<td>100</td>
</tr>
<tr>
<td>Enabling or Disabling Application Groups in Junos OS Application Identification</td>
<td>105</td>
</tr>
<tr>
<td>Application Identification Support for Unified Policies</td>
<td>106</td>
</tr>
<tr>
<td>Understanding Unified Policies on Security Devices</td>
<td>106</td>
</tr>
<tr>
<td>Benefits</td>
<td>107</td>
</tr>
<tr>
<td>Understanding How Unified Policies Use AppID Information</td>
<td>107</td>
</tr>
<tr>
<td>Understanding Dependent Dynamic Application Identification</td>
<td>107</td>
</tr>
<tr>
<td>Dynamic Application Classification States</td>
<td>108</td>
</tr>
<tr>
<td>Configuring Transactions Limit For Application Identification</td>
<td>108</td>
</tr>
<tr>
<td>High Availability Support for Application Identification for Unified Policies</td>
<td>109</td>
</tr>
<tr>
<td>Enabling or Disabling Application System Cache for Application Services</td>
<td>111</td>
</tr>
<tr>
<td>Application Identification Support for Micro-Applications</td>
<td>113</td>
</tr>
<tr>
<td>Micro-Application Classification</td>
<td>113</td>
</tr>
<tr>
<td>Dependent Application List and Default Protocols and Ports</td>
<td>114</td>
</tr>
<tr>
<td>Policy Enforcement for Micro-Applications</td>
<td>114</td>
</tr>
<tr>
<td>Installing Micro-Applications</td>
<td>114</td>
</tr>
<tr>
<td>Enabling and Disabling Micro-Applications Detection</td>
<td>115</td>
</tr>
<tr>
<td>Example: Configuring Micro-Applications</td>
<td>115</td>
</tr>
<tr>
<td>Secure Web Proxy</td>
<td>122</td>
</tr>
<tr>
<td>Secure Web Proxy Overview</td>
<td>122</td>
</tr>
<tr>
<td>Benefit</td>
<td>123</td>
</tr>
<tr>
<td>Limitation</td>
<td>123</td>
</tr>
<tr>
<td>How Secure Web Proxy Works on SRX Series Devices</td>
<td>123</td>
</tr>
<tr>
<td>Example—Configure Secure Web Proxy on an SRX Series Device</td>
<td>126</td>
</tr>
<tr>
<td>Application Services Modules</td>
<td>135</td>
</tr>
<tr>
<td>Application Firewall</td>
<td>135</td>
</tr>
<tr>
<td>Application Firewall Overview</td>
<td>135</td>
</tr>
<tr>
<td>Limitations with Stateful Firewalls</td>
<td>136</td>
</tr>
<tr>
<td>Application Firewall</td>
<td>136</td>
</tr>
<tr>
<td>Benefit of Application Firewall</td>
<td>136</td>
</tr>
</tbody>
</table>
Limitations | 355

**SSL Certificates | 356**

Configuring and Loading SSL Certificates | 356

Configuring a Root CA Certificate | 357

- Generate a Root CA Certificate with CLI | 358
- Generate a Root CA Certificate with OpenSSL | 359

Configuring a Trusted CA Profile Group | 360

Importing a Root CA Certificate into a Browser | 362

Certificate Chain Implementation | 363

Ignore Server Authentication Failure | 369

- Server Authentication | 369
- Client Authentication | 369

Certificate Revocation Lists for SSL Proxy | 370

- Working with the Certificate Revocation Lists for SSL Proxy | 370

SSL Performance Enhancements | 371

- Optimizing the SSL Performance | 372
- Session Resumption | 373
- Session Renegotiation | 373
- Dynamic Resolution of Domain Names | 373

**Cipher Suites for SSL Proxy | 374**

Cipher Suites | 374

- Supported Cipher Suites | 374

- Configuring Cipher Suites for SSL Proxy | 379

- ECDSA Cipher Suite Support for SSL Proxy | 380

- Configuring Server Certificates of Key Size 4096 Bits on SRX300 and SRX320 | 380

**Configuring SSL Proxy | 382**

Configuring SSL Proxy Forward Proxy | 382

- SSL Proxy Configuration Overview | 383
- Configuring a Root CA Certificate | 384

- Generate a Root CA Certificate with CLI | 384
- Generate a Root CA Certificate with OpenSSL | 385

- Configuring a CA Profile Group | 386

- Importing a Root CA Certificate into a Browser | 388
## SSL Decryption Mirroring | 429

- Understanding SSL Decryption Mirroring Functionality | 429
  - SSL Decryption Mirroring Before or After Policy Enforcement | 430
  - SSL Decryption Mirroring Support | 430
  - Benefits of SSL Decryption Mirroring | 431
  - Limitations | 431
- SSL Decryption Mirroring Support in Chassis Cluster | 431
  - Configuring SSL Decryption Mirroring | 431

## SSL Proxy Logs | 436

- SSL Proxy Logs | 436
  - SSL Proxy Logs | 436
- Enabling Debugging and Tracing for SSL Proxy | 438

## Operational Commands to Troubleshoot SSL Sessions | 439

- Displaying Active SSL Sessions | 441
- Displaying Active SSL Sessions Details | 441
- Displaying Specific SSL Session Details | 443
- Display SSL Certificates | 444
- Display SSL Certificate Information | 444
- Display SSL Certificate Details | 446
- SSL Proxy Counters All | 447
- SSL Proxy Counters Information | 449
- SSL Proxy Counters Errors | 450
- Display SSL Proxy Profile Details | 451
- Display SSL Proxy Profiles | 451
- Display SSL Proxy Session Cache Statistics | 452
- Display SSL Proxy Session Cache Summary | 453
- Display SSL Proxy Session Cache Details | 453
- Display SSL Proxy Certificate Cache Entry Statistics | 455
- Display SSL Proxy Certificate Cache Entry Summary | 456
- Display SSL Proxy Certificate Cache Entry Details | 456
- Display SSL Proxy Status | 457
- Display SSL Termination Counter Details | 458
- Display SSL Termination Counters Errors | 459
Configuration Statements

active-probe-params | 476
actions (Services SSL Proxy) | 480
actions (Services SSL Initiation) | 483
address-mapping (Application Identification) | 485
advance-policy-based-routing | 487
advance-policy-based-routing (Security Zones) | 492
appfw-profile (System) | 493
appfw-rule | 494
appfw-rule-set | 496
application-firewall | 498
application (Application Identification) | 500
application-firewall (Application Services) | 504
application-identification | 505
application-group (Services) | 511
application-services (Security Policies) | 513
application-system-cache | 515
http (icap-redirect profile) | 560
icap-redirect | 561
icmp-mapping (Application Identification) | 563
ip-protocol-mapping (Application Identification) | 564
initiation (Services) | 565
level (Services) | 567
log (Services) | 568
maximum-transactions | 570
metrics-profile | 571
mirror-decrypt-traffic | 573
no-application-identification (Services) | 575
no-application-system-cache (Services) | 576
ngfw | 577
over (Application Identification) | 579
overlay-path | 581
packet-capture | 583
passive-probe-params | 586
policy (advanced-policy-based-routing) | 588
policy (Security Policies) | 590
port-range (Application Identification) | 594
preferred-ciphers | 595
profile (icap-redirect) | 596
profile (Rule Sets) | 598
profile (Services SSL Proxy) | 599
profile (Services Proxy) | 603
protocol (Services Proxy) | 605
profile (SSL Initiation) | 606
profile (SSL Termination) | 609
protocol-version | 611
proxy (Services) | 612
rate-limiters | 614
renegotiation (Services) | 616
root-ca (Services) | 617
routing-instance (Advanced Policy-Based Routing) | 618
rule (Advanced Policy-Based Routing) | 619
rule-sets (CoS AppQoS) | 621
server (icap-redirect profile) | 624
secure-proxy | 626
server-certificate (Services) | 627
session-update-interval | 628
signature | 629
size (Services) | 630
ssl (Services) | 631
ssl-proxy (Application Services) | 634
statistics (Services) | 635
sla-options | 636
sla-rule | 637
source-identity | 641
termination (Services) | 643
traceoptions (advanced policy-based routing) | 645
traceoptions (Services Application Identification) | 647

trusted-ca (Services) | 649

traceoptions (Services SSL) | 650

tunables | 653

underlay-interfaces | 655

whitelist (Services) | 657

whitelist-url-categories | 658

Configuration Statements (Legacy Application Firewall)

rule (Application Firewall) | 660

rule-sets (Security Application Firewall) | 662

ssl-encryption | 664

then (Security Application Firewall) | 665

traceoptions (Security Application Firewall) | 667

profile (Application Firewall) | 669

Operational Commands

clear security advance-policy-based-routing sla statistics | 675

clear security application-firewall rule-set statistics | 676

clear security application-firewall rule-set statistics logical-system | 677

clear services application-identification application-statistics | 679

clear services application-identification application-statistics cumulative | 680

clear services application-identification application-statistics interval | 681

clear services application-identification application-system-cache (Junos OS) | 682

clear services application-identification counter (Values) | 684

clear services application-identification packet-capture counters | 686

clear services icap-redirect statistic | 687
clear services ssl proxy statistics  |  689
request security pki ca-certificate ca-profile-group load  |  690
request security pki local-certificate export  |  692
request security pki local-certificate generate-self-signed  |  693
request security pki local-certificate load  |  695
request services application-identification application  |  696
request services application-identification clear packet-capture all  |  698
request services application-identification download  |  699
request services application-identification download status  |  701
request services application-identification group  |  702
request services application-identification install  |  704
request services application-identification install status  |  705
request services application-identification proto-bundle-status  |  706
request services application-identification uninstall  |  707
request services application-identification uninstall status  |  708
show class-of-service application-traffic-control counter  |  709
show class-of-service application-traffic-control statistics rate-limiter  |  715
show class-of-service application-traffic-control statistics rule  |  719
show security advance-policy-based-routing detail  |  722
show security advanced-policy-based-routing policy-name  |  726
show security advance-policy-based-routing profile  |  731
show security advance-policy-based-routing statistics  |  733
show security advance-policy-based-routing status  |  739
show security advance-policy-based-routing sla active-probe-statistics  |  740
show security advance-policy-based-routing sla profile (Application Name)  |  742
show security advance-policy-based-routing sla profile (Application Name) | 744
show security advance-policy-based-routing sla profile (Next-Hop) | 746
show security advance-policy-based-routing sla profile (Status) | 751
show security advance-policy-based-routing sla statistics | 753
show security advance-policy-based-routing sla status | 755
show security advance-policy-based-routing sla version | 756
show security application-firewall rule-set | 757
show security application-firewall rule-set logical-system | 762
show security application-tracking counters | 766
show security flow session | 768
show security flow session ssl | 778
show security flow session application-firewall | 782
show security pki ca-certificate | 790
show security pki local-certificate (View) | 795
show security policies | 803
show services application-identification application | 820
show services application-identification application-system-cache (View) | 829
show services application-identification commit-status | 834
show services application-identification counter (AppSecure) | 836
show services application-identification entries | 844
show services application-identification group | 847
show services application-identification packet-capture counters | 850
show services application-identification statistics applications | 852
show services application-identification statistics application-groups | 856
show services application-identification status | 860
About the Documentation

Use this guide to configure and operate Juniper Networks' AppSecure suite of application-aware security services in Junos OS on NFX Series and SRX Series devices to provide visibility, enforcement, and control over the types of applications traversing in the networks.

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 xxiv defines notice icons used in this guide.
**Table 1: Notice Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Info Icon" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution Icon" /></td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="image" alt="Warning Icon" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="image" alt="Laser Warning Icon" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td><img src="image" alt="Tip Icon" /></td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td><img src="image" alt="Best Practice Icon" /></td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

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

**Table 2: Text and Syntax Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>user@host&gt; configure</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td><code>user@host&gt; show chassis alarms</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>No alarms currently active</code></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>• Introduces or emphasizes important new terms.</td>
<td>• A policy term is a named structure that defines match conditions and actions.</td>
</tr>
<tr>
<td></td>
<td>• Identifies guide names.</td>
<td>• <em>Junos OS CLI User Guide</em></td>
</tr>
<tr>
<td></td>
<td>• Identifies RFC and Internet draft titles.</td>
<td>• RFC 1997, <em>BGP Communities Attribute</em></td>
</tr>
</tbody>
</table>
Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italic text like this</em></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[edit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root@# set system domain-name domain-name</td>
</tr>
<tr>
<td><strong>Text like this</strong></td>
<td>Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.</td>
<td>• To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The console port is labeled CONSOLE.</td>
</tr>
<tr>
<td>&lt; &gt; (angle brackets)</td>
<td>Encloses optional keywords or variables.</td>
<td>stub &lt;default-metric metric&gt;</td>
</tr>
<tr>
<td></td>
<td>(pipe symbol)</td>
<td>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.</td>
</tr>
<tr>
<td># (pound sign)</td>
<td>Indicates a comment specified on the same line as the configuration statement to which it applies.</td>
<td>rsvp # Required for dynamic MPLS only</td>
</tr>
<tr>
<td>[] (square brackets)</td>
<td>Encloses a variable for which you can substitute one or more values.</td>
<td>community name members [ community-ids ]</td>
</tr>
<tr>
<td>Indentation and braces { }</td>
<td>Identifies a level in the configuration hierarchy.</td>
<td>[edit] routing-options { static { route default { nexthop address; retain; } } }</td>
</tr>
<tr>
<td>; (semicolon)</td>
<td>Identifies a leaf statement at a configuration hierarchy level.</td>
<td></td>
</tr>
</tbody>
</table>

**GUI Conventions**
Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents graphical user interface (GUI) items you click or select.</td>
<td>• In the Logical Interfaces box, select <strong>All Interfaces</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To cancel the configuration, click <strong>Cancel</strong>.</td>
</tr>
<tr>
<td><strong>&gt;</strong> (bold right angle bracket)</td>
<td>Separates levels in a hierarchy of menu selections.</td>
<td>In the configuration editor hierarchy, select <strong>Protocols &gt; Ospf</strong>.</td>
</tr>
</tbody>
</table>

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:

  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 Juniper Care or Partner Support Services 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.

- **Product warranties**—For product warranty information, visit [https://www.juniper.net/support/warranty/](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/](https://www.juniper.net/customers/support/)
- **Search for known bugs**: [https://prsearch.juniper.net/](https://prsearch.juniper.net/)
- **Find product documentation**: [https://www.juniper.net/documentation/](https://www.juniper.net/documentation/)
- **Find solutions and answer questions using our Knowledge Base**: [https://kb.juniper.net/](https://kb.juniper.net/)
- **Download the latest versions of software and review release notes**: [https://www.juniper.net/customers/csc/software/](https://www.juniper.net/customers/csc/software/)
- **Search technical bulletins for relevant hardware and software notifications**: [https://kb.juniper.net/InfoCenter/](https://kb.juniper.net/InfoCenter/)
- **Join and participate in the Juniper Networks Community Forum**: [https://www.juniper.net/company/communities/](https://www.juniper.net/company/communities/)
- **Create a service request online**: [https://myjuniper.juniper.net](https://myjuniper.juniper.net)

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

**Creating a Service Request with JTAC**

You can create a service request with JTAC on the Web or by telephone.

- Visit [https://myjuniper.juniper.net](https://myjuniper.juniper.net).
- 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://support.juniper.net/support/requesting-support/](https://support.juniper.net/support/requesting-support/).
Understanding Application Security

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 Juniper Networks' SRX Series Services Gateways and NFX Series devices to 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.
- SSL Proxy—Provides visibility of encrypted traffic to allow deep packet inspection (DPI).

AppSecure works with additional content security through integrated unified threat management (UTM), intrusion prevention systems (IPS), and Juniper Networks Sky Advanced Threat Prevention (Sky ATP) on the security devices 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

- Application Identification | 32
- Application Firewall | 135
- Application Tracking | 167
- Application QoS | 188
- SSL Proxy | 351
CHAPTER

Application Identification

Application Identification  |  32
Predefined Application Signatures for Application Identification  |  56
Custom Application Signatures for Application Identification  |  85
Predefined and Custom Application Groups for Application Identification  |  98
Application Identification Support for Unified Policies  |  106
Secure Web Proxy  |  122
Application Identification enables you to see the applications on your network and learn how they work, their behavioral characteristics, and their relative risk. Using several 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**

**IN THIS SECTION**

- Junos OS Next-Generation Application Identification | 33
- Benefits of Application Identification | 33
- Application Signature Mapping | 34
- Application Identification Match Sequence | 34
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 SRX 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 35 shows the sequence in which mapping techniques are applied and how the application is determined.
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.

- **Application Tracking (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.
• 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.

• Application Quality of Experience (AppQoE)— Monitors the performance of applications, and based on the score, selects the best possible link for that application traffic.

SEE ALSO

Understanding Application Tracking | 168
Understanding Application Quality of Service (AppQoS) | 188

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.
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.

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.
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.

ASC entries expire after the configured ASC timeout. ASC entries are not refreshed even when there are cache hits (matching entry in ASC found) during the timeout period.

**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 | 105 |

### 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 including security policies, application firewall (AppFW), application tracking (AppTrack), application quality of service (AppQoS), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services including advanced policy-based routing (APBR) 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 security 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 was enabled by default. You can manually disable it by using the `set services application-identification no-application-system-cache` command.

```
user@host# set services application-identification no-application-system-cache
```
**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.
NOTE: On for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, when there are a large number of ASC entries (10,000 or more), and the entries are to be listed in the output for the command `show services application-identification application-system-cache`, a CLI session timeout occurs.

SEE ALSO

- Understanding Application Identification Techniques | 32
- Enabling or Disabling Application System Cache for Application Services | 38

### 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 security 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 statistics 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.

Starting from Junos OS Release 15.1X49-D120, on all SRX Series devices, the default time interval for application identification statistics collection time is changed from 1 minute to 1440 minutes.

**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.

Starting from Junos OS Release 15.1X49-D120, 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

Understanding Application Identification Techniques

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

Application Identification Inspection Limit

Starting in Junos OS Releases 15.1X49-D200 and 19.4R1, you have the flexibility to configure the application identification inspection limits:

- Inspection Limit for TCP and UDP Sessions
  
  You can set the byte limit and the packet limit for application identification (AppID) in a UDP or in a TCP session. AppID concludes the classification based on the configured inspection limit. On exceeding the limit, AppID terminates the application classification.

  If AppID does not conclude the final classification within the configured limits, and a pre-matched application is available, AppID concludes the application as the pre-matched application. Otherwise, the application is concluded as junos:UNKNOWN provided the global AppID cache is enabled. The global AppID cache is enabled by default.
To configure the byte limit and the packet limit, use the following configuration statements from the [edit] hierarchy:

- user@host# set services application-identification inspection-limit tcp byte-limit byte-limit-number packet-limit packet-limit-number
- user@host# set services application-identification inspection-limit udp byte-limit byte-limit-number packet-limit packet-limit-number

Table 3 on page 44 provides the range and default value for configuring the byte limit and the packet limit for TCP and UDP sessions.

<table>
<thead>
<tr>
<th>Session</th>
<th>Limit</th>
<th>Range</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Byte limit</td>
<td>0 through 4294967295</td>
<td>6000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For Junos OS Release 15.1X49-D200, the default value is 10000.</td>
</tr>
<tr>
<td></td>
<td>Packet limit</td>
<td>0 through 4294967295</td>
<td>Zero</td>
</tr>
<tr>
<td>UDP</td>
<td>Byte limit</td>
<td>0 through 4294967295</td>
<td>Zero</td>
</tr>
<tr>
<td></td>
<td>Packet limit</td>
<td>0 through 4294967295</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For Junos OS Release 15.1X49-D200, the default value is 20.</td>
</tr>
</tbody>
</table>

The byte limit excludes the IP header and the TCP/UDP header lengths.

If you set the both the byte-limit and the packet-limit options, AppID inspects the session until both the limits are reached.

You can disable the TCP or UDP inspection limit by configuring the corresponding byte-limit and the packet-limit values to zero.

- **Global Offload Byte Limit (Other Sessions)**

  You can set the byte limit for the AppID to conclude the classification and identify the application in a session. On exceeding the limit, AppID terminates the application classification and takes one of the following decisions:

  - If a pre-matched application is available, AppID concludes the application classification as the pre-matched application in following cases:
    - When AppID does not conclude the final classification within the configured byte limit
- When the session is not offloaded due to tunnelling behavior of some applications

- If a pre-matched application is not available, AppID concludes the application as junos:UNKNOWN, provided the global AppID cache is enabled. The global AppID cache is enabled by default. See Enabling or Disabling Application System Cache for Application Services.

To configure the byte limit, use the following configuration statement from the [edit] hierarchy:

```plaintext
set services application-identification global-offload-byte-limit byte-limit-number
```

The default value for the global-offload-byte-limit option is 10000.

You can disable the global offload byte limit by configuring the global-offload-byte-limit value to zero.

The byte limit excludes the IP header and the TCP/UDP header lengths.

**Enable Performance Mode Option**

Starting in Junos OS Releases 15.1X49-D200 and 19.4R1, the maximum packet threshold for DPI performance mode option set services application-identification enable-performance-mode max-packet-threshold value is deprecated—rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration. This option was used for setting the maximum packet threshold for the DPI performance mode.

If your configuration includes enabled performance mode option with max-packet-threshold in Junos OS 15.1X49-D200 and 19.4R1 releases, AppID concludes the application classification on reaching the lowest value configured in the TCP or UDP inspection limit or global offload byte limit, or in the maximum packet threshold for DPI performance mode option.

**Application Identification Support for Applications Hosted on Content Delivery Network (CDN)**

Starting in Junos OS Release 20.1R1 and 19.1R3, you can enable application identification (AppID) to classify a web application that is hosted on a content delivery network (CDN) such as AWS, Akamai, Azure, Fastly, and Cloudflare and so on accurately. Use the following configuration statement to enable CDN application classification:

```plaintext
[edit]
user@host# user@hots# set service application-identification enable-cdn-application-detection
```

When you apply the configuration, AppID identifies and classifies actual applications that are hosted on the CDN.
**Maximum Memory Limit for DPI**

Starting in Junos OS Release 20.1R1 and 19.1R3, you can configure the maximum memory limit for deep packet inspection (DPI) by using the following configuration statement:

```
user@host# set services application-identification max-memory memory-value
```

You can set 1 through 200000 MB as memory value.

Once the JDPI memory consumption reaches to 90% of the configured value, then DPI stops processing new sessions.

**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 security 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
   ```

Starting in Junos OS Releases 15.1X49-D200 and 19.4R1, the maximum packet threshold for DPI performance mode option `set services application-identification enable-performance-mode max-packet-threshold value` is deprecated—rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration. This option was used for setting the maximum packet threshold for the DPI performance mode.

3. Commit the configuration.
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)**

```bash
user@host> show services application-identification status
```

```
pic: 2/1

Application Identification
Status: Enabled
Sessions under app detection: 0
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 | 550

---

**Packet Capture of Unknown Application Traffic**

**IN THIS SECTION**

- Packet Capture of Unknown Application Traffic Overview | 49
- Configure Packet Capture of Unknown Application Traffic | 49

Starting in Junos OS Release 20.2R1, you can use the packet capture of unknown applications functionality to gather more details about an unknown application on your security device.
Packet Capture of Unknown Application Traffic Overview

You can use the packet capture of unknown applications feature to gather more details about an unknown application on your security device. Unknown application traffic is the traffic that does not match an application signature.

Once you’ve configured packet capture options on your security device, the unknown application traffic is gathered and stored on the device in a packet capture file (.pcap). You can use the packet capture of an unknown application to define a new custom application signature. You can use this custom application signature in a security policy to manage the application traffic more efficiently.

You can send the .pcap file to Juniper Networks for analysis in cases where the traffic is incorrectly classified, or to request creation of an application signature.

Benefits of Packet Capture of Unknown Application Traffic

You can use the packet capture of unknown application traffic to:

- Gather more insight about an unknown application
- Analyze unknown application traffic for potential threats
- Assist in creation of security policy rules
- Enable custom application signature creation

NOTE: Implementing security policies that block all unknown application traffic could cause issues with network-based applications. Before applying these types of policies, be sure to validate that this approach does not cause issues in your environment. You must carefully analyze the unknown application traffic, and you can define the security policy accordingly.

Configure Packet Capture of Unknown Application Traffic

Before You Begin

To enable packet capture of unknown application traffic, you must:

- Install a valid application identification feature license on your SRX Series device. See Managing Junos OS Licenses.
- Download and install the Junos OS application signature package. See Download and Install Junos OS Application Signature Package.
- Ensure you have Junos OS Release 20.2R1 or later version on your security device.
Overview
In this example, you'll learn how to configure the packet capture of unknown applications on your security device by completing the following steps:

- Define Packet Capture Options on page 50
- Set Packet Capture Mode on page 51
- Enable Packet Capture Globally or at Policy Level on page 51
- Access Packet Capture File on page 52

Configuration
In this example, you enable packet capturing on your security device by defining packet capture options such as maximum packet limit, maximum byte limit, and number of files. To learn about the packet capture configuration options, see packet-capture before you start the configuration.

Define Packet Capture Options

Step-by-Step Procedure
To set the packet capture options:

1. Set the maximum number of UDP packets per session.

   [edit]
   user@host# set services application-identification packet-capture max-packets 10

2. Set the maximum number of TCP bytes per session.

   [edit]
   user@host# set services application-identification packet-capture max-bytes 2048

3. Set the maximum number of packet capture files to be created before the oldest file is overwritten by a new file which is known as file rotate frequency.

   [edit]
   user@host# set services application-identification packet-capture max-files 30
Set Packet Capture Mode

In this step, you set the packet capture mode.

You can capture the packets for the unknown application traffic in either of the following modes:

• ASC mode—Capture the packet for unknown application when the application is classified as junos:UNKNOWN and has a matching entry in the application system cache (ASC). This mode is enabled by default.

• Aggressive mode—Capture all traffic before AppID classifies the applications. In this mode, the system captures all application traffic irrespective of an available ASC entry. Packet capture starts for the first packet of the first session. Note that the aggressive mode is a more resource-intensive mode.

To enable aggressive mode, use the following command:

[edit]
user@host# set services application-identification packet-capture aggressive-mode

We do not recommend using aggressive mode unless you need to capture the first occurrence of a flow prior. The default behavior of the device relies on the ASC.

Enable Packet Capture Globally or at Policy Level

You can configure the packet capture globally to capture all unknown application traffic or enable the packet capture of application traffic specific to a security policy. In this example, you'll enable packet capture of unknown application traffic at the security policy level.

Step-by-Step Procedure

• Configure packet capture of unknown application traffic that matches the security policy P1 rules.

[edit]
user@host# set security policies from-zone untrust to-zone trust policy P1 match source-address any
user@host# set security policies from-zone untrust to-zone trust policy P1 match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy P1 match application any
user@host# set security policies from-zone untrust to-zone trust policy P1 match dynamic-application junos:UNKNOWN
user@host# set security policies from-zone untrust to-zone trust policy P1 then permit application-services packet-capture

To enable packet capture of unknown application traffic at the security policy level, you must include junos:UNKNOWN as the dynamic-application match conditions.

When you configure the security policy (P1), the system captures the packet details for the application traffic that matches the security policy match criteria.

Results
From configuration mode, confirm your configuration by entering the `show services application-identification packet-capture` command and `show security policies` hierarchy level. If the output does not display the intended configuration, follow the configuration instructions in this example to correct it.

```
[edit services application-identification]
user@host# show packet-capture
{
    max-packets 10;
    max-bytes 2048;
    max-files 30;
}
```

```
[edit security policies]
user@host# show
from-zone untrust to-zone trust {
    policy P1 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application [ junos:UNKNOWN ];
        }
        then {
            permit {
                application-services {
                    packet-capture;
                }
            }
        }
    }
}
```

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

**Access Packet Capture File**

After you complete the configuration and commit it, you can view the packet capture (.pcap) file. The system generates a unique packet capture file for each destination IP address, destination port, and protocol.

**Step-by-Step Procedure**

To view the packet capture file:

1. Navigate to the directory where packet capture files are stored on the device.
Locate the packet capture file. For example, locate the `5.0.0.1_3548_6.pcap` file. The packet capture file is saved in `destination-IP-address. destination-port.protocol. pcap` format.

You can download the packet capture file by using SFTP or SCP and read the packet capture file by using Wireshark or any other packet capture reader tools.

Figure 2 on page 53 shows a sample packet capture file generated for the unknown application traffic.

**Figure 2: Sample Packet Capture File**

![Sample Packet Capture File](image)

**NOTE:** In some situations network traffic drops could cause the device to be unable to capture all packets. In this case, the `.pcap` file will reflect the missing packets.

The security device saves the packet capture details for all the traffic matching the three matching criteria (destination IP address, destination port, and protocol) in the same file irrespective of global or policy-level configuration. The system maintains the cache with the destination IP address, destination port, and the protocol and does not accept the repeated capturing of the same traffic more than the allowed limit. You can set the packet capture file options mentioned in packet-capture.
**Verification**

**Viewing Packet Capture Details**

**Purpose**
View the packet capture details to confirm that your configuration is working.

**Action**
Use the `show services application-identification packet-capture counters` command.

```
user@host> show services application-identification packet-capture counters
```

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total sessions captured</td>
<td>1</td>
</tr>
<tr>
<td>Total packets captured</td>
<td>6</td>
</tr>
<tr>
<td>Active sessions being captured</td>
<td>0</td>
</tr>
<tr>
<td>Sessions ignored because of memory allocation failures</td>
<td>0</td>
</tr>
<tr>
<td>Packets ignored because of memory allocation failures</td>
<td>0</td>
</tr>
<tr>
<td>Ipc messages ignored because of storage limit</td>
<td>0</td>
</tr>
<tr>
<td>Sessions ignored because of buffer-packets limit</td>
<td>0</td>
</tr>
<tr>
<td>Packets ignored because of buffer-packets limit</td>
<td>0</td>
</tr>
<tr>
<td>Inconclusive sessions captured</td>
<td>0</td>
</tr>
<tr>
<td>Inconclusive sessions ignored</td>
<td>0</td>
</tr>
<tr>
<td>Cache entries timed out</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**
From this sample output, you can get details such as the number of sessions being captured, and the number of sessions already captured. For more details about the packet capture counters, see `show services application-identification packet-capture counters`.

**SEE ALSO**
- `request services application-identification clear packet-capture all`
- `clear services application-identification packet-capture counters`

**WHAT'S NEXT**
For more information on application identification, see `Application Identification`. For details about custom applications, see `Custom Application Signatures for Application Identification`
Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2R1</td>
<td>Starting in Junos OS Release 18.2R1, the default behavior of the ASC is changed</td>
</tr>
<tr>
<td>18.2R1</td>
<td>In releases before Junos OS Release 18.2R1, application caching was enabled by default. You can manually disable it by using the <code>set services application-identification no-application-system-cache</code> command.</td>
</tr>
<tr>
<td>15.1X49-D120</td>
<td>Starting from Junos OS Release 15.1X49-D120, 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.</td>
</tr>
<tr>
<td>19.4R1</td>
<td>Starting in Junos OS Releases 15.1X49-D200 and 19.4R1, you have the flexibility to configure the application identification inspection limits:</td>
</tr>
<tr>
<td>19.4R1</td>
<td>Starting in Junos OS Releases 15.1X49-D200 and 19.4R1, the maximum packet threshold for DPI performance mode option <code>set services application-identification enable-performance-mode max-packet-threshold value</code> is deprecated</td>
</tr>
<tr>
<td>Junos OS 20.2R1</td>
<td>Starting in Junos OS Release 20.2R1, you can use the packet capture of unknown applications functionality to gather more details about an unknown application on your security device.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- Understanding Application Security | 29
- Predefined Application Signatures for Application Identification | 56
- Custom Application Signatures for Application Identification | 85
- Predefined and Custom Application Groups for Application Identification | 98
Predefined Application Signatures for Application Identification

IN THIS SECTION

- Understanding the Junos OS Application Package Installation | 56
- Installing and Verifying Licenses for an Application Signature Package | 59
- Downloading and Installing the Junos OS Application Signature Package Manually | 61
- Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package | 66
- Downloading Junos OS Application Signature Package from A Proxy Server | 69
- Example: Scheduling the Application Signature Package Updates | 73
- Scheduling the Application Signature Package Updates As Part of the IDP Security Package | 75
- Example: Downloading and Installing the Application Identification Package in Chassis Cluster Mode | 78
- Verifying the Junos OS Application Identification Extracted Application Package | 82
- Uninstalling the Junos OS Application Identification Application Package | 84

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

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” on page 66.

**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” on page 61 or “Example: Scheduling the Application Signature Package Updates” on page 73.

**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: Starting from Junos OS Release 15.1X49-D50 and Junos OS Release 17.3, 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 reenable AppFW and AppQoS rules once the upgrade or downgrade procedure is complete.

NOTE: On all security devices, J-Web pages for AppSecure Services are preliminary. We recommend using the CLI for configuration of AppSecure features.

NOTE: This feature requires a license. To understand more about Junos OS application signature package, see, Installing and Verifying Licenses for an Application Signature Package. Please refer to the Juniper Licensing Guide for general information about License Management. Please refer to the product Data Sheets at SRX Series Services Gateways for details, or contact your Juniper Account Team or Juniper Partner.

**Upgrading to Next-Generation Application Identification**

Starting from Junos OS Release 12.1X47-D10, next-generation application identification is supported. You must install Junos OS Release 12.1X47-D10 to migrate from existing, or legacy, application identification to next-generation application identification.

Security devices installed with Junos OS builds with legacy application identification include legacy application identification security packages. When you upgrade these devices with Junos OS Release 12.1X47-D10, 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 | 36 |
| Understanding the IDP Signature Database |
| Downloading and Installing the Junos OS Application Signature Package Manually | 61 |
| Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package | 66 |
| Example: Scheduling the Application Signature Package Updates | 73 |

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.

Starting from Junos OS 15.1X49-D30 and Junos OS Release 17.3R1, on SRX1500 devices, AppSecure is part of Junos Software Enhanced (JSE) software license package. There is no separate license key for AppSecure is available. You must use JSE software license on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Starting from Junos OS 15.1X49-D30 and Junos OS Release 17.3R1, on SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Junos Software Enhanced (JSE) software license package. There is no separate license key for AppSecure is available. You must use JSE software license on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Starting from 15.1X49-D65 and Junos OS Release 17.3R1, on SRX4100, and SRX4200 devices, AppSecure is part of Junos Software Enhanced (JSE) license package. There is no separate license key for AppSecure is available. You must use JSE software license on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Starting from Junos OS Release 17.4R1, for SRX4600, application signatures are included by default. Junos Software Base (JSB) package does not include application signatures. Please refer to the product Data Sheets at SRX Series Services Gateways for details, or contact your Juniper Account Team or Juniper Partner.

You can install the license on the SRX Series 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
  ```
Paste the license key and press Enter to continue.

• Verify the license is installed on your device.

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

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

License identifier: JUNOSXXXXXX
License version: 2
Valid for device: AA4XXX005
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)

Downloading and Installing the Junos OS Application Signature Package
Manually

IN THIS SECTION

• Requirements | 62
• Overview | 62
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 security 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.

This example uses the following hardware and software components:

- An SRX Series device
- Junos OS Release 12.1X47-D10

**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.
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:

```bash
user@host> request services application-identification install status

Install application package 2345 succeed
```

- To view the protocol bundle status:

```bash
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.

![Configuration Settings]

**Meaning**

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

**SEE ALSO**

- Understanding the Junos OS Application Package Installation | 56
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 SRX Series 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.

This example uses the following hardware and software components:

- An SRX Series device
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.
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


```
[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

---

**Downloading Junos OS Application Signature Package from A Proxy Server**

---

**IN THIS SECTION**

- Requirements | 70
- Overview | 70
- Configuration | 71
- Verification | 71
This example shows how to create a proxy profile and use it for downloading the application signature package from a proxy server.

Requirements

This example uses the following hardware and software components:

- Valid application identification feature license installed on an SRX Series device.
- SRX Series device with Junos OS Release 18.3R1 or later. This configuration example is tested for Junos OS Release 18.3R1.

Overview

You must download and install the application signature package that is hosted on an external server on the SRX Series device. Starting from Junos OS Release 18.3R1, you can download the application signature package using a proxy server.

To enable downloading signature package from the proxy server:

1. Configure a profile with host and port details of the proxy server using the `set services proxy profile` command.
2. Use the `set services application-identification download proxy-profile profile-name` command to connect to the proxy server and download the application signature package.

When you download the signature package, the request is routed through the proxy host to the actual server hosting the signature package. The proxy host relays the response back from the actual host. The download retrieves the application package from the Juniper Networks security website https://signatures.juniper.net/cgi-bin/index.cgi.

**NOTE:** Support for the proxy profile configuration is available for only HTTP connections.

In this example, you create a proxy profile, and refer the profile when you download the application signature package from the external host. Table 4 on page 70 provides the details of the parameters used in this example.

**Table 4: Proxy Profile Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Profile-1</td>
</tr>
<tr>
<td>IP address of the proxy server</td>
<td>5.0.0.1</td>
</tr>
</tbody>
</table>
Table 4: Proxy Profile Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number of the proxy server</td>
<td>3128</td>
</tr>
</tbody>
</table>

**Configuration**

Create a proxy profile and apply it for downloading the application package through the proxy server.

1. Create a proxy profile for protocol HTTP.

   ```
   user@host# set services proxy profile Profile-1 protocol http
   ```

2. Specify the IP address of the proxy server.

   ```
   user@host# set services proxy profile Profile-1 protocol http host 5.0.0.1
   ```

3. Specify the port number used by the proxy server.

   ```
   user@host# set services proxy profile Profile-1 protocol http port 3128
   ```

4. Download the application package from the proxy host.

   ```
   user@host# set services application-identification download proxy-profile Profile-1
   ```

You can disable the proxy server for downloading application signature package when not required.

- Disable the proxy server for application signature download.

  ```
  user@host# delete services application-identification download proxy-profile p1
  ```

**Verification**

*Verifying Application Signature Download Through the Proxy Server*

**Purpose**

Display the details for the application signature package download through a proxy server.

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

<table>
<thead>
<tr>
<th>Application Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>Sessions under app detection</strong></td>
</tr>
<tr>
<td><strong>Max TCP session packet memory</strong></td>
</tr>
<tr>
<td><strong>Force packet plugin</strong></td>
</tr>
<tr>
<td><strong>Force stream plugin</strong></td>
</tr>
<tr>
<td><strong>DPI Performance mode:</strong></td>
</tr>
<tr>
<td><strong>Statistics collection interval</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application System Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>Cache lookup security-services</strong></td>
</tr>
<tr>
<td><strong>Cache lookup miscellaneous-services</strong></td>
</tr>
<tr>
<td><strong>Max Number of entries in cache</strong></td>
</tr>
<tr>
<td><strong>Cache timeout</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Bundle</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Download Server</strong></td>
</tr>
<tr>
<td><strong>AutoUpdate</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proxy Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Profile</strong></td>
</tr>
<tr>
<td><strong>Proxy Address</strong></td>
</tr>
<tr>
<td><strong>Slot 1:</strong></td>
</tr>
<tr>
<td><strong>Application package version</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>PB Version</strong></td>
</tr>
<tr>
<td><strong>Engine version</strong></td>
</tr>
<tr>
<td><strong>Sessions</strong></td>
</tr>
</tbody>
</table>

**Meaning**
In the command output, you can find the proxy profile details in **Proxy Profile** and **Proxy Address** fields.

**Verifying Application Signature Download Status**

**Purpose**
Check the application package download status.

**Action**
From operational mode, enter the `request services application-identification download status` command.

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

Application package 3058 is downloaded successfully
```

**Meaning**
The command displays the application signature package download status.

---

**Example: Scheduling the Application Signature Package Updates**

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

**Requirements**

Before you begin:

- Ensure that your security 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.
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

GUI Step-by-Step Procedure

To set up the automatic download and periodic update with the J-Web interface:

1. Enter Configure>Security>AppSecure Settings to display the Applications Signature page.

2. Click Global Settings.

3. Click the Download Scheduler tab, and modify the following fields:
   - URL: https://signatures.juniper.net/cgi-bin/index.cgi
   - Enable Schedule Update: Select the check box.
   - Interval: 48

4. Click Reset Setting to clear the existing start time, enter the new start time in YYYY-MM-DD.hh:mm format, and click OK.
   - Start Time: 2019-06-30.10:00:00

5. Click Commit Options>Commit to commit your changes.

6. Click Check Status to monitor the progress of an active download or update, or to check the outcome of the latest update.

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 10 am on December 10:

```
[edit]
user@host# set services application-identification download automatic interval 48 start-time 2019-06-30.10:00:00
```

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 | 56
- Downloading and Installing the Junos OS Application Signature Package Manually | 61
- Verifying the Junos OS Application Identification Extracted Application Package | 82

Scheduling the Application Signature Package Updates As Part of the IDP Security Package
The configuration instructions in this example describe 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 security 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.

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

GUI Step-by-Step Procedure

To set up the automatic download and periodic update with the J-Web interface:

1. Enter Configure>Security>IDP>Signature Updates to display the Security IDP Signature Configuration page.

2. Click Download Settings and modify the URL: https://signatures.juniper.net/cgi-bin/index.cgi

3. Click the Auto Download Settings tab, and modify the following fields:

   - Interval: 48
   - Start Time: 2013-12-10.23:59:55
   - Enable Schedule Update: Select the check box.

4. Click Reset Setting to clear the existing fields, enter the new values. Click OK.

5. Click Commit Options>Commit to commit your changes.

6. Click Check Status to monitor the progress of an active download or update, or to check the outcome of the latest update.
**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.
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 | 56
- Downloading and Installing the Junos OS Application Signature Package Manually | 61
- Verifying the Junos OS Application Identification Extracted Application Package | 82

Example: Downloading and Installing the Application Identification Package in Chassis Cluster Mode

This example shows how to download and install the application signature package database to a device operating in chassis cluster mode.

Requirements

Before you begin:

- Set the chassis cluster node ID and cluster ID. See Example: Setting the Node ID and Cluster ID for Security Devices in a Chassis Cluster.
- Ensure that your security 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 application identification feature license.

Overview

If you use application identification, you can download the predefined application signature package database. Juniper Networks regularly updates the database and makes it available on the Juniper Networks website. This package includes application objects that can be used to match traffic in IDP, application firewall policies, and application tracking. For more details, see "Understanding the Junos OS Application Package Installation” on page 56.

When you download the application identification security package on a device operating in chassis cluster mode, the security package is downloaded to the primary node and then synchronized to the secondary node.

Downloading and Installing the Application Identification Package

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 download and install an application package:

1. Download the application package on the primary node.

   {primary:node0}[edit]
   
   user@host> request services application-identification download

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

2. Check the application package download status.

   {primary:node0}[edit]
   
   user@host> request services application-identification download status

   On a successful download, the following message is displayed

   Application package 2345 is downloaded successfully
The application package is installed in the application signature database on the primary node, and application identification files are synchronized on the primary and secondary nodes.

3. Update the application package using `install` command.

   [primary:node0][edit]

   user@host> request services application-identification install

   node0:
   -----------------------------------------------------------------------------------------------
   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

   node1:
   -----------------------------------------------------------------------------------------------
   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

4. Check the application package update status. The command output displays information about the downloaded and installed versions of the application package.

   [primary:node0][edit]

   user@host> request services application-identification install status

   node0:
   -----------------------------------------------------------------------------------------------
   Install application package 2345 succeed

   node1:
   -----------------------------------------------------------------------------------------------
   Install application package 2345 succeed
NOTE: It is possible that an application signature is removed from the new 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.

NOTE: While downloading the application signature package on the primary node, sometimes, due to unexpected failover, the primary node might not able to download the application signature package completely. As a workaround, you must delete the /var/db/appid/sec-download/.apppack_state and restart the device.

To uninstall an application package:

1. Uninstall the application package using **uninstall** command.

   ```
   [primary:node0][edit]

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

   node0:
   
   ---------------------------------------------------------------
   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
   node1:
   
   ---------------------------------------------------------------
   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 status of the application package.

   ```
   [primary:node0][edit]

   user@host> request services application-identification uninstall status
   ```
3. 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

SEE ALSO

- Understanding the Junos OS Application Package Installation | 56
- Verifying the Junos OS Application Identification Extracted Application Package | 82

**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 | 56
- Downloading and Installing the Junos OS Application Signature Package Manually | 61
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 | 707
- request services application-identification uninstall status | 708
### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.4R1</td>
<td>Starting from Junos OS Release 17.4R1, for SRX4600, application signatures are included by default.</td>
</tr>
<tr>
<td>15.1X49-D65</td>
<td>Starting from 15.1X49-D65 and Junos OS Release 17.3R1, on SRX4100, and SRX4200 devices, AppSecure is part of Junos Software Enhanced (JSE) license package.</td>
</tr>
<tr>
<td>15.1X49-D40</td>
<td>Starting from Junos OS 15.1X49-D30 and Junos OS Release 17.3R1, on SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Junos Software Enhanced (JSE) software license package.</td>
</tr>
<tr>
<td>15.1X49-D30</td>
<td>Starting from Junos OS 15.1X49-D30 and Junos OS Release 17.3R1, on SRX1500 devices, AppSecure is part of Junos Software Enhanced (JSE) software license package.</td>
</tr>
<tr>
<td>12.1X47-D10</td>
<td>Starting from Junos OS Release 12.1X47-D10, next-generation application identification is supported.</td>
</tr>
</tbody>
</table>

### RELATED DOCUMENTATION

- Application Identification  | 32
- Custom Application Signatures for Application Identification  | 85
- Predefined and Custom Application Groups for Application Identification  | 98

### Custom Application Signatures for Application Identification

### IN THIS SECTION

- Understanding Junos OS Application Identification Custom Application Signatures  | 86
- Example: Configuring Junos OS Application Identification Custom Application Signatures  | 91
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**

---

**Custom Application Signatures Overview**

Junos OS application identification feature provides you the flexibility to create custom signatures to identify any application, whether it is web-based or a client-server application. You can create custom application signatures for applications based on ICMP, IP protocol, IP address, and Layer 7.

In general, custom application signatures are unique to your environment and are mostly used to inspect internal or custom applications. Once you create custom application signatures, AppID classifies and inspects in the same manner as standard applications. Since custom application signatures are not part of the predefined application package, they are saved in the configuration hierarchy, not in the predefined application signature database.

You must download install the application signature package on your device to configure custom signatures. When the custom signatures are configured, you cannot uninstall the application signature package. All custom application signatures are carried forward as-is when you upgrade your system to a new software version.
Enhancements to Custom Application Signatures

Starting in Junos OS Release 20.1R1, we’ve enhanced the custom applications signature functionality by providing a new set of applications and contexts.

Custom application signature contexts are now part of application signature package. If you want to use the newly introduced application and contexts for custom application signatures, you must download and install the latest application signature package version 3248 or later. You can upgrade the application signature package separately without upgrading Junos OS.

Supported Types of Custom Application Signatures

Security devices support the following types of custom signatures:

- ICMP-based mapping
- Address-based mapping
- IP protocol-based mapping
- Layer 7-based and TCP/UDP stream-based mapping

In all supported custom application signatures, ICMP-based, IP protocol-based, and address-based custom applications have more priority than Layer 7-based and TCP/UDP stream-based custom applications. Custom application signatures priority order is—ICMP-based, IP protocol-based, address-based, and Layer7-based or TCP/UDP stream-based custom applications.

**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. The ICMP mapping technique does not support ICMPv6 traffic.

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

**Address-Based Mapping**

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

- For configuring Layer 3 and Layer 4 address-based custom applications, you must match the IP address and port range to destination IP address and port. When both IP address and port are configured, both criteria must match destination 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 only by 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.
• When you configure an address-based application and a TCP/UDP stream-based application, and if a session matches both applications, the TCP/UDP stream-based application is reported as application and address-based application is reported as extended application.

CAUTION: 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.

**IP Protocol-Based Mapping**

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

IP protocol based custom application signatures do not work as expected in Junos OS Releases in 19.2 through Junos OS Releases 19.4. Starting in Junos OS Release 20.1R1, you can use IP protocol-based custom application signatures.

Suggested workaround:

• If you are configuring unified policy, use service-based application configuration. Example:

```
user@host# set applications application application-name protocol IP-proto-number
```

Example:

```
user@host# set applications application A1 protocol 2
```

• If you are using legacy application firewall, use predefined IP protocol applications. Example

```
user@host# set security application-firewall rule-sets rule-set-name rule rule-name match dynamic-application application-name
```

Example:

```
user@host# set security application-firewall rule-sets RS-1 rule R1 match dynamic-application junos:IPP-IGMP
```

**Layer 7-Based and TCP/UDP Stream-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. 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.

Benefits of Using Custom Application Signatures

- Enforce security policy unique to your networking environment based on specific applications
- Bring visibility for unknown or unclassified applications
- Identify applications over Layer 7 and transiting or temporary applications, and to achieve further granularity of known applications
- Perform quality-of-service (QoS) for any specific application

Limitations

The following features are not supported:

- Some of the PCRE-based expressions and unicode-based characters (if not supported in Hyperscan)
- Enforcing of order among members in Layer 7-based signatures
- The wildcard address for address-based signatures (Layer 3 and Layer 4)

Additional Configuration Options for Custom Application Signatures

Starting in Junos OS Release 20.1R1 and if you are using application signature package version 3248 or later, you can configure the following options for custom application signatures:

**Custom Application Pattern Depth**

You can specify the byte limit for AppID to identify the custom application pattern for the applications running over TCP or UDP or Layer 7 applications.

To configure the limit, use the following configuration statements from the [edit] hierarchy:

```
user@host# set services application-identification application application-name over application signature signature-name member number depth
```
Example:

```
user@host# set services application-identification application my_custom_address over HTTP signature my_addr_sig1 member m01 depth 256
```

For Layer 7 custom applications, the depth is considered from the beginning of the Layer 7 context. For TCP/UDP stream-based custom applications, depth is considered from the beginning of the TCP/UDP payload.

**Custom Applications Inspection Byte Limit**

You can set the inspection byte limit for AppID to conclude the classification and identify the custom application in a session. On exceeding the limit, AppID terminates the application classification. You can use this option to improve the application traffic throughput.

To configure the application byte limit, use the following configuration statements from the [edit] hierarchy:

```
user@host# set services application-identification custom-application-byte-limit byte-number
```

Example:

```
user@host# set services application-identification custom-application-byte-limit 400
```

If you have configured a custom application signature over a predefined application and if AppID has already identified the predefined application, DPI continues with the custom signature identification. While the custom signature identification is in-progress, the classification is marked as non-final. If no custom application is identified within the custom application byte limit, and if predefined application is already identified, then AppID concludes the predefined application as final and offloads the session.

**Priority for Custom Applications**

In releases prior to Junos OS 20.1R1, the default priority for the custom application signatures was high which allowed custom signatures to take precedence over the predefined applications. Starting Junos OS release 20.1R1, the default priority for the custom application signature is low.

When AppID identifies a custom application with low priority before identifying a predefined application, it waits until predefined application classification is final. If there is no predefined application match available and the custom application is identified, then AppID terminates the classification with the identified custom application.

If you want to override the predefined applications priority with custom application signatures, you must explicitly set the priority to high for the custom application signatures.

To configure the high priority for custom applications, use the following configuration statements from the [edit] hierarchy:
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.

**Before You Begin:**

- Install a valid application identification feature license on your SRX Series device. See [Managing Junos OS Licenses](#).
- This configuration example is tested using Junos OS Release 20.1R1.
- Ensure that your security device with application signature package installed. See "[Downloading and Installing the Junos OS Application Signature Package Manually](#)" on page 61.
- To use enhanced custom application signatures, upgrade latest application signature package version 3284 or later. Check your application signature version using the following command:
Overview

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

Use the following steps to configure custom application signatures:

1. Define attributes such as context, patterns, direction, port range and so on for your security device to match the application traffic.

2. Configure inspection limit, pattern depth, and priority (optional configurations) to enhance custom applications application identification process.

3. Attach the custom application to a security policy that allows or denies the application traffic.

4. View application signatures and application signature groups by using the `show services application-identification application` and `show services application-identification group` commands.

Examples of Custom Application Configuration

Step-by-Step Procedure

- Set inspection limit for custom applications.

  ```
  [edit ]
  user@host# set services application-identification custom-application-byte-limit 400
  ```

- Set priority for custom applications.

  ```
  [edit ]
  user@host# set services application-identification application test cacheable
  user@host# set services application-identification application test priority high
  ```
- Configure TCP stream-based custom signatures:

```plaintext
[edit ]
user@host# set services application-identification application my_custom_tcp over TCP signature s1 member m01 context stream
user@host# set services application-identification application my_custom_tcp over TCP signature s1 member m01 pattern .*install.*
user@host# set services application-identification application my_custom_tcp over TCP signature s1 member m01 direction any
user@host# set services application-identification application my_custom_tcp over TCP signature s1 member m01 depth 100
```

- Configure FTP context-based custom signatures:

```plaintext
[edit ]
user@host# set services application-identification application my_custom_ftp over FTP signature sig1 member m01 depth 60
user@host# set services application-identification application my_custom_ftp over FTP signature sig1 member m01 context ftp-file-name
user@host# set services application-identification application my_custom_ftp over FTP signature sig1 member m01 pattern .*install.*
user@host# set services application-identification application my_custom_ftp over FTP signature sig1 member m01 direction client-to-server
```

- Configure HTTP context-based custom signatures:

```plaintext
[edit ]
user@host# set services application-identification application my_custom_http over HTTP signature s1 member m01 context http-header-host
user@host# set services application-identification application my_custom_http over HTTP signature s1 member m01 pattern .*agent1.*
user@host# set services application-identification application my_custom_http over HTTP signature s1 member m01 direction client-to-server
user@host# set services application-identification application my_custom_http over HTTP signature s1 member m01 depth 100
```

- Configure SSL context-based custom signatures:

```plaintext
[edit]
user@host# set services application-identification application my_custom_ssl over SSL signature s1 member m01 context ssl-server-name
```
Configure ICMP-based custom application signatures:

```
[edit]
user@host# set services application-identification application my_custom_icmp icmp-mapping type 100
user@host# set services application-identification application my_custom_icmp icmp-mapping code 1
```

Configure Layer 3 or Layer 4 address-based custom application signatures:

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

Configure IP protocol mapping-based custom application signatures:

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

Create a security policy with custom applications as match criteria.

```
user@host# set security policies from-zone untrust to-zone trust policy 1 match source-address any
user@host# set security policies from-zone untrust to-zone trust policy 1 match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy 1 match application any
user@host# set security policies from-zone untrust to-zone trust policy 1 match dynamic-application my_custom_http
```
user@host# set security policies from-zone untrust to-zone trust policy 1 then permit

We are using my_custom_http for this example. Similarly, you can create different security policies and specify other custom applications such as my_custom_ftp, my_custom_tcp, my_custom_ssl, my_custom_address, my_custom_icmp, my_custom_ip_proto as match condition for the dynamic application as per your requirement.

- Enable application tracking.

user@host# set security zones security-zone trust application-tracking

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
custom-application-byte-limit 100;
application my_custom_address {
  address-mapping ADDR-SAMPLE {
    filter {
      ip 192.0.2.1/24;
      port-range {
        udp 5000-6000;
      }
    }
  }
}
application my_custom_ftp {
  over FTP {
    signature sig1 {
      member m01 {
        depth 60;
        context ftp-file-name;
        pattern "install.*";
        direction client-to-server;
      }
    }
  }
}
application my_custom_http {
over HTTP {
    signature s1 {
        member m01 {
            depth 100;
            context http-header-host;
            pattern "agent1.*";
            direction client-to-server;
        }
    }
}

application my_custom_icmp {
    icmp-mapping {
        type 100;
        code 1;
    }
}

application my_custom_ip_proto {
    ip-protocol-mapping {
        protocol 2;
    }
}

application my_custom_ssl {
    over SSL {
        signature s1 {
            member m01 {
                depth 100;
                context ssl-server-name;
                pattern "example\.com";
                direction client-to-server;
            }
        }
    }
}

application my_custom_tcp {
    over TCP {
        signature s1 {
            member m01 {
                depth 100;
                context stream;
                pattern "install.*";
                direction any;
            }
        }
    }
}
application test {
  cacheable;
  priority high;
}

[edit security policies]
user@host# show
from-zone untrust to-zone trust {
  policy 1 {
    match {
      source-address any;
      destination-address any;
      application any;
      dynamic-application [my_custom_http];
    }
    then {
      permit;
    }
  }
}

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

Verification

Verifying the Custom Application Definitions

Purpose
Display the custom application signatures 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.

user@host> show services application-identification application detail test

Application Name: test
Application type: TEST
Description: N/A
Meaning
The output of the command displays custom application name, type, description, ID, and the priority.

See `show services application-identification application`

SEE ALSO

- Understanding the Junos OS Application Package Installation | 56
- Customizing Application Groups for Junos OS Application Identification | 99

RELATED DOCUMENTATION

- Application Identification | 32
- Predefined Application Signatures for Application Identification | 56
- Predefined and Custom Application Groups for Application Identification | 98

Predefined and Custom Application Groups for Application Identification

IN THIS SECTION

- Customizing Application Groups for Junos OS Application Identification | 99
- Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management | 100
- Enabling or Disabling Application Groups in Junos OS Application Identification | 105
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

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.

As the predefined signature database changes, the content of a predefined application group can be modified to include new signatures.

**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.

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.
NOTE: Starting in Junos OS Release 18.2R2 and Junos OS Release 18.4R1, encrypted applications such as HTTP, SMTP, IMAP and POP3 over SSL are identified as junos:HTTPS, junos:SMTPS, junos:IMAPS, and junos:POP3S in Junos OS predefined applications and application sets.

For example: If you configure a security policy to allow or deny HTTPS traffic, you must specify application matching criteria as junos:HTTPS.

In previous Junos OS Releases, both HTTP and encrypted HTTP (HTTPS) applications can be configured using a same application matching criteria as junos:HTTP.

SEE ALSO

| Understanding the Junos OS Application Identification Database | 36 |

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

IN THIS SECTION

- Requirements | 100
- Overview | 101
- Configuration | 101

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" on page 61 or "Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package" on page 66.
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

IN THIS SECTION

- Configuring Junos OS Application Identification User-Defined Application Groups | 101
- Deleting an Application from a User-Defined Application Group | 103
- Creating Child Application Groups for an Application Group | 104

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
```
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.
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
   user@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
```
If you are done configuring the device, enter `commit` from configuration mode.

SEE ALSO

- Understanding Junos OS Application Identification Custom Application Signatures | 86

### 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 | 37
Application Identification Support for Unified Policies

Understanding Unified Policies on Security Devices

With the growing popularity of Web applications, and because of the shift from traditional, full client-based applications to the Web, more and more traffic is being transmitted over HTTP. Applications such as instant messaging, peer-to-peer file sharing, Webmail, social networking, and IP voice and video collaboration evade security mechanisms by changing communication ports and protocols. Managing changes in the application behavior requires constant modification to the security rules, and maintenance of the security policy rules poses a major challenge. To handle such changes in application behavior, you need security policies to manage dynamic applications.

As a response to this challenge, starting in Junos OS Release 18.2R1, Juniper Networks SRX Series Services Gateways and vSRX support unified policies, allowing granular control and enforcement of dynamic Layer 7 applications within the security policy. Unified policies are security policies that enable you to use dynamic applications as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time.
A unified policy leverages the application identity information determined from the application identification (AppID) module. After a particular application is identified, an action such as permit, deny, reject, or redirect is applied to the traffic according to the policy configured on the device.

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 at Layer 7 based on its AppID information.

AppID is enabled when you configure a security policy with dynamic applications or when you enable any services such as application policy-based routing (APBR), application tracking (Apptrack), application quality of service (AppQoS), application firewall (AppFW), IDP, or Juniper Sky ATP in the security policy.

**Benefits**

- Simplifies application-based security policy management at Layer 7.
- Enables your device to adapt to the dynamic traffic changes in the network.
- Provides greater control and extensibility to manage dynamic applications traffic than a traditional security policy.

**Understanding How Unified Policies Use AppID Information**

Accurate traffic classification is essential for network security in cloud and data center architectures. Identifying and classifying different types of application traffic (transacted on HTTP) is also a challenge as Web applications include documents, data, images, and audio and video files.

AppID detects the applications on your network regardless of the port, protocol, and encryption (TLS/SSL or SSH) or other evasive tactics. It uses deep packet inspection (DPI) techniques, a signature database, and well-known addresses and ports to identify applications. AppID provides the information such as dynamic application classification, default protocol and port of an application. For any application that is included in the dependent list of another application, AppID provides the information of dependent application.

A unified policy leverages the information from AppID to match the application and take action as specified in the policy. In a unified policy configuration, you can use a predefined dynamic application (from the application identification signature package) or a user-defined custom application as match condition.

**Understanding Dependent Dynamic Application Identification**

A dependent application list includes applications over which a dynamic application can be identified. For example, the dependent application list for Facebook comprises HTTP2 and SSL.
The default protocol and port of a dynamic application includes the protocol and port defined for that application. If the protocol and port for that application is not defined, then the list of default protocols and ports of its dependent applications is considered.

For example, the Facebook-Access application depends on applications such as HTTP, SSL, and HTTP2. Therefore, the default protocol and ports of these dependent applications are considered for the Facebook-Access application.

**NOTE:** The dependent application list and protocol and port mapping of an application might change during runtime whenever a new application signature pack is installed or a custom application configuration changes. AppID provides these details to the security policy.

Dynamic Application Classification States

During the application identification process, DPI processes every packet and classifies it into one of the following states until the application is finally identified:

- **Pre-match**—Before an application is identified by the DPI.
- **Transaction final**—For dynamic applications, one transaction is complete, but identification of the application is not final. Applications over Layer 7 can keep changing with each transaction because they have dependent applications. For example, Facebook applications have dependent applications such as HTTP, SSL, and so on.
- **Final match**—A matched application over Layer 7 is considered as the final match according to the configured maximum number of transactions. That is, the match is considered as final only after the maximum number of transactions are complete.

Before identifying the final application, the policy cannot be matched precisely. A potential policy list is made available, and the traffic is permitted using the potential policy from the list. After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect are applied to the traffic as specified in the policy rules.

Application classification is not terminated for applications that are transaction-based, such as Facebook. To terminate the classification for such applications, you can choose to consider the results from multiple transactions as the final classification.

Configuring Transactions Limit For Application Identification

You can configure the maximum number of transactions before concluding the final results for identifying an application using the `set services application-identification maximum-transactions transactions-number` statement. When you configure the maximum number of transactions, DPI is not terminated until the configured number of transactions are completed.
Example:

```
user@host# set services application-identification maximum-transactions 5
```

You can configure a transaction number from 0 through 25. By default, five transactions are considered.

If you set the transaction count as 0, the transaction does not terminate the DPI. The final match for the application might not be available; and the final security policy is not applied.

Table 5 on page 109 shows the different states of application identification classification when the maximum transaction is set as five. Note that the values in the table are for example and are not actual values. The exact transaction might vary depending on the traffic pattern.

Table 5: Application Identification Transactions Example

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Application Identified</th>
<th>Application Identification State</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>First packet of the session</td>
<td>None</td>
<td>Pre-match</td>
<td>0</td>
</tr>
<tr>
<td>Intermediate application</td>
<td>SSL</td>
<td>Pre-match</td>
<td>1</td>
</tr>
<tr>
<td>Intermediate application identified in decrypted payload</td>
<td>HTTP</td>
<td>Pre-match</td>
<td>2</td>
</tr>
<tr>
<td>Intermediate application identified</td>
<td>FACEBOOK-ACCESS</td>
<td>Pre-match</td>
<td>3</td>
</tr>
<tr>
<td>Intermediate application identified</td>
<td>FACEBOOK-CHAT</td>
<td>Final Transaction (Transaction =1)</td>
<td>4</td>
</tr>
<tr>
<td>Final application identified</td>
<td>FACEBOOK-MAIL</td>
<td>Final Match (Transaction = 2)</td>
<td>4</td>
</tr>
</tbody>
</table>

NOTE: In unified policies, configuring dynamic applications that can be identified based on Layer 3 or Layer 4 information (except ICMP-based applications) is not supported. Instead, you can use the junos-defaults group that contains predefined values for Layer 3 and Layer 4 based applications.

High Availability Support for Application Identification for Unified Policies

When an application is identified, its classification information is saved in the application system cache (ASC).
When your security device (example: SRX Series device) is operating in chassis cluster mode, the information saved in the ASC is synchronized between the primary node and the secondary node.

In case of dynamic application classification, per session application classification information from the DPI is synchronized with the secondary node when the application classification is final.

During a failover, the application classification information on the secondary node is in either of the following states:

- Application not identified
- Final application identified

After a failover, the application classification information that is available in the new primary node is considered as the final match. The same information is synchronized with the new secondary node as the classification does not proceed further after a failover. The example in Table 2 Table 6 on page 110 shows application classification status in a chassis cluster setup.

### Table 6: Application Classification Status in a Chassis Cluster Setup

<table>
<thead>
<tr>
<th>Application Identification Status</th>
<th>Chassis Cluster Node</th>
<th>Before Failover</th>
<th>After Failover</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final application is identified.</td>
<td>Primary node</td>
<td>Identified</td>
<td>Identified</td>
<td>No change after failover because complete application classification is synchronized to the secondary node.</td>
</tr>
<tr>
<td>Identified application: SSL:Facebook</td>
<td>Secondary node</td>
<td>application: SSL:Facebook</td>
<td>application: SSL:Facebook</td>
<td></td>
</tr>
<tr>
<td>Final application is not identified. (Partial application is identified.)</td>
<td>Primary node</td>
<td>Identified</td>
<td>Identified</td>
<td>Application identification does not proceed further after a failover.</td>
</tr>
<tr>
<td>Identified application: SSL</td>
<td>Secondary node</td>
<td>application: not available</td>
<td>application: APP-INVALID</td>
<td></td>
</tr>
</tbody>
</table>


Table 6: Application Classification Status in a Chassis Cluster Setup (continued)

<table>
<thead>
<tr>
<th>Application Identification Status</th>
<th>Chassis Cluster Node</th>
<th>Before Failover</th>
<th>After Failover</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final application is not identified. (Partial application is identified)</td>
<td>Primary node</td>
<td>Identified application: not available</td>
<td>Identified application: APP-INVALID</td>
<td>In this case, a failover occurred after the first packet inspection, and no application is identified. Application identification does not proceed further after a failover.</td>
</tr>
<tr>
<td></td>
<td>Secondary node</td>
<td>Identified application: not available</td>
<td>Identified application: APP-INVALID</td>
<td></td>
</tr>
</tbody>
</table>

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 including security policies, application firewall (AppFW), application tracking (AppTrack), application quality of service (AppQoS), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services including advanced policy-based routing (APBR) 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 security 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 was enabled by default. You can manually disable it by using the `set services application-identification no-application-system-cache` command.

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

SEE ALSO

- Understanding Application Identification Techniques | 32
- Verifying Application System Cache Statistics | 40
Application Identification Support for Micro-Applications

Starting in Junos OS Release 19.2R1 onwards, you can manage the applications at a sub-function level with application identification feature. In this document, we refer application sub-functions as micro-applications.

Micro-applications are part of application signature package. You must enable micro-application detection in application identification and then use them as matching criteria in security policy.

AppID detects the applications at sub-function level on your network and security policy leverages the application identity information determined from the application identification (AppID) module. After a particular application is identified, an action such as permit, deny, reject, or redirect is applied to the traffic according to the policy configured on the device.

Micro-applications concept is similar to transaction-based applications, where the nested application over a base application continuously change for the same session.

Example:

Consider a dynamic application MODBUS. READ and WRITE are sub functions or operations of MODBUS application. For these sub-functions, we must define micro-applications such as MODBUS-READ and MODBUS-WRITE. Application classification path can keep changing between MODBUS:MODBUS-READ and MODBUS:MODBUS-WRITE. In this case, MODBUS is the base application and MODBUS-READ and MODBUS-WRITE are nested applications, that is, micro-applications.

You can configure the micro-applications at the same hierarchy as predefined dynamic application in a security policy and take the action based on the policy rules.

By configuring these micro-applications in security policies, you can allow or deny MODBUS sub-functions rather than blocking or allowing the entire MODBUS application.

Micro-Application Classification

Application classification for micro-applications does not reach to the final match because, the micro-application keep changing for the session. A matched application is considered as the final match only after the maximum number of transactions are complete.

AppID has the maximum transaction limit as 25, however each service module has it's own limit based on it's own requirements. If service specific limit is reached before the maximum transaction limit (25), then the service module marks it's policy as final. However, AppID continues application classification and offloads the session on reaching the limit of 25.
You can use the `set services application-identification max-transactions` command to configure the transaction limit.

**Dependent Application List and Default Protocols and Ports**

A dependent application list includes applications over which a dynamic application can be identified. The default protocol and port of a dynamic application includes the protocol and port defined for that application.

Dependent application list and default protocols and ports are used by unified policy for enforcing the security policy. Dependent application list and default protocols and ports of micro application is same as that of base application.

Example: Dependent application list and default ports of micro-application MODBUS-READ is same as dependent application list and default ports of MODBUS.

**Policy Enforcement for Micro-Applications**

A security policies enforce rules for transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on traffic as it passes through the device. If you have configured a security policy with micro-application as match criteria, then the policy module requires micro-application identification information from AppID.

Application classification with micro-applications does not reach the final match because, the micro-application keep changing for the session. However, final match for the application is required for policy lookup and processing of the policy. You can use the `edit security policies unified-policy-max-lookups` command to limit the number of policy lookups.

After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect are applied to the traffic as specified in the policy rules.

**Installing Micro-Applications**

Micro applications are part of application signature package. When you download application signature package and install it, micro applications are also installed and are available for configuring in the security policies. You can view the details of the micro applications using the `show services application-identification status` command.

**NOTE:** If you have configured micro-applications in a security policy starting in Junos OS Release 19.2, it is not possible to downgrade to the previous version of Junos OS release. To downgrade to the previous version of Junos OS releases, you must remove the micro applications configured in your security policies.
Enabling and Disabling Micro-Applications Detection

You can enable or disable micro-application detection. By default, detection of micro-applications are disabled. You must enable micro-applications to use them in your security policy.

You can enable or disable micro-applications using the following commands:

- Enable micro-applications detection (from configuration mode).
  
  `user@host# set services application-identification micro-apps`

- Disable a specific micro-application (from operational mode).

  `user@host> request services application-identification application disable application-name`

Example:

  `user@host>request services application-identification application disable junos:MODBUS`

Example: Configuring Micro-Applications

This example shows how to configure micro-applications in a security policy to enforce the policy at sub-function level.
Requirements

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 19.2R1 or later. This configuration example is tested on Junos OS Release 19.2R1.
- Valid application identification feature license installed on an SRX Series device.

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" on page 61 or "Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package" on page 66.

Overview

In this example, you create a security policy with micro-applications MODBUS-READ-COILS and MODBUS-WRITE-SINGLE-COIL, MODBUS-READ-COILS, MODBUS-WRITE-MULTIPLE-COILS. Application traffic matching these micro-applications is permitted.

Configuration

IN THIS SECTION

- Configuring Security Policy with Micro-Applications | 116
- Configuring Application Quality-of-Service with Micro-Applications | 118

Configuring Security Policy with Micro-Applications

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 micro-apps
set security policies from-zone untrust to-zone trust policy P1 match source-address any
set security policies from-zone untrust to-zone trust policy P1 match destination-address any
set security policies from-zone untrust to-zone trust policy P1 match application any
```
set security policies from-zone untrust to-zone trust trust policy P1 match dynamic-application
  junos:MODBUS-READ-COILS
set security policies from-zone untrust to-zone trust trust policy P1 match dynamic-application
  junos:MODBUS-WRITE-SINGLE-COIL
set security policies from-zone untrust to-zone trust trust policy P1 match dynamic-application
  junos:MODBUS-WRITE-MULTIPLE-COILS
set security policies from-zone untrust to-zone trust trust policy P1 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.

To configure a custom application group for application identification:

1. Enable micro-applications detection.

   [edit]
   user@host# set services application-identification micro-apps

2. Define a security policy with other policy matching criteria.

   [edit]
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 match source-address any
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 match destination-address any
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 match application any

3. Define application and micro-application as matching criteria.

   [edit]
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 match dynamic-application
     junos:MODBUS-READ-COILS
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 match dynamic-application
     junos:MODBUS-WRITE-SINGLE-COIL
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 match dynamic-application
     junos:MODBUS-WRITE-MULTIPLE-COILS

4. Define the policy action.

   [edit]
   user@host# set security policies from-zone untrust to-zone trust trust policy P1 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.

```
[edit]
user@host# show security policies from-zone untrust to-zone trust
from-zone untrust to-zone trust {
    policy P1 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application [ junos:MODBUS-READ-COILS junos:MODBUS-WRITE-SINGLE-COIL
                              junos:MODBUS-WRITE-MULTIPLE-COILS ];
        }
        then {
            permit;
        }
    }
}
```

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

**Configuring Application Quality-of-Service with Micro-Applications**

**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:


```
[edit]
user@host# set class-of-service application-traffic-control rate-limiters RL1 bandwidth-limit 1000
user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 match application
    junos:MODBUS-READ-COILS
user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 then dscp-code-point 111110
user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 then loss-priority high
user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 then rate-limit client-to-server RL1
user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 then log
```

2. Create a security policy.
3. Define the policy action.

```plaintext
[edit security]
user@host# set security policies from-zone untrust to-zone trust policy 1 match source-address any
user@host# set security policies from-zone untrust to-zone trust policy 1 match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy 1 match application any
```

**Results**

From configuration mode, confirm your configuration by entering the `how class-of-service` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```plaintext
[edit]
user@host# show class-of-service
application-traffic-control {
  rate-limiters RL1 {
    bandwidth-limit 1000;
  }
  rule-sets RS1 {
    rule 1 {
      match {
        application junos:MODBUS-READ-COILS;
      }
      then {
        dscp-code-point 111110;
        loss-priority high;
        rate-limit {
          client-to-server RL1;
        }
        log;
      }
    }
  }
}
```

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.
[edit]
user@host# show security policies from-zone untrust to-zone trust
from-zone untrust to-zone trust {
    policy 1 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application [ junos:MODBUS-READ-COILS];
        }
        then {
            permit {
                application-services {
                    application-traffic-control {
                        rule-set RS1;
                    }
                }
            }
        }
    }
}

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

Verification

Verifying Micro-Applications Status

Purpose
Verify that micro-applications are enabled.

Action
Use the show services application-identification status command to get the details of the micro-applications.

<table>
<thead>
<tr>
<th>Application Identification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Sessions under app detection</td>
<td>0</td>
</tr>
<tr>
<td>Max TCP session packet memory</td>
<td>0</td>
</tr>
<tr>
<td>Force packet plugin</td>
<td>Disabled</td>
</tr>
<tr>
<td>Force stream plugin</td>
<td>Disabled</td>
</tr>
<tr>
<td>Statistics collection interval</td>
<td>1440 (in minutes)</td>
</tr>
</tbody>
</table>

Application System Cache
Verifying Micro-Applications Statistics

Purpose
Verify that micro-application are applied.

Action
Use the show services application-identification statistics applications command to get the details of the micro-applications.

Sample Output

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODBUS-READ-COILS</td>
<td>1</td>
<td>1026</td>
<td>No</td>
</tr>
<tr>
<td>MODBUS-WRITE-SINGLE-COIL</td>
<td>1</td>
<td>1254</td>
<td>No</td>
</tr>
</tbody>
</table>

Last Reset: 2018-12-16 01:45:47 PST
See Also

Understanding Junos OS Application Identification Custom Application Signatures | 86

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2R1</td>
<td>Starting in Junos OS Release 18.2R1, the default behavior of the ASC is changed</td>
</tr>
<tr>
<td>18.2R1</td>
<td>In releases before Junos OS Release 18.2R1, application caching was enabled by default. You can manually disable it by using the <code>set services application-identification no-application-system-cache</code> command.</td>
</tr>
</tbody>
</table>

Related Documentation

Application Identification | 32

Secure Web Proxy

You can use a Juniper Networks SRX Series device to configure secure Web proxy to selectively bypass the external proxy server for the traffic based on application types. Read this topic to understand how secure Web proxy works and how you can configure it on your SRX Series device.

Secure Web Proxy Overview

You can use secure Web proxy to enable traffic for selected applications to bypass the external proxy server and be sent directly to a webserver.
With secure Web proxy configured, when your security device receives a request from a client, the device examines the HTTP header for the application and selectively redirects the request to the webserver based on the application type.

As a result, your security device performs *transparent proxy* between the client and the webserver for the specified applications and provides better quality of service for the application traffic. Bypassing works only for the requests that include a specific application type and are destined to a specific external proxy server.

To use secure Web proxy on an SRX Series device, you must create a secure Web proxy profile. This profile includes the details of the external proxy server and specifies the dynamic application or application group that can bypass the external proxy server.

Starting in Junos OS Release 19.2R1, you can configure secure Web proxy on the following SRX Series devices—SRX300, SRX320, SRX340, SRX345, SRX550, SRX1500, SRX4100, SRX4200, and vSRX.

**Benefit**

- Secure Web proxy provides better quality of service for the selected application traffic by providing direct connections to the webserver

**Limitation**

An SRX Series device operating in chassis cluster mode does not support the secure Web proxy functionality.

**How Secure Web Proxy Works on SRX Series Devices**

*Figure 3 on page 124* and *Figure 5 on page 125* show how an SRX Series device provides the secure Web proxy service.
Figure 3: Secure Web Proxy on SRX Series Device
To use secure Web proxy on your SRX Series device, you must:

1. Create a secure Web proxy profile, which includes the details about the external proxy server and the dynamic application or application group that can bypass the external proxy server.

2. Create a security policy to manage the traffic passing through the device.

3. Attach the secure Web proxy profile to the security policy and apply the profile as an application service for the permitted traffic.

When a client initiates a request, the SRX Series device examines the application traffic and identifies which traffic can bypass the external proxy server based on the secure Web proxy profile and security policy rules.

For example, if you use Microsoft Office 365, you can specify an Office 365 application group, such as junos:OUTLOOK or junos:OFFICE365-CREATE-CONVERSATION, in the secure Web proxy profile. The SRX Series device forwards the Office 365 application traffic directly to the Office 365 server, bypassing...
the external proxy server. Connections that do not match the applications are routed to the external proxy server.

The SRX Series device performs secure Web proxy through the following steps:

1. The client's browser sends an HTTP connect request to the external proxy server.

2. The SRX Series device intercepts the TCP connections. The device identifies the application in the HTTP header and does a DNS resolution.

3. If the traffic parameters match the security policy rules and the secure Web proxy profile specifications, the SRX Series device operates in transparent mode. The device uses the client's IP address in transparent mode to initiate a new connection with the webserver, bypassing the external proxy server.

4. The SRX Series device sends the connect response from the webserver to the client.

5. For the remaining traffic, the SRX Series device operates in pass-through mode and allows the HTTP connect request to go to the external proxy server.

Example—Configure Secure Web Proxy on an SRX Series Device

This example shows how to configure secure Web proxy on SRX Series devices.

Requirements

This example uses the following hardware and software components:

- A Juniper Networks SRX Series device (SRX300, SRX320, SRX340, SRX345, SRX550, SRX1500, SRX4100, SRX4200, or vSRX).
- Junos OS Release 19.2R1 or later. We’ve tested this example using Junos OS Release 19.2R1.
- IP address and port number of the external proxy server.
Overview

Figure 7 on page 127 shows the topology used in this example.

Figure 6: Topology For Configuring Secure Web Proxy

In this example, the interfaces ge-0/0/1 and ge-0/0/2 are in the trust zone and are connected to the client and external proxy server, respectively. The interface ge-0/0/0 is in the untrust zone and is connected to the webserver through the Internet gateway. You configure a secure Web proxy profile, specifying Office 365 applications.

After you complete the configuration, the SRX Series device will forward the Office 365 traffic directly to the webserver, bypassing the external proxy server for Office 365 traffic.

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.

```plaintext
set interfaces ge-0/0/0 unit 0 family inet address 203.0.113.0
set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1
set interfaces ge-0/0/2 unit 0 family inet address 192.0.2.2
set security zones security-zone trust interfaces ge-0/0/0/0.0 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/2.0 host-inbound-traffic system-services all
```
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 the CLI User guide.

In this procedure you configure interfaces and security zones.

1. **Configure the interfaces.**

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 203.0.113.0
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 192.0.2.2
   ```

2. **Assign the interfaces to the security zones and configure the inbound traffic for all system services.**

   ```
   [edit]
   user@host# set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all
   user@host# set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services all
   user@host# set security zones security-zone untrust interfaces ge-0/0/2.0 host-inbound-traffic system-services all
   ```

3. **Configure a custom application group for Office 365.**

   ```
   [edit]
   user@host# set services application-identification application-group office-365-group applications
   junos:OUTLOOK
   user@host# set services application-identification application-group office-365-group applications
   junos:OFFICE365-CREATE-CONVERSATION
   ```
4. Create a security proxy profile by specifying the Office 365 application details and the IP address and port details of the external proxy server.

```plaintext
[edit]
user@host# set services web-proxy secure-proxy profile office365-profile proxy-address external_proxy ip 5.0.0.1/32
user@host# set services web-proxy secure-proxy profile office365-profile proxy-address external_proxy port 8080
user@host# set services web-proxy secure-proxy profile office365-profile dynamic-web-application junos:office-365
user@host# set services web-proxy secure-proxy profile office365-profile dynamic-web-application-group office-365-group
```

5. Define the security policy for the traffic originating from the client to the Internet gateway device.

```plaintext
[edit]
user@host# set security policies from-zone trust to-zone untrust policy 1 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy 1 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy 1 match application any
```

6. Define the policy action to apply the secure Web proxy profile on the traffic that matches the policy rules.

```plaintext
[edit]
user@host# set security policies from-zone trust to-zone untrust policy 1 then permit application-services web-proxy profile-name office365-profile
```

**Results**

From configuration mode, confirm your configuration by entering the `show services web-proxy secure-proxy`, `show security policies`, and `show security zones` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```plaintext
[edit ]
user@host# show services web-proxy secure-proxy
profile office365-profile {
    proxy-address external_proxy {
        ip 5.0.0.1/32;
        port 8080;
    }
    dynamic-web-application junos:office-365
    dynamic-web-application-group office-365-group
```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
  policy 1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          web-proxy {
            profile-name office365-profile;
          }
        }
      }
    }
  }
}

[edit]
user@host# show security zones
security-zone untrust {
  interfaces {
    ge-0/0/0.0 {
      host-inbound-traffic {
        system-services {
          all;
        }
      }
    }
  }
}
security-zone trust {
  interfaces {
    ge-0/0/1.0 {
      host-inbound-traffic {
        system-services {
          all;
        }
      }
    }
  }
}
Verification

Verify Session Details

Purpose
Verify the details of the session in which the secure Web proxy is applied.

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

Meaning
In the sample output, the ID-477 is the client session and the ID-478 is the proxy session. In the second session, notice that the traffic from client 6.0.0.1 is directly going to the webserver 13.107.7.190.

Display Secure Web Proxy Session Statistics

Purpose
Display the details of the session in which the secure Web proxy is applied.
Action
From operational mode, enter the `show services web-proxy session detail` and `show services web-proxy session summary` commands.

```
user@host> show services web-proxy session detail

Web Proxy sessions:
Client Session ID: 38569, Proxy Session ID: 38570
Client: 6.0.0.1/53454 ---> 5.0.0.1/8080
Proxy : 6.0.0.1/53454 ---> 13.107.7.190/443
Proxy Request: CONNECT:www.office.com:443
Dynamic Web App: junos:OFFICE365-CREATE-CONVERSATION

Client Session ID: 38562, Proxy Session ID: 38564
Client: 6.0.0.1/53451 ---> 5.0.0.1/8080
Proxy : 6.0.0.1/53451 ---> 40.126.5.35/443
Proxy Request: CONNECT:login.microsoftonline.com:443
Dynamic Web App: junos:OFFICE365-CREATE-CONVERSATION

Client Session ID: 38567, Proxy Session ID: 38568
Client: 6.0.0.1/53453 ---> 5.0.0.1/8080
Proxy : 6.0.0.1/53453 ---> 13.107.246.10/443
Proxy Request: CONNECT:aadcdn.msauth.net:443
Dynamic Web App: junos:OFFICE365-CREATE-CONVERSATION

Client Session ID: 38571, Proxy Session ID: 0
Client: 6.0.0.1/53455 ---> 5.0.0.1/8080
Proxy : 6.0.0.1/53455 ---> 52.96.40.242/443
Proxy Request: CONNECT:outlook.office365.com:443
Dynamic Web App: junos:OWA

Client Session ID: 38561, Proxy Session ID: 38565
Client: 6.0.0.1/53450 ---> 5.0.0.1/8080
Proxy : 6.0.0.1/53450 ---> 40.126.5.35/443
Proxy Request: CONNECT:login.microsoftonline.com:443
Dynamic Web App: junos:OFFICE365-CREATE-CONVERSATION
```

```
user@host> show services web-proxy session summary

Web Proxy sessions:
Client Session
```

Proxy Session
6.0.0.1/63638 ---> 5.0.0.1/8080
6.0.0.1/63638 ---> 13.107.7.190/443

Meaning
In these samples, notice the details of the client session and the proxy session. You can also see proxy requests and dynamic web applications.
Application Services Modules

Application Firewall | 135
Application Tracking | 167
Application QoS | 188
Advanced Policy-Based Routing | 213
Application Quality of Experience | 283
Application-Based Multipath Routing | 332
Application Firewall

Application firewall (AppFW) provides policy-based enforcement and control on traffic based on application signatures. By using AppFW, you can block any application traffic not sanctioned by the enterprise. For more information, see the following topics:

Application Firewall Overview

Limitations with Stateful Firewalls | 136
Application Firewall | 136
Benefit of Application Firewall | 136
Application Firewall with Unified Policies | 136
Limitations with Stateful Firewalls

Traditionally stateful firewalls used to control applications such as HTTP, SMTP, and DNS because these applications used well-known standards ports only. However, now it is possible to run these applications on any port as long as the client and server are using same protocol and same ports. Because of this standard stateful firewalls are not able to detect evasive applications. 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.

This limitation of stateful firewalls, in which firewalls inspect traffic based on Layer 3 and Layer 4, left open to allow application layer exploits.

Application Firewall

Juniper Networks' application firewall (AppFW) leverages the results from the application identification to make an informed decision to permit, deny, reject, or redirect the traffic based on applications. AppFW enables you to enforce the policy control on Layer 7 traffic.

The AppFW allows you to block the applications based on their application signatures, while still allowing other HTTP traffic to pass through the firewall. For example, an application firewall rule could block HTTP traffic from Facebook but allow Web access to HTTP traffic from MS Outlook.

Benefit of Application Firewall

- Provides granular security control to high-risk applications based on user-defined policies.
- Adds flexibility by providing policy control over application access based on the requirements.

Application Firewall with Unified Policies

Starting in Junos OS release 18.2R1, you can use unified policies to avail the same functionality of an AppFW configuration. Unified policies leverage the application identity information from the application identification (AppID) service to permit, deny, reject, or redirect the traffic. A unified policy configuration handles all application firewall functionality and simplifies the task of configuring a firewall policy.

Read one of the following topic for configuring AppFW:

- If you are using Junos OS version 18.2 and later releases, you must configure Unified policies to get same benefits as traditional AppFW. See "Application Firewall Support with Unified Policies" on page 137.
- If you are using Junos OS version prior to Junos OS 18.2, you can configure traditional AppFW. See "Traditional Application Firewall" on page 145.
Application Firewall Support with Unified Policies

Starting in Junos OS Release 18.2R1, SRX Series devices and vSRX instances support unified policies, allowing granular control and enforcement of Layer 7 dynamic applications within the traditional security policy.

Unified policies are the security policies that enable you to use dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time.

- If you are planning to upgrade to Junos OS Release 18.2R1 and later releases, note the following points regarding using APPFW functionality:
  - All existing AppFW related CLI statements and commands are deprecated. That is—
    Starting in Junos OS Release 18.2R1 Application Firewall (AppFW) functionality is deprecated—rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration. As a part of this change, the [edit security application-firewall] hierarchy and all the configuration options under this hierarchy are deprecated.
  - Configuring a traditional AppFW policy and a unified policy in the same security policy is not supported. The system displays the following error message if you attempt to do so:

    Traditional AppFW and dynamic-application can't be applied to same policy

- If you are downgrading from Junos OS Release 18.2R1 to any earlier versions of Junos OS:
  - You must delete all unified policies to avoid a commit check failure after a downgrade.

For example on configuring a unified policies, see Configuring Unified Security Policies.

SEE ALSO

- Application Identification Support for Unified Policies | 106
Example: Configure Application Firewall with Unified Policy

This example describes how to configure a unified policy to allow or block traffic based on the applications.

System Requirements

System Requirements
This example uses the following hardware and software components:

- SRX Series device running Junos OS Release 18.2R1. This configuration example is tested with Junos OS release 19.1R1.

Before You Begin
- Install a valid application identification feature license on your SRX Series device. See Managing Junos OS Licenses.
- Download and install the Junos OS application signature package. Downloading and Installing the Junos OS Application Signature Package.

Overview

In this example, you create a very common scenario to block certain application and application group such as Yahoo-Mail and Facebook-Access.

Topology
This example uses the topology as shown in Figure 8 on page 139.
This example uses following zones and interfaces configuration.

- The client system is connected to the ge-0/0/0.0 interface with IP address 4.0.0.254/24. It is part of the trust zone.
- The server system is connected to the ge-0/0/1.0 interface with IP address 5.0.0.254/24. It is part of the untrust zone.

Create a security policy configuration to block certain applications using the following steps:

- Create a security policy for the traffic from zone trust to untrust to block the access to the Yahoo-Mail or Facebook-Access applications.
- Create a redirect message for the denied or rejected traffic to inform the user about the status of their request.
- Create a default policy to allow rest of the traffic.

**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 dynamic-application profile profile1 redirect-message type custom-text content "THIS APPLICATION IS BLOCKED"
set security policies from-zone trust to-zone untrust policy policy-1 match source-address any
set security policies from-zone trust to-zone untrust policy policy-1 match destination-address any
set security policies from-zone trust to-zone untrust policy policy-1 match application any
set security policies from-zone trust to-zone untrust policy policy-1 match dynamic-application junos:YAHOO-MAIL
```
set security policies from-zone trust to-zone untrust policy policy-1 match dynamic-application junos:FACEBOOK-ACCESS
set security policies from-zone trust to-zone untrust policy policy-1 then reject profile profile1
set security policies default-policy permit-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet address 4.0.0.254/24
set interfaces ge-0/0/1 unit 0 family inet address 5.0.0.254/24

Step-by-Step Procedure

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 the CLI User guide.

To configure a unified policy using dynamic applications:

1. Configure security zones and interfaces.

   [edit]
   user@host#set security zones security-zone trust host-inbound-traffic system-services all
   user@host#set security zones security-zone trust interfaces ge-0/0/0.0
   user@host#set security zones security-zone untrust host-inbound-traffic system-services all
   user@host#set security zones security-zone untrust interfaces ge-0/0/1.0
   user@host#set interfaces ge-0/0/0 unit 0 family inet address 4.0.0.254/24
   user@host#set interfaces ge-0/0/1 unit 0 family inet address 5.0.0.254/24

2. Create redirect profile.

   [edit]
   user@host#set security dynamic-application profile profile1 redirect-message type custom-text content "THIS APPLICATION IS BLOCKED"

3. Create a security policy with a dynamic application as the match criteria.

   [edit]
   user@host#set security policies from-zone trust to-zone untrust policy policy-1 match source-address any
   user@host#set security policies from-zone trust to-zone untrust policy policy-1 match destination-address any
   user@host#set security policies from-zone trust to-zone untrust policy policy-1 match application any
4. Create a default policy to permit the remaining traffic.

    [edit]
    user@host# set security policies default-policy permit-all

**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.
reject {
  profile profile1;
}
}
}
}
default-policy {
  permit-all;
}
}
}
zones {
  security-zone trust {
    host-inbound-traffic {
      system-services {
        ping;
      }
    }
    interfaces {
      ge-0/0/0.0;
    }
  }
  security-zone untrust {
    host-inbound-traffic {
      system-services {
        ping;
      }
    }
    interfaces {
      ge-0/0/1.0;
    }
  }
}

[edit]

user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 4.0.0.254/24;
    }
  }
}
If you are done configuring the device, enter commit from configuration mode.

Verification

In this section

Verifying Policy Action | 143
Verifying Unified Policy Configuration | 144

Use the following procedures to verify if the policy configuration.

Verifying Policy Action

Purpose
Verify that the unified policy has blocked that configured applications.

Action
From your Web browser, try to access the application. For example, Yahoo-Mail. The system displays the redirect message as shown in the following image.

![Redirect Message](image)

**Meaning**
Whenever the security policy rejects traffic based on the dynamic application, the output displays the redirect message as configured by you in the dynamic application profile.

**Verifying Unified Policy Configuration**

**Purpose**
Verify that the unified policy configuration is correct.

**Action**

From operational mode, enter the `show security policies detail` command to display a detailed summary of all security policies on the device.

```
user@host> show security policies detail
```

```
Default policy: permit-all
Pre ID default policy: permit-all
**Policy: policy-1, action-type: reject**, State: enabled, Index: 7, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source vrf group: any
  Destination vrf group: any
  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 ports: [0-0]

Dynamic Application:
  junos: FACEBOOK-ACCESS: 244
  junos: YAHOO-MAIL: 236
  dynapp-redir-profile: profile1(1)

  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No

Meaning
The output displays information about security policy. Verify the following information:

- Configured policy name policy-1 and policy action reject.
- Configured dynamic applications junos: FACEBOOK-ACCESS and junos: YAHOO-MAIL.
- Redirect profile profile1.

SEE ALSO
  dynamic-application (Security Policies)

Traditional Application Firewall

IN THIS SECTION
  * Understanding How Application Firewall Works | 146
  * Application Firewall Rule Sets and Rules | 146
  * Application Firewall with ALG | 147
  * Unknown Applications | 147
  * Session Logging for Application Firewalls | 147
  * Application Firewall Support in Chassis Cluster | 148
This topic includes the following sections:

**Understanding How Application Firewall Works**

As you can use existing security policy to enforce traditional firewall controls on the traffic, you can use AppFW module to block certain application traffic, based on their application signatures, while still allowing other HTTP traffic to pass through the firewall.

Security device processes traffic in the following sequence when you have configured a AppFW:

1. Security policy matches the zone pair specified in the policy.
2. Security policy matches the packets with matching conditions (source and destination IP addresses, source and destination ports, and application type)
3. Security policy applies one of the following actions to the 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 security device must be reassembled before forwarding.

**Application Firewall Rule Sets and Rules**

Consider following when configuring application firewall:

- You can apply one AppFW rule set to multiple different security policies.
- You can configure an AppFW inside a logical system.
- You can configure multiple dynamic applications in a rule and multiple rules in a rule set. However, there is a limit to the overall number of rule sets and rules.
- You can configure a dynamic application group as match criteria in a rule. An application group includes multiple related applications. For more information, see "Predefined and Custom Application Groups for Application Identification" on page 98.
- The default rule defines the action required for any traffic that does not match any rule. So, a AppFW rule set must contain a default rule.
Application Firewall with ALG

On your security devices, when you enable ALG, application identification includes the ALG results to identify the applications in the control session. AppFW permits ALG data sessions whenever control sessions are permitted. If the control session is denied, there will be no data sessions. If you disable ALG, application identification relies on signatures to identify the application in the control and data sessions. If a signature match is not found, the application is considered unknown. AppFW handles the applications based on the application identification result.

Unknown Applications

Application identification classifies unknown dynamic applications with ID junos:UNKNOWN. AppID uses the reserved keyword junos:UNKNOWN in the following cases

- 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.

Session Logging for Application Firewalls

You can log the traffic by enabling the log option under a security policy. Note the following while you inspect a log message when AppFW is configured as given in Table 7 on page 147:

Table 7: Session Logging for Application Firewall Configuration

<table>
<thead>
<tr>
<th>Security Policy Action</th>
<th>Log Creation</th>
<th>More Details</th>
</tr>
</thead>
</table>
| Permit                 | Creates a session and logs a session create message | When security policy permit action creates a session even before the AppFW rules are applied, log message includes one of the following update:  
- If the application is already identified, its information is added to the session create message.  
- If the application is in the process of being identified, the dynamic application field are updated as UNKNOWN. |
Table 7: Session Logging for Application Firewall Configuration

<table>
<thead>
<tr>
<th>Security Policy Action</th>
<th>Log Creation</th>
<th>More Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject/Deny</td>
<td>Logs reject or deny message, but does not create a session.</td>
<td>When an AppFW rule denies or rejects traffic, the log message includes one of the following phrases in the reason field:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• appfw deny or appfw deny redirect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• appfw reject or appfw reject redirect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• policy deny</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• policy reject</td>
</tr>
</tbody>
</table>

Application Firewall Support in Chassis Cluster

When your security device is in chassis cluster mode, the AppFW action before and after the failover depends on the application identification state, as shown in Table 8 on page 148.

Table 8: Application Firewall Actions

<table>
<thead>
<tr>
<th>Before Failover</th>
<th>Application ID State</th>
<th>Application Firewall Action</th>
<th>After Failover</th>
<th>Application ID State</th>
<th>Application Firewall Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Success</td>
<td>Deny</td>
<td></td>
<td>Success</td>
<td>Deny</td>
</tr>
<tr>
<td></td>
<td>Success</td>
<td>Permit</td>
<td></td>
<td>Success</td>
<td>Permit</td>
</tr>
<tr>
<td></td>
<td>Pending</td>
<td>—</td>
<td>UNKOWN</td>
<td>Action based on the rule defined for unknown application</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If there is no rule defined for unknown, then the default rule is applied</td>
<td></td>
</tr>
</tbody>
</table>

Note the following when you have your security device in chassis cluster mode:

- When you enable application identification, the pre-match state application IDs are not synced to other node. If there are any failover sessions, which were still under classification, will not have any application IDs assigned. This could result in application statistics and counters mismatch.
• In-service software upgrade (unified ISSU) is not supported due to lack of chassis cluster infrastructure support. Thus, the failover event is controlled through the application firewall policy by allowing or denying the unknown dynamic applications.

SEE ALSO

Understanding Security Policy Elements
Security Policies Overview
Understanding Security Policy Rules

Creating Redirects in Application Firewall

When AppFW denies or rejects traffic, it does not notify clients that such action is taken. Clients being unaware that their request is rejected, might keep on trying to access the Web page. To alleviate this inconvenience, the Junos OS allows you to provide an explanation for the action or to redirect the client to an informative webpage. Following examples show you how to create a redirect message.

Redirect with Block Message

Use the block-message option with the reject or deny action in AppFW rule.

```
.....
rule 1 {
    match {
        dynamic-application junos:FACEBOOK-CHAT
    }
    then {
        reject {
            block-message;
        }
    }
}
.....
```

When AppFW rejects the traffic, a splash screen displays the following default message to the user:

```
user-name, Application Firewall has blocked your request to application FACEBOOK-CHAT at dst-ip:dst-port accessed from src-ip:src-port.
```
Customize Redirect Message

You can customize the redirect action by including additional text on the splash screen or by specifying a URL to which you can redirect a user. To customize the block message, you must create a block message profile at [edit security application-firewall] hierarchy level and define the type and content as shown in the following sample.

```
...  
  profile Redirect-Profile {  
    block-message {  
      type {  
        custom-text {  
          content “YOUR APPLICATION IS BLOCKED AS PER THE ORGANIZATION POLICY”;
        }
      }
    }
  }
... 
```

Next, you refer the block message profile in the AppFW rule set, and apply it to one or more of the rules using the `block-message` option;

```
rule-sets Ruleset-1 {  
  rule 1 {  
    match {  
      dynamic-application junos:FACEBOOK-CHAT;
    }  
    then {  
      reject {  
        block-message;
      }
    }
  }  
  profile Redirect-Profile;
}
```

In this case, AppFW displays the configured block message whenever it rejects the traffic based on the configured rule.

Customize Redirect Message with URL

When AppFW rejects or redirects the traffic, you can redirect the client to the specified Web page for further action. The URL can be hosted on either the SRX Series device or an external server.
You can set the redirects to the other server by configuring block-message type as custom-redirect-url as shown in the sample below:

```
profile Redirect-Profile {
    block-message {
        type {
            custom-redirect-url {
                content http://abc.company.com/information;
            }
        }
    }
}
```

Next, you refer the block message profile in the AppFW rule set, and apply to one or more of the rules using the block-message option as shown in the following sample:

```
rule-sets Ruleset-1 {
    rule 1 {
        match {
            dynamic-application junos:FACEBOOK-CHAT;
        }
        then {
            reject {
                block-message;
            }
        }
    }
    profile Redirect-Profile;
}
```

In this case, AppFW redirects the use to the URL http://abc.company.com/information whenever it rejects the traffic based on the configured rule.

### Example: Configuring Application Firewall

**IN THIS SECTION**

- Before You Begin | 152
- Overview | 152
This example shows how to configure application firewall rule sets within the security policy.

**Before You Begin**

- Valid application identification feature license installed on an SRX Series device. See Managing Junos OS Licenses.
- Download and install the Junos OS application signature package. Downloading and Installing the Junos OS Application Signature Package.

**System Requirements**

- SRX Series device with Junos OS Release 15.1X49-D60 or later. This configuration example is tested for Junos OS Release 15.1X49-D60.

**Overview**

In this example, you create application firewall for the following two common scenarios as described in Table 9 on page 152.

**Table 9: Configure Application Firewall to Permit or Deny Traffic**

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Steps to Follows</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block a certain application and allow other applications</td>
<td>Configure a security policy to allow HTTP traffic.</td>
<td>Security policy permits or drops the traffic based on matching specified Layer 3 or Layer 4 criteria.</td>
</tr>
<tr>
<td></td>
<td>Configure an AppFW rule set with following options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rules with dynamic applications that you want to block</td>
<td>AppFW assess the permitted traffic at Layer 7 based on its application ID.</td>
</tr>
<tr>
<td></td>
<td>• Action to deny dynamic application traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default rule to permit other traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer the AppFW rule set in the security policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AppFW blocks the traffic matching the configured dynamic applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default policy permits other traffic.</td>
</tr>
</tbody>
</table>
Table 9: Configure Application Firewall to Permit or Deny Traffic (continued)

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Steps to Follows</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow a certain application and block other applications</td>
<td>Configure a security policy to allow HTTP traffic.</td>
<td>Security policy permits or drops the traffic based on matching specified Layer 3 or Layer 4 criteria.</td>
</tr>
<tr>
<td></td>
<td>Configure an AppFW rule set with following options:</td>
<td>AppFW assess the permitted traffic at Layer 7 based on its application ID.</td>
</tr>
<tr>
<td></td>
<td>• Rules with dynamic applications that you want to permit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Action to permit dynamic application traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default rule to block other traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer the AppFW rule set in the security policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AppFW permits the traffic matching the configured dynamic applications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default policy blocks other traffic.</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: On all SRX Series devices, J-Web pages for AppSecure Services are preliminary. We recommend using CLI for configuration of AppSecure features.

Configuration

Application Firewall Rule to Explicitly Deny Certain Application and Permit All Else

In this example, you block dynamic-applications junos:FACEBOOK-CHAT junos:FACEBOOK-FARMVILLE and allow remaining traffic.

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 any
set security policies from-zone untrust to-zone trust policy policy1 match destination-address any
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 application-firewall rule-sets rs1 rule r1 match dynamic-application
  [junos:FACEBOOK-CHAT,junos:FACEBOOK-FARMVILLE]
set security application-firewall rule-sets rs1 rule r1 then 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. Define the application firewall rule set to deny traffic from selected dynamic applications.

   ```bash
   [edit security application-firewall rule-sets rs1]
   user@host# set rule r1 match dynamic-application [junos:FACEBOOK-CHAT,junos:FACEBOOK-FARMVILLE]
   user@host# set rule r1 then deny
   user@host# set default-rule permit
   ```

2. Configure the security policy to allow HTTP traffic and invoke application firewall rule set rs1.

   ```bash
   [edit security policies from-zone untrust to-zone trust policy policy1]
   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 rs1
   ```

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.
null
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 security 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 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 rs2
   ```

2. Define the application firewall rule set 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: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.

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

Verification

**IN THIS SECTION**

- Verifying Application Firewall Configuration | 157

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

**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 Application Firewall with Application Groups

The application identification (AppID) module manages predefined application groups. An application group includes related applications under a single name for simplified, consistent reuse when using in any application services. An application group can contain multiple applications and application groups simultaneously. It is possible to assign one application to multiple groups.

You can configure a AppFW rule to permit or to deny traffic by specifying a predefined application group along with applications as match criteria.

Advantage of using predefined application groups is - As the application signature database changes, the predefined application group is modified automatically to include new signatures. In this case, if you already have a AppFW rule with predefined application group, the inclusion of new signatures in the application group does not affect the existing AppFW rule.

This example shows how to configure application groups in a AppFW rule set.
Before You Begin

- Install a valid application identification feature license on your SRX Series device. See Managing Junos OS Licenses.
- Download and install the Junos OS application signature package. Downloading and Installing the Junos OS Application Signature Package.

System Requirements

- SRX Series device with Junos OS Release 15.1X49-D60 or later. This configuration example is tested for Junos OS Release 15.1X49-D60.

Overview

In this example, you configure a security policy to control outbound traffic from the trust zone to the untrust zone. Next you create a AppFW rule to allow specific application traffic (junos:GOOGLETALK), but deny all other known similar application traffic (social networking traffic) using application group.

It is very important to note the order of AppFW rules because, the predefined group junos:social-networking includes the junos:GOOGLETALK application. To allow junos:GOOGLETALK traffic and deny the rest of the group, you must place the rule permitting junos:GOOGLETALK traffic before the rule denying traffic from the rest of the applications in the group.

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.

```plaintext
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 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 the rule sequence is very important. You must place the rule with junos:GOOGLETALK before the rule with junos:social-networking. Otherwise, AppFW rule denies even GOOGLETALK traffic along junos:social-networking.

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]
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
            }
        }
    }
}
...
This example describes how to configure a AppFW when you have enabled the SSL proxy.

For **application junos-https**, SSL proxy detects an SSL session based on the dynamic application identified for that session. In case if any known Web servers are running nonstandard ports, you can use a custom Junos OS application to identify the application. However, if the Web servers are not known, for example on the Internet, you can use **application any**. Non-SSL sessions that come across the policy rule are ignored by SSL proxy. A syslog SSL_PROXY_SESSION_IGNORE is sent out for these sessions. Juniper Networks recommends that you use application "any" with caution because this can result in a lot of traffic, incurring initial SSL proxy processing and thereby impacting performance.

The security device bypasses SSL proxy services if when SSL proxy profile is attached to the security rule, when none of the services (AppFW, IDP, or AppTrack) are configured.

**Requirements**

Before you begin:

- Install a valid application identification feature license on your SRX Series device. See Managing Junos OS Licenses.
- Download and install the Junos OS application signature package. Downloading and Installing the Junos OS Application Signature Package.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See Example: Configuring Security Policy Applications and Application Sets.
- Create a SSL proxy profile that enables SSL proxy by means of a policy. See “Configuring SSL Forward Proxy” on page 382.
**System Requirements**

- SRX Series device with Junos OS Release 15.1X49-D60 or later. This configuration example is tested for Junos OS Release 15.1X49-D60.

**Overview**

In this example, you configure two security policies with AppFW rule sets to permit or deny traffic from plain text or encrypted traffic:

- Allow the encrypted version of Oracle and deny any other encrypted traffic.
- Allow all HTTP traffic, except Hulu.

**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 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 match application junos-https
set security policies from-zone Z_1 to-zone Z_2 policy policy1 then permit application-services application-firewall
  rule-set appfw-rs-1
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 policy2 match source-address any
set security policies from-zone Z_1 to-zone Z_2 policy policy2 match destination-address any
set security policies from-zone Z_1 to-zone Z_2 policy policy2 match application junos-http
set security policies from-zone Z_1 to-zone Z_2 policy policy2 then permit application-services application-firewall
  rule-set appfw-rs-2
set security application-firewall rule-sets appfw-rs-1 rule rule1 match dynamic-application [junos:ORACLE]
set security application-firewall rule-sets appfw-rs-1 rule rule1 then permit
set security application-firewall rule-sets appfw-rs-1 rule rule1 then deny
set security application-firewall rule-sets appfw-rs-2 rule rule1 match dynamic-application [junos:HULU]
set security application-firewall rule-sets appfw-rs-2 rule rule1 then deny
set security application-firewall rule-sets appfw-rs-2 default-rule 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 *CLI User Guide*.

1. Configure a security policy to process the traffic with AppFW rule set and SSL proxy profile.

```
[edit security policies from-zone Z_1 to-zone Z_2 policy policy1
 user@host# set match source-address any
 user@host# set match destination-address any
 user@host# set match application junos-https
 user@host# set then permit application-services application-firewall rule-set appfw-rs-1
 user@host# set then permit application-services ssl-proxy profile-name ssl-profile-1
```

2. Configure another security policy with AppFW rule set.

```
[edit security policies from-zone Z_1 to-zone Z_2 policy policy2
 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 appfw-rs-2
```

3. Define the AppFW rule set to permit an encrypted version of Oracle traffic and to deny any other encrypted traffic.

```
[edit security application-firewall rule-sets appfw-rs1]
 user@host# set rule rule1 match dynamic-application [junos:ORACLE]
 user@host# set rule rule1 then permit
 user@host# set default-rule deny
```

4. Define another AppFW rule set to allow all plain text traffic except Hulu.

```
[edit security application-firewall rule-sets appfw-rs2]
 user@host# set rule rule1 match dynamic-application [junos:HULU]
 user@host# set rule rule1 then deny
 user@host# set default-rule permit
```

**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.

If you are done configuring the device, enter `commit` from configuration mode.
NOTE:

**Verifying Application Firewall In an SSL Proxy Enabled Policy**

**Purpose**
Verify that the application is configured correctly when SSL proxy is enabled in a policy.

**Action**
From operational mode, enter the `show security policies` command.

The following output shows the options for the `show security flow session` command.

```
user@host> show security flow session ?
```

Possible completions:
- `<[Enter]>` Execute this command
- `application` Application protocol name
- `application-firewall` Show application-firewall sessions
- `application-firewall-rule-set` Show application firewall sessions matching rule-set name
- `brief` Show brief output (default)
- `destination-port` Destination port (1..65535)
- `destination-prefix` Destination IP prefix or address
- `dynamic-application` Dynamic application name
- `extensive` Show detailed output
- `+ encrypted` Show encrypted traffic
- `family` Show session by family
- `idp` Show idp sessions
- `interface` Name of incoming or outgoing interface
- `nat` Show sessions with network address translation
- `protocol` IP protocol number
- `resource-manager` Show sessions with resource manager
- `session-identifier` Show session with specified session identifier
- `source-port` Source port (1..65535)
- `source-prefix` Source IP prefix or address
- `summary` Show output summary
- `tunnel` Show tunnel sessions
- `|` Pipe through a command
To display SSL encrypted UNKNOWN sessions, use the `show security flow session application-firewall dynamic-application junos:SSL extensive` command.

To display all HTTPS sessions, use the `show security flow session application-firewall dynamic-application junos:HTTP encrypted extensive` command.

SEE ALSO

<table>
<thead>
<tr>
<th>SSL Proxy Overview</th>
<th>351</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Firewall, IDP, and Application Tracking with SSL Proxy Overview</td>
<td>406</td>
</tr>
</tbody>
</table>

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2R1</td>
<td>Starting in Junos OS Release 18.2R1 Application Firewall (AppFW) functionality is deprecated—rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration. As a part of this change, the <code>edit security application-firewall</code> hierarchy and all the configuration options under this hierarchy are deprecated.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

| Application Identification | 32 |
| Application Tracking | 167 |
| Application QoS | 188 |
| Advanced Policy-Based Routing | 213 |
| SSL Proxy | 351 |

Application Tracking

IN THIS SECTION

- Understanding Application Tracking | 168
- Example: Configuring Application Tracking | 177
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 Application Tracking

**IN THIS SECTION**
- Benefits of Application Tracking | 169
- Application Tracking Log Messages Fields | 170

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**

- Provides visibility into the types of applications traversing through your security 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

Starting from Junos OS Release 15.1X49-D100, 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.

Starting from Junos OS Release 15.1X49-D100, a new AppTrack log for route update is added to include 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.

Starting from Junos OS Release 17.4R1, 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.1.1.1.1.2.129 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" 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.1.1.1.1.2.129 source-address="4.0.0.1" source-port="33040" destination-address="5.0.0.1" destination-port="80" service-name="junos-http"
Starting in Junos OS Release 18.4R1 and Junos OS Release 18.3R2, in the APPTRACK_SESSION_ROUTE_UPDATE log, the encrypted field displays the value as N/A as shown in the following sample:

APPTRACK_SESSION_ROUTE_UPDATE [user@host.1.1.1.1 source-address="4.0.0.1" source-port="251" destination-address="5.0.0.1" destination-port="250" service-name="None" application="HTTP" nested-application="UNKNOWN" nat-source-address="4.0.0.1" nat-source-port="251" nat-destination-address="5.0.0.1" nat-destination-port="250" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="rule1" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" source-zone-name="trust" destination-zone-name="untrust" session-id-32="866" username="N/A" roles="DEPT1" encrypted="N/A" profile-name="profile1" rule-name="facebook1" routing-instance="instance1" destination-interface-name="ge-0/0/2.0" category="Web" sub-category="Social-Networking"]

Starting in Junos OS Release 18.4R1, in the APPTACK_SESSION_CLOSE and APPTACK_SESSION_CLOSE_LS log includes the multipath rule name as shown in the following sample:

2018-10-25T01:00:18.179-07:00 multihome-spoke RT_FLOW - APPTACK_SESSION_CLOSE [junos@2636.1.1.2.129 reason="idle Timeout" source-address="19.0.0.2" source-port="34880" destination-address="9.0.0.2" destination-port="80" service-name="junos-http" application="HTTP" nested-application="GOOGLE-GEN" nat-source-address="19.0.0.2" nat-source-port="34880" nat-destination-address="9.0.0.2" nat-destination-port="80" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="rule1" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" source-zone-name="trust" destination-zone-name="untrust1" session-id-32="9628" packets-from-client="347" bytes-from-client="18199" packets-from-server="388" bytes-from-server="131928" elapsed-time="411" username="N/A" roles="N/A" encrypted="N/A" profile-name="apbr-p1" rule-name="rule1" routing-instance="TC1_VPN" destination-interface-name="gr-0/0/0.4" uplink-incoming-interface-name="" uplink-tx-bytes="0" uplink-rx-bytes="0" multipath-rule-name="multi1"]
Starting from Junos OS Release 18.2R1, AppTrack session close logs include new fields to record the packet bytes transmitted and received through the uplink interfaces. The packet bytes transmitted and received through the uplink interfaces are reported by `uplink-tx-bytes`, `uplink-rx-bytes`, and `uplink-incoming-interface-name` fields.

Example:

```plaintext
APPTTRACK_SESSION_CLOSE [user@host.1.1.2.137 reason="TCP FIN" source-address="4.0.0.1" source-port="40297" destination-address="5.0.0.1" destination-port="110" service-name="junos-pop3" application="POP3" nested-application="UNKNOWN" nat-source-address="4.0.0.1" nat-source-port="40297" nat-destination-address="5.0.0.1" nat-destination-port="110" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="permit-all" source-zone-name="UNTRUST" destination-zone-name="TRUST" session-id-32="81" packets-from-client="7" bytes-from-client="1959" packets-from-server="6" bytes-from-server="68643" elapsed-time="130" username="N/A" roles="N/A" encrypted="No" profile-name="pf1" rule-name="facebook1" routing-instance="instance1" destination-interface-name="gr-0/0/0.0" uplink-tx-bytes="1959" uplink-rx-bytes="68643" uplink-incoming-interface-name="gr-0/0/0.0"]
```

A new syslog message `RT_FLOW_NEXTHOP_CHANGE` is generated whenever there is a change in the route or in the next-hop on the APBR and AppTrack enabled sessions.

Starting from Junos OS Release 18.2R1, new application tracking messages are added for AppQoE (application quality of experience). The new Apptrack messages provide information such as active and passive metric report, switching of application traffic path as shown in the following samples:

```plaintext
APPQOEBEST_PATH_SELECTED [junos@2636.1.1.2.129 source-address="20.1.1.1" source-port="47335" destination-address="151.101.9.67" destination-port="443" apbr-profile="apbrProf1" apbr-rule="rule1" application="HTTP" nested-application="CNN" group-name="N/A" service-name="junos-https" protocol-id="6" source-zone-name="trust" destination-zone-name="untrust" session-id-32="611" username="N/A" roles="N/A" routing-instance="ri3" destination-interface-name="gr-0/0/0.2" ip-dscp="0" sla-rule="SLA1" elapsed-time="2" bytes-from-client="675" bytes-from-server="0" packets-from-client="7" packets-from-server="0" previous-interface="gr-0/0/0.2" active-probe-params="PP1" destination-group-name="p1"]

APPQOE_PASSIVE_SLA_METRIC_REPORT [junos@2636.1.1.2.129 source-address="20.1.1.1" source-port="47335" destination-address="151.101.9.67" destination-port="443" apbr-profile="apbrProf1" apbr-rule="rule1" application="HTTP" nested-application="CNN" group-name="N/A" service-name="junos-https" protocol-id="6" source-zone-name="trust" destination-zone-name="untrust" session-id-32="611" username="N/A" roles="N/A" routing-instance="ri3" destination-interface-name="gr-0/0/0.2" ip-dscp="0" sla-rule="SLA1" ingress-jitter="0" egress-jitter="0" rtt-jitter="0" rtt="0" pkt-loss="0" bytes-from-client="1073" bytes-from-server="6011" packets-from-client="12" packets-from-server="13" monitoring-time="990" active-probe-params="PP1" destination-group-name="p1"]

APPQOE_SLA_METRIC_VIOLATION [junos@2636.1.1.2.129 source-address="20.1.1.1" source-port="35264" destination-address="151.101.193.67" destination-port="443"
```


Starting in Junos OS Release 15.1X49-D170, AppTrack session create, session close, route update, and volume update logs are enhanced to include VRF-name for both Source-VRF and Destination-VRF. The new Apptrack messages provide information such as VRF-name for both Source-VRF and Destination-VRF as shown in the following sample:

```
<14>12018-10-03T00:35:22.015-07:00 pdt-porter-vsr4 RT_FLOW -
APPTrack_SESSION_ROUTE_UPDATE [junos@2636.1.1.1.2.129 source-address="1.3.0.10" source-port="990" destination-address="8.3.0.10" destination-port="8080" application="HTTP" policy-name="1" protocol-id="6" nat-source-address="1.3.0.10" nat-destination-address="8.3.0.10" nat-source-port="8080" nat-destination-port="8080" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" src-nat-rule-name="N/A" dst-nat-rule-name="N/A"

<14>12018-10-03T00:35:22.015-07:00 pdt-porter-vsr4 RT_FLOW -
APPTrack_SESSION_CREATE [junos@2636.1.1.1.2.129 source-address="1.3.0.10" source-port="990" destination-address="8.3.0.10" destination-port="8080" application="HTTP" policy-name="1" protocol-id="6" nat-source-address="1.3.0.10" nat-destination-address="8.3.0.10" nat-source-port="8080" nat-destination-port="8080" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" src-nat-rule-name="N/A" dst-nat-rule-name="N/A" src-nat-rule-name="N/A" dst-nat-rule-name="N/A"

<14>12019-01-21T04:51.036-08:00 idpdevsx6-vsr2-10 RT_FLOW -
APPTrack_SESSION_VOL_UPDATE [junos@2636.1.1.1.2.129 source-address="4.0.0.1"
```
Starting in Junos OS Release 19.1R1, AppTrack session close logs include new field source identity to check the session create log and session close log with user name and roles. The new Aptrack messages provide information such as user name and roles as shown in the following sample:

APPQOE_BEST_PATH.Selected [junos@2636.1.1.2.129 source-address="20.1.1.1" source-port="47335" destination-address="151.101.9.67" destination-port="443" apbr-profile="apbrProf1" apbr-rule="rule1" application="HTTP" nested-application="CNN" group-name="N/A" service-name="junos-https" protocol-id="6" source-zone-name="trust" destination-zone-name="untrust" session-id-32="611" username="N/A" roles="N/A" routing-instance="ri3" destination-interface-name="ge-0/0/0.2" ip-dscp="0" sla-rule="SLA1" elapsed-time="2" bytes-from-client="675" bytes-from-server="0" packets-from-client="7" packets-from-server="0" previous-interface="gr-0/0/0.2" active-probe-params="PP1" destination-group-name="p1"]

Starting in Junos OS Release 19.3R1, AppTrack session logs such as session close, volume update, route update, and RT_FLOW_NEXTHOP_CHANGE include dscp-value and apbr-rule-type options.
• **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="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" 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"

destination-interface-name="st0.0" dscp-value="13" apbr-rule-type="dscp"

• **APPTRACK_SESSION_ROUTE_UPDATE** [junos@2636.1.1.1.2.129 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" dscp-value="13" apbr-rule-type="application-dscp"

• **APPTRACK_SESSION_VOL_UPDATE** [junos@2636.1.1.1.2.129 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" dscp-value="13" apbr-rule-type="application-dscp"

• **RT_FLOW_NEXTHOP_CHANGE** [junos@2636.1.1.1.2.129 source-address="4.0.0.1" source-port="1999"

destination-address="157.240.23.35" destination-port="80" service-name="junos-http"

application="UNKNOWN" nested-application="UNKNOWN" nat-source-address="4.0.0.1"

nat-port="1999" nat-destination-address="157.240.23.35" nat-destination-port="80"

src-nat-rule-name="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="1"

source-zone-name="trust" destination-zone-name="untrust" session-id-32="3287"

packets-from-client="1" bytes-from-client="60" packets-from-server="0" elapsed-time="0"

username="N/A" roles="N/A" encrypted="No" profile-name="profile1"

rule-name="rule1" routing-instance="R11" destination-interface-name="ge-0/0/1.0"

last-destination-interface-name="ge-0/0/4.0" uplink-incoming-interface-name=""

last-incoming-interface-name="N/A" uplink-tx-bytes="0" uplink-rx-bytes="0" apbr-policy-name="sla1"

dscp-value="13" apbr-rule-type="dscp"

Starting in Junos OS Release 20.1R1, AppTrack session logs such as session close, volume update, route
update include apbr-rule-type options.
• **APPTRACK_SESSION_VOL_UPDATE** [junos@2636.1.1.1.2.129 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" apbr-rule-type="default"]

• **APPTRACK_SESSION_ROUTE_UPDATE** [junos@2636.1.1.1.2.129 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" apbr-rule-type="default"]

• **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="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" 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" destination-interface-name="st0.0" apbr-rule-type="default"]

**SEE ALSO**

- Example: Configuring Application Tracking | 177
- Disabling AppTrack | 37
- Understanding Application Identification Techniques | 32
Example: Configuring Application Tracking

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" on page 61 or "Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package" on page 66. 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: J-Web pages for AppSecure Services are preliminary. 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: On SRX5600, and SRX5800 devices, 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
```
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 (...).

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

**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
```

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>1</td>
<td>2291</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTP</td>
<td>1</td>
<td>942</td>
<td>No</td>
</tr>
<tr>
<td>SSL</td>
<td>1</td>
<td>2291</td>
<td>Yes</td>
</tr>
<tr>
<td>unknown</td>
<td>1</td>
<td>100</td>
<td>No</td>
</tr>
<tr>
<td>unknown</td>
<td>1</td>
<td>100</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>AVT counters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session create messages</td>
<td>1</td>
</tr>
<tr>
<td>Session close messages</td>
<td>1</td>
</tr>
<tr>
<td>Session volume updates</td>
<td>0</td>
</tr>
<tr>
<td>Failed messages</td>
<td>0</td>
</tr>
</tbody>
</table>

**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)`

### Example: Configuring Application Tracking When SSL Proxy Is Enabled

**IN THIS SECTION**

- Requirements | 184
- Overview | 184
- Configuration | 184
This example 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” on page 382.

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.

```plaintext
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” on page 163.

SEE ALSO

- SSL Proxy Overview | 351
- Application Firewall, IDP, and Application Tracking with SSL Proxy Overview | 406
Disabling Application Tracking

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.
## Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.3R1</td>
<td>Starting in Junos OS Release 19.3R1, AppTrack session logs such as session close, volume update, route update, and RT_FLOW_NEXTHOP_CHANGE include <strong>dscp-value</strong> and <strong>apbr-rule-type</strong> options.</td>
</tr>
<tr>
<td>19.3R1</td>
<td>Starting in Junos OS Release 20.1R1, AppTrack session logs such as session close, volume update, route update include <strong>apbr-rule-type</strong> options.</td>
</tr>
<tr>
<td>19.1R1</td>
<td>Starting in Junos OS Release 19.1R1, AppTrack session close logs include new field source identity to check the session create log and session close log with user name and roles.</td>
</tr>
<tr>
<td>18.2R1</td>
<td>Starting from Junos OS Release 18.2R1, AppTrack session close logs include new fields to record the packet bytes transmitted and received through the uplink interfaces.</td>
</tr>
<tr>
<td>18.2R1</td>
<td>Starting from Junos OS Release 18.2R1, new application tracking messages are added for AppQoE (application quality of experience).</td>
</tr>
<tr>
<td>17.4R1</td>
<td>Starting from Junos OS Release 17.4R1, AppTrack session create, session close, and volume update logs include the new fields <strong>category</strong> and <strong>subcategory</strong></td>
</tr>
<tr>
<td>15.1X49-D170</td>
<td>Starting in Junos OS Release 15.1X49-D170, AppTrack session create, session close, route update, and volume update logs are enhanced to include VRF-name for both Source-VRF and Destination-VRF.</td>
</tr>
<tr>
<td>15.1X49-D100</td>
<td>Starting from Junos OS Release 15.1X49-D100, AppTrack session create, session close, and volume update logs include a new field called <strong>destination interface</strong>.</td>
</tr>
<tr>
<td>15.1X49-D100</td>
<td>Starting from Junos OS Release 15.1X49-D100, a new AppTrack log for route update is added to include APBR profile, rule, and routing instance details.</td>
</tr>
</tbody>
</table>

### RELATED DOCUMENTATION

- Application Identification | 32
- Application Firewall | 135
- Application QoS | 188
- Advanced Policy-Based Routing | 213
- SSL Proxy | 351
Application QoS

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

**Understanding Application Quality of Service (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 the security 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 User Guide (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 User Guide (Security Devices) for information about configuring queues and schedulers.)

For SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, 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
```

For SRX100, SRX210, SRX220, SRX240, SRX550, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX650, SRX1500, SRX4100, SRX4200, and SRX4600 devices and vSRX instances, 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 queue queue-number forwarding-class-name
```

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 10 on page 190 provides a list of Junos OS default DSCP alias names and bitmap values.

**Table 10: Standard CoS Aliases and Bit Values**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Bit Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>101110</td>
</tr>
<tr>
<td>af11</td>
<td>001010</td>
</tr>
<tr>
<td>af12</td>
<td>001100</td>
</tr>
<tr>
<td>af13</td>
<td>001110</td>
</tr>
<tr>
<td>af21</td>
<td>010010</td>
</tr>
<tr>
<td>af22</td>
<td>010100</td>
</tr>
</tbody>
</table>
See Default CoS Values and Aliases for more details.

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 User Guide (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**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Bit Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>af23</td>
<td>010110</td>
</tr>
<tr>
<td>af31</td>
<td>011010</td>
</tr>
<tr>
<td>af32</td>
<td>011100</td>
</tr>
<tr>
<td>af33</td>
<td>011110</td>
</tr>
<tr>
<td>af41</td>
<td>100010</td>
</tr>
<tr>
<td>af42</td>
<td>100100</td>
</tr>
<tr>
<td>af43</td>
<td>100110</td>
</tr>
<tr>
<td>be</td>
<td>000000</td>
</tr>
<tr>
<td>cs1</td>
<td>001000</td>
</tr>
<tr>
<td>cs2</td>
<td>010000</td>
</tr>
<tr>
<td>cs3</td>
<td>011000</td>
</tr>
<tr>
<td>cs4</td>
<td>100000</td>
</tr>
<tr>
<td>cs5</td>
<td>101000</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110000</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111000</td>
</tr>
</tbody>
</table>
• 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:

<table>
<thead>
<tr>
<th>Rate Limiter Name</th>
<th>Profile</th>
<th>bandwidth-limit</th>
<th>burst-size-limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>limiter-1</td>
<td></td>
<td>200</td>
<td>26000</td>
</tr>
<tr>
<td>limiter-2</td>
<td></td>
<td>200</td>
<td>26000</td>
</tr>
<tr>
<td>limiter-3</td>
<td></td>
<td>200</td>
<td>26000</td>
</tr>
<tr>
<td>limiter-4</td>
<td></td>
<td>400</td>
<td>52000</td>
</tr>
<tr>
<td>Rate Limiter Name</td>
<td>Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bandwidth-limit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>limiter-5</td>
<td>400</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>burst-size-limit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>52000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

```bash
[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 security 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 SRX Series 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
```

• This option is supported only on for SRX300, SRX320, SRX340, SRX345 devices.

### 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*
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: J-Web pages for AppSecure Services are preliminary. 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.

For SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, use the following command:

```
[edit]
user@host# set class-of-service forwarding-classes class my-app-fc queue-num 0
```
For SRX100, SRX210, SRX220, SRX240, SRX550, SRX300, SRX320, SRX340, SRX345, SRX550M, SRX650, and SRX1500 devices, use the following command:

```bash
[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:** For SRX5400, SRX5600, and SRX5800 devices, 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

```bash
[edit]
user@host# set class-of-service application-traffic-control rate-limiters test-r1 bandwidth-limit 100
user@host# set class-of-service application-traffic-control rate-limiters test-r1 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.

```bash
[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.

```bash
[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 (...).

```plaintext
... 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

<table>
<thead>
<tr>
<th>IN THIS SECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying Flow Session Configuration</td>
</tr>
<tr>
<td>Verifying Session Statistics</td>
</tr>
<tr>
<td>Verifying Rate-Limiter Statistics</td>
</tr>
<tr>
<td>Verifying Rule Statistics</td>
</tr>
</tbody>
</table>

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
```
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

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Application</th>
<th>Client-to-server Rate(kbps)</th>
<th>Server-to-client Rate(kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp-test1</td>
<td>HTTP</td>
<td>test-r2</td>
<td>200</td>
</tr>
<tr>
<td>ftp-test1</td>
<td>HTTP</td>
<td>test-r2</td>
<td>200</td>
</tr>
<tr>
<td>ftp-test1</td>
<td>FTP</td>
<td>test-r1</td>
<td>100</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Rule</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp-test1</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>ftp-test1</td>
<td>1</td>
<td>200</td>
</tr>
</tbody>
</table>

pic: 2/0

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Rule</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp-test1</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>ftp-test1</td>
<td>1</td>
<td>200</td>
</tr>
</tbody>
</table>
```

**Meaning**
This command provides information on the number of (session) hits for a rule under each rule set.
Application Quality of Service Support for Unified Policies

Starting in Junos OS Release 18.2R1, SRX Series devices and vSRX instances support unified policies, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy.

Unified policies are the security policies that enable you to use dynamic applications as part of the existing 5-tuple or 6-tuple (5-tuple with a user firewall) match conditions to detect application changes over time.

Application quality of service (AppQoS) is supported when the security device is configured with unified policies. You can configure a default AppQoS rule set to manage unified policy conflicts if multiple security policies match the traffic.

AppQoS rule sets are included in the unified policy to implement application-aware quality-of-service control. You can configure a rule set with rules under the `application-traffic-control` option, and attach the AppQoS rule set to a unified security policy as an application service. If the traffic matches the specified dynamic application and the policy action is permit, the application-aware quality of service is applied.

Note the following AppQoS functionality in unified policies:

- Upgrading from traditional security policy to a unified policy—In a unified policy, when you configure the `dynamic-application` option as `none`, the AppQoS rule set is applied during the security policy match and the AppQoS looks for the corresponding rule for the identified traffic. This is the same behavior for AppQoS functionality in Junos OS releases prior to Release 18.2R1.

- AppQoS rule with a unified policy—In the application traffic control configuration, the AppQoS rule set is configured with the match condition as `application-any` and in the unified policy, a specific dynamic application is used as the match condition, then, the AppQoS functionality works according to the rule in the unified policy.

Understanding Default Application Quality of Service Rule Set for Unified Policies

You can configure an AppQoS default rule set to manage security policy conflicts.

The initial policy lookup phase occurs prior to identifying a dynamic application. If there are multiple policies present in the potential policy list that contain different AppQoS rule sets, then the security device applies the default AppQoS rule set until a more explicit match has occurred.
You can set an AppQoS as a default AppQoS rule set under the edit security ngfw hierarchy level. The default AppQoS rule set is leveraged from one of the existing AppQoS rule sets, which are configured under the [edit class-of-service application-traffic-control] hierarchy level.

Table 11 on page 204 summarizes the usage of the default AppQoS rule set under different scenarios in a unified policy.

**Table 11: AppQoS Rule Set Usage in Unified Policies**

<table>
<thead>
<tr>
<th>Application Identification Status</th>
<th>AppQoS Rule Set Usage</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No security policy conflict.</td>
<td>The AppQoS rule set under the [edit class-of-service application-traffic-control] hierarchy is applied when the traffic matches the security policy.</td>
<td>AppQoS is applied as in the AppQoS rule set.</td>
</tr>
<tr>
<td>Security policy conflict and conflicting polices have distinct AppQoS rule sets.</td>
<td>The default AppQoS rule set is not configured or is not found.</td>
<td>Session is ignored because the default AppQoS profile is not configured. As a result, even if the final matched policy in the policy conflict scenario has an AppQoS rule set, this rule set is not applied. We recommend configuring a default AppQoS rule set to manage security policy conflicts.</td>
</tr>
<tr>
<td>Final application is identified</td>
<td>The default AppQoS rule set is configured.</td>
<td>AppQoS is applied as in the default AppQoS rule set.</td>
</tr>
<tr>
<td></td>
<td>The matching security policy has an AppQoS rule set, which is same as the default AppQoS rule set.</td>
<td>AppQoS is applied as in the default AppQoS rule set.</td>
</tr>
<tr>
<td></td>
<td>The matching security policy does not have an AppQoS rule set.</td>
<td>Default AppQoS rule set is not applied and AppQoS is not applied for the session.</td>
</tr>
<tr>
<td></td>
<td>The Matching security policy has an AppQoS rule set different from the default AppQoS rule set, which is already applied.</td>
<td>Default AppQoS rule set remains as the default AppQoS rule set.</td>
</tr>
</tbody>
</table>

When a default AppQoS rule set is applied on the traffic and the final security policy has a different AppQoS rule set, in such cases switching from the default AppQoS rule set to the AppQoS rule set in the final security policy is not supported.
Default Application Quality of Service Rule Set In Different Scenarios

The following links are to examples that discuss the default AppQoS rule sets in different scenarios:

Table 12 on page 205 shows different AppQoS rule sets that are configured for unified policies with dynamic applications as the match condition.

**Table 12: Different AppQoS Rule Sets in Unified Policies**

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Defined Zone</th>
<th>Defined IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>AppQoS Rule Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>AppQoS</td>
<td>AppQoS-2</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>AppQoS</td>
<td>AppQoS-3</td>
</tr>
</tbody>
</table>

In this example, any AppQoS rule sets (AppQoS-1, AppQoS-2, AppQoS-3) can be configured as a default AppQoS rule set under the [security ngfw] hierarchy level. It is not necessary for a default rule set to be part of a security policy configuration. Any AppQoS rule set under the [edit class-of-service application-traffic-control] hierarchy level can be assigned as the default AppQoS rule set.

**No Policy Conflict—All Policies Have the Same AppQoS Rule Set**

All matching policies have the same AppQoS rule set as shown in Table 13 on page 206.
### Table 13: All Matching Policies Have Same AppQoS Rule Sets

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>AppQoS Rule Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
</tbody>
</table>

In this scenario, the policies Policy-P1 and Policy-P2 have the same AppQoS rule set; that is, AppQoS-1. The rule set AppQoS-1 is applied. Policy-P3 is not configured in this scenario.

If you have configured the rule set AppQoS-2 as the default rule set, it is not applied. That's because there is no conflict in the AppQoS rule sets in the conflicted policies (Policy-P1 and Policy-P2).

**No Policy Conflict—All Policies Have the Same AppQoS Rule Set and the Final Policy Has No AppQoS Rule Set**

All matching policies have the same AppQoS rule set as shown in Table 14 on page 206 and the final policy has no AppQoS rule set.

### Table 14: All Matching Policies Have Same AppQoS Rule Sets and the Final Policy Has No AppQoS Rule Set

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>AppQoS Rule Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>Other</td>
<td>None</td>
</tr>
</tbody>
</table>

In this scenario, both Policy-P1 and Policy-P2 have the same AppQoS rule set, that is, AppQoS-1. In this case, the rule set AppQoS-1 is applied.

When the final policy Policy-P3 is matched, AppQoS ignores the session, because the AppQoS rule set is not configured for Policy-P3.

If the final security policy does not have any AppQoS rule set, then AppQoS is not applied on the traffic. All AppQoS settings that are applied in the prematch stage are reverted to the original values.

**Policy Conflict—No AppQoS Rule Set is Configured for the Final Policy**

The default AppQoS rule set (in this scenario AppQoS-1) is applied during the potential policy match as shown in Table 15 on page 207. The final policy Policy-P3 has no AppQoS rule set.
Table 15: Matching Policies Have Different AppQoS Rule Sets and the Final Policy Has No AppQoS Rule Set

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>AppQoS Rule Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>AppQoS</td>
<td>AppQoS-2</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>Other</td>
<td>NA</td>
</tr>
</tbody>
</table>

AppQoS ignores the session if the final matching policy Policy-P3 is applied.

If the final security policy does not have any AppQoS rule set, then AppQoS is not applied on the traffic. In this case, all AppQoS settings that are applied in the prematch stage are reverted to the original values.

**Policy Conflict—Default AppQoS Rule Set and a Different AppQoS Rule Set for the Final Policy**

The ruleset AppQoS-1 is configured as a default rule set and is applied when the final application is not yet identified. The final policy Policy-P3 has a different AppQoS rule set (AppQoS-3) as shown in Table 16 on page 207.

Table 16: Different AppQoS Rule Set for the Final Policy

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>AppQoS Rule Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>AppQoS</td>
<td>AppQoS-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>AppQoS</td>
<td>AppQoS-2</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>AppQoS</td>
<td>AppQoS-3</td>
</tr>
</tbody>
</table>

When the final application is identified, the policy Policy-P3 is matched and applied. In this case, the rule set AppQoS-3 is not applied. Instead the rule set AppQoS-1 is applied as the default rule set and remains as the default rule set.

**Limitation of AppQoS with Unified Policies**

When a security policy is applied to the matching traffic, the AppQoS rule set is applied to the permitted traffic. If the security policy and the applied AppQoS rule set have different dynamic applications, then a conflict might occur as shown in the following example:
In this example, the application traffic control rule is configured for junos:GOOGLE and the security policy match condition for the dynamic application is junos: FTP. In such cases, conflicts might occur when the final policy is applied.

SEE ALSO

- Application Identification Support for Unified Policies | 106

**Example: Configuring Application Quality of Service with Unified Policy**

**IN THIS SECTION**

- Requirements | 209
- Overview | 209
- Configuration | 209
- Verification | 211

This example shows how to enable application quality of service (AppQoS) within a unified policy to provide prioritization and rate limiting for the traffic.
Requirements

This example uses the following hardware and software components:

- SRX Series device running Junos OS Release 18.2R1 and later. This configuration example is tested for Junos OS Release 18.2R1.

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

Overview

In this example, you configure an AppQoS rule set and invoke AppQoS as an application service in the security policy for the Facebook application.

You define a default AppQoS rule set under the [edit security ngfw] hierarchy level to manage security policy conflicts, if any.

Configuration

Step-by-Step Procedure

To configure AppQoS with a unified policy:

1. Define an AppQoS rule set.

   ```
   [edit]
   user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 match application junos:FACEBOOK-APP
   user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 then forwarding-class fc-appqos loss-priority medium-low dscp-code-point 101110 log
   user@host# set class-of-service application-traffic-control rule-sets RS1 rule 1 then rate-limit client-to-server Ratelim1
   user@host# set class-of-service application-traffic-control rate-limiters Ratelim1 bandwidth-limit 1000
   ```

2. Configure a default AppQoS rule set. Select the rule set RS1 that is created under the application traffic control as the default AppQoS rule set.

   ```
   [edit]
   user@host# set security ngfw default-profile application-traffic-control rule-set RS1
   ```

3. Associate the class-of-service rule set to the unified policy.

   ```
   [edit]
   ```
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 (...).

```
... policies {
    from-zone trust to-zone untrust {
        policy permit-all {
            match {
                source-address any;
                destination-address any;
                application any;
                dynamic-application junos:FACEBOOK-APP;
            }
            then {
                permit {
                    application-services {
                        application-traffic-control {
                            rule-set RS1;
                        }
                    }
                }
            }
        }
    }
...```
ngfw {
    default-profile {
        application-traffic-control {
            rule-set RS1;
        }
    }
}

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

Verification

**IN THIS SECTION**

- Verifying Flow Session Configuration | 211
- Verifying Rule Statistics | 212

Confirm that the configuration is working properly.

**Verifying Flow Session Configuration**

**Purpose**
Display AppQoS session statistics.

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

**Sample Output**

```
pic: 0/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>2</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>1</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>1</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>1</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>1</td>
</tr>
</tbody>
</table>
```
### Meaning
The output displays the number of sessions processed, marked, and honored. The rate-limiting statistics count the number of directional session flows that have been rate limited.

### Verifying Rule Statistics

#### Purpose
Display the AppQoS 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
```

<table>
<thead>
<tr>
<th>pic: 0/0</th>
<th>Ruleset</th>
<th>Rule</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Meaning
The output provides information on the number of sessions matched for the rule under each AppQoS rule set.

### SEE ALSO
- `ngfw | 577`

### RELATED DOCUMENTATION
- Application Identification | 32
- Application Firewall | 135
- Application Tracking | 167
- Advanced Policy-Based Routing | 213
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**

IN THIS SECTION

- Application Identification  | 214
- Filter-Based Forwarding or Policy-Based Routing (PBR)  | 214
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.

Starting with Junos OS Release 15.1X49-D60, SRX Series Services Gateways support advanced policy-based routing (APBR) to address these challenges.

This topic includes the following sections:

**Application Identification**

Juniper Networks security 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)**

Security 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 9 on page 216 shows the sequence in which APBR techniques are applied.

Figure 9: 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**

Starting with Junos OS Release 15.1X49-D110 and Junos OS Release 17.4R1, SRX Series Services gateways 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 10 on page 218* shows the sequence in which APBR techniques with midstream support are applied.
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 Application Tracking" on page 168 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 requires 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.

Support for reverse rerouting is available starting in Junos OS Release 15.1X49-D130 and later releases.

**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:

• Redirecting the route for the traffic depends on the presence of an entry in the application system cache (ASC). Routing will succeed only if the ASC lookup is successful. For the first session, when the ASC is not present for the traffic, the traffic traverses through a default route (non-APBR route) to the destination (this limitation is applicable only for the releases before Junos OS 15.1X49-D110).

• 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.

SEE ALSO

Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution | 222
Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution

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

Requirements

This example uses the following hardware and software components:

- Valid application identification feature license installed on an SRX Series device.
- SRX Series device with Junos OS Release 15.1X49-D60 or later. This configuration example is tested for Junos OS Release 15.1X49-D60.

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 11 on page 223 shows the topology used in this configuration example.
Figure 11: Topology For Advanced Policy-Based Routing (APBR)

Table 17 on page 223 provides the details of the parameters used in this example.

Table 17: APBR Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Instance</td>
<td></td>
<td>Routing instance of type forwarding is used for forwarding the traffic.</td>
</tr>
<tr>
<td></td>
<td>Instance name—R1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instance type— forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static route— 1.0.0.254/8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next-hop— 1.0.0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instance name—R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instance type— forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static route— 2.0.0.254/8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next-hop— 2.0.0.1</td>
<td></td>
</tr>
<tr>
<td>RIB Group</td>
<td>apbr_group</td>
<td>Name of the routing information base (RIB) (also known as routing table) group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This RIB group is configured to import interface route entries from inet.0, RI1.inet.0, RI2.inet.0, and RI3.inet.0.</td>
</tr>
<tr>
<td>APBR Profile</td>
<td>profile-1</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 17: APBR Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rule name—ruleApp1</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• matching application—junos:HTTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Associated routing instance—R1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rule name—ruleApp2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• matching application—junos:web:social-networking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Routing instance—R2</td>
<td></td>
</tr>
</tbody>
</table>

| 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.

```plaintext
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 SRX 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-0/0/1.0
set security zones security-zone trust interfaces ge-0/0/2.0
set security zones security-zone trust advanced-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-0/0/1.0
   user@host# set security zones security-zone trust interfaces ge-0/0/2.0
   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.

```plaintext
[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;
        }
    }
```
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.

<table>
<thead>
<tr>
<th>Advance Profile Based Routing statistics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Processed:</td>
</tr>
<tr>
<td>ASC Success:</td>
</tr>
<tr>
<td>Rule match success:</td>
</tr>
<tr>
<td>Route modified:</td>
</tr>
<tr>
<td>AppID Requested:</td>
</tr>
</tbody>
</table>

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.

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

Starting in Junos OS Release 18.2R1, 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 includes the set of rules that contains set of dynamic applications and dynamic 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**

**IN THIS SECTION**

- Requirements | 232
- Overview | 232
- Configuration | 232
- Verification | 236
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:

- SRX Series device with Junos OS Release 18.2R1 or later. This configuration example is tested on Junos OS Release 18.2R1.
- Valid application identification feature license installed on an SRX Series device.

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-0/0/1.0
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.
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 R1.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-0/0/1.0;
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.

<table>
<thead>
<tr>
<th>Sessions Processed</th>
<th>18994</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppID cache hits</td>
<td>18994</td>
</tr>
<tr>
<td>AppID requested</td>
<td>0</td>
</tr>
<tr>
<td>Rule matches</td>
<td>0</td>
</tr>
<tr>
<td>Route changed on cache hits</td>
<td>0</td>
</tr>
<tr>
<td>Route changed midstream</td>
<td>0</td>
</tr>
<tr>
<td>Zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Drop on zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Next hop not found</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 | 213
Understanding URL Category-Based Routing

Starting in Junos OS Release 18.3 R1, URL category-based routing is supported on SRX Series devices and vSRX instances. URL category-based routing enables you to use URL categories as match criteria in an APBR profile. The URL categories are based on the destination server IP address, and the category identification is leveraged from the Enhanced Web Filtering (EWF) and local Web filtering results obtained from the unified threat management (UTM) module.

URL category-based routing enables you to identify and selectively route Web traffic (HTTP and HTTPS) to a specified destination.

Web filtering classifies websites into the categories according to host, URL, or IP address, and performs the filtering based on those categories. You can configure APBR profiles by specifying a URL category as the match condition in the rule. The APBR profile rule matches the traffic with specified match criteria, and after a successful match, the configured APBR profile is applied as the application service for the session. For example, suppose you want to route all the traffic belonging to a specific website category, such as social media, through a specific next hop. In this case, you can create a new APBR profile with the list of URL categories such as Enhanced_Social_Web_Facebook, Enhanced_Social_Web_Linkedin, Enhanced_Social_Web_Twitter or Enhanced_Social_Web_Youtube or any other custom URL as match criteria in the policy. The traffic that matches one of the defined URL categories in the rule is forwarded using the routes of the specific routing instance.

When an APBR profile matches the traffic against the URL categories included in the rule, APBR queries the Web filtering module to get the URL category details. If the URL category is not available in the URL filtering cache, then the security device sends a request to the private cloud configured with Web filtering for the categorization details. If the traffic does not match any URL categories, the request is uncategorized, and the session undergoes normal processing (non-APBR route).

**NOTE:** If the private cloud configured with EWF does not respond to the URL category request within an interval of 3 seconds, then the session undergoes normal processing (non-APBR route).

Rule Processing in an APBR Profile

You can provide advanced policy-based routing by classifying the traffic based on applications' attributes and applying policies based on these attributes to redirect the traffic. To do this, you must define the APBR profile and associate it to a APBR policy. You can create an APBR profile to include multiple rules with either dynamic applications, application groups or both, or a URL category as match criteria. The rules configured in the APBR profile can include either of the following:

- One or more applications, dynamic applications, or application groups
- URL category (IP destination address)—EWF or local Web filtering.
In an APBR profile, rule lookup is performed for both the match criteria. If only one match criteria is available, the rule lookup is done based on the available match criteria.

The APBR profile includes the rules to match the traffic with applications or URL categories and the action to redirect the matching traffic to the specified routing instance for the route lookup.

In Junos OS Release 18.3R1, the URL category match is done based on the destination IP address; because of this, URL category-based rule match is terminated at the first packet of the session. As a dynamic application might be identified in the middle of the session, the matching process for the dynamic application rules continues until the process of application identification is complete.

**Benefits of URL Category-Based Routing**

- Using URL-based categories enables you to have granular control over Web traffic. The traffic belonging to specific categories of websites is redirected through different paths, and based on the category, it is subjected to further security processing, including SSL decryption for HTTPS traffic.

- Traffic-handling capabilities based on URL categories enable you to use different paths for selected websites. Using different paths results in better quality of experience (QoE) and also enables you to utilize the available bandwidth effectively.

- SD-WAN solutions can utilize URL category-based routing in addition to the dynamic application-based routing.

- URL category-based routing can be used for local Internet breakout solutions as it can work with source NAT configuration changes.

**Limitations of URL Category-Based Routing**

Using URL categories in an APBR profile has the following limitations:

- Only the destination IP address is used for the URL category identification in an APBR profile. URL categories based on the host, or on the URL or the SNI field are not supported.

- You can configure either a dynamic application or a URL category as the match condition in an APBR profile rule. Configuring a rule with both URL category and dynamic application results in a commit error.
This example shows you how to configure URL category-based routing.

Requirements

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 18.3 R1 or later. This configuration example is tested on Junos OS Release 18.3 R1.
- Valid application identification feature license installed on the SRX Series device.
- The Enhanced Web Filtering (EWF) option requires you to purchase a Juniper Networks Web filtering license. No license is required for local Web filtering.

Overview

This example shows how to configure APBR on your SRX Series device to forward social media traffic arriving at the trust zone to a specific device or to an interface using URL category-based routing.

When traffic arrives, 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 IP address as specified in the routing instance. The static route configured in the routing table is added to 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 to an interface.

In this example, you complete the following configurations:

- Enable either of the following types of Web filtering:
  - Enhanced Web Filtering (EWF)—When you enable EWF on the device, the EWF engine intercepts the HTTP and the HTTPS requests and categorizes the URL into one of the 95 or more predefined categories
and also provides site reputation information. See "Configuring URL-Based Routing by Using Local Web Filtering" on page 246.

- Local Web filtering—When you enable local Web filtering, you can configure custom URL categories with multiple URL lists and apply them to a UTM Web filtering profile with actions such as permit, permit and log, block, and quarantine. To use local Web filtering, you must create a Web filtering profile and ensure that category custom is part of the profile. See “Configuring URL Category-Based Routing by Using EWF” on page 241.

- Define the routing instances and the routing information base (RIB; also known as routing table group.)
- Define the APBR profile and associate it to an APBR policy.

Configuring URL Category-Based Routing by Using EWF

### IN THIS SECTION

- Enabling Enhanced Web Filtering | 242
- Defining the Routing Instance and the RIB Group | 243
- Configuring the APBR Profile | 243
- Configuring the APBR Policy and Attaching the APBR Profile | 244

This section provides the steps to configure URL category-based routing using EWF. Table 18 on page 241 provides the details of the parameters used in this example.

**Table 18: Configuration Parameters for URL Category-Based Routing Using EWF**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APBR profile</td>
<td>apbr-pr1</td>
<td>Name of the APBR profile.</td>
</tr>
<tr>
<td>APBR policy</td>
<td>p1</td>
<td>Name of the APBR policy.</td>
</tr>
<tr>
<td>Rule</td>
<td>Rule name—rule rule-social-nw</td>
<td>Name of the APBR profile rule.</td>
</tr>
<tr>
<td></td>
<td>Matching URL category—Enhanced_Facebook_Apps</td>
<td>The APBR profile rule matches the traffic to the defined URL categories and redirects the matching traffic to the specified routing instance (example: RI1) for the route lookup.</td>
</tr>
<tr>
<td></td>
<td>Policy action—associate with routing instance RI1</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Enhanced_Social_Web_Facebook</td>
<td>Category defined in the APBR profile rule for matching the traffic.</td>
</tr>
</tbody>
</table>
Table 18: Configuration Parameters for URL Category-Based Routing Using EWF (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing instance</td>
<td></td>
<td>Routing instance of type forwarding is used for forwarding the traffic.</td>
</tr>
<tr>
<td></td>
<td>• Instance name—RI1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Instance type—forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Static route—1.0.0.254/8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Next-hop—1.0.0.1</td>
<td></td>
</tr>
<tr>
<td>All the qualified traffic destined for the static route (with IP address 1.0.0.254/8) is forwarded to the next-hop device (with IP address 1.0.0.1).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIB group</td>
<td>apbr_group</td>
<td>Name of the RIB group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The RIB group shares interface routes with the forwarding routing instances. To ensure that the next hop is resolvable, interface routes from the main routing table are shared through a RIB group with the routing tables specified in the routing instances.</td>
</tr>
</tbody>
</table>

To perform URL category-based routing using EWF, you must complete the following procedures:

**Enabling Enhanced Web Filtering**

**Step-by-Step Procedure**

To use URL categories as match criteria in an APBR profile, you must enable EWF in UTM.

**NOTE:** The EWF option requires you to purchase a Juniper Networks Web filtering license. No license is required for local Web filtering.

1. Enable EWF by specifying the Web filtering type as `juniper-enhanced`.

   ```plaintext
   [edit]
   user@host# set security utm feature-profile web-filtering type juniper-enhanced
   ```

2. Set the cache size as 500 and cache timeout as 1800 seconds for the configured EWF engine.

   ```plaintext
   [edit]
   user@host# set security utm feature-profile web-filtering juniper-enhanced cache size 500
   user@host# set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800
   ```

For more information about EWF configuration, see [Enhanced Web Filtering (EWF)](Enhanced Web Filtering (EWF)).
Defining the Routing Instance and the RIB Group

Step-by-Step Procedure

Define routing instance and the RIB group.

1. Create the routing instance to forward traffic to the different next hops. In this step, you configure the static route 1.0.0.254/8, and the next-hop address as 1.0.0.1.

   [edit]
   user@host# set routing-instances RI1 instance-type forwarding
   user@host# set routing-instances RI1 routing-options static route 1.0.0.254/8 next-hop 1.0.0.1

2. Create a RIB group.

   [edit]
   user@host# set routing-options interface-routes rib-group inet apbr_group
   user@host# set routing-options rib-groups apbr_group import-rib inet.0
   user@host# set routing-options rib-groups apbr_group import-rib RI1.inet.0

   Interface routes from the main routing table (inet.0) are shared through a RIB group with the routing table specified in the routing instance RI1.inet.0.

Configuring the APBR Profile

Step-by-Step Procedure

Create a rule for the Facebook applications and forward the matching traffic to the routing instance RI1.

1. Create the APBR profile and define the match criteria for the URL category.

   [edit]
   user@host# set security advance-policy-based-routing profile apbr-pr1 rule rule-social-nw match category Enhanced_Social_Web_Facebook

   The APBR profile rule matches the traffic to the defined URL category—that is, the Facebook application in this example.

2. Specify the action for the traffic matching the URL category.

   [edit]
   user@host# set security advance-policy-based-routing profile apbr-pr1 rule rule-social-nw then routing-instance RI1

   In this step, you are specifying that the traffic that matches the apbr-pr1 rule is to be redirected to the routing instance RI1.
Configuring the APBR Policy and Attaching the APBR Profile

Step-by-Step Procedure

Associate the application profile to the APBR policy to enable URL category-based routing.

1. Define the APBR policy. Specify the policy match condition as any for the source address, destination address, and application.

   ```
   [edit]
   user@host# set security advance-policy-based-routing from-zone trust policy p1 match source-address any
   user@host# set security advance-policy-based-routing from-zone trust policy p1 match destination-address any
   user@host# set security advance-policy-based-routing from-zone trust policy p1 match application any
   ```

   When traffic arrives, it is matched by the APBR policy rules.

2. Attach the APBR profile to the policy.

   ```
   [edit]
   user@host# set security advance-policy-based-routing from-zone trust policy p1 then
   application-services advance-policy-based-routing-profile apbr-pr1
   ```

   When the traffic matches the APBR policy (p1) rules, the APBR profile apbr-pr1 is applied to the traffic as the action of the APBR policy. The traffic that matches the Facebook application is redirected to the routing instance RI1 according to the APBR profile rule rule-social-nw.

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.

```
policy p1 {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        application-services {
            advance-policy-based-routing-profile apbr-pr1;
        }
    }
}

[edit]

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

[edit]

user@host# show routing-instances
RR11 {
    instance-type forwarding;
    routing-options {
        static {
            route 1.0.0.254/8 next-hop 1.0.0.1;
        }
    }
}

If you are done configuring the device, enter commit from configuration mode.
Configuring URL-Based Routing by Using Local Web Filtering

**IN THIS SECTION**
- Enabling Local Web Filtering | 247
- Defining the Routing Instance and the RIB Group | 248
- Configuring the APBR Profile | 248
- Configuring APBR Policy and Attaching the APBR Profile | 249

This section provides the steps to configure URL category-based routing by using local Web filtering.

Table 19 on page 246 provides the details of the parameters used in this example.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APBR profile</td>
<td>apbr-pr2</td>
<td>Name of the APBR profile.</td>
</tr>
<tr>
<td>APBR policy</td>
<td>p2</td>
<td>Name of the APBR policy.</td>
</tr>
<tr>
<td>Rule</td>
<td>Rule name—rule2</td>
<td>Name of the APBR profile rule.</td>
</tr>
<tr>
<td></td>
<td>Matching URL</td>
<td>The APBR profile rule matches the traffic to the defined URL categories and redirects the matching traffic to the specified routing instance (example: RI2) for the route lookup.</td>
</tr>
<tr>
<td></td>
<td>category—custom</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy action—associate with routing instance RI2</td>
<td></td>
</tr>
<tr>
<td>Custom Category (URL Pattern)</td>
<td>203.0.113.0</td>
<td>Category defined in the APBR profile rule for matching the traffic.</td>
</tr>
<tr>
<td></td>
<td>203.0.113.10</td>
<td></td>
</tr>
<tr>
<td>Routing instance</td>
<td>Instance name—RI2</td>
<td>Routing instance of type forwarding is used for forwarding the traffic.</td>
</tr>
<tr>
<td></td>
<td>Instance type—forwarding</td>
<td>All the qualified traffic destined for the static route (with IP address 5.0.0.10) is forwarded to the next-hop device (with IP address 9.0.0.1).</td>
</tr>
<tr>
<td></td>
<td>Static route—5.0.0.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next-hop—9.0.0.1</td>
<td></td>
</tr>
</tbody>
</table>
Table 19: APBR Configuration Parameters for URL Category-Based Routing Using Local Web Filtering (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>apbr_group2</td>
<td>Name of the RIB group. The RIB group shares interface routes with the forwarding routing instances. To ensure that the next hop is resolvable, interface routes from the main routing table are shared through a RIB group with the routing tables specified in the routing instances.</td>
</tr>
</tbody>
</table>

To perform URL category-based routing using local Web filtering, you must complete the following procedures:

**Enabling Local Web Filtering**

**Step-by-Step Procedure**

To use URL categories as match criteria in an APBR profile, you must enable local Web filtering in UTM.

1. Enable local Web filtering by specifying the Web filtering type as juniper-local.

   ```
   [edit]
   user@host# set security utm feature-profile web-filtering type juniper-local
   ```

2. Create custom objects and URL pattern lists.

   ```
   [edit]
   user@host# set security utm custom-objects url-pattern local1 value 203.0.113.0
   user@host# set security utm custom-objects url-pattern local1 value 203.0.113.10
   ```

   In this step, a pattern that matches the IP address 203.0.113.0 or 203.0.113.10 on HTTP is created.

3. Configure the custom URL category list.

   ```
   user@host# set security utm custom-objects custom-url-category custom value local1
   ```

   The URL category specified in this example is custom, where you can add URL lists. In this step, you are adding the URL list local1, which includes the patterns matching the addresses 203.0.113.1 and 203.0.113.10 that are created in step 2.

4. Configure a Web filtering profile.
A Web filtering profile includes a user-defined category with a permit action.

For more information about local Web filtering configuration, see Local Web Filtering.

Defining the Routing Instance and the RIB Group

Step-by-Step Procedure
Define the routing instance and the RIB group.

1. Create the routing instance to forward traffic to the different next hops. In this example, you configure the static route 5.0.0.0/10, using the next-hop address of 9.0.0.1.

```
[edit]
user@host# set routing-instances RI2 instance-type forwarding
user@host# set routing-instances RI2 routing-options static route 5.0.0.0/16 next-hop 9.0.0.1
```

2. Create a RIB group.

```
[edit]
user@host# set routing-options interface-routes rib-group inet apbr_group2
user@host# set routing-options rib-groups apbr_group2 import-rib inet.0
user@host# set routing-options rib-groups apbr_group2 import-rib RI2.inet.0
```

Interface routes from the main routing table (inet.0) are shared through a RIB group with the routing table specified in the routing instance (RI2.inet.0).

Configuring the APBR Profile

Step-by-Step Procedure
Create a rule to forward the traffic matching the custom URL pattern to the routing instance RI2.

1. Create the APBR profile and define the match criteria for the URL category.

```
[edit]
user@host# set security advance-policy-based-routing profile apbr-pr2 rule rule2 match category custom
```

The APBR profile rule matches the traffic to the defined custom URL category—that is, traffic with URL patterns matching the addresses 203.0.113.1 and 203.0.113.10 in this example.

2. Specify the action for the traffic matching the URL category.
In this step, you are specifying that the traffic that matches the rule is to be redirected to the routing instance RI2.

**Configuring APBR Policy and Attaching the APBR Profile**

**Step-by-Step Procedure**
Associate the APBR profile to the APBR policy to enable URL category-based routing.

1. Define the APBR policy. Specify the policy match condition as any for the source address, destination address, and application.

```plaintext
[edit]
user@host# set security advance-policy-based-routing profile apbr-pr2 rule rule2 then routing-instance RI2
```

When traffic arrives, is matched by the APBR policy rules.

2. Attach the APBR profile to the policy.

```plaintext
[edit]
user@host# set security advance-policy-based-routing from-zone trust policy p2 match source-address any
user@host# set security advance-policy-based-routing from-zone trust policy p2 match destination-address any
user@host# set security advance-policy-based-routing from-zone trust policy p2 match application any
```

When the traffic matches the APBR policy (p2) rules, the APBR profile apbr-pr2 is applied to the traffic as the action of the APBR policy. The traffic that matches the Facebook application is redirected to the routing instance RI2 according to the APBR profile rule rule2.

**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.

```plaintext
[edit security]
user@host# show advance-policy-based-routing
profile apbr-pr2 {
  rule rule2 {
    match {
```
category custom;
}
then {
    routing-instance RI2;
}
}
}
from-zone trust {
policy p2 {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        application-services {
            advance-policy-based-routing-profile apbr-pr2;
        }
    }
}
}

[edit]

user@host# show routing-options
interface-routes {
    rib-group inet apbr_group2;
}
rib-groups {
    apbr_group2 {
        import-rib [ inet.0 RI2.inet.0 ];
    }
}

[edit]

user@host# show routing-instances
RI2 {
    instance-type forwarding;
    routing-options {
        static {
            route 5.0.0.0/10 next-hop 9.0.0.1;
        }
    }
}
If you are done configuring the device, enter **commit** from configuration mode.

**Verification**

**Verifying APBR Statistics**

**Purpose**
Display the statistics for APBR, such as the number of sessions processed for the application-based routing, the 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.

```
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

**Meaning**
The command output displays the following details:

- Sessions processed for the application-based routing
- The number of times the presence of an entry in the application system cache (ASC) is found
- The number of times the application traffic matches the APBR profile and APBR is applied for the session
- The number of times application identification (AppID) was consulted to identify application traffic
- The number of times the APBR is applied for the session

### Bypassing Application Services in an APBR Rule

You can create an APBR profile to include multiple rules with either dynamic applications, application groups or both, or a URL category as match criteria on security devices. URL category-based routing
enables you to identify and selectively route Web traffic (HTTP and HTTPS) to a specified destination or to another device where further inspection on the Web traffic is required. In such cases, you can select not to apply or bypass application services on the session that is to be forwarded to the device for further inspection.

Starting in Junos OS Release 19.1R1, you can bypass application services for a session that is re-routed using the APBR rule.

The following sequences are involved in bypassing the application services:

1. APBR uses the application details to look for a matching rule in the APBR profile (application profile).
2. If a matching APBR rule is found, the traffic is redirected to the specified routing instance for the route lookup.
3. If you configure the option to bypass application services on the sessions in an APBR rule, then an attempt is done to bypass the application services to the session.
4. A log message is generated or updated to indicate the bypassing of the application services on the session.

You can bypass the application services including security policies, application quality of service (AppQoS), Juniper Sky ATP, IDP, Security Intelligence (SecIntel) and UTM using the APBR rule.

For bypass to be effective, it is required that the APBR rule is matched in the first packet. If the rule is matched after the first packet, and the rule has a bypass option configured, the bypass option is ignored and the application services are not bypassed.

ALG Service is not bypassed due to this feature as bypassing the ALG could potentially result in the correlated (data) session not being matched to appropriate security policy.

**Example: Bypassing Application Services by Using APBR Rule**

---

**IN THIS SECTION**

- Requirements | 253
- Overview | 253
- Configuration | 254
- Verification | 257
This example shows you how to bypass application services on the session using APBR rule. Using URL category-based routing, you can identify and selectively route Web traffic (HTTP and HTTPS) to a specified destination or to another device. Here, you can configure to bypass the application services on the session where further inspection on the Web traffic could be performed.

Requirements

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 19.1R1 or later. This configuration example is tested on Junos OS Release 19.1R1.
- Valid application identification feature license installed on the SRX Series device.

Before you begin:

- Define routing instance and RIB group.
- Appropriate security policies to enforce rules for the transit traffic, to specify what traffic can pass through the device, and the actions that need to take place on the traffic as it passes through the device.

Overview

This example shows how to configure APBR on your SRX Series device to forward social media traffic arriving at the trust zone to a specific device or to an interface using URL category-based routing and bypass the application services on the same session.

In this example, you complete the following configurations:

- Define the APBR profile and associate it to a APBR policy. The APBR profile includes the rules to match the traffic with applications and URL categories.
- Next, specify the action of the APBR profile rule. That is, to redirect the matching traffic to the specified routing instance for the route lookup.
- Specify application bypass option for the matching traffic.

When traffic arrives, it is matched by the APBR profile, and if a matching rule is found, the packets are forwarded to the static route. All traffic destined for the static route is transmitted to the next-hop address for transit to a specific device or to an interface. Since you configured application bypass option for the matching traffic, the traffic forwarded to the specific device at next-hop address is not applied with application services.
Configuration

This section provides steps to configure URL category-based routing by using enhanced Web filtering (EWF) and also enable by passing application services on the traffic.

**Enabling Enhanced Web Filtering**

**Step-by-Step Procedure**

To use URL categories as match criteria in an APBR profile, you must enable EWF in UTM.

1. Enable EWF by specifying the Web filtering type as `juniper-enhanced`.

   ```bash
   [edit]
   user@host# set security utm feature-profile web-filtering type juniper-enhanced
   ```

2. Set the cache size as 500 and cache timeout as 1800 seconds for the configured EWF engine.

   ```bash
   [edit]
   user@host# set security utm feature-profile web-filtering juniper-enhanced cache size 500
   user@host# set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800
   ```

   For more information about EWF configuration, see Enhanced Web Filtering (EWF).

**Configuring the APBR Rule**

**Step-by-Step Procedure**
Create a rule for the Facebook applications and forward the matching traffic to the routing instance RI1.

1. Create the APBR profile and define the match criteria for the URL category.

   `[edit]`
   
   `user@host# set security advance-policy-based-routing profile apbr-pr1 rule rule-social-nw match category Enhanced_Social_Web_Facebook`

   The APBR profile rule matches the traffic to the defined URL category—that is, the Facebook application in this example.

2. Specify the action for the traffic matching the URL category.

   `[edit]`
   
   `user@host# set security advance-policy-based-routing profile apbr-pr1 rule rule-social-nw then routing-instance RI1`

   In this step, you are specifying that the traffic that matches the apbr-pr1 rule is to be redirected to the routing instance RI1.

3. Specify the bypassing application services for the traffic matching the APBR rule.

   `[edit]`
   
   `user@host# set security advance-policy-based-routing profile apbr-pr1 rule rule-social-nw then application-services-bypass`

   In this step, you are specifying that the traffic that matches the apbr-pr1 rule is to be bypassed application services.

---

**Configuring APBR Policy and Attaching the APBR Profile**

**Step-by-Step Procedure**

Associate the application profile to the APBR policy to enable URL category-based routing.

1. Define the APBR policy. Specify the policy match condition as `any` for the source address, destination address, and application.

   `[edit]`
   
   `user@host# set security advance-policy-based-routing from-zone trust policy p1 match source-address any`
   `user@host# set security advance-policy-based-routing from-zone trust policy p1 match destination-address any`
   `user@host# set security advance-policy-based-routing from-zone trust policy p1 match application any`

   When traffic arrives, it is matched by the APBR policy rules.
2. Attach the APBR profile to the policy.

```bash
[edit]
user@host# set security advance-policy-based-routing from-zone trust policy p1 then application-services advance-policy-based-routing-profile apbr-pr1
```

When the traffic matches the APBR policy (p1) rules, the APBR profile apbr-pr1 is applied to the traffic as the action of the APBR policy. The traffic that matches the Facebook application is redirected to the routing instance RI1 according to the APBR profile rule rule-social-nw. Also application services are bypassed for the session as specified in APBR profile rule rule-social-nw.

**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.

```bash
[edit security]

user@host# show advance-policy-based-routing
profile apbr-pr1 {
  rule rule-social-nw {
    match {
      category Enhanced_Social_Web_Facebook;
    }
    then {
      routing-instance RI1;
      application-services-bypass;
    }
  }
}
}
from-zone trust {
  policy p1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      application-services {
        advance-policy-based-routing-profile apbr-pr1;
      }
    }
  }
}
```
If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

**Verifying APBR Statistics**

**Purpose**
Display the statistics for APBR, such as the number of sessions processed for the application-based routing, the 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.

```
user@host> show security advance-policy-based-routing statistics
```

<table>
<thead>
<tr>
<th>Advance Profile Based Routing statistics:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions Processed</td>
<td>110</td>
</tr>
<tr>
<td>AppID cache hits</td>
<td>110</td>
</tr>
<tr>
<td>AppID requested</td>
<td>0</td>
</tr>
<tr>
<td>Rule matches</td>
<td>2</td>
</tr>
<tr>
<td>Route changed on cache hits</td>
<td>1</td>
</tr>
<tr>
<td>Route changed midstream</td>
<td>1</td>
</tr>
<tr>
<td>Zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Drop on zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Next hop not found</td>
<td>0</td>
</tr>
<tr>
<td>Application Services Bypass</td>
<td>1</td>
</tr>
</tbody>
</table>

**Meaning**
The command output displays the following details:

- Sessions processed for the application-based routing
- The number of times the presence of an entry in the application system cache (ASC) is found
- The number of times the application traffic matches the APBR profile and APBR is applied for the session
- The number of times application identification (AppID) was consulted to identify application traffic
- The number of times the APBR is applied for the session
- The number of times the application services are bypassed for the session
Support for User Source Identity in APBR Policies

Starting in Junos OS Release 19.1R1, you can configure advanced policy-based routing (APBR) policies by defining user source identity as one of the match criteria along with source addresses, destination addresses, and applications. After a successful match, the APBR profile configured with the APBR policy is applied as an application service for the session. The source identity enables you to leverage user information stored in a repository such as user identification table (UIT).

The source-identity field specifies the users and roles to which the policy applies. When the source-identity field is specified in a policy as a matching criterion, user and role information must be retrieved before policy lookup can proceed. Using the source-identity option as a matching criterion in the APBR policy is optional. If the value in the source-identity field is configured as any or there is no entry in the source-identity field, user information and role information are not required and the other match criteria are used for policy lookup.

You can specify one or more users or user roles using the source-identity field with the following keywords:

- authenticated-user—Users that have been authenticated.
- unauthenticated-user—Users that have not been authenticated.
- any—All users regardless of authentication status. If the source-identity field is not configured or is set to any, only other matching criteria are used for matching.
- unknown-user—Users that can not be authenticated due to an authentication server disconnection, such as a power outage.

On your security device, the user identification table (UIT) provides user and role information for an active user who has already been authenticated. Each entry in the table maps an IP address to an authenticated user and any role.

UIT contains the IP address, username, and role information for all authenticated user. The entries in the user identification table are ordered by IP address.

On your security device, the type of UIT supported is local authentication table. The local authentication table serves as the authentication source for the information required by APBR policies. Local authentication table is a static UIT created on the device either manually or programmatically using CLI commands. All users included in the local authentication table are considered authenticated users. To retrieve user and role information, a search is performed in the authentication table for an entry with an IP address corresponding to the traffic. When a matching IP address is found, user and role information is retrieved from the table entry and are associated with the traffic. If not found, the user is classified as an unauthenticated user.

User and role information can be created on the device manually or ported from a third-party authentication server, but the data in the local authentication table is not updated in real time.
During APBR policy lookup, if a user and user role that are configured in the APBR policy, but the entry is not present in the local authentication table, then the policy does not match. Hit count value that display the utility rate of security policies according to the number of hits they receive, does not increment.

For more information on user role retrieval and the policy lookup process, see User Role Firewall Security Policies.

Benefits

- Enables you to define the routing behavior at more granular levels to ensure safe enforcement of policy on the application traffic traversing the network.
- Provides more flexible traffic-handling capabilities and offers granular control for forwarding packets based on the roles and business requirements of users.

Local Authentication Table

You can manage the local authentication table with CLI commands that add or delete entries. You can add IP addresses, usernames, and roles from a third-party authentication source to the local authentication table programmatically using CLI commands. If an authentication source defines users and groups, the groups can be configured as roles and associated with the user as usual.

Use the following command to add an entry to a local authentication table. The entries in the table are entered using the IP address.

```
user@host >request security user-identification local-authentication-table add user user-name ip-address ip-address role [role-name role-name]
```

Example:

```
user@host >request security user-identification local-authentication-table add user-name user1 ip-address 2.2.2.2 roles role1
```

Use the following command to delete an entry by IP address or by username.

```
user@host >request security user-identification local-authentication-table delete (ip-address | user-name)
```

Use the following command to clear the local authentication table:

```
user@host >clear security user-identification local-authentication-table
```
Use the following command to display the content of the local authentication table:

```
user@host > show security user-identification local-authentication-table all (brief | extensive)
```

For more information, see Local Authentication Table.

**Example: Configuring Advanced Policy-Based Routing Policies with Source Identity**

**IN THIS SECTION**

- Requirements | 260
- Overview | 260
- Configuration | 261
- Verification | 264

This example shows how to configure an APBR policy with source identity and how to apply the APBR profile on a session that matches the APBR policy rules.

**Requirements**

This example uses the following hardware and software components:

- An SRX Series device with Junos OS Release 19.1R1 or later. This configuration example is tested on Junos OS Release 19.1R1.
- Valid application identification feature license installed on an SRX Series device.

**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 a routing instance and a RIB group.
- Create an ABPR profile.
- 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-0/0/1.0
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 match source-identity identity-1
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 add an entry to a local authentication table.

1. Enter the username, IP address, and user role details.

   ```
   user@host> request security user-identification local-authentication-table add username user1 ip-address 2.2.2.2 roles role1
   ```
**Step-by-Step Procedure**

To apply APBR on traffic that matches 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-0/0/1.0
   ```

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 match source-identity identity-1
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;
            source-identity identity-1;
        }
    }
}
{ }
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-0/0/1.0;
  }
}

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

Verification

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 advance-policy-based-routing detail` command.

```
user@host> show security advance-policy-based-routing detail
```

```
Policy: SLA1, State: enabled, Index: 5
  Policy Type: Configured
  Sequence number: 1
  From 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]
  APBR-Profile: profile1
  Source identities:
    identity-1
```

Meaning

The command output displays the source identity details in the `Source identities` field.

SEE ALSO

- Understanding Advanced Policy-Based Routing | 213

Using DSCP as Match Criteria in APBR Rules

**IN THIS SECTION**

- Introduction | 266
- Use Case | 266
This topic includes the following sections:

**Introduction**

Application identification techniques rely on deep packet inspection (DPI). There are some cases where DPI engine might not be able to identify the application, for example—encrypted traffic. If you apply APBR rules on such traffic, the traffic undergoes normal processing without APBR functionality applied on it.

Starting in Junos OS release 19.3R1, SRX Series devices support configuring DSCP values in an APBR rule as match criteria to perform APBR functionality on the DSCP-tagged traffic.

You can configure DSCP value in addition to the other matching criteria of the APBR rule such as dynamic application, and dynamic application group.

By configuring the DSCP value in an APBR rule, you can extend the APBR service to the traffic with the DSCP markings.

**Use Case**

You can use APBR rules with DSCP as match criteria for the encrypted traffic.

**Limitation**

- Support not available for configuring rules with DSCP value and URL category in a single APBR profile.

**APBR Rule Lookup When Using a DSCP Value as Match Criteria**

In a APBR rule, you can configure a DSCP value or dynamic applications or combination of both.

If you have configured both DSCP and dynamic application in a APBR rule, the rule is considered as match if the traffic matches all the criteria specified in the rule. If there are multiple DSCP values present in the APBR rule, then if any one criteria matches, it is considered as match.

A APBR profile can contain multiple rules, each rule with a variety of match conditions.

In case of multiple APBR rules in a APBR profile, the rule lookup uses the following priority order:

1. Rule with DSCP + dynamic application
2. Rule with dynamic application
3. Rule with DSCP value

If a APBR profile contains multiple rules, the system performs rule lookup and applies the rule in the following order:

- System applies the DSCP-based rules for the first packet of the session.
- System continues to check if any application information available either from DPI classification or application system cache (ASC).
- In the middle of the session, if DPI identifies a new application, the system performs a rule lookup and applies new rule (application-based rule or DSCP-based rule or combination of both) as applicable.
- Identifying application and rule lookup continues till the DPI identifies an application as the final application or maximum reroute value is reached.
- If the rule lookup does not match any rule, no further action is taken.

Let’s understand how APBR performs rule lookup and applies the rules with the following two examples:

**Example 1**

In this example, you configure three APBR rules with— one with DSCP value 30, next rule with application as HTTP, and the third rule with both DSCP value as 30 and application as HTTP. Configure maximum route change value as 1 (default value).

Table 20 on page 267 shows how APBR performs rule lookup and applies the rules.

**Table 20: APBR Rules with DSCP and Dynamic Application**

<table>
<thead>
<tr>
<th>Session</th>
<th>Traffic Type</th>
<th>ASC Cache</th>
<th>DPI Classification</th>
<th>Matching Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>First session</td>
<td>DSCP=30</td>
<td>NA</td>
<td>NA</td>
<td>Rule 1</td>
</tr>
<tr>
<td>Midstream session</td>
<td>DSCP=30</td>
<td>Yes</td>
<td>HTTP</td>
<td>Rule 3</td>
</tr>
<tr>
<td></td>
<td>Application = HTTP</td>
<td></td>
<td></td>
<td>The traffic switches because rule lookup matched the new rule.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When traffic switches based on rule change in the middle of the session, the count for maximum route change reduces to 0. Now no further route change takes place in this scenario.</td>
</tr>
</tbody>
</table>

**Example 2**

In this example, you configure three APBR rules with— one with DSCP value 30, next rule with DSCP value 60, and the third rule with both DSCP value as 30 and application as HTTP.
Table 21 on page 268 shows how APBR performs rule lookup and applies the rules.

### Table 21: APBR Rules with Only DSCP Values

<table>
<thead>
<tr>
<th>Session</th>
<th>Traffic Type</th>
<th>ASC Cache</th>
<th>DPI Classification</th>
<th>Matching Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>First session</td>
<td>DSCP=30</td>
<td>NA</td>
<td>NA</td>
<td>Rule 1</td>
</tr>
<tr>
<td>Midstream session</td>
<td>DSCP=60</td>
<td>Yes</td>
<td>DSCP=60</td>
<td>Rule 2; Rule 3 does not match with traffic</td>
</tr>
<tr>
<td></td>
<td>Application = HTTP</td>
<td></td>
<td>HTTP</td>
<td>because DSCP value is changed from 30 to 60 in midstream.</td>
</tr>
</tbody>
</table>

### Configure APBR Rules with DSCP Values as Match Criteria

This example shows how to configure APBR rules with DSCP values as match criteria.

**Requirements**

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 19.3R1 or later. This configuration example is tested on Junos OS Release 19.3R1.
- Any supported SRX Series device.
- Valid application identification feature license installed on the SRX Series device.
Overview

In this example, you want to forward HTTP traffic and traffic tagged with DSCP value 56 and DSCP value 46 to a specific device or interfaces at Site 1, Site 2, and Site 3 respectively. Security device forwards the traffic based on an application or DSCP value to a preferred route by using APBR feature.

When traffic arrives at the trust zone, APBR matches the traffic with configured APBR profile rules. If the traffic matches the rule, APBR forwards the traffic to the specific destination as defined in the APBR rule.

For example, you configure APBR to route the traffic to different destinations based on the type of the application as specified below:

- Rule 1—Forward HTTP traffic from Client 1 to the Site 1 using next-hop address 192.0.2.254.
- Rule 2—Forward traffic with DSCP value 56 and HTTP application to Site 2 using next-hop device 192.0.3.254.
- Rule 3—Forward traffic with DSCP value 46 to Site 3 using the next-hop device 192.0.4.254.

Figure 12 on page 269 shows the topology used in this example.

Table 22 on page 269 provides the details of the parameters used in this example.

Table 22: Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Associated Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APBR profile</td>
<td>P1</td>
<td>Name of the APBR profile.</td>
<td>Configure the profile with rules to match the applications and DSCP values and specify destination (example: routing-instances) for the matching traffic.</td>
</tr>
</tbody>
</table>
Table 22: Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Associated Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIB group</td>
<td>RI1.inet.0</td>
<td>Associated routing instance—RI1</td>
<td>Configure the RIB group to import interface route entries from inet.0, RI1.inet.0, RI2.inet.0, and RI3.inet.0.</td>
</tr>
<tr>
<td></td>
<td>RI1.inet.2</td>
<td>Associated routing instance—RI2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RI1.inet.3</td>
<td>Associated routing instance—RI3</td>
<td></td>
</tr>
</tbody>
</table>
| Routing instance | RI1 | Static route— 192.0.0.0/16  
Next-hop—192.0.2.254 | Configure the routing instances to include next-hop IP address. APBR forwards the qualified traffic destined for the static route to the next-hop device address in Site 1, Site 2, and Site 3. |
|             | RI2 | Static route— 192.0.0.0/16  
Next-hop—192.0.3.254 |             |
|             | RI3 | Static route— 192.0.0.0/16  
Next-hop—192.0.4.254 |             |
| APBR Rule   | R1 | Matching application—junos:HTTP  
Associated routing instance—RI1 | Configure the APBR rules and specify dynamic application or DSCP values as matching criteria. |
|             | R2 | matching DSCP value— 56 and application—junos:HTTP  
Associated routing instance—RI2 | APBR forwards the matching traffic to the associated routing instance. |
|             | R3 | matching DSCP value— 46  
Associated routing instance—RI3 |             |

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 untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1/24
set interfaces ge-0/0/2 unit 0 family inet address 192.0.3.1/24
set interfaces ge-0/0/3 unit 0 family inet address 192.0.4.1/24
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone untrust interfaces ge-0/0/3.0
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-0/0/0/0.0
set interfaces ge-0/0/0/0 unit 0 family inet address 4.0.0.1/24
set routing-instances RI1 instance-type forwarding
set routing-instances RI1 routing-options static route 192.0.0.0/16 next-hop 192.0.2.254
set routing-instances RI2 instance-type forwarding
set routing-instances RI2 routing-options static route 192.0.0.0/16 next-hop 192.0.3.254
set routing-instances RI3 instance-type forwarding
set routing-instances RI3 routing-options static route 192.0.0.0/16 next-hop 192.0.4.254
set routing-options rib-group 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 routing-options rib-groups apbr-group import-rib RI3.inet.0
set routing-options interface/routes rib-group import inet apbr-group
set security advance-policy-based-routing profile p1 rule R1 match dynamic-application junos:HTTP
set security advance-policy-based-routing profile p1 rule R1 then routing-instance RI1
set security advance-policy-based-routing profile p1 rule R2 match dscp 56
set security advance-policy-based-routing profile p1 rule R2 match dynamic-application junos:HTTP
set security advance-policy-based-routing profile p1 rule R2 then routing-instance RI2
set security advance-policy-based-routing profile p1 rule R3 match dscp 46
set security advance-policy-based-routing profile p1 rule R3 then routing-instance RI3
set security zones security-zone trust advance-policy-based-routing-profile p1
set security zones security-zone trust advance-policy-based-routing-profile p1

Configure APBR rule with DSCP and dynamic application as match criteria.

1. Define security zones and interfaces.

[edit]
user@host# set interfaces ge-0/0/0/1 unit 0 family inet address 192.0.2.1/24
user@host# set interfaces ge-0/0/0/2 unit 0 family inet address 192.0.3.1/24
user@host# set interfaces ge-0/0/0/3 unit 0 family inet address 192.0.4.1/24
user@host# set security zones security-zone untrust host-inbound-traffic system-services all
user@host# set security zones security-zone untrust host-inbound-traffic protocols all
user@host# set security zones security-zone untrust host-inbound-traffic interfaces ge-0/0/1.0
user@host# set security zones security-zone untrust interfaces ge-0/0/2.0
user@host# set security zones security-zone untrust interfaces ge-0/0/3.0

2. Define interface and security zones for the ingress interface connecting the client device.

[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
3. Configure the routing instances.

```
[edit]
user@host# set routing-instances RI1 instance-type forwarding
user@host# set routing-instances RI1 routing-options static route 192.0.0.0/16 next-hop 192.0.2.254
user@host# set routing-instances RI2 routing-options static route 192.0.0.0/16 next-hop 192.0.3.254
user@host# set routing-instances RI3 instance-type forwarding
user@host# set routing-instances RI3 routing-options static route 192.0.0.0/16 next-hop 192.0.4.254
```

4. 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 rib-groups apbr-group import-rib inet.0
user@host# set routing-options rib-groups apbr-group import-rib RI1.inet.0
user@host# set routing-options rib-groups apbr-group import-rib RI2.inet.0
user@host# set routing-options rib-groups apbr-group import-rib RI3.inet.0
user@host# set routing-options interface-routes rib-group inet apbr-group
```

5. Define the APBR rule with dynamic application HTTP as match criteria.

```
[edit]
user@host# set security advance-policy-based-routing profile p1 rule R1 match dynamic-application
  junos:HTTP
user@host# set security advance-policy-based-routing profile p1 rule R1 then routing-instance RI1
```

APBR routes the traffic matching the HTTP application to the routing instance RI1.

6. Create another rule for DSCP and HTTP application.

```
[edit]
user@host# set security advance-policy-based-routing profile p1 rule R2 match dscp 56
user@host# set security advance-policy-based-routing profile p1 rule R2 match dynamic-application
  junos:HTTP
user@host# set security advance-policy-based-routing profile p1 rule R2 then routing-instance RI2
```

APBR routes the traffic matching the DSCP value 56 to the routing instance RI2.
7. Define one more rule with DSCP value 46.

```
[edit]
user@host# set security advance-policy-based-routing profile p1 rule R3 match dscp 46
user@host# set security advance-policy-based-routing profile p1 rule R3 then routing-instance RI3
user@host# set security zones security-zone trust advance-policy-based-routing-profile p1
```

APBR routes the traffic matching the DSCP value 46 to the routing instance RI3.

8. Apply the APBR profile to the security zone.

```
[edit]
user@host# set security zones security-zone trust advance-policy-based-routing-profile p1
```

Results

From configuration mode, confirm your configuration by entering the `show security advance-policy-based-routing`, `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 interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 4.0.0.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.0.2.1/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 192.0.3.1/24;
        }
    }
}
```
ge-0/0/3 {
    unit 0 {
        family inet {
            address 192.0.4.1/24;
        }
    }
}

[edit]
user@host# show routing-instances
RI1 {
    instance-type forwarding;
    routing-options {
        static {
            route 192.0.0.0/16 next-hop 192.0.2.254;
        }
    }
}
RI2 {
    instance-type forwarding;
    routing-options {
        static {
            route 192.0.0.0/16 next-hop 192.0.3.254;
        }
    }
}
RI3 {
    instance-type forwarding;
    routing-options {
        static {
            route 192.0.0.0/16 next-hop 192.0.4.254;
        }
    }
}

[edit]
user@host# show security advance-policy-based-routing
profile p1 {
    rule R1 {
        match {
            dynamic-application junos:HTTP;
        }
    }
}
then {
    routing-instance RI1;
}
}

rule R2 {
    match {
        dynamic-application junos:HTTP;
        dscp 56;
    }
    then {
        routing-instance RI2;
    }
}

rule R3 {
    match {
        dscp 46;
    }
    then {
        routing-instance RI3;
    }
}

[edit]

user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
        ge-0/0/2.0;
        ge-0/0/3.0;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
}
Once you complete the configuration, 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.

```bash
user@host> show security advance-policy-based-routing statistics
```

**Advance Profile Based Routing statistics:**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions Processed</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit on cache hit</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit on HTTP Proxy/ALG</td>
<td>0</td>
</tr>
<tr>
<td>URL cat rule hit on cache hit</td>
<td>0</td>
</tr>
<tr>
<td>DSCP rule hit on first packet</td>
<td>0</td>
</tr>
<tr>
<td>App and DSCP hit on first packet</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>URL cat rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>App and DSCP rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>DSCP rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>Route changed on cache hits</td>
<td>0</td>
</tr>
<tr>
<td>Route changed on HTTP Proxy/ALG</td>
<td>0</td>
</tr>
<tr>
<td>Route changed midstream</td>
<td>0</td>
</tr>
<tr>
<td>Zone mismatch</td>
<td>0</td>
</tr>
</tbody>
</table>
Meaning
The command output displays the following details:

• Sessions processed for the application-based routing.
• The number of times the application traffic or DSCP-tagged traffic matches the APBR profile.
• The number of times traffic is switched to different route in the midstream.

Verifying Advanced Policy-Based Routing Sessions

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.

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.

Disable APBR Midstream Routing for Specific APBR Rule

Why Selectively Disabling the Midstream Routing is Required?

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. If you set this option to 0, the APBR is disabled for the particular session. However, this option also disables the APBR functionality globally on your device which might not be required.

**Selectively Disabling APBR In Midstream**

Starting in Junos OS Release 19.4R1, you can selectively turn-off the APBR service in the middle of a session for a specific APBR rule, while retaining the global APBR functionality for the remaining sessions. When you disable midstream routing for a specific APBR rule, the system does not apply midstream APBR for corresponding application traffic, and routes the traffic through a non-APBR route.

To selectively disable the midstream APBR, you can configure the APBR rule with disable midstream routing option (`disable-midstream-routing`) at `[edit security advance-policy-based-routing profile apbr-profile-name rule apbr-rule-name]` hierarchy level.

**Table 23 on page 278** shows the behavior of the selectively disabling midstream APBR option.

**Table 23: Selectively Disabling APBR in Midstream for Different Scenarios**

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Traffic Matches APBR Rule</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Sessions (when the cache entry does not exists for the session)</td>
<td>With <code>disable-midstream-routing</code> option</td>
<td>Session uses the default route.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <code>max-route-change</code> value is not decremented.</td>
</tr>
<tr>
<td></td>
<td>Without <code>disable-midstream-routing</code> option</td>
<td>Apply midstream APBR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Apply APBR till the last application is identified or as defined in the <code>max-route-change</code> option.</td>
</tr>
<tr>
<td>Established Sessions (when the cache entry exists for the session)</td>
<td>With <code>disable-midstream-routing</code> option</td>
<td>Apply APBR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disengage APBR for the further sessions. That is—even if further applications are identified in the session after the cache hit, APBR is not applied to them.</td>
</tr>
<tr>
<td></td>
<td>Without <code>disable-midstream-routing</code> option</td>
<td>Apply APBR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continue to apply APBR till the last application is identified or as defined in the <code>max-route-change</code> option.</td>
</tr>
</tbody>
</table>
Disabling midstream routing for a specific APBR rule will reroute the application traffic back through a default non-APBR route.
Using Disable Midstream Routing Option to Selectively Disable APBR for Specific APBR Rule

If you have already configured an APBR rule for a specific application, and now you want to selectively disable the APBR midstream routing, use the following option:

```
user@host# set security advance-policy-based-routing profile apbr-profile-name rule apbr-rule-name disable-midstream-routing
```

Example:

```
[edit security advance-policy-based-routing]
user@host# show
profile p1 {
  rule r1 {
    disable-midstream-routing;
    match {
      dynamic-application junos:YAHOO;
    }
    then {
      routing-instance RI1;
    }
  }
  from-zone trust {
    policy policy-1 {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        application-services {
          advance-policy-based-routing-profile profile-1;
        }
      }
    }
  }
}
```

Use the `show security advance-policy-based-routing statistics` command to verify the APBR status:
In this sample output, the fields **Midstream disabled rule hit on cache hit** and **Midstream disabled rule hit midstream** indicate the number of times a route remains unchanged in the middle of a session after the rule with defined application is matched and the number of times the rule with a disabled midstream has a matching entry in the application system cache (ASC).

### Default Mechanism to Forward the Traffic Through APBR Rule

Starting in Junos OS 20.1R1 Release, you can configure "any" as match criteria for dynamic application in a APBR rule. The criteria "any" acts as a wildcard and applies to any dynamic application.

**Example**

```
user@hots# set security advance-policy-based-routing profile p1 rule R1 match dynamic-application any
user@hots# set security advance-policy-based-routing profile p1 rule R1 then routing-instance RI1
```

Application traffic that match the other parameters in a APBR rule matches the policy regardless of the dynamic application type.
Note the following while using the **any** keyword for dynamic applications in an APBR rule:

- You can configure only one APBR rule with **any** keyword for the dynamic application in an APBR profile.
- Configuring a same APBR rule with DSCP and URL-based categories with the **any** keyword is not supported.
- APBR rule with dynamic applications configured as **any** is applied only during the first packet processing.
- Configuring a same APBR rule with dynamic application as **any** and other dynamic applications or dynamic application groups is not supported.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.4R1</td>
<td>Starting in Junos OS Release 19.4R1, you can selectively turn-off the APBR service in the middle of a session for a specific APBR rule, while retaining the global APBR functionality for the remaining sessions.</td>
</tr>
<tr>
<td>19.3R1</td>
<td>Starting in Junos OS release 19.3R1, SRX Series devices support configuring DSCP values in an APBR rule as match criteria to perform APBR functionality on the DSCP-tagged traffic.</td>
</tr>
<tr>
<td>19.1R1</td>
<td>Starting in Junos OS Release 19.1R1, you can bypass application services for a session that is re-routed using the APBR rule.</td>
</tr>
<tr>
<td>19.1R1</td>
<td>Starting in Junos OS Release 19.1R1, you can configure advanced policy-based routing (APBR) policies by defining user source identity as one of the match criteria along with source addresses, destination addresses, and applications.</td>
</tr>
<tr>
<td>17.4</td>
<td>Starting with Junos OS Release 15.1X49-D110 and Junos OS Release 17.4R1, SRX Series Services gateways 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)</td>
</tr>
<tr>
<td>15.1X49-D60</td>
<td>Starting with Junos OS Release 15.1X49-D60, SRX Series Services Gateways support advanced policy-based routing (APBR).</td>
</tr>
<tr>
<td>15.1X49-D123</td>
<td>Support for reverse rerouting is available starting in Junos OS Release 15.1X49-D130 and later releases.</td>
</tr>
</tbody>
</table>

### RELATED DOCUMENTATION

- Application Identification | 32
Application Quality of Experience

IN THIS SECTION
- Application Quality of Experience (AppQoE) | 283
- Example: Application Quality of Experience (AppQoE) | 291
- Understanding AppQoE Configuration Limits | 310
- Understanding Application Path Selection Based on Link Preference and Priority | 311
- Example: Configuring Link Preference and Priority for AppQoE | 314
- Understanding System log Messages for AppQoE | 321
- Disable AppQoE Logging | 323
- Configure SLA Export Factor | 324
- Configure Violation Count | 324
- Application Quality of Experience (AppQoE) Based on the DSCP Bits of Incoming Traffic | 325
- AppQoE Support for Granular APBR Rules | 327
- AppQoE Multi-homing with Active-Active Deployment | 330

Application Quality of Experience (AppQoE)

IN THIS SECTION
- Introduction to Application Quality of Experience | 284
- Benefits of Application Quality of Experience | 285
- Supported Use Cases | 285
- Limitations | 285
- Understanding Application Quality of Experience Terminology | 286
- How Application Quality of Experience Works? | 287
This topic includes following sections:

**Introduction to Application Quality of Experience**

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.

**Supported SRX Series Devices**

AppQoE is supported on vSRX instances, SRX300 line of devices, SRX550M, SRX1500, SRX4100, and SRX4200 devices.

You can configure an AppQoE SLA service between two SRX Series device endpoints (book-ended) and both SRX Series devices must have the same version of the Junos OS image.

You can configure vSRX instances, SRX300 line devices, SRX550M as spoke devices and SRX1500, SRX4100 and SRX4200 as hub devices.

Starting in Junos OS Release 15.1X49-D160 and in Junos OS 19.1R1, AppQoE is supported on SRX4100 and SRX4200 device when the device is operating in chassis cluster mode. You can configure the device to operate both in active/active and in active/passive modes and deploy the device as spoke device in SD-WAN deployments.
NOTE: When the device is operating in chassis cluster mode, if the secondary node (node 1), through which traffic is forwarded, is rebooted, multiple switching of the application traffic between the links across secondary node links occurs. This happens when the available links on primary node (node 0) are having less active probe SLA path score compared to the secondary node links. This behavior continues until AppQoE active probe SLA path score results are available to indicate that there is 100% packet loss on all the links on secondary node.

Benefits of Application Quality of Experience

- 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 security devices at the branch offices and remote offices connect directly to a specific SRX 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 security device at the branch office or remote site is configured to connect directly to any other security device in the network that is also part of mesh.

Limitations

Implementation of AppQoE on security 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 security 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 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.

• The SRX4600 device has the following limitations:
  • The class of service (CoS) for generic routing encapsulation (GRE) is not supported when AppQoE is configured.
  • Passive probe details might not be available for the each short-lived session.
  • Synchronization of the session states might not happen on secondary node in Z-line mode traffic processing when device is operating in chassis cluster mode.

Understanding Application Quality of Experience 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 Application Quality of Experience 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 Application Quality of Experience 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 SRX Series 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.

**NOTE:** Starting in Junos OS Release 18.3R1 and in Junos OS Release 15.1X49-D150, on all supported SRX Series devices and vSRX instances, in order to detect if a link or path is down by passive probes, a minimum of three probe requests and 100% packet loss must occur in a sampling period for a given session to trigger SLA violation.

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 an 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 security 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

- Supported SRX Series device with Junos OS Release 18.2 and Junos OS Release 15.1X49-D150 or later. This configuration example is tested for Junos OS Release 18.2.
- Valid application identification feature license installed on an SRX Series 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.

#### 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 13 on page 292 shows the topology used in this configuration example.

Figure 13: Topology for AppQoE Configuration

Table 24 on page 292 provides the details of the parameters used in this example.

Table 24: AppQoE Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APBR profile</td>
<td>apbr1</td>
<td>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.</td>
</tr>
<tr>
<td>APBR rule</td>
<td>rule-app1</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>rule-app2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rule-app2</td>
<td></td>
</tr>
<tr>
<td>Routing Instance</td>
<td>appqoe-vrf</td>
<td>Instance type as routing and forwarding (VRF) instance</td>
</tr>
<tr>
<td>RIB group</td>
<td>lanvrf</td>
<td>Name of the routing information base (RIB) (also known as routing table) group.</td>
</tr>
</tbody>
</table>
### Table 24: AppQoE Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define AppQoE as service</td>
<td>system-services=appqoe</td>
<td>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.</td>
</tr>
<tr>
<td>SLA rule</td>
<td>• sla1</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• sla2</td>
<td>An SLA rule is associated with an APBR rule, which is matched to the application or application group.</td>
</tr>
<tr>
<td>SLA options</td>
<td>local-route-switch = enabled</td>
<td>Specify local route switch option. This option enables switching of application traffic to an alternate path if an SLA violation occurs.</td>
</tr>
<tr>
<td>SLA metrics profile</td>
<td>• metric1</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• metric2</td>
<td></td>
</tr>
<tr>
<td>Active probes</td>
<td>• probe1</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• probe2</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Overlay path</td>
<td>overlay-path1</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>Tunnel</td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>path2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tunnel</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Local IP addresses- 1.1.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remote IP addresses- 1.1.1.1</td>
</tr>
<tr>
<td></td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Local IP addresses- 1.1.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remote IP addresses- 1.1.1.1</td>
</tr>
<tr>
<td></td>
<td>path3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tunnel</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Local IP addresses- 2.1.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remote IP addresses- 2.1.1.1</td>
</tr>
<tr>
<td></td>
<td>Probe</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Local IP addresses- 2.1.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remote IP addresses- 2.1.1.1</td>
</tr>
<tr>
<td></td>
<td>Destination Grouping</td>
<td>destination-path-group-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 security devices using the following commands:

```
[edit]
user@host set security flow tcp-mss ipsec-vpn mss 1200
user@host set 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@host set services application-identification application jun-appqoe priority high
user@host set 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-0/0.1 gr-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
```
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
   ```
**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
   ```
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. See also `destination-path-group`.

   ```
   user@host# set security advance-policy-based-routing destination-path-group destination-path-group-1
   ```

   ```
   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.

   ```bash
   user@host# set security advance-policy-based-routing sla-rule sla1 switch-idle-time 60
   ```

2. Define switch idle time for the SLA rule.

   ```bash
   user@host# set security advance-policy-based-routing sla-rule sla1 metrics-profile metric1
   ```

3. Associate active probe parameter (probe1) to the SLA rule.

   ```bash
   user@host# set security advance-policy-based-routing sla-rule sla1 active-probe-params probe1
   ```

4. Define passive probe parameters.

   ```bash
   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
   ```

   **NOTE:** Starting in Junos OS Release 19.2 onwards, you can configure the `violation-count` and the `sla-export-factor` parameters in `[edit security advance-policy-based-routing sla-rule rule-name]` hierarchy.

   You can configure the `violation-count` for both active probe parameters and passive probe parameters. The `violation-count` option configured in `[edit security advance-policy-based-routing sla-rule rule-name passive-probe-params]` hierarchy is overridden by `[edit security advance-policy-based-routing sla-rule rule-name violation-count]` option. The violation count configured for passive probe parameter will be ignored and violation count default value is used. A warning message is also displayed when you attempt to commit the configuration.
**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 {
        R1-appqoe;
    }
    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 Probes Sent: 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 profile apbr-1 destination-group-name d1 status apbr1 application junos:HTTP` 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:

<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Src-IP</th>
<th>Dst-IP</th>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing-Jit(us)</td>
<td>Egr-Jit(us)</td>
<td>host</td>
<td>destination</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
## Meaning
The output shows RTT, jitter and packet-loss measured between the installed probe points.

## Understanding AppQoE Configuration Limits

Starting in Junos OS Release 15.1X49-D160 and in Junos OS Release 19.1R1, AppQoE enforces the configuration limit for overlay paths, metric profiles, probe parameters, and SLA rules per profile when you configure application-specific SLA rules and associates the SLA rules to an APBR profile.

If you configure the parameters more than the allowed limit, error messages are displayed when you commit the configuration.

Examples of error messages:

```
[edit security advance-policy-based-routing]
'sla-rule sla0'
    Cannot configure more than 32 sla rules
error: configuration check-out failed
```

```
[edit security advance-policy-based-routing]
'overlay-path grep2'
```

### NOTE:
The following sample error messages are from the SRX4100 and SRX4200 device. The value of the configuration limit might not reflect exact number supported; the numbers might differ between the supported devices.
Understanding Application Path Selection Based on Link Preference and Priority

One of the important requirements of a software-defined WAN (SD-WAN) is to measure the quality of underlay network paths and, based on the results, determine the best paths to use for the delivery of each packet.

Starting in Junos OS Release 18.4R1 and in Junos OS Release 15.1X49-D160, you can configure application-specific quality of experience (AppQoE) to select the application path based on the link priority and the link type when multiple paths that meet the SLA requirements are available.

You can select an MPLS or Internet link as the preferred path, assign the priority between 1 through 255 with a lower value indicating a more preferred link. A value of one (1) indicates highest priority. If there are multiple paths available, the path which has the highest priority is selected.

For example, if an MPLS path is selected for VoIP traffic and quality degradation occurs during a call because of jitter or packet loss, the packets are sent through another path (Internet) that meets SLA requirements. Now application traffic is sent through the Internet path and if the quality in the Internet path is degraded, the path is switched back to MPLS.

You can configure the link priority and link type of each underlay interface in an advanced policy-based routing (APBR) rule, and the same parameters are inherited by the corresponding overlay. An underlay interface in this case is the final outgoing interface in the routing topology for the overlay.
For example, in a network infrastructure, if the underlay is a fourth-generation (4G) LTE connection, then the dialer interface can be configured as the underlay interface for AppQoE. Similarly, if the underlay is a DSL connection, then the corresponding Point-to-Point Protocol over Ethernet (PPPoE) interface can be configured as the underlay interface for AppQoE.

**Benefits of Application Path Preference and Priority**

- Provides flexibility of selecting the best path for application traffic.
- Enables routing of application traffic over the cost-effective connectivity option while ensuring SLA requirements (latency and jitter) are met.
- Supports dynamic path switching if the selected application path experiences a degradation in quality.

**Path Selection Mechanism**

Application traffic is routed through separate links based on the link preference as following:

- AppQoE path selection mechanism includes a list of best paths to a specific destination that meets the SLA requirements. From this list, AppQoE selects a path that matches the link preference configured by the user.
- If there are multiple such paths, the path that has the highest priority among them is selected.
- If there is no priority or link type preference configured, then a random path or the default path is selected.
- If no links that meet the SLA requirements are available, then the best available link in terms of the highest SLA score and link type preference, in case strict affinity is configured, is selected.
- If multiple links that meet the SLA requirements are available, then the one with the highest priority is selected.

**Configuring Link Type and Link Priority for Application Path**

You can configure the link type either as IP or MPLS and set the priority for the underlay links. Priority can be any value from the range of values (1-255) with a lower value indicating a more preferred link. A value of one (1) indicates highest priority.

The following steps summarize how to specify a path for the application traffic based on link preference:

- Define the link type (IP or MPLS) and link priority (1 through 255) for the underlay links in the APBR profile.
- Configure an APBR rule for one or more than one applications (example: for HTTP) or application groups.
- Associate the APBR rule with the APBR profile. Because the APBR rule is defined for an application or a group of applications, you can enforce the link preference at the application or application group level.
• Specify the link type preference as IP or as MPLS and specify the link-type affinity as strict in an SLA rule. If you do not specify the link-type affinity, the default affinity (loose) is selected. The SLA rule is attached to the APBR profile.

NOTE: You can select an MPLS or Internet (IP) or Any link as the preferred path. If you do not select IP or MPLS, the preferred link type Any is selected when the link-type affinity is configured as the default link type affinity (loose). Configuring the link type as Any when the link type affinity is configured as strict is not supported.

• In the APBR profile, traffic matching the applications and application groups as per APBR rule, is forwarded to the static route and the next-hop address as specified in the routing instance. The application traffic is assigned to a particular path/link based on the configured link type and preference for underlay interfaces and the specified link-type affinity used in the SLA rule.

If you do not configure link preference in the SLA rule, then the default values for link type and link priority are considered.

Understanding Link-Type Affinity for the Preferred Link

You can configure the link-type affinity as strict for the preferred link type. For the strict affinity, the AppQoE ensures that the path selected is always of the preferred link type. The default link-type affinity is loose. When you do not configure the link-type affinity as strict, then the default value is applied. That is—if there are no SLA meeting links belonging to the preferred link type, then AppQoE selects a link outside the preferred link type that meets the SLA.

AppQoE specifies a path for the application traffic according to the configured link preference and link-type affinity.

The path selection mechanism checks if there are already assigned overlay links based on the SLA metrics of the application is available as follows:

• Yes—The best path for the application is searched for the database.

• No—The path selection mechanism attempts to find a path based on the link-type affinity, type, and priority:
  • Strict—If the link-type affinity is configured as strict, then a new set of overlay links that meet the defined link type is created. Among them, an overlay link with the highest SLA score is selected.

  If multiple links with the highest SLA score are available, then the link with highest priority is selected.

  • Default (loose)—If the link-type affinity is not configured as strict, then an overlay link with the highest SLA score is selected. If there are no links meeting the SLA requirements and belonging to the preferred link type available, then AppQoE selects a link outside of the preferred link type that meets the SLA requirements. However, path selection mechanism continues to check for a preferred link meeting
the SLA requirements. Once the preferred link type meeting the SLA requirement is available, then the application traffic is switched back to that link.

If there are multiple links with the highest priority, then a random link among them is selected.

**Limitation**

In the middle of a session, switching from a link with a lower priority value that meets the SLA requirements to a link with a higher priority is not supported when the link with higher priority meets the SLA requirements.

**Example: Configuring Link Preference and Priority for AppQoE**

This example shows how to configure AppQoE to select the link based on the link priority and the link type when multiple links that meet the SLA requirements are available.

**Requirements**

- Supported SRX Series device with Junos OS Release 18.4 and Junos OS Release 15.1X49-D160 or later. This configuration example is tested for Junos OS Release 18.4.
- Valid application identification feature license installed on an SRX Series 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.
- Application tracking support enabled for the zone. See Application Tracking.

**Overview**

Before you begin:
• Complete APBR profile configuration and define SLA rules. See Example: Application Quality of Experience (AppQoE).

You configure AppQoE to select the link based on the link priority and the link type. You can configure the link type either as IP or MPLS and set the priority for the underlay links. You can also configure the link-type affinity as strict for the preferred link type.

You can define the link type and priority for the underlay links in the SLA rule. The SLA rule is assigned to an APBR profile. Because the APBR rule is defined for an application or a group of applications, you can enforce the link preference at the application or application group level. The link preference configuration is applied for the application traffic matching the APBR rule.

Figure 14 on page 315 shows the topology used in this example.

Figure 14: Topology for Configuring Link Type and Link Priority for Application Path

Table 25 on page 315 and Table 26 on page 316 provide the details of the parameters used in this example.

Table 25: AppQoE Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APBR profile</td>
<td>apbr1</td>
<td>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.</td>
</tr>
<tr>
<td>APBR rule</td>
<td>rule1</td>
<td>Define the rules for the APBR profile. Associate the rule with one or more than one application (example: for junos:HTTP, junos:SSH).</td>
</tr>
</tbody>
</table>
Table 25: AppQoE Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLA rule</td>
<td>sla1</td>
<td>Individual applications and application group must have an SLA rule attached. An SLA rule is associated with an APBR rule, which is matched to the application or application group.</td>
</tr>
</tbody>
</table>

| Link-type affinity | Strict | For strict affinity, AppQoE ensures that the path selected is always of the preferred link type. |

Table 26: Link Preference Parameters for Underlay Interfaces

<table>
<thead>
<tr>
<th>SLA Rule</th>
<th>Underlay Interfaces</th>
<th>Link Type</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>sla1</td>
<td>ge-0/0/1</td>
<td>MPLS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/2</td>
<td>MPLS</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3</td>
<td>IP</td>
<td>3</td>
</tr>
</tbody>
</table>

In this example, you configure the link ge-0/0/1 with link type as MPLS and priority as 1, ge-0/0/2 with link type as MPLS with priority 2, and ge-0/0/3 with link type as IP with priority 3. All the links have same the SLA score as defined in the SLA rule (sla1). For the SLA rule (sla1), configure the link type preference as MPLS.
The following examples show how the path selection mechanism selects the link based on preferred link and the link-type affinity. The topology used in this example is shown in Figure 15 on page 317 and the configured link type and link-type affinity is shown in Table 27 on page 317.

**Figure 15: Path Section Mechanism Example**

![Path Selection Mechanism Example Diagram]

**Table 27: Link Type and Priority Details**

<table>
<thead>
<tr>
<th>Links</th>
<th>Link Type</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1</td>
<td>MPLS</td>
<td>1</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>MPLS</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>IP</td>
<td>3</td>
</tr>
</tbody>
</table>

- Case 1: When preferred link type is configured as MPLS and link-type affinity is configured as loose (default option), the path selection mechanism details are provided in Table 28 on page 317.

**Table 28: Case 1: Preferred Link Type is MPLS and Link-Type Affinity is Default (Loose)**

<table>
<thead>
<tr>
<th>Link Selected For Traffic</th>
<th>Change in Situation</th>
<th>Which Links are Eligible</th>
<th>Traffic Switched To</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1</td>
<td>An SLA violation is reported in ge-0/0/1</td>
<td>ge-0/0/2 and ge-0/0/3</td>
<td>ge-0/0/2</td>
<td>Link ge-0/0/2 is selected because it has higher priority.</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>An SLA violation is reported in ge-0/0/2</td>
<td>ge-0/0/3</td>
<td>ge-0/0/3</td>
<td>Link ge-0/0/3 is selected because it is only remaining eligible link meeting SLA requirements.</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>SLA violation is cleared in ge-0/0/1</td>
<td>ge-0/0/3 and ge-0/0/1</td>
<td>ge-0/0/1</td>
<td>Traffic is switched back to preferred link ge-0/0/1 (MPLS) from the link ge-0/0/3 (IP).</td>
</tr>
</tbody>
</table>
Case 2: When the preferred link type is MPLS and link-type affinity configured as strict, the path selection mechanism details are provided in Table 29 on page 318.

Table 29: Case 2: Preferred Link Type is MPLS and Link-Type Affinity is Strict

<table>
<thead>
<tr>
<th>Link Selected For Traffic</th>
<th>Change in Situation</th>
<th>Which Links are Eligible</th>
<th>Traffic Switched To</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1</td>
<td>An SLA violation is reported in ge-0/0/1</td>
<td>ge-0/0/2 and ge-0/0/3</td>
<td>ge-0/0/2</td>
<td>Link ge-0/0/2 is selected because it is matching the link type preference MPLS.</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>An SLA violation is reported in ge-0/0/2</td>
<td>ge-0/0/3</td>
<td>ge-0/0/2</td>
<td>Link ge-0/0/2 remains as the selected path. Because of the strict affinity, ge-0/0/3 (which has link type configured as IP) is not selected.</td>
</tr>
</tbody>
</table>

NOTE: When there are multiple interfaces meeting the SLA requirements are available, the path is selected based on link-type preference, and then link priority. If all links have the same link-type preference and priority, then a random selection of the link is done.

Configuration

Configure Link Preference and Priority

Step-by-Step Procedure

Configure AppQoE to select the link based on the link priority and the link type:

1. Create an APBR profile with three rules matching application HTTP and SSH with link type and preference for underlay interfaces.

```
user@host# set security advance-policy-based-routing underlay-interfaces interface ge-0/0/1 unit 0 link-type MPLS priority 1
user@host# set security advance-policy-based-routing underlay-interfaces interface ge-0/0/2 unit 0 link-type MPLS priority 2
user@host# set security advance-policy-based-routing underlay-interfaces interface ge-0/0/3 unit 0 link-type IP priority 3
```
2. Configure the SLA rule (sla1) with preferred link type as **MPLS** and link-type affinity as **strict**.

```bash
user@host# set security advance-policy-based-routing sla-rule sla1 preferred-link-type MPLS
user@host# set security advance-policy-based-routing sla-rule sla1 link-type-affinity strict
```

3. Associate an SLA rule with the APBR profile.

```bash
user@host# set security advance-policy-based-routing profile apbr1 rule rule1 match dynamic-application
   junos:HTTP

user@host# set security advance-policy-based-routing profile apbr1 rule rule1 match dynamic-application
   junos:SSH

user@host# set security advance-policy-based-routing profile apbr1 rule rule1 then sla-rule sla1
```

**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 advance-policy-based-routing]
user@host# show
profile apbr1 {
   rule rule1 {
      match {
         dynamic-application [junos:SSH junos:HTTP];
      }
      then {
         routing-instance appqoe-vrf;
         sla-rule {
            sla1;
         }
      }
   }
}
underlay-interface ge-0/0/1 {
   unit 0 {
      link-type MPLS;
      priority 1;
   }
}
```
Verify AppQoE Configuration

**Displaying SLA Statistics**

**Purpose**
Display the details of the SLA statistics based on the 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: 766
  - Possible Passive Probe Sessions: 3
  - Passive Probe Sessions Sampled: 3
  - Passive Probe Ongoing Sessions: 0
  - SLA violations: 79

- **Active Probe Statistics**
  - Active Probe Paths: 0
  - Active Probe Session: 3
### Understanding System log Messages for AppQoE

Starting in Junos OS Release 19.2R1, the support for the application-level logging is available for AppQoE on SRX Series devices. This feature is introduced to reduce the impact on CSO or log collector device while processing large number of system log messages generated at the session-level. The security device maintains session-level information and provides system log messages for the session level. With application-level logging replacing session-level logging, the overhead on security device decreases and AppQoE log throughput increases.

AppQoE sends following system log messages:

- **APPQOE_SLA_METRIC_VIOLATION**: When a violation is detected for a session and when a session's path is resolved as a result of moving to a new link.

- **APPQOE_BEST_PATH_SELECTED**: When a session switches the path for its data traffic.

With application-level logging, all session-level logs are supported at the application-level. The AppQoE functionality of sending real-time probes, measuring the SLA metrics, violation detection, and path-switch continues at the session-level. However, as part of application-level summarization feature, datapath sessions notify the SLA metrics, violation information, and path switch to AppQoE database. The information thus received from datapath is aggregated at the application-level, and then sent in the form of system logs to collector device.

Table 30 on page 322 provides details of new application-level logs are supported from Junos OS Release 19.2R1 onwards.
Table 30: Application-Level Log Messages

<table>
<thead>
<tr>
<th>System Log Message</th>
<th>Description</th>
</tr>
</thead>
</table>
| APPQOE_APP_SLA_METRIC_VIOLATION | • This system log message is generated the first time the application is in violation.  
• The SLA metrics are measured for each application session in the data path. The SLA violation metrics continue to be measured at the session-level only. However, the metrics or data pertaining to the SLA violation are sent to the AppQoE database by all data sessions of that application when their SLA is violated.  
• In the case of dual CPE, the node which is active for the application generates the APPQOE_APP_SLA_METRIC_VIOLATION report. |
| APPQOE_APP_BEST_PATH_SELECTED | • This system log message is generated when an application goes through a path switch. This log report is also generated to clear the violation happened because of self heal (when the SLA violation is cleared by itself before any change in the link).  
• For application-level logging, once an application or a link switches to an alternate path, AppQoE sends the log message APPQOE_APP_BEST_PATH_SELECTED to the collector device. |
| APPQOE_APP_PASSIVE_SLA_METRIC_REPORT | • This system log message is generated for passive probe SLA metrics data. This message is generated once the number of samples collected meet with the SLA export factor.  
• With the support of application-level logging, each probe candidate session sends information to AppQoE where the metrics are aggregated and averaged out before it is sent to the collector. Therefore the passive SLA report thus aggregated at the application level includes the averaged data from all of those application data sessions. |

Application-level logging introduces the following AppQoE functionality changes:

• Active probe maintains and uses only real-time RTT and jitter values. For packet loss, it refers the previous session's cause because packet loss can be calculated only at the end of the window.

• During configuration commit, active probe sets RTT and jitter values to highest 32-bit value for all entries.

• Active probe retains previous session's values until the a proper real-time value of the metrics are available.

• When a 100% packet loss is experienced in active probing, all other metrics are set to highest 32-bit value.
**Reporting of Invalid Values for RTT and Jitter**

When the data for RTT and Jitter is not available, log messages sent with an invalid value of 0xFFFFFFFF and it can be ignored by the log collector. Table 31 on page 323 provides some possible scenarios when the invalid RTT and Jitter is sent.

**Table 31: Application-Level Log Messages Affected by Invalid Data for RTT and Jitter**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Affected System Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>100% packet loss:</td>
<td>APPQOE_APP_PASSIVE_SLA_METRIC_REPORT</td>
</tr>
<tr>
<td></td>
<td>APPQOE_APP_SLA_METRIC_VIOLATION</td>
</tr>
<tr>
<td>Packet-loss greater than 0 and less than 100%:</td>
<td>APPQOE_APP_PASSIVE_SLA_METRIC_REPORT</td>
</tr>
<tr>
<td></td>
<td>APPQOE_APP_SLA_METRIC_VIOLATION</td>
</tr>
<tr>
<td>No Packet-loss</td>
<td>APPQOE_APP_SLA_METRIC_VIOLATION</td>
</tr>
<tr>
<td></td>
<td>APPQOE_APP_PASSIVE_SLA_METRIC_REPORT</td>
</tr>
</tbody>
</table>

**Disable AppQoE Logging**

By default AppQoE log-type is set as system log. If you want to disable AppQoE, then configure the log-type as disabled in the following configuration:

1. Disable AppQoE logging

   ```
   [edit]
   user@host# set security advance-policy-based-routing sla-options log disabled
   ```

2. Enable AppQoE logging

   ```
   [edit]
   user@host# set security advance-policy-based-routing sla-options log system log
   ```
Configure SLA Export Factor

You can configure the SLA export factor to report probe metrics at the application level.

1. Configure SLA export factor at SLA rule level.

   ```
   [edit]
   user@host# set security advance-policy-based-routing sla-rule rule-name sla-export-factor number
   ```

   Example:

   ```
   [edit]
   user@host# set security advance-policy-based-routing sla-rule RULE_1 sla-export-factor 5
   ```

   When you configure the `sla-export-factor` as 5, passive probe results are exported once at the end of the 5th, 10th, and 15th probe interval. You can use a passive probe report to report any data that remains unreported in the probe interval at the end of a session.

   With application level summarization, each probe candidate session must send data to central location where the metrics are aggregated. The data thus aggregated is sent out once the configured SLA export factor is met.

Configure Violation Count

You can configure the violation count to report probe metrics at the application level. Violation count indicates the number of violations that must occur in a sampling-period for a given session before a link is marked as having violated the SLA.

1. Configure violation count at SLA rule level.

   ```
   [edit]
   user@host# set security advance-policy-based-routing sla-rule rule-name violation-count number
   ```

   Example:

   ```
   [edit]
   user@host# set security advance-policy-based-routing sla-rule RULE_1 violation-count 5
   ```

   In this example, when you configure the violation count as 5, then the link is marked as violated SLA after 5 consecutive times the violation has occurred.
Application Quality of Experience (AppQoE) Based on the DSCP Bits of Incoming Traffic

AppQoE depends on application identification to associate an SLA with the incoming traffic. AppQoE utilizes APBR to select the best possible link for the application traffic in order to meet performance requirements specified as in SLA.

Application identification techniques rely on deep packet inspection (DPI). There are some cases where DPI engine might not be able to identify the application, for example—encrypted traffic. As a result, AppQoE might not be able to identify the application and associate any SLA to the incoming traffic. Because of this, you might not be able to provide quality of experience (QoE) for the traffic.

To overcome this scenario, Starting in Junos OS Release 19.4R1, AppQoE supports SLA-based path selection for the incoming traffic on the basis of DSCP value.

Starting from Junos OS Release 19.3R1, SRX Series devices introduced APBR functionality on the DSCP-tagged traffic. You can configure an APBR rule with dynamic-application or application group, DSCP value or combination of both dynamic-application and DSCP value. Using this enhancement, AppQoE selects the best possible link for the application traffic based on the application signature or DSCP value or combination of both application identification and DSCP value.

DSCP Support in APBR

In a APBR rule, you can configure a DSCP value or dynamic applications or combination of both.

When you configure both DSCP and dynamic application in a APBR rule, the rule is considered as match if the traffic matches all the criteria specified in the rule. When there are multiple DSCP values present in the APBR rule, then if any one criteria matches, it is considered as match.

A APBR profile can contain multiple rules, each rule with a variety of match conditions.

In case of multiple APBR rules in a APBR profile, the rule lookup uses the following priority order:

1. Rule with DSCP + dynamic application
2. Rule with dynamic application
3. Rule with DSCP value

To understand how the APBR performs rule lookup and applies the rules, see Using DSCP as Match Criteria in APBR Rules.

AppQoE Functionality for the Traffic based on the DSCP Value

Network Service Orchestrator can map application to DSCP value at external service function and the same is provisioned at the gateway router to map the DSCP to desired SLA profile.
Figure 16 on page 326 shows a scenario where AppQoE performs SLA-based path selection for the incoming traffic on the basis of DSCP value and application signature in a gateway router use case.

Figure 16: Path Selection for the Traffic Based on DSCP Value and Application

For the traffic based on the DSCP value, AppQoE works as follows:

- All the traffic entering the gateway router from LAN undergoes application identification. Until DPI identifies an application, the system forwards the traffic stream to a default forwarding virtual routing and forwarding (VRF) instance. VRF includes an outgoing interface associated to it.

- Junos OS application identification identifies applications and once an application is identified, its information is saved in the application system cache (ASC).

- The system continues to check if any application information available either from DPI classification or ASC.

- The APBR mechanism classifies sessions based on well-known applications signatures and DSCP values and uses policy to identify the best possible route for the application. The APBR policy maps application traffic to a specific VRF.

- The presence of an SLA rule in the APBR configuration triggers the AppQoE functionality; AppQoE performs SLA-based path selection for the traffic based on the application or DSCP value.

For more information on configuring APBR with DSCP as match criteria, see Advanced Policy-Based Routing.

**DSCP-Based SLA Rule and Passive Probes**

A single DSCP includes multiple application categories bundled into it. Different application categories have their individual traffic pattern. In such a scenario, detection of violation using passive probes and applying it to all the sessions might cause false negative and false positive. As a workaround, avoid using
passive probing when you have configured DSCP-based SLA rule. You can use active probes for the
destination path group to which the traffic is forwarded.

Limitations

AppQoE deployments with DSCP-based rules on the device in chassis cluster mode have the following
limitations:

- If the rule match is completed before the application identification is done, and AppQoE moves the
  session to the other node, then application identification does not complete. This condition occurs when
  the DSCP-based rule is configured.

- If you have configured two APBR rules—1) with DSCP value 2) with both DSCP and dynamic application,
  and assigned the same DSCP value in both the rules, on receiving the first packet, APBR matches with the
  DSCP rule. In case the best path is identified on the other node, then the session is moved to the other
  node. In this scenario, the application sessions are matched against the DSCP rule and not with the
  APP+DSCP rule.

AppQoE Support for Granular APBR Rules

Starting in Junos OS Release 20.1R1, AppQoE utilizes the granular rule matching functionality provided
by APBR to provide the quality of experience (QoE) based on the application traffic.

AppQoE utilizes AppID and APBR capabilities to identify specific applications and application groups and
specifies a path for certain traffic by associating SLA (service-level agreement) profiles to a routing instance
on which the application traffic is sent as per APBR rules.

In Junos OS Release 18.2R1, APBR supported configuring policies by defining source addresses, destination
addresses, and applications as match conditions. After a successful match, the configured APBR profile is
applied as an application service for the session. In Junos OS Release 20.1R1, AppQoE leverages the
APBR enhancement and selects the best possible link for the application traffic as sent by APBR to meet
performance requirements specified in SLA.

Let's understand the new enhancement with a workflow and a sample configuration.
Workflow for AppQoE

You can define APBR policies for a security zone. APBR uses the following sequences to match the traffic by a policy and apply rule to forward the traffic:

1. APBR policy rules match the traffic at the ingress zone. The policy match conditions include the source address, destination address, source identity (optional), and application.

2. APBR policy action specifies the APBR profile for the matching traffic.

3. The APBR profile configuration includes the set of rules that contains set of dynamic applications, or dynamic applications group or DSCP value as match condition. The action part of the rules defines:
   - The routing instance to forward the traffic and then transit traffic to a specific device or interface.
   - SLA rule to trigger AppQoE functionality.

4. AppQoE initiates active and passive probes for performance measurements.

5. AppQoE specifies a path for the application traffic according to the SLA rules.

Sample Configuration

In this example, you want to forward Telnet and HTTPS traffic arriving at the trust zone to a specific device or interface through a best available link. When traffic arrives at the trust zone, APBR matches the traffic with matching criteria source address, destination address and applications defined in policies POLICY-1 and POLICY-2. If traffic matches the policy, corresponding APBR profiles PROFILE-1 or PROFILE-2 are applied.

APBR uses the application details to look for a matching rule in the profile. If a matching rule is found, the traffic is redirected to the specified routing instance as defined in the rule.

AppQoE checks whether an SLA is enabled for this session. If the session is a candidate for an SLA measurement, AppQoE initiates active and passive probes for performance measurements. AppQoE measures the application SLA across multiple WAN links, and maps the application traffic to a path among the available links.

```
[edit security address-book]
user@host# show
global {
  address a1 1.1.1.1/32;
  address b1 15.15.15.2/32;
}
A1 {
  address example {
    dns-name www.facebook.com {
    }
  }
}```
[edit security advance-policy-based-routing]
user@host# show from-zone trust

......
policy POLICY-1 {
  match {
    source-address address-1;
    destination-address A1;
    application junos-https;
  }
  then {
    application-services {
      advance-policy-based-routing-profile PROFILE-1;
    }
  }
}

......

policy POLICY-2 {
  match {
    source-address address-1;
    destination-address address-2;
    application junos-telnet;
  }
  then {
    application-services {
      advance-policy-based-routing-profile PROFILE-2;
    }
  }
}

......

[edit security advance-policy-based-routing]
user@host# show profile PROFILE-1

......
rule RULE-1 {
  match {
    dynamic-application [junos:YAHOO-MAIL junos:FACEBOOK-ACCESS ];
  }
  then {
    routing-instance appqoe-vrf;
  }
}
The output sample is truncated to display configuration details for APBR policy and APBR profile. For more information, see following topics:

- Configuring Advanced Policy-Based Routing Policies
- Example: Application Quality of Experience (AppQoE)

## AppQoE Multi-homing with Active-Active Deployment

Starting In Junos OS Release 20.2R1, AppQoE is enhanced to support multi-homing with active-active deployment. Previously, AppQoE supported multihoming with active-standby deployment.

In active-active deployment, the spoke device connects to multiple hub devices. Application traffic can transit through any of the hub devices if the link to the hub device meets SLA requirements. Application traffic can seamlessly switch between the hub devices in case of SLA violation or the active hub device is not responding.

Figure 1 shows a mesh topology. In this topology, an end point is reachable through more than one node.
To enable multihoming in active-active mode, you must configure the BGP multipath to allow the device to select multiple equal-cost BGP paths to reach a given destination.

When you enable BGP multipath, the device selects multiple equal-cost BGP paths to reach a given destination, and all these paths are installed in the forwarding table. AppQoE completes the route lookup and gets the next-hop route details along with the corresponding overlay-links. AppQoE obtains the overlay-link property from the configured destination path group.

Based on the application’s SLA requirements and link preferences, AppQoE determines the best link among all the links in that destination-path-group. In case of SLA violation, based on the SLA score and link preferences, AppQoE selects alternate links across all the configured destination-path-group if the end-point is reachable through those links.

For more information on BGP multipath configuration, see Examples: Configuring BGP Multipath.

**Limitation**

In certain scenario when next-hop ID for the route changes, the existing sessions remain on the SLA-violated link even though another link that meets SLA requirements is available. However, the new sessions are not impacted in this case and they are routed through the links that meet SLA requirements.
## Application-Based Multipath Routing Overview

Traffic for video and voice are sensitive to packet loss, latency and jitter. Packet loss directly leads to degradation in the quality of voice and video calls. in voice or video calls.
To ensure timely delivery of these sensitive application traffic, application-based multipath routing (also referred as multipath routing in this document) is supported on SRX Series devices to allow the sending device to create copies of packets, send each copy through two or more WAN links.

Multipath identifies two or more paths based on the SLA configuration and sends out a copy of the original traffic on all the identified paths.

On the other end, among the multiple copies of the packet received, the receiving device selects the first received packet and drops the subsequent ones. On the receiving device, while the copy of the packet is in progress, multipath calculates the jitter and packet loss for the combined links and then estimates the jitter and packet loss for the same traffic on individual links. You can compare the reduction in packet loss when combined links are used instead of individual links used for traffic.

Sending the multiple copies of the application traffic ensures that if there is a packet loss or delay, the other link might still deliver the packet to the endpoint.

SRX Series devices support application-based multipath routing starting in Junos OS Release 15.1X49-D160. Starting in Junos OS Release 19.2R1 and Junos OS Release 15.1X49-D170, application-based multipath routing support is available when device is operating in chassis cluster mode.

Multipath routing leverages following functionality:

- Application identification details from Deep Packet Inspection (DPI)
- APBR functionality for packet forwarding feature
- AppQoE service for SLA association.

**Supported Use Cases**

- SD-WAN hub and spoke topology
- SD-WAN mesh topology

**Limitations**

- All the selected WAN links must be of ECMP paths for a destination.
- All the selected WAN interfaces which need to be a part of multipath routing sessions must belong to one single zone
- Multipath routing feature is supported only between two book-ended security devices.
Benefits of Multipath Routing

- Multipath support in SD-WAN use case enhances application experience by reducing packet loss, faster delivery of the packet, and less jitter that results in better quality of service for the traffic especially for the voice and video traffic.

Understanding Workflow in Multipath Routing

The following sequences are involved in applying multipath routing:

- Junos OS application identification identifies applications and once an application is identified, its information is saved in the application system cache (ASC).

- Application policy-based routing (APBR) queries the application system cache (ASC) module to get the application attributes details.

- 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 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 candidate for an SLA measurement, and if multipath routing is configured, then multipath routing is triggered.

- Based on the SLA rule, multipath routing obtains the underlay link types and corresponding overlays on which packet duplication needs to be performed. Multipath routing can be triggered based on the configuration of an SLA rule. When multipath routing is configured within an SLA rule for a specific application, AppQoE functionality is disabled for all sessions of that application matching the SLA rule.

- Based on the application traffic and the configured bandwidth limit, multipath identifies two or more paths and triggers a copy of the original traffic on all the identified paths. Multipath routing path selection is done on the overlay paths. The parameters to limit the bandwidth is based on the underlay link-speed and selection is based on link-type.

- On the receiving device, while the copy of the packet is in progress, multipath calculates the jitter and packet loss for the combined links and then estimates the jitter and packet-loss for same traffic on individual links.

- On the receiving device, multipath routing accepts packets of a session arriving through different links, maintain sequence of a packet arriving on different CoS queues, and drop any duplicates.

Multipath routing copies packets on all the links belonging to a rule till the bandwidth limit is reached. The bandwidth limit is calculated based on the least link speed identified for that rule. This is applicable for all the sessions for all the applications which match that multipath routing rule. Once the limit is reached, multipath routing stops copying of packets and starts a timer for a time period as configured in max-time-wait option in the multipath routing configuration. When the timer expires, it restarts the copying of the packets again.
Example: Configuring Application-Based Multipath Routing

This example shows how to configure multipath routing to provide quality of experience (QoE) by enabling real-time monitoring of the application traffic according to the specified SLA.

Requirements

- Supported SRX Series device with Junos OS Release 15.1X49-D160, Junos OS Release 19.2R1, or later. This configuration example is tested for Junos OS Release 15.1X49-D160.
- Valid application identification feature license installed on a security 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.
- Ensure that the following features are configured:
  - Application Identification
  - APBR
  - AppQoE
  - Link Preference and Priority for AppQoE

Overview

To ensure uninterrupted delivery of these sensitive application traffic, application-based multipath routing is supported on security devices to allow the sending device to create copies of packets, and send each copy through two WAN links to the destination.

Multipath routing identifies two paths based on the SLA configuration and creates duplicate copy of the application traffic and sends the traffic simultaneously on different physical paths. On the receiving device, while the copy of the packet is in progress, multipath routing estimates on the reduction in jitter, RTT and
packet loss and analyzes the quality of service for routing the traffic to the best link to provide SLA to the end user. This also helps in estimation on the reduction in jitter, RTT and packet loss is done. If both the copies are received on the remote end, then the first received packet is considered, and drops the subsequent ones.

Table 32 on page 336 provides the details of the parameters used in this example.

Table 32: Configuration Parameters for Multipath Rule, SLA Rule, and APBR

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multipath rule (multi1)</td>
<td>Number of paths</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>bandwidth-limit</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Maximum time to wait</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Link type</td>
<td>MPLS, IP</td>
</tr>
<tr>
<td></td>
<td>application</td>
<td>junos:YAHOO, junos:GOOGLE</td>
</tr>
<tr>
<td></td>
<td>application-group</td>
<td>junos:web</td>
</tr>
<tr>
<td>SLA rule (sla1)</td>
<td>Associated multipath rule</td>
<td>multi1</td>
</tr>
<tr>
<td>APBR profile (apbr1)</td>
<td>Match applications</td>
<td>junos:YAHOO</td>
</tr>
<tr>
<td>APBR rule</td>
<td></td>
<td>rule1</td>
</tr>
<tr>
<td>SLA rule</td>
<td></td>
<td>sla1</td>
</tr>
<tr>
<td>Underlay interface</td>
<td></td>
<td>ge-0/0/2 and ge-0/0/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Speed: 800 Mbps</td>
</tr>
</tbody>
</table>

In this example, you configure a multipath rules for junos:YAHOO and junos:GOOGLE application traffic. Then configure an SLA rule and associate multipath rules with multipath rule.

Next, associate the SLA rules with APBR rules created for the Yahoo application. APBR uses the application details to look for a matching rule in the APBR profile (application profile).

Multipath rule is applied on the traffic matching junos:YAHOO or junos:GOOGLE, and forwarded to and the next-hop address as specified in the routing instance.

Multipath routing obtains the underlay link types and corresponding overlays on which packet duplication is required based on the SLA rule. Based on the application traffic and the configured bandwidth limit, multipath identifies two or more paths and triggers a copy of the original traffic on all the identified paths.
When traffic reaches on receiving end, the receiving device accepts packets of a session arriving through different links, and maintains sequence of a packet arriving on different CoS queues and drops any duplicate packets.

**NOTE:** Ensure that configuration is the same across the devices on both the sending-side and on the receiving-side device is such that devices can to act as both sender and a receiver.

### Configuration

**Configure Multipath Rules for Application Traffic (Device Configured to Send Traffic)**

#### Step-by-Step Procedure

Configure APBR profiles for different application traffic and associate SLA rule and multipath rule.

1. Create routing instances.

   ```
   user@host# set routing-instances TC1_VPN instance-type vrf
   user@host# set routing-instances TC1_VPN route-distinguisher 150.0.0.1:101
   user@host# set routing-instances TC1_VPN vrf-target target:100:101
   user@host# set routing-instances TC1_VPN vrf-table-label
   user@host# set routing-instances TC1_VPN routing-options static route 19.0.0.0/8 next-table Default_VPN.inet.0
   ```

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 Default-VPN-to-TC1_VPN import-rib [ Default_VPN.inet.0 TC1_VPN.inet.0 ]
   ```

3. 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 untrust1 host-inbound-traffic system-services appqoe
   ```

4. Create the APBR profile and define the rules.

   ```
   user@host# set security advance-policy-based-routing profile apbr1 rule rule1 match dynamic-application junos:GOOGLE
   ```
5. Configure active probe parameters.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings data-fill juniper</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings data-size 100</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings probe-interval 30</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings probe-count 30</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings burst-size 1</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings sla-export-interval 60</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing active-probe-params</td>
</tr>
<tr>
<td>probe1 settings dscp-code-points 000110</td>
</tr>
</tbody>
</table>

6. Configure metrics profile.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>user@host# set security advance-policy-based-routing metrics-profile</td>
</tr>
<tr>
<td>metric1 sla-threshold delay-round-trip 120000</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing metrics-profile</td>
</tr>
<tr>
<td>metric1 sla-threshold jitter 21000</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing metrics-profile</td>
</tr>
<tr>
<td>metric1 sla-threshold jitter-type egress-jitter</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing metrics-profile</td>
</tr>
<tr>
<td>metric1 sla-threshold packet-loss 2</td>
</tr>
</tbody>
</table>

7. Configure underlay interfaces.

If link-type is not configured under the underlay interfaces option, the default link-type IP is used and default link-speed of 1000 Mbps is considered.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>user@host# set security advance-policy-based-routing underlay-interface</td>
</tr>
<tr>
<td>ge-0/0/2 unit 0 link-type MPLS</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing underlay-interface</td>
</tr>
<tr>
<td>ge-0/0/2 unit 0 speed 800</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing underlay-interface</td>
</tr>
<tr>
<td>ge-0/0/3 unit 0 link-type MPLS</td>
</tr>
<tr>
<td>user@host# set security advance-policy-based-routing underlay-interface</td>
</tr>
<tr>
<td>ge-0/0/3 unit 0 speed 500</td>
</tr>
</tbody>
</table>

8. Configure overlay paths.
user@host# set security advance-policy-based-routing overlay-path overlay-path1 tunnel-path local ip-address 40.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path1 tunnel-path remote ip-address 40.1.1.1
user@host# set security advance-policy-based-routing overlay-path overlay-path1 probe-path local ip-address 40.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path1 probe-path remote ip-address 40.1.1.1
user@host# set security advance-policy-based-routing overlay-path overlay-path2 tunnel-path local ip-address 41.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path2 tunnel-path remote ip-address 41.1.1.1
user@host# set security advance-policy-based-routing overlay-path overlay-path2 probe-path local ip-address 41.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path2 probe-path remote ip-address 41.1.1.1
user@host# set security advance-policy-based-routing overlay-path overlay-path3 tunnel-path local ip-address 42.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path3 tunnel-path remote ip-address 42.1.1.1
user@host# set security advance-policy-based-routing overlay-path overlay-path3 probe-path local ip-address 42.1.1.2
user@host# set security advance-policy-based-routing overlay-path overlay-path3 probe-path remote ip-address 42.1.1.1

9. Configure destination path groups.

user@host# set security advance-policy-based-routing destination-path-group site1 probe-routing-instance transit
user@host# set security advance-policy-based-routing destination-path-group site1 overlay-path overlay-path1
user@host# set security advance-policy-based-routing destination-path-group site1 overlay-path overlay-path2
user@host# set security advance-policy-based-routing destination-path-group site1 overlay-path overlay-path3

10. Configure multipath rule.

user@host# set security advance-policy-based-routing multipath-rule multi1 bandwidth-limit 60
user@host# set security advance-policy-based-routing multipath-rule multi1 application junos:YAHOO
user@host# set security advance-policy-based-routing multipath-rule multi1 application junos:GOOGLE
user@host# set security advance-policy-based-routing multipath-rule multi1 application-group junos:web
11. Configure SLA rule.

user@host# set security advance-policy-based-routing sla-rule sla1 switch-idle-time 40
user@host# set security advance-policy-based-routing sla-rule sla1 metrics-profile metric1
user@host# set security advance-policy-based-routing sla-rule sla1 active-probe-params probe1
  sampling-percentage 25
user@host# set security advance-policy-based-routing sla-rule sla1 passive-probe-params
  violation-count 2
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 type book-ended

12. Associate an SLA rule to multipath rule.

user@host# set security advance-policy-based-routing sla-rule sla1 multipath-rule multi1

Configure Multipath Rules for Application Traffic (Device Configured to Receive Traffic)

Step-by-Step Procedure

The variables configured in this step are the same for both the sending and receiving device.

1. Configure multipath rule on the receiving device.

user@host# set security advance-policy-based-routing multipath-rule multi1 bandwidth-limit 60
user@host# set security advance-policy-based-routing multipath-rule multi1 application junos:YAHOO
user@host# set security advance-policy-based-routing multipath-rule multi1 application junos:GOOGLE
user@host# set security advance-policy-based-routing multipath-rule multi1 application-group junos:web
user@host# set security advance-policy-based-routing multipath-rule multi1 link-type MPLS
user@host# set security advance-policy-based-routing multipath-rule multi1 link-type IP

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.

Hub-side device multipath rule configuration
[edit security]
user@host# show advance-policy-based-routing multipath-rule multi1
multipath-rule multi1 {
    bandwidth-limit 60;
    application [ junos:YAHOO junos:GOOGLE ];
    application-group junos:web;
    link-type [ MPLS IP ];
    number-of-paths 2;
}

[edit security]
user@host# show advance-policy-based-routing profile apbr1 {
    rule rule1 {
        match {
            dynamic-application [ junos:GOOGLE, junos:YAHOO ];
            dynamic-application-group [ junos:web ];
        }
        then {
            routing-instance TC1_VPN;
            sla-rule {
                sla1;
            }
        }
    }
}

active-probe-params probe1 {
    settings {
        data-fill {
            juniper;
        }
        data-size {
            100;
        }
        probe-interval {
            30;
        }
        probe-count {
            30;
        }
        burst-size {
            1;
        }
        sla-export-interval {

60;
}
dscp-code-points {
  000110;
}
}
}
metrics-profile metric1 {
  sla-threshold {
    delay-round-trip {
      120000;
    }
    jitter {
      21000;
    }
    jitter-type {
      egress-jitter;
    }
    packet-loss {
      2;
    }
  }
}
underlay-interface ge-0/0/2 {
  unit 0 {
    link-type MPLS;
    speed 800;
  }
}
underlay-interface ge-0/0/3 {
  unit 0 {
    link-type MPLS;
    speed 500;
  }
}
overlay-path overlay-path1 {
  tunnel-path {
    local {
      ip-address {
        40.1.1.2;
      }
    }
    remote {
      ip-address {

40.1.1.1;
}
}
}
probe-path {
  local {
    ip-address {
      40.1.1.2;
    }
  }
  remote {
    ip-address {
      40.1.1.1;
    }
  }
}
}
overlay-path overlay-path2 {
  tunnel-path {
    local {
      ip-address {
        41.1.1.2;
      }
    }
    remote {
      ip-address {
        41.1.1.1;
      }
    }
  }
  probe-path {
    local {
      ip-address {
        41.1.1.2;
      }
    }
    remote {
      ip-address {
        41.1.1.1;
      }
    }
  }
}
overlay-path overlay-path3 {

tunnel-path {
    local {
        ip-address {
            42.1.1.2;
        }
    }
    remote {
        ip-address {
            42.1.1.1;
        }
    }
}

probe-path {
    local {
        ip-address {
            42.1.1.2;
        }
    }
    remote {
        ip-address {
            42.1.1.1;
        }
    }
}

destination-path-group site1 {
    probe-routing-instance {
        transit;
    }
    overlay-path overlay-path1;
    overlay-path overlay-path2;
    overlay-path overlay-path3;
}

sla-rule sla1 {
    switch-idle-time {
        40;
    }
    metrics-profile {
        metric1;
    }
    active-probe-params {
        probe1;
    }
    passive-probe-params {
If you are done configuring the device, enter commit from configuration mode.

**Verification**

*Displaying Multipath Rule Status*

**Purpose**
Display the details of the multipath rule on the device configured to send traffic.

**Action**
From operational mode, enter the `show security advance-policy-based-routing multipath rule` command.

```
user@host>show security advance-policy-based-routing multipath rule multi1
```

**Multipath Rule Status:**

**Multipath Rule Information:**
- Multipath rule name: `multi1`
- Multipath rule type: `Packet-Copy`
- Multipath rule state: `Active`
Configured number of paths: 2
Configured application groups: junos:web
Configured applications: junos:GOOGLE, junos:YAHOO

Path Group Information:
Total path groups: 1
Path-Group-Id State Avl-Num-Paths
1 Active 3

Sender Information:
Statistics:
Current Sessions: 0
Ignored Sessions: 0
Applications Matched: 1
Applications Switched: 0
Stopped due to Bandwidth Limit: 0
Packets in path inactive state: 26
Packets in path active state: 2416
Midstream Packets Ignored: 0
Total Packets Processed: 2442
Total Packets Copied: 2442

Status:
Policy reference count: 2383
Credit Limit (Mbps): 480
Policer Rate (Kbits per ms): 480
Bandwidth Limit: Not-Reached
Maximum Wait Time (secs): 30
Time to Reinforce (secs): 0
Application Hit List: junos:YAHOO

Path Groups Information:
Total sender path groups: 1
Path-Group-Id: 1, Cur-Num-Paths: 2

Path Information:
Dst-IP Pkts-Sent Link-type
40.1.1.2 2416 IP
41.1.1.2 2416 MPLS

COS Q Statistics:
Total sender cos queues: 8
COS-Q-Id Pkts-Sent
0 2416
1 0
2 0
3 0
4 0
5 0
Meaning
The command output displays the multipath rule details.

Display Multipath Rule Statistics for An Application

Purpose
Display the details of the application traffic on the device configured to receive traffic

Action
From operational mode, enter the `show security advance-policy-based-routing multipath rule rule-name application application-name` command.

```
user@host> show security advance-policy-based-routing multipath rule multi1 application junos:YAHOO
```

Multipath Rule Status:
  Multipath Rule Information:
    Multipath rule name        multi1
    Multipath rule type        Packet-Copy
    Multipath rule state       Active
    Configured number of paths 2
    Configured applications   junos:YAHOO
  Sender Information:
    Statistics:
      Current Sessions    0
      Ignored Sessions    1
      Applications Matched 1
      Applications Switched 0
      Stopped due to Bandwidth Limit 0
      Packets in path inactive state 0
      Packets in path active state 627
      Midstream Packets Ignored 0
      Total Packets Processed 627
      Total Packets Copied 627

Meaning
The command output displays the multipath rule for the application.

Displaying Multipath Rule Policies

Purpose
Display the details of the multipath rule on the device configured to send traffic.

**Action**
From operational mode, enter the `show security advance-policy-based-routing multipath rule` command.

```bash
user@host> show security advance-policy-based-routing multipath rule
```

**Meaning**
The command output displays the details on the traffic handled with multipath rule applied.

**Displaying Multipath Rule Status**

**Purpose**
Display the details of the multipath rule on the device configured to receive traffic

**Action**
From operational mode, enter the `show security advance-policy-based-routing multipath rule` command.

```bash
user@host> show security advance-policy-based-routing multipath rule
```

**Meaning**
The command output displays the details on the traffic handled with multipath rule applied.
Path Group Information:
Total path groups : 1
Path-Group-Id  State               Avl-Num-Paths
  1              Active              3

Receiver Information:
Path Groups Information:
Total receiver path groups : 1
Path-Group-Id : 1, Avg-Pkt-Loss(%) : 0, Avg-Ingress-Jitter(us) : 171
Path Information:

<table>
<thead>
<tr>
<th>Dst-IP</th>
<th>Pkts-Rcvd</th>
<th>Pkt-Loss(%)</th>
<th>Ingress-Jitter(us)</th>
<th>Reduction-Pkt-Loss(%)</th>
<th>Reduction-Ingress-Jitter(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.1.1.1</td>
<td>2442</td>
<td>0</td>
<td>165</td>
<td>0</td>
<td>-6</td>
</tr>
<tr>
<td>41.1.1.1</td>
<td>2442</td>
<td>0</td>
<td>158</td>
<td>0</td>
<td>-13</td>
</tr>
</tbody>
</table>

Cos Q Statistics:
Total receiver cos queues: 8

<table>
<thead>
<tr>
<th>COS-Q-Id</th>
<th>Pkts-Rcvd</th>
<th>Out-Of-Seq-Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4884</td>
<td>2442</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Meaning
Output displays details related to multipath rule.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1X49-D170</td>
<td>Starting in Junos OS Release 19.2R1 and Junos OS Release 15.1X49-D170, application-based multipath routing support is available when device is operating in chassis cluster mode.</td>
</tr>
<tr>
<td>15.1X49-D160</td>
<td>SRX Series devices support application-based multipath routing starting in Junos OS Release 15.1X49-D160.</td>
</tr>
</tbody>
</table>
SSL Proxy

SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. Better visibility into application usage can be made available when SSL forward proxy is enabled.

SSL Proxy Overview

SSL proxy is supported on SRX Series devices only.

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet. SSL, also called Transport Layer Security (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private-public key exchange pairs for this level of security.

SSL proxy is transparent proxy that performs SSL encryption and decryption between the client and the server.

How Does SSL Proxy Work?

SSL proxy provides secure transmission of data between a client and a server through a combination of following:

- **Authentication** - Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a webserver.
- **Confidentiality** - SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications; thus ensures privacy of communications.
- **Integrity** - Message integrity ensures that the contents of a communication are not tampered.

SRX Series device acting as SSL proxy manages SSL connections between the client at one end and the server at the other end and performs following actions:
• SSL session between client and SRX Series - Terminates an SSL connection from a client, when the SSL sessions are initiated from the client to the server. The SRX Series device decrypts the traffic, inspects it for attacks (both directions), and initiates the connection on the clients' behalf out to the server.

• SSL session between server and SRX Series - Terminates an SSL connection from a server, when the SSL sessions are initiated from the external server to local server. The SRX Series device receives clear text from the client, and encrypts and transmits the data as ciphertext to the SSL server. On the other side, the SRX Series decrypts the traffic from the SSL server, inspects it for attacks, and sends the data to the client as clear text.

• Allows inspection of encrypted traffic.

SSL proxy server ensures secure transmission of data with encryption technology. SSL relies on certificates and private-public key exchange pairs to provide the secure communication. For more information, see "SSL Certificates" on page 356.

To establish and maintain an SSL session between the SRX Series device and its client/server, the SRX series device applies security policy to the traffic that it receives. When the traffic match the security policy criteria, SSL proxy is enabled as an application service within a security policy.

SSL Proxy with Application Security Services

Figure 18 on page 353 shows how SSL proxy works on an encrypted payload.
When Advanced Security services such as application firewall (AppFW), Intrusion Detection and Prevention (IDP), application tracking (AppTrack), UTM, and SkyATP is configured, the SSL proxy acts as an SSL server by terminating the SSL session from the client and establishing a new SSL session to the server. The SRX Series device decrypts and then reencrypts all SSL proxy traffic.

IDP, AppFW, AppTracking, advanced policy-based routing (APBR), UTM, SkyATP, and ICAP service redirect can use the decrypted content from SSL proxy. If none of these services are configured, then SSL proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy.

**Types of SSL Proxy**

SSL proxy is a transparent proxy that performs SSL encryption and decryption between the client and the server. SRX acts as the server from the client's perspective and it acts as the client from the server's perspective. On SRX Series devices, client protection (forward proxy) and server protection (reverse proxy) are supported using same echo system SSL-T-SSL [terminator on the client side] and SSL-I-SSL [initiator on the server side].

SRX Series device support following types of SSL proxy:
• Client-protection SSL proxy also known as forward proxy—The SRX Series device resides between the internal client and outside server. Proxying outbound session, that is, locally initiated SSL session to the Internet. It decrypts and inspects traffic from internal users to the web.

• Server-protection SSL proxy also known as reverse proxy—The SRX Series device resides between the internal server and outside client. Proxying inbound session, that is, externally initiated SSL sessions from the Internet to the local server.

For more information on SSL forward proxy and reverse proxy, see "Configuring SSL Proxy" on page 382.

Supported SSL Protocols

The following SSL protocols are supported on SRX Series devices for SSL initiation and termination service:

• TLS version 1.0—Provides authentication and secure communications between communicating applications.

• TLS version 1.1—This enhanced version of TLS provides protection against cipher block chaining (CBC) attacks.

• TLS version 1.2 — This enhanced version of TLS provides improved flexibility for negotiation of cryptographic algorithms.

Starting with Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, TLS version 1.1 and TLS version 1.2 protocols are supported on SRX Series devices along with TLS version 1.0. Starting with Junos OS Release 15.1X49-D20 and Junos OS Release 17.3R1, the SSL protocol 3.0 (SSLv3) support is deprecated.

Benefits of SSL Proxy

• Decrypts SSL traffic to obtain granular application information and enable you to apply advanced security services protection and detect threats.

• Enforces the use of strong protocols and ciphers by the client and the server.

• Provides visibility and protection against threats embedded in SSL encrypted traffic.

• Controls what needs to be decrypted by using Selective SSL Proxy.

Logical Systems Support

It is possible to enable SSL proxy on firewall policies that are configured using logical systems; however, note the following limitations:

• The "services" category is currently not supported in logical systems configuration. Because SSL proxy is under "services," you cannot configure SSL proxy profiles on a per-logical-system basis.
Because proxy profiles configured at a global level (within “services ssl proxy”) are visible across logical system configurations, it is possible to configure proxy profiles at a global level and then attach them to the firewall policies of one or more logical systems.

Limitations

On all SRX Series devices, the current SSL proxy implementation has the following connectivity limitations:

- The SSLv3.0 protocol support is deprecated.
- The SSLv2 protocol is not supported. SSL sessions using SSLv2 are dropped.
- Only X.509v3 certificate is supported.
- Client authentication of SSL handshake is not supported.
- SSL sessions where client certificate authentication is mandatory are dropped.
- SSL sessions where renegotiation is requested are dropped.

On SRX Series devices, for a particular session, the SSL proxy is only enabled if a relevant feature related to SSL traffic is also enabled. Features that are related to SSL traffic are IDP, application identification, application firewall, application tracking, advanced policy-based routing, UTM, SkyATP, and ICAP redirect service. If none of these features are active on a session, the SSL proxy bypasses the session and logs are not generated in this scenario.

SEE ALSO

<table>
<thead>
<tr>
<th>SSL Certificates</th>
<th>356</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SSL Proxy</td>
<td>382</td>
</tr>
<tr>
<td>Unified Policies for SSL Proxy</td>
<td>405</td>
</tr>
<tr>
<td>ICAP Service Redirect</td>
<td>416</td>
</tr>
<tr>
<td>SSL Decryption Mirroring</td>
<td>429</td>
</tr>
<tr>
<td>SSL Proxy Logs</td>
<td>436</td>
</tr>
</tbody>
</table>
SSL Certificates

IN THIS SECTION

- Configuring and Loading SSL Certificates | 356
- Configuring a Root CA Certificate | 357
- Configuring a Trusted CA Profile Group | 360
- Importing a Root CA Certificate into a Browser | 362
- Certificate Chain Implementation | 363
- Ignore Server Authentication Failure | 369
- Certificate Revocation Lists for SSL Proxy | 370
- SSL Performance Enhancements | 371

SRX Series device acting as SSL proxy manages SSL connections between the client at one end and the server at the other end. SSL proxy server ensures secure transmission of data with encryption technology. SSL relies on certificates and private-public key exchange pairs to provide the secure communication. In this topic, you learn about how to generate and install SSL certificate on your security device for SSL connections.

Configuring and Loading SSL Certificates

Figure 19 on page 357 displays an overview of how SSL proxy is configured. Configuring SSL proxy includes:

- Configuring the root CA certificate
- Loading a CA profile group
- Configure SSL proxy profile and associate root CA certificate and CA profile group
- Applying an SSL proxy profile to a security policy
Figure 19: SSL Proxy Configuration Overview

1. Define a root CA certificate.
   - Generate a root CA certificate.
   - Import a root CA certificate.

2. Configure a trusted CA profile or group.
   - Configure a trusted CA profile group.
   - Configure a single trusted CA profile.

3. Configure an SSL proxy profile.
   - Create an SSL proxy profile.
   - Apply the root CA certificate to the SSL proxy profile.
   - Apply the configured trusted CA list for your profile.
   - (Optional) Configure SSL proxy logging.
   - (Optional) Create whitelists of exempted destinations.

4. Apply the SSL proxy profile to a security policy.
   - Apply the SSL proxy profile to a security policy.

Let's discuss these procedures in detail in the following sections:

### Configuring a Root CA Certificate

**IN THIS SECTION**
- Generate a Root CA Certificate with CLI | 358
- Generate a Root CA Certificate with OpenSSL | 359
A CA can issue multiple certificates in the form of a tree structure. A root certificate is the topmost certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the signature or trustworthiness of the root certificate. This is somewhat like the notarizing of an identity.

To configure a root CA certificate you must

1. Obtaining a root CA certificate (by either or importing one)
   - Generating a self-signed certificate. You can generate a root CA certificate using one of the following ways:
     - Junos OS CLI on an SRX Series device
     - OpenSSL on a UNIX device.
   - Obtain a certificate from an External CA (not covered in this topic)

2. Applying root CA to an SSL proxy profile.

Generate a Root CA Certificate with CLI

To define a self-signed certificate in CLI, you must provide the following details:

- Certificate identifier (generated in the previous step)
- Fully qualified domain name (FQDN) for the certificate
- e-mail address of the entity owning the certificate
- Common name and the organization involved

Generate a root CA certificate using the Junos OS CLI:

1. From operational mode, generate a PKI public/private key pair for a local digital certificate.
   
   Example:
   ```
   user@host> request security pki generate-key-pair certificate-id SECURITY-cert size 2048 type ecdsa
   ```

2. Define a self-signed certificate.

   Example:
   ```
   user@host> request security pki local-certificate generate-self-signed certificate-id SECURITY-cert
   domain-name labs.abc.net subject DC=mydomain.net,L=Sunnyvale,O=Mydomain,OU=LAB,CN=SECURITY
   email lab@labs.abc.net add-ca-constraint
   ```
By configuring the **add-ca-constraint** option, you make sure that the certificate can be used for signing other certificates.

3. From configuration mode, apply the loaded certificate as root-ca in the SSL proxy profile.

   ```bash
   [edit]
   user@host# set services ssl proxy profile profile-name root-ca certificate-id
   ```

   Example:

   ```bash
   [edit]
   user@host# set services ssl proxy profile SECURITY-SSL-PROXY root-ca SECURITY-cert
   ```

4. Import the root CA as a trusted CA into client browsers. This is required for the client browsers to trust the certificates signed by the SRX Series device. See "Importing a Root CA Certificate into a Browser" on page 362.

**Generate a Root CA Certificate with OpenSSL**

To generate a root CA certificate using OpenSSL:

1. Create folders **keys** and **certs**.

   ```bash
   mkdir /etc/pki/tls/keys
   mkdir /etc/pki/tls/certs
   ```

2. Change to the **openssl** directory.

   ```bash
   cd /etc/pki/tls
   ```

3. Create a CA certificate key.

   ```bash
   % openssl genrsa -des3 -out keys/ssl-proxy-ca.key 2048
   ```

   This step creates an RSA key using the 3DES encryption named **ca.key** that is 2048 in length. You also need to enter a password that is used to encrypt the private key. This is critical to security if the key is lost because it will still be encrypted.

4. Create a CA certificate based on the CA private key (created in the previous step).
The expiration date for this certificate is 3 years or 1095 days. However, you can set it to a different value. When creating the certificate, you need to enter the password and the certificate information that includes distinguished name (DN), country name, and so forth.

5. Import the CA private and public keys into the SRX Series device. Copy the `ca.key` and `ca.cer` keys to the `/var/tmp` directory on the SRX Series device. You can copy using SCP, or open the files and copy them into “vi” on the SRX Series device to create new files.

6. From configuration mode, apply the loaded certificate as root-ca in the SSL proxy profile.

```
user@host> request security pki local-certificate load certificate-id ssl-inspect-ca key /var/tmp/ssl-proxy-ca.key filename /var/tmp/ssl-inspect-ca.cer passphrase password
```

7. Import the root CA as a trusted CA into client browsers. This is required for the client browsers to trust the certificates signed by the SRX Series device. See "Importing a Root CA Certificate into a Browser" on page 362.

---

**Configuring a Trusted CA Profile Group**

The CA profile defines the certificate information for authentication. It includes the public key that SSL proxy uses when generating a new certificate. Junos OS allows you to create a group of CA profiles and load multiple certificates in one action, view information about all certificates in a group, and delete unwanted CA groups. When a connection is initiated, the connecting device (such as a Web browser) checks whether the certificate is issued by a trusted CA. Without these certificates, browsers cannot validate the identity of most websites and mark them as untrusted sites.

Configuring a trusted CA profile group includes following steps:

- Obtaining a list of trusted CA certificates. You can obtain trusted CA certificates using one of the following methods:
  - Junos OS provides a default list of trusted CA certificates as a PEM file (for example, `trusted_CA.pem`). After you download the Junos OS package, the default certificates are available on your system.
From operational mode, load the default trusted CA certificates (the group name identifies the CA profile group):

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name group-name filename default
```

Example:
```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name SECURITY-CA-GROUP filename default
```

We recommend using this method.

- Define your own list of trusted CA certificates and import them on your system. You get the list of trusted CAs in a single PEM file (for example `IE-all.pem`) and save the PEM file in a specific location (for example, `/var/tmp`). See Knowledge Base Article KB23144.

From operational mode, load the trusted list to the device (the group name identifies the CA profile group):

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name SECURITY-CA-GROUP filename /var/tmp/IE-all.pem
```

Example:
```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name SECURITY-CA-GROUP filename /var/tmp/custom-file.pem
```

- Download the latest CA bundle list from another 3rd party such as Mozilla (https://curl.haxx.se/docs/caextract.html). The list of trusted Certificate Authority can change over time, ensure that you use the latest CA bundle.

- Import your own trusted CA certificates using the Public Key Infrastructure (PKI). The PKI helps verify and authenticate the validity of the trusted CA certificates. You create CA profile groups that include trusted CA certificates, then import the group on your device for server authentication.

- Attaching the CA group to the SSL proxy profile.

- Attach all CA profile groups:

  Example:

  ```
  [edit]
  user@host# set services ssl proxy profile PROFILE-1 trusted-ca all
  ```

- Attach one CA profile group (the group name identifies the CA profile group).
Example:

```
[edit]
user@host# set services ssl proxy profile PROFILE-1 trusted-ca orgA-ca-profile
```

You can easily display information about all certificates in a CA profile group:

```
user@host> show security pki ca-certificates ca-profile-group group-name
```

You can delete a CA profile group. Remember that deleting a CA profile group deletes all certificates that belong to that group:

```
user@host> clear security pki ca-certificates ca-profile-group group-name
```

WHAT'S NEXT

Now proceed with SSL proxy profile configuration and apply SSL proxy profile to security policy. See Configuring SSL Proxy | 382.

### Importing a Root CA Certificate into a Browser

In order to have your browser or system automatically trust all certificates signed by the root CA configured in the SSL proxy profile, you must instruct your platform or browser to trust the CA root certificate.

To import a root CA certificate:

1. Generate a PEM format file for the configured root CA.

```
request security pki local-certificate export certificate-id root-ca type pem filename path/file-name.pem
```

2. Import a root CA certificate into a browser.

   From Internet Explorer (version 8.0):
   a. From the Tools menu, select **Internet Options**.
   b. On the Content tab, click **Certificates**.
c. Select the **Trusted Root Certification Authorities** tab and click **Import**.

d. In the Certificate Import Wizard, navigate to the required root CA certificate and select it.

From Firefox (version 39.0):

a. From the Tools menu, select **Options**.

b. From the Advanced menu, select the **Certificates** tab and click **View Certificate**.

c. In the Certificate Manager window, select the **Authorities** tab and click **Import**.

d. Navigate to the required root CA certificate and select it.

From Google Chrome (45.0):

a. From the Settings menu, select **Show Advanced Settings**.

b. From the Advanced menu, select the **Certificates** tab and click **View Certificate**.

c. Under HTTPS/SSL, click **Manage Certificates**.

d. In the Certificate window, select **Trusted Root Certification Authorities** and click **Import**.

e. In the Certificate Import Wizard, navigate to the required root CA certificate and select it.

---

**Certificate Chain Implementation**

---

**IN THIS SECTION**

- Requirements  | 364
- Overview      | 364
- Configuration | 366
Starting in Junos OS Release 15.1X49-D30, SSL forward proxy supports the certificate chain implementation. Let's discuss about understanding certificate chain concepts and how to configure it on SRX Series device.

- **Certificate Authority (CA)**— CA is a trusted third party responsible for validating the identities of entities (such as websites, email addresses, or companies, or individual persons) and issues a digital certificate by binding cryptographic keys. If your organization owns a CA server, then you become your own CA and use self-signed certificate.

- **Root Certificate**— A Root certificate is a certificate issued by a trusted certificate authority (CA). The root certificate is the topmost certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the signature or trustworthiness of the root certificate. These certificates are used to establish connection between two endpoints.

- **Intermediate CA Certificate**— An intermediate CA certificate is a subordinate certificate signed by the trusted root specifically to validate an end-entity certificates.

- **Certificate Chain**— An certificate chain is the ordered list of certificates that contains the SSL certificate, intermediate certificate, and root certificate. Some certificate authorities (CAs) do not sign with their root certificate, but instead use an intermediate certificate. An intermediate CA can sign certificates on behalf of the root CA certificate. The root CA signs the intermediate certificate, forming a chain of trust.

The intermediate certificate must be installed on the same server as the SSL certificate so that the connecting device (browsers, applications, mobile device, etc.) can trust it.

When you initiate a connection, the connecting device (such as a Web browser) checks whether the certificate is authentic and is issued by a trusted certificate authority that is embedded in the browser's trusted store.

If the SSL certificate is not from a trusted CA, then the connecting device continues to check if the SSL certificate is issued by a intermediate CA and this intermediate CA is signed by a root CA. The check continues till the root CA is found. If it finds a root CA, a secure connection is established. If it doesn't find a root CA, then the connection is dropped, and your web browser displays an error message about invalid certificate or certificate not trusted.

This example shows how to install the certificate chain to enable browsers to trust your certificate.

**Requirements**

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

**Overview**

In this example, you have a domain, example.domain-1, and you want to purchase a certificate from XYZ-Authority for your domain. However, XYZ-Authority is not a Root-CA and the visiting Web browser trusts only Root-CA certificate. In other words, its certificate is not directly embedded in your Web browser and therefore it is not explicitly trusted.
In this case, trust is established in the following manner using the certificate chain (of intermediate certificates).

Let's try to visualize this chain through Figure 20 on page 365. The image depicts a full certificate chain, from the root CA certificate to the end-user certificate. The chain terminates at the end-user certificate.

**Figure 20: Certification Path from the Certificate Owner to the Root CA**

Table 33: Certificate Chaining Details

<table>
<thead>
<tr>
<th>User</th>
<th>Uses Certificate</th>
<th>Signed By</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.domain-1</td>
<td>End User Certificate</td>
<td>XYZ-Authority</td>
<td>End User Certificate. The one the one you purchase from the CA.</td>
</tr>
<tr>
<td>XYZ-Authority</td>
<td>Certificate-1</td>
<td>Intermediate CA-1</td>
<td>Intermediate Certificate</td>
</tr>
<tr>
<td>Intermediate CA-3</td>
<td>Certificate-4</td>
<td>Root-CA</td>
<td></td>
</tr>
</tbody>
</table>
When you install your end-user certificate for the server example.domain-1, you must bundle all the intermediate certificates and install them along with your end-user certificate. The certificate chain includes all the certificates starting from Certificate-1 to Root-CA certificate. Because the web browser trusts the root CA, it also implicitly trusts all the intermediate certificates. If the SSL certificate chain is invalid or broken, your certificate will not be trusted by some devices.

NOTE:

- All certificates must be in Privacy-Enhanced Mail (PEM) format.
- When you import the concatenated certificate file into the device, the CA provides a bundle of chained certificates that must be added to the signed server certificate. The server certificate must appear before the chained certificates in the combined file.

Configuration

IN THIS SECTION

- Configuring the Certificate Chain on the Device | 367

Configuring the SSL certificate chain includes the following tasks:

- Purchase an SSL certificate from a CA that includes a signing certificate and a respective key.
- Configure a trusted CA profile group.
- Load the signing certificate and the key on your device.
- Load the intermediate and root CA in public key infrastructure (PKI) memory. This certificate file contains all the required CA certificates, one after each other, in PEM format.
• Create a trusted CA profile for the intermediate or root CA certificate.

• Set up your device to use the signing certificate received from the CA by configuring and applying the SSL proxy profile to a security policy. SSL forward proxy stores this certificate chain information (CA certificate profile name) in the respective SSL profile. As a part of security policy implementation, SSL profiles having the certificate chain information and CA certificates are used.

The following components are involved in certificate chain processing:

• Administrator loads the certificate chain and the local certificate (signing certificate) into the PKI daemon certificate cache.

• The Network Security Daemon (nsd) sends a request to the PKI daemon to provide the certificate chain information for a signing certificate configured in the SSL proxy profile.

This example assumes that you have already purchased an SSL certificate from a CA.

**Configuring the Certificate Chain on the Device**

**Step-by-Step Procedure**

To configure certificate chain:

• Load the local certificate into the PKI memory.

```bash
user@host> request security pki local-certificate load filenamessl_proxy_ca.crt keysslserver.key certificate-id ssl-inspect-ca
```

The following message is displayed:

```
Local certificate loaded successfully
```

Note that the certificate ID will be used under the `root-ca` section in the SSL proxy profile.

• Load the intermediate or root CA certificate in the PKI memory.

```bash
user@host> request security pki ca-certificate ca-profile-group load ca-group-name ca-latest filename ca-latest.cert.pem
```

The CA profile includes the certificate information used for authentication. It includes the public key that SSL proxy uses when generating a new certificate.

```bash
Do you want to load this CA certificate? [yes,no] (no) yes
Loading 1 certificates for group 'ca-latest'.
ca-latest_1: Loading done.
```
This certificate will be attached as a certificate chain.

- Attach the CA profile group to the SSL proxy profile. You can attach trusted CA one at a time or load all in one action.

  ```
  user@host# set services ssl proxy profile ssl-profile trusted-ca all
  ```

- Apply the signing certificate as root-ca in the SSL proxy profile.

  ```
  user@host# set services ssl proxy profile ssl-profile root-ca ssl-inspect-ca
  ```

- Create a security policy and specify the match criteria for the policy. As match criteria, specify the traffic for which you want to enable SSL proxy. This example assumes that you have already created security zones based on the requirements.

  ```
  user@host# set security policies from-zone trust to-zone untrust policy 1 match source-address any
  user@host# set security policies from-zone trust to-zone untrust policy 1 match destination-address any
  user@host# set security policies from-zone trust to-zone untrust policy 1 match application any
  user@host# set security policies from-zone trust to-zone untrust policy 1 then permit application-services ssl-proxy profile-name ssl-profile
  ```

SSL forward proxy stores this certificate chain information (CA certificate profile name) into respective the SSL profile. As a part of security policy implementation, SSL profiles having the certificate chain information and CA certificates are used.

You can view the certificate chain on the connecting Web browser (that is, the client).

SEE ALSO

- Example: Loading CA and Local Certificates Manually
- Example: Configuring a Device for Peer Certificate Chain Validation
Ignore Server Authentication Failure

Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

Server authentication is governed by setting the `ignore-server-auth-failure` option in the SSL proxy profile. The results of setting this option is available in Table 34 on page 369.

```bash
[edit]
user@host# set services ssl proxy profile profile-name actions ignore-server-auth-failure
```

Table 34: Ignore Server Authentication Failure Option

<table>
<thead>
<tr>
<th>SSL Proxy Profile Action</th>
<th>Results</th>
</tr>
</thead>
</table>
| The `ignore-server-auth-failure` option is not set (Default option) | - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.  
- If authentication fails, the connection is dropped. |
| The `ignore-server-auth-failure` option is set | - If the certificate is self-signed, a new certificate is generated by replacing the keys. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.  
- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to SSL-PROXY:Dummy_Cert:Generated Due To SRV Auth Failure.  
This ensures that the client browser displays a warning that the certificate is not valid.  
- We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions. See "Enabling Debugging and Tracing for SSL Proxy" on page 438. |

Client Authentication

Currently, client authentication is not supported in SSL proxy. If a server requests client authentication, a warning is issued that a certificate is not available. The warning lets the server determine whether to continue or to exit.
Certificate Revocation Lists for SSL Proxy

Working with the Certificate Revocation Lists for SSL Proxy

Certificate authority (CA) periodically publishes a list of revoked certificate using a certificate revocation list (CRL). The security device downloads and caches the most recently issued CRL. The CRL contains the list of digital certificates with serial numbers that have been canceled before their expiration date.

CA revokes the issued certificate if there is any chance that the certificate is compromised. Some other reasons for revoking a certificate are:

- Unspecified (no particular reason is given).
- Private key associated with the certificate or CA that issued the certificate was compromised.
- The owner of the certificate is no longer affiliated with the issuer of the certificate
- Another certificate replaces the original certificate.
- The CA that issued the certificate has ceased to operate.
- The certificate is on hold pending further action. It is treated as revoked but might be accepted in the future.

When a participating device uses a digital certificate, it checks the certificate signature and validity. By default, CRL verification is enabled on SSL proxy profile.

Starting with Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, SRX Series devices support certificate revocation list (CRL). CRL validation on SRX Series device involves checking for the revoked certificates from servers.

On SRX Series device, the certificate revocation checking is enabled by default for SSL proxy profile. You can enable or disable the CRL validation to meet your specific security requirements.

- Disable CRL verification.

    [edit]
    user@host# set services ssl proxy profile profile-name actions crl disable
• Re-enable CRL verification.

```plaintext
[edit]
user@host# delete services ssl proxy profile profile-name actions crl disable
```

You can allow or drop the sessions when a CRL information is not available for reasons such as failed CRL download or unavailability of the CRL path in the root or intermediate certificate.

• Allow the sessions when CRL information is not available.

```plaintext
[edit]
user@host# set services ssl proxy profile profile-name actions crl if-not-present allow
```

• Drop the sessions when CRL information is not available.

```plaintext
[edit]
user@host# set services ssl proxy profile profile-name actions crl if-not-present drop
```

• Configure an SRX Series device to accept a certificate without a reliable confirmation available on the revocation status and allow the sessions when a certificate is revoked and the revocation reason is on hold.

```plaintext
[edit]
user@host# set services ssl proxy profile profile-name actions crl ignore-hold-instruction-code
```

SEE ALSO

Understanding Online Certificate Status Protocol and Certificate Revocation Lists

### SSL Performance Enhancements

#### IN THIS SECTION

- Optimizing the SSL Performance | 372
- Session Resumption | 373
SSL performance enhancement on SRX Series device includes following features:

**Optimizing the SSL Performance**

The SSL/TLS handshake is a CPU-intensive process. Since SSL/TLS is the most widely used security protocol on the web, it’s performance results in significant impact on the web performance.

Starting from Junos OS Release 15.1X49-D120, you can use the following options for optimizing the performance:

- Use optimized RSA key exchanges
- Use Authenticated Encryption with Associated Data (AEAD)—AES128-CBC-SHA, AES256-CBC-SHA
- Maintaining certificate cache—Certificate cache stores the interdicted server certificate along with the server certificate details. During SSL/TLS handshake, SSL proxy can present the cached interdicted certificate to client instead of generating the new interdicted certificate.

Examples:

Set the certificate cache timeout to 300 seconds. This configuration lets the certificate cache to store the certificate details for 300 seconds. Default is 600 seconds.

```
[edit]
user@host# set services ssl proxy global-config certificate-cache-timeout 300
```

Disable the certificate cache. This configuration allows the SSL full handshake for a new connection.

```
[edit]
user@host# set services ssl proxy global-config disable-cert-cache
```

Invalidate the existing certificate cache.

```
[edit]
user@host# set services ssl proxy global-config invalidate-cache-on-crl-update
```

Improving the SSL performance results in improved website performance without compromising security and maximized user experience.
**Session Resumption**

On your security device, an SSL session resumes a previous session using a previous session ID. It saves the client and server the computational overhead of a complete SSL handshake and generation of master keys. An SSL session resumption includes the following steps:

- A session caching mechanism caches 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. This results in improved throughput while maintaining an appropriate level of security.

**Session Renegotiation**

The SRX Series device support session renegotiation. After a session is created and SSL tunnel transport is established, a change in SSL parameters requires renegotiation. SSL proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0, TLS v1.1, and TLS v1.2) renegotiation. When session resumption is enabled, session renegotiation is useful in the following situations:

- Cipher keys need to be refreshed after a prolonged SSL session.
- Stronger ciphers need to be applied for a more secure connection.

If you modify the SSL proxy profile by changing a certificate, or cipher strength, or trusted CA list, then the system flushes the cache entries when you commit the modified policy. In this case, a full handshake is required to establish the new SSL parameters. (There is no impact to non-SSL sessions.)

If the SSL proxy profile is not altered, cache entries corresponding to that profile are not flushed and the session continues.

**Dynamic Resolution of Domain Names**

The IP addresses associated with domain names are dynamic and can change at any time. Whenever a domain IP address changes, it is propagated to the SSL proxy configuration (similar to what is done in the firewall policy configuration).

**Release History Table**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1X49-D30</td>
<td>Starting with Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, SRX Series devices support certificate revocation list (CRL).</td>
</tr>
</tbody>
</table>
Cipher Suites for SSL Proxy

IN THIS SECTION

- Cipher Suites | 374

Read this topic to understand more about cipher suites supports and managing digital certificates for SSL proxy on SRX Series devices.

Cipher Suites

This topic includes the following sections:

Supported Cipher Suites

SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL relies on digital certificates and private-public key exchange pairs for client and server authentication to ensure secure communication.

Let's get familiar with all the terms we are going to refer in this section.

- **Digital Certificate or CA Certificate** — A digital certificate is an electronic means for verifying your identity through a trusted third party, known as a certificate authority (CA). Alternatively, you can use a self-signed certificate to attest to your identity. Each certificate contains a cryptographic key to encrypt plaintext or decrypt cyphertext.
- **Certificate Contents**—A digital certificate associates a public key with the identity of an individual entity to whom it is issuing the digital certificate. A digital certificate includes the following identification attributes:
  - Identification and signature of the Certificate Authority that issued the certificate.
  - Validity period
  - Serial number
  - Certificate issuer details
  - Information about the subject includes identifying information (the distinguished name) and the public key.

- **Cipher Suite**—A cipher suite is a set of cryptographic algorithms. An SSL cipher comprises encryption ciphers, an authentication method, and compression. On SRX Series device, SSL sessions use key exchange method by which cryptographic keys are exchanged between the client and the servers using cryptographic algorithm. The kind of key exchange algorithm and the cipher suites used must be supported by both sides.

  SSL sessions use the algorithms from a cipher suite to:
  - Securely establish a secret key between two communicating parties
  - Protect the confidentiality of data in transit

*Table 35 on page 375* provides the details of RSA keys supported on various SRX Series devices.

**Table 35: Maximum Key Sizes Supported on SRX Series Devices**

<table>
<thead>
<tr>
<th>SRX Series Devices</th>
<th>Supported RSA Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRX300, SRX320, SRX340, SRX345, SRX550, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800</td>
<td>512 bits, 1024 bits, 2048 bits, 4096 bits</td>
</tr>
</tbody>
</table>

- Starting with Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, server certificates of key size 4096 bits are supported. Prior to Junos OS Release 15.1X49-D30, server certificates with key size greater than 2048 bits were not supported because of cryptography hardware limitations.

- Starting in Junos OS Release 18.1R1, SSL proxy support is available on SRX300 and SRX320 devices. On SRX300 and SRX320 devices, server certificates with key size 4096 bits are not supported.

*Table 36 on page 376* displays a list of supported ciphers. NULL ciphers are excluded.
<table>
<thead>
<tr>
<th>SSL Cipher</th>
<th>Key Exchange Algorithm</th>
<th>Data Encryption</th>
<th>Message Integrity</th>
<th>Preferred Ciphers Category</th>
<th>Earliest Supported Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-ECDSA-AES-256-GCM-SHA384</td>
<td>ECDHE/DSA key exchange</td>
<td>256-bit AES/GCM</td>
<td>SHA384 hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES-128-GCM-MB-256</td>
<td>ECDHE/DSA key exchange</td>
<td>128-bit AES/GCM</td>
<td>SHA256 hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES-256-CBC-SHA384</td>
<td>ECDHE/DSA key exchange</td>
<td>256-bit AES/CBC</td>
<td>SHA384 hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES-128-CBC-MB-256</td>
<td>ECDHE/DSA key exchange</td>
<td>128-bit AES/CBC</td>
<td>SHA256 hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES-256-ES-CBC-SHA384</td>
<td>ECDHE/DSA key exchange</td>
<td>256-bit AES/CBC</td>
<td>SHA hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES-128-ES-CBC-SHA384</td>
<td>ECDHE/DSA key exchange</td>
<td>128-bit AES/CBC</td>
<td>SHA hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE-ECDSA-DES-CBC-ECDHE/SHA384</td>
<td>ECDHE/DSA key exchange</td>
<td>3DES EDE/CBC</td>
<td>SHA hash</td>
<td>Strong</td>
<td>Junos OS Release 18.3R1</td>
</tr>
<tr>
<td>ECDHE/ECDSA-AES-256-GCM-MB-256</td>
<td>ECDHE/DSA key exchange</td>
<td>256-bit AES/GCM</td>
<td>SHA384 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>ECDHE/ECDSA-AES-256-CBC-SHA384</td>
<td>ECDHE/DSA key exchange</td>
<td>256-bit AES/CBC</td>
<td>SHA384 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>ECDHE-RSA-AES-256-CBC-SHA</td>
<td>ECDHE/RSA key exchange</td>
<td>256-bit AES/CBC</td>
<td>SHA hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>ECDHE-RSA-DES-CBC3-SHA</td>
<td>ECDHE/RSA key exchange</td>
<td>DES CBC</td>
<td>SHA hash</td>
<td>Medium</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
</tbody>
</table>
Table 36: Supported SSL Cipher List (continued)

<table>
<thead>
<tr>
<th>SSL Cipher</th>
<th>Key Exchange Algorithm</th>
<th>Data Encryption</th>
<th>Message Integrity</th>
<th>Preferred Ciphers Category</th>
<th>Earliest Supported Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>ECDHE/RSA key exchange</td>
<td>128-bit AES/GCM</td>
<td>SHA256 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-CBC-SHA256</td>
<td>ECDHE/RSA key exchange</td>
<td>128-bit AES/CBC</td>
<td>SHA256 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-CBC-SHA</td>
<td>ECDHE/RSA key exchange</td>
<td>128-bit AES/CBC</td>
<td>SHA hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>RSA-AES256-GCM-SHA384</td>
<td>ECDHE/RSA key exchange</td>
<td>256-bit AES/GCM</td>
<td>SHA384 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>RSA-AES256-CBC-SHA256</td>
<td>ECDHE/RSA key exchange</td>
<td>256-bit AES/CBC</td>
<td>SHA256 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>RSA-AES128-GCM-SHA256</td>
<td>ECDHE/RSA key exchange</td>
<td>128-bit AES/GCM</td>
<td>SHA256 hash</td>
<td>Strong</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>RSA-AES128-CBC-SHA256</td>
<td>ECDHE/RSA key exchange</td>
<td>128-bit AES/CBC</td>
<td>SHA256 hash</td>
<td>Medium</td>
<td>Junos OS Release 15.1X49-D10</td>
</tr>
<tr>
<td>RSA-AES128-CBC-SHA</td>
<td>RSA key exchange</td>
<td>128-bit AES/CBC</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-AES256-CBC-SHA</td>
<td>RSA key exchange</td>
<td>256-bit AES/CBC</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
</tbody>
</table>

Starting in Junos OS Release 18.4R1, support for some ciphers in custom ciphers are deprecated. Table 37 on page 378 provides the list of the deprecated ciphers.
### Table 37: List of Deprecated Ciphers

<table>
<thead>
<tr>
<th>SSL Cipher</th>
<th>Key Exchange Algorithm</th>
<th>Data Encryption</th>
<th>Message Integrity</th>
<th>Preferred Ciphers Category</th>
<th>Earliest Supported Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-RC4-128-MD5</td>
<td>RSA key exchange</td>
<td>128-bit RC4</td>
<td>Message Digest 5 (MD5) hash</td>
<td>Medium</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-RC4-128-SHA</td>
<td>RSA key exchange</td>
<td>128-bit RC4</td>
<td>Secure Hash Algorithm (SHA) hash</td>
<td>Medium</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-EXPORT-1024-RC4-56-MD5</td>
<td>RSA 1024 bit export</td>
<td>56-bit RC4</td>
<td>MD5 hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-EXPORT-1024-RC4-56-SHA</td>
<td>RSA 1024 bit export</td>
<td>56-bit RC4</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-EXPORT-RC4-40-MD5</td>
<td>RSA-export</td>
<td>40-bit RC4</td>
<td>MD5 hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-EXPORT-DES40-CBC-SHA</td>
<td>RSA-export</td>
<td>40-bit DES/CBC</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-EXPORT-1024-DES-CBC-SHA</td>
<td>RSA 1024 bit export</td>
<td>DES/CBC</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-3DES-EDE-CBC-SHA</td>
<td>RSA key exchange</td>
<td>3DES EDE/CBC</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
<tr>
<td>RSA-DES-CBC-SHA</td>
<td>RSA key exchange</td>
<td>DES CBC</td>
<td>SHA hash</td>
<td>Weak</td>
<td>Junos OS Release 12.1</td>
</tr>
</tbody>
</table>

Note the following:

- Supported SSL ciphers for HTTPS firewall authentication are RSA-3DES-EDE-CBC-SHA, RSA-AES-128-CBC-SHA, and RSA-AES-256-CBC-SHA.

- Cipher suites that have "export" in the title are intended for use outside of the United States and might have encryption algorithms with limited key sizes. Export ciphers are not enabled by default. You need to either configure the export ciphers to enable or install a domestic package.

- ECDHE-based cipher suits support the perfect forward secrecy feature in SSL proxy.
Perfect forward secrecy is a specific key agreement protocols which ensures that all transactions sent over the Internet are secure. Perfect forward secrecy generates a unique session key for every session initiated by user. This ensures that the compromise of a single session key has no impact on data other than that exchanged in the specific session protected by that particular key.

**Configuring Cipher Suites for SSL Proxy**

You can use following options in SSL proxy profile configuration to set cipher suites:

- **Preferred Ciphers**—Preferred ciphers allow you to define an SSL cipher with acceptable key strength: strong, medium, or weak.

  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. Custom ciphers allow you to define your own cipher list. To configure custom ciphers, you must set preferred-ciphers to custom. Example:

  ```
  set services ssl proxy profile profile-name preferred-ciphers custom
  ```

- **Custom Ciphers**—Custom ciphers allow you to define your own cipher list. Example:

  ```
  set services ssl proxy profile profile-name custom-ciphers ecdhe-ecdsa-with-aes-256-cbc-sha384
  set services ssl proxy profile profile-name custom-ciphers ecdhe-ecdsa-with-aes-128-cbc-sha256
  ```

Use the following steps to configure an SSL proxy with custom ciphers:

- Generate a root CA certificate or you can import your own trusted CA certificate and private and public keys into the device.
- Create an SSL proxy profile and associate root CA certificate (Root CA or the server certificate).
- Enable preferred-cipher in the SSL proxy as a custom-cipher and attach custom cipher

Example:

This example shows how to create a custom cipher. In this example, you set `preferred-cipher` to custom and add the cipher list (`ecdhe-ecdsa-with-aes-256-cbc-sha384` and `ecdhe-ecdsa-with-aes-128-cbc-sha256`):

```
request security pki local-certificate load filename rootCA.pem key rootCA.key certificate-id rootCAEcds

set services ssl proxy profile profile-name server-certificate rootCAEcds

Or

set services ssl proxy profile profile-name root-ca rootCAEcds
```
Proceed with configuring the SSL proxy profile and applying the SSL proxy profile to a security policy.

**ECDSA Cipher Suite Support for SSL Proxy**

Starting in Junos OS Release 18.3R1, SRX Series devices support ECDSA cipher suites for SSL proxy. ECDSA is a version of the Digital Signature Algorithm (DSA) and is based on Elliptic-curve cryptography (ECC). To use ECDSA ciphers on your security device, you must ensure to:

- Include the certificates containing ECC-capable public keys on the device. Support is available for the Elliptic Curve Cryptography (ECC) certificate only with the Elliptic Prime Curve 256 bit (P-256).

- Include the ECDSA certificate option for the root CA. You can include one RSA certificate and one ECDSA certificate each. Having both ECC and RSA certificate allows you to perform ECC-based key exchange or RSA-based key exchange depending on the client and the server device's compatibility.

- For reverse proxy, include the ECDSA certificate for the server certificate. No restriction on the number of ECDSA or RSA certificate inclusion.

- A trusted CA certificate can either be an RSA-based certificate and an ECDSA-based certificate. All features supported on an RSA-based certificate such as certificate cache, certificate revocation list (CRL), certificate chain are supported on an ECDSA certificate.

**Configuring Server Certificates of Key Size 4096 Bits on SRX300 and SRX320**

Starting in Junos OS Release 19.4R1, SRX300 and SRX320 devices support RSA certificates with key size 4096 bits. This support is available only when the SRX300 and SRX320 devices are operating in standalone mode.

You must explicitly configure the SSL proxy profile on SRX300 and SRX320 devices to use the server certificate with key size 4096 bits. Example:

**SSL Forward Proxy Profile**

```bash
proxy {
    profile sslfp-proxy-profile {
        trusted-ca all;
    }
}
```
SSL Reverse Proxy Profile

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.4R1</td>
<td>Starting in Junos OS Release 19.4R1, SRX300 and SRX320 devices support RSA certificates with key size 4096 bits</td>
</tr>
<tr>
<td>18.4R1</td>
<td>Starting in Junos OS Release 18.4R1, support for some ciphers in custom ciphers are deprecated.</td>
</tr>
<tr>
<td>18.3R1</td>
<td>Starting in Junos OS Release 18.3R1, SRX Series devices support ECDSA cipher suites for SSL proxy. ECDSA is a version of the Digital Signature Algorithm (DSA) and is based on Elliptic-curve cryptography (ECC).</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- SSL Proxy | 351
- SSL Certificates | 356
Configuring SSL Proxy

SRX Series device support SSL forward proxy and SSL reverse proxy.

Configuring SSL Forward Proxy

IN THIS SECTION

- SSL Proxy Configuration Overview | 383
- Configuring a Root CA Certificate | 384
- Generate a Root CA Certificate with CLI | 384
- Generate a Root CA Certificate with OpenSSL | 385
- Configuring a CA Profile Group | 386
- Importing a Root CA Certificate into a Browser | 388
- Applying an SSL Proxy Profile to a Security Policy | 389
- Configuring SSL Proxy Logging | 391
- Configuring Certificate Authority Profiles | 391
- Exporting Certificates to a Specified Location | 393
- Ignoring Server Authentication | 393
SSL Proxy Configuration Overview

Figure 19 on page 357 displays an overview of how SSL proxy is configured. Configuring SSL proxy includes:

- Configuring the root CA certificate
- Loading a CA profile group
- Configure SSL proxy profile and associate root CA certificate and CA profile group
- Create a security policy by defining input traffic match criteria
- Applying an SSL proxy profile to a security policy
- Optional steps such as creating whitelists and SSL proxy logging

Figure 21: SSL Proxy Configuration Overview

1. Define a root CA certificate.
   - Generate a root CA certificate.
   - or
   - Import a root CA certificate.

2. Configure a trusted CA profile or group.
   - Configure a trusted CA profile group.
   - or
   - Configure a single trusted CA profile.

3. Configure an SSL proxy profile.
   - Create an SSL proxy profile.
   - Apply the root CA certificate to the SSL proxy profile.
   - Apply the configured trusted CA list for your profile.
   - (Optional) Configure SSL proxy logging.
   - (Optional) Create whitelists of exempted destinations.

4. Apply the SSL proxy profile to a security policy.
   - Apply the SSL proxy profile to a security policy.
Configuring a Root CA Certificate

A CA can issue multiple certificates in the form of a tree structure. A root certificate is the topmost certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the signature or trustworthiness of the root certificate. This is somewhat like the notarizing of an identity.

You can configure a root CA certificate by first obtaining a root CA certificate (by either generating a self-signed one or importing one) and then applying it to an SSL proxy profile. There are two ways you can obtain a root CA certificate—by using the Junos OS CLI on an SRX Series device or by using OpenSSL on a UNIX device.

Generate a Root CA Certificate with CLI

To define a self-signed certificate in CLI, you must provide the following details:

- Certificate identifier (generated in the previous step)
- Fully qualified domain name (FQDN) for the certificate
- E-mail address of the entity owning the certificate
- Common name and the organization involved

Generate a root CA certificate using the Junos OS CLI:

1. From operational mode, generate a PKI public/private key pair for a local digital certificate.

   ```
   user@host> request security pki generate-key-pair certificate-id certificate-id size size type type
   ```

   Example:

   ```
   user@host> request security pki generate-key-pair certificate-id SECURITY-cert size 2048 type ecdsa
   ```

2. Define a self-signed certificate.

   ```
   user@host> request security pki local-certificate generate-self-signed certificate-id certificate-id domain-name domain-name subject subject email email-id add-ca-constraint
   ```

   Example:

   ```
   user@host> request security pki local-certificate generate-self-signed certificate-id SECURITY-cert domain-name labs.abc.net subject DC=mydomain.net,L=Sunnyvale,O=Mydomain,OU=LAB,CN=SECURITY email lab@labs.abc.net add-ca-constraint
   ```
By configuring the **add-ca-constraint** option, you make sure that the certificate can be used for signing other certificates.

3. From configuration mode, apply the loaded certificate as root-ca in the SSL proxy profile.

   ```
   [edit]
   user@host# set services ssl proxy profile profile-name root-ca certificate-id
   ```

   Example:

   ```
   [edit]
   user@host# set services ssl proxy profile SECURITY-SSL-PROXY root-ca SECURITY-cert
   ```

4. Import the root CA as a trusted CA into client browsers. This is required for the client browsers to trust the certificates signed by the SRX Series device. See "Importing a Root CA Certificate into a Browser" on page 362.

### Generate a Root CA Certificate with OpenSSL

To generate a root CA certificate using OpenSSL:

1. Create folders **keys** and **certs**.

   ```
   mkdir /etc/pki/tls/keys
   mkdir /etc/pki/tls/certs
   ```

2. Change to the **openssl** directory.

   ```
   cd /etc/pki/tls
   ```

3. Create a CA certificate key.

   ```
   % openssl genrsa -des3 -out keys/ssl-proxy-ca.key 2048
   ```

   This step creates an RSA key using the 3DES encryption named **ca.key** that is 2048 in length. You also need to enter a password that is used to encrypt the private key. This is critical to security if the key is lost because it will still be encrypted.

4. Create a CA certificate based on the CA private key (created in the previous step).
The expiration date for this certificate is 3 years or 1095 days. However, you can set it to a different value. When creating the certificate, you need to enter the password and the certificate information that includes distinguished name (DN), country name, and so forth.

5. Import the CA private and public keys into the SRX Series device. Copy the `ca.key` and `ca.cer` keys to the `/var/tmp` directory on the SRX Series device. You can copy using SCP, or open the files and copy them into “vi” on the SRX Series device to create new files.

```
user@host> request security pki local-certificate load certificate-id ssl-inspect-ca key /var/tmp/ssl-proxy-ca.key filename /var/tmp/ssl-inspect-ca.cer passphrase password
```

6. From configuration mode, apply the loaded certificate as root-ca in the SSL proxy profile.

```
[edit]
user@host# set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
```

7. Import the root CA as a trusted CA into client browsers. This is required for the client browsers to trust the certificates signed by the SRX Series device. See "Importing a Root CA Certificate into a Browser" on page 362.

### Configuring a CA Profile Group

The CA profile defines the certificate information for authentication. It includes the public key that SSL proxy uses when generating a new certificate. Junos OS allows you to create a group of CA profiles and load multiple certificates in one action, view information about all certificates in a group, and delete unwanted CA groups.

You can load a group of CA profiles by obtaining a list of trusted CA certificates, defining a CA group, and attaching the CA group to the SSL proxy profile.

1. Obtain a list of trusted CA certificates by using one of the following methods. When a connection is initiated, the connecting device (such as a Web browser) checks whether the certificate is issued by a trusted CA. Without these certificates, browsers cannot validate the identity of most websites and mark them as untrusted sites.

   - Junos OS provides a default list of trusted CA certificates that you can load on your system. The Junos OS package contains the default CA certificates as a PEM file (for example, `trusted_CA.pem`). After you download the Junos OS package, the default certificates are available on your system.
From operational mode, load the default trusted CA certificates (the group name identifies the CA profile group):

```bash
user@host> request security pki ca-certificate ca-profile-group load ca-group-name group-name filename default
```

Example:

```bash
user@host> request security pki ca-certificate ca-profile-group load ca-group-name SECURITY-CA-GROUP filename default
```

We recommend using this method.

- Alternatively, you can define your own list of trusted CA certificates and import them on your system. You get the list of trusted CAs in a single PEM file (for example `IE-all.pem`) and save the PEM file in a specific location (for example, `/var/tmp`). See Knowledge Base Article KB23144.

From operational mode, load the trusted list to the device (the group name identifies the CA profile group):

```bash
user@host> request security pki ca-certificate ca-profile-group load ca-group-name group-name filename /var/tmp/IE-all.pem
```

Example:

```bash
user@host> request security pki ca-certificate ca-profile-group load ca-group-name SECURITY-CA-GROUP filename /var/tmp/custom-file.pem
```

- Download the latest CA bundle list from another 3rd party such as Mozilla (https://curl.haxx.se/docs/caextract.html). The list of trusted Certificate Authority can change over time, ensure that you use the latest CA bundle.

- Import your own trusted CA certificates using the Public Key Infrastructure (PKI). The PKI helps verify and authenticate the validity of the trusted CA certificates. You create CA profile groups that include trusted CA certificates, then import the group on your device for server authentication.

2. Attach the trusted CA or trusted CA group to the SSL proxy profile. You can attach all trusted CA or one trusted CA at a time:

- Attach all CA profile groups:

  ```bash
  [edit]
  user@host# set services ssl proxy profile profile-name trusted-ca all
  ```

  Example
• Attach one CA profile group (the group name identifies the CA profile group).

Example

You can easily display information about all certificates in a CA profile group:

You can delete a CA profile group. Remember that deleting a CA profile group deletes all certificates that belong to that group:

**Importing a Root CA Certificate into a Browser**

In order to have your browser or system automatically trust all certificates signed by the root CA configured in the SSL proxy profile, you must instruct your platform or browser to trust the CA root certificate.

To import a root CA certificate:

1. Generate a PEM format file for the configured root CA.

   `request security pki local-certificate export certificate-id root-ca type pem filename path/file-name.pem`

2. Import a root CA certificate into a browser.

   From Internet Explorer (version 8.0):
   
   a. From the Tools menu, select **Internet Options**.

   b. On the Content tab, click **Certificates**.
c. Select the **Trusted Root Certification Authorities** tab and click **Import**.

d. In the Certificate Import Wizard, navigate to the required root CA certificate and select it.

From Firefox (version 39.0):

a. From the Tools menu, select **Options**.

b. From the Advanced menu, select the **Certificates** tab and click **View Certificate**.

c. In the Certificate Manager window, select the **Authorities** tab and click **Import**.

d. Navigate to the required root CA certificate and select it.

From Google Chrome (45.0):

a. From the Settings menu, select **Show Advanced Settings**.

b. From the Advanced menu, select the **Certificates** tab and click **View Certificate**.

c. Under HTTPS/SSL, click **Manage Certificates**.

d. In the Certificate window, select **Trusted Root Certification Authorities** and click **Import**.

e. In the Certificate Import Wizard, navigate to the required root CA certificate and select it.

**Applying an SSL Proxy Profile to a Security Policy**

SSL proxy is enabled as an application service within a security policy. In a security policy, you specify the traffic that you want the SSL proxy enabled on as match criteria and then specify the SSL proxy CA profile to be applied to the traffic. **Figure 22 on page 390** displays a graphical view of SSL proxy profile and security policy configuration.
Figure 22: Applying an SSL Proxy Profile to a Security Policy

To enable SSL proxy in a security policy:

This example assumes that you have already created security zones trust and untrust and creating a security policy for the traffic from trust zone to untrust zone.

1. Create a security policy and specify the match criteria for the policy. As match criteria, specify the traffic for which you want to enable SSL proxy.

Example:

```
user@host# set security policies from-zone trust to-zone untrust policy policy-name match source-address any
```
2. Apply the SSL proxy profile to the security policy.

3. Configure SSL Proxy Logging

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.

You can use `enable-flow-tracing` option to enable debug tracing.

4. Configure Certificate Authority Profiles

A certificate authority (CA) profile configuration contains information specific to a CA. You can have multiple CA profiles on an SRX Series device. For example, you might have one profile for orgA and one for orgB. Each profile is associated with a CA certificate. If you want to load a new CA certificate without removing the older one then create a new CA profile (for example, Microsoft-2008). You can group multiple CA profiles in one trusted CA group for a given topology.

In this example, you create a CA profile called ca-profile-security with CA identity microsoft-2008. You then create proxy profile to the CA profile.

1. From configuration mode, configure the CA profile used for loading the certificate.
2. Commit the configuration.

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

3. From operational mode, load the certificate using PKI commands.

```
user@host> request security pki ca-certificate load ca-profile profile-name filename
```

Example:

```
user@host> request security pki ca-certificate load ca-profile ca-profile-security filename srx-123.crt
```

4. From configuration mode, disable the revocation check (if required).

```
[edit]
user@host# set security pki ca-profile profile-name ca-identity ca-identity revocation-check disable
```

Example:

```
[edit]
user@host# set security pki ca-profile ca-profile-security ca-identity example.com revocation-check disable
```

5. From configuration mode, configure the loaded certificate as a trusted CA in the SSL proxy profile.

```
[edit]
user@host# set services ssl proxy profile ssl-proxy-profile-name trusted-ca ca-profile-name
```

Example:

```
[edit]
```
NOTE: More than one trusted CA can be configured for a profile.

6. (Optional) If you have multiple trusted CA certificates, you do not have to specify each trusted CA separately. You can load all the trusted CA certificates using the following command from configuration mode.

```
[edit]
user@host# set services ssl proxy profile ssl-proxy-profile-name root-ca ssl-inspect-ca
user@host# set services ssl proxy profile ssl-proxy-profile-name trusted-ca all
```

NOTE: Alternatively, you can import a set of trusted CAs from your browser into the SRX Series device. See Knowledge Base article KB23144.

Exporting Certificates to a Specified Location

When a self-signed certificate is generated using a PKI command, the newly generated certificate is stored in a predefined location (`/var/db/certs/common/local`).

Use the following command to export the certificate to a specific location (within the device). You can specify the certificate ID, the filename, and the type of file format (DER/PEM):

```
user@host> request security pki local-certificate export certificate-id certificate-id filename filename type der
```

Ignoring Server Authentication

Junos OS allows you to configure an option to ignore server authentication completely. If you configure your system to ignore authentication, then any errors encountered during server certificate verification at the time of the SSL handshake are ignored. Commonly ignored errors include the inability to verify CA signature, incorrect certificate expiration dates, and so forth. If this option is not set, all the sessions where the server sends self-signed certificates are dropped when errors are encountered.

We do not recommend using this option for authentication because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause of dropped SSL sessions.
From configuration mode, specify to ignore server authentication:

```
[edit]
user@host# set services ssl proxy profile profile-name actions ignore-server-auth-failure
```

SEE ALSO

Understanding Certificates and PKI
Understanding Self-Signed Certificates
show services ssl proxy statistics  | 906
clear services ssl proxy statistics  | 689

SSL Reverse Proxy

IN THIS SECTION

- Overview  | 394
- Configuring the SSL Reverse Proxy  | 398
- Verifying the SSL Reverse Proxy Configuration on the Device  | 399

Overview

The proxy model implementation for server protection (often called reverse proxy) is supported on SRX Series devices to provide improved handshaking and support for more protocol versions. You can enable Layer 7 services (application security, IPS, UTM, SKY ATP) on the traffic decrypted by SSL reverse proxy.

Starting in Junos OS Release 15.1X49-D80 and 17.3R1, SSL reverse proxy is supported on SRX5000 Series, SRX4100, SRX4200, SRX1500 devices.

NOTE:

Starting in Junos OS Release 15.1X49-D80 and 17.3R1, we recommend using the SSL reverse proxy and Intrusion Detection and Prevention (IDP) instead of using the IDP SSL inspection functionality.
Starting from Junos OS 15.1X49-D80 and 17.3R1, IDP SSL Inspection is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Table 38 on page 395 provides the changes applicable on SRX Series devices post 15.1X48-D80 and 17.3R1 releases.

Table 38: Comparing Reverse Proxy Before and After Junos OS Release 15.1X49-D80

<table>
<thead>
<tr>
<th>Feature</th>
<th>Prior to 15.1X49-D80</th>
<th>15.1X49-D80 and 17.3R1 later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy model</td>
<td>Runs only in tap mode. Instead of participating in SSL handshake, it listens to the SSL handshake, computes session keys and then decrypts the SSL traffic.</td>
<td>Terminates client SSL on the SRX Series device and initiates a new SSL connection with a server. Decrypts SSL traffic from the client/server and encrypts again (after inspection) before sending to the server/client.</td>
</tr>
<tr>
<td>Protocol version</td>
<td>Does not support TLS Version 1.1 and 1.2.</td>
<td>Supports all current protocol versions.</td>
</tr>
<tr>
<td>Key exchange methods</td>
<td>• Supports RSA&lt;br&gt;• Does not support DHE.</td>
<td>• Supports RSA&lt;br&gt;• Support DHE or ECDHE</td>
</tr>
<tr>
<td>Echo system</td>
<td>Tightly coupled with IDP engine and its detector.</td>
<td>Uses existing SSL forward proxy with TCP proxy underneath.</td>
</tr>
<tr>
<td>Security services</td>
<td>Decrypted SSL traffic can be inspected only by IDP.</td>
<td>Just like forward proxy, decrypted SSL traffic is available for all security services.</td>
</tr>
<tr>
<td>Ciphers supported</td>
<td>Limited set of ciphers are supported.</td>
<td>All commonly used ciphers are supported.</td>
</tr>
</tbody>
</table>

You must configure either root-ca or server-certificate in an SSL proxy profile. Otherwise the commit check fails. See Table 39 on page 395.

Table 39: Supported SSL Proxy Configurations

<table>
<thead>
<tr>
<th>server-certificate configured</th>
<th>root-ca configured</th>
<th>Profile type</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Commit check fails. You must configure either server-certificate or root-ca.</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Commit check fails. Configuring both server-certificate and root-ca in the same profile is not supported.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Forward proxy</td>
</tr>
</tbody>
</table>
# Supported SSL Proxy Configurations (continued)

<table>
<thead>
<tr>
<th>server-certificate configured</th>
<th>root-ca configured</th>
<th>Profile type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>Reverse proxy</td>
</tr>
</tbody>
</table>

Configuring multiple instances of forward and reverse proxy profiles are supported. But for a given firewall policy, only one profile (either a forward or reverse proxy profile) can be configured. Configuring both forward and reverse proxy on the same device is also supported.

You cannot configure the previous reverse proxy implementation with the new reverse proxy implementation for a given firewall policy. If both are configured, you will receive a commit check failure message.

The following are the minimum steps to configure reverse proxy:

1. Load the server certificates and their keys into the SRX Series device certificate repository using the CLI command `request security pki local-certificate load filename filename key key certificate-id certificate-id passphrase example@1234`. For example:

```plaintext
user@host> request security pki local-certificate load filename /cf0/cert1.pem key /cf0/key1.pem certificate-id server1_cert_id passphrase example@1234
```

2. Attach the server certificate identifier to the SSL Proxy profile using the CLI command `set services ssl proxy profile profile server-certificate certificate-id passphrase example@1234`. For example

```plaintext
user@host# set services ssl proxy profile server-protection-profile server-certificateserver2_cert_id
```

3. Use the `show services ssl` CLI command to verify your configuration. For example:

```plaintext
user@host# show services ssl
profile server-protection-profile {
    server-certificate [server1_cert_id , server2_cert_id];
    actions {
        logs {
            all;
        }
    }
}
```

The SSL forward proxy and reverse proxy require a profile to be configured at the firewall rule level. In addition, you must also configure server certificates with private keys for reverse proxy. During an SSL
handshake, the SSL proxy performs a lookup for a matching server private key in its server private key
hash table database. If the lookup is successful, the handshake continues. Otherwise, SSL proxy aborts
the hand shake. Reverse proxy does not prohibit server certificates. It forwards the actual server
certificate/chain as is to the client without modifying it. Intercepting the server certificate occurs only with
forward proxy.

The following shows example forward and reverse proxy profile configurations.

```plaintext
# show services ssl
...
proxy {
    profile ssl-inspect-profile-dut { # For forward proxy. No server cert/key is needed.
        trusted-ca all;
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-1 {
        trusted-ca all;
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-2 {
        trusted-ca all;
        root-ca ssl-inspect-ca;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
    profile ssl-server-protection { # For reverse proxy. No root-ca is needed.
        server-certificate ssl-server-protection;
    }
```
Configuring the SSL Reverse Proxy

This example shows how to configure reverse proxy to enable server protection. For server protection, additionally, server certificate(s) with private key(s) must be configured.

A reverse proxy protects servers by hiding the details of the servers from the clients, thereby adding an extra layer of security.

To configure an SSL reverse proxy, you must:

- Load the server certificate(s) and their key(s) into SRX Series device's certificate repository.
- Attach the server certificate identifier(s) to the SSL proxy profile.
- Apply SSL proxy profile as application services in a security policy.

To configure SSL reverse proxy:

1. Load the signing certificate and the respective key for the SSL proxy profile in PKI memory.

```
user@host> request security pki local-certificate load filename /cf0/cert1.pem key /cf0/key1.pem
       certificate-id server1_cert_id
```

2. Attach the server certificate to the SSL proxy profile.

```
user@host# set services ssl proxy profile server-protection-profile server-certificate server1_cert_id
```

3. Create a security policy and specify the match criteria for the policy. As match criteria, specify the traffic for which you want to enable SSL proxy.

```
user@host# set security policies from-zone untrust to-zone trust policy1 match source-address any
user@host# set security policies from-zone untrust to-zone trust policy1 match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy1 match application any
```
4. Apply the SSL proxy profile to the security policy. This example assumes that security zones are created as per requirements.

```bash
user@host# set security policies from-zone untrust to-zone trust policy 1 then permit application-services ssl-proxy server-protection-profile
```

**Verifying the SSL Reverse Proxy Configuration on the Device**

**Purpose**
Viewing the SSL reverse proxy statistics on the SRX Series device.

**Action**
You can view the SSL proxy statistics by using the `show services ssl proxy statistics` command.

```bash
root@mullai> show services ssl proxy statistics
PIC:spu-1 fpc[0] pic[1] -------
  sessions matched           0
  sessions whitelisted       0
  sessions bypassed:non-ssl  0
  sessions bypassed:mem overflow 0
  sessions bypassed:low memory 0
  sessions created           0
  sessions ignored           0
  sessions active            0
  sessions dropped           0
```
Creating a Whitelist of Exempted Destinations for SSL Proxy
SSL encryption and decryption might consume memory resources on the SRX Series devices. To limit this, you can selectively bypass SSL proxy processing for some sessions such as sessions that transacts with familiar trusted servers or domains. You can also exempt the sessions with financial and banking sites due to legal requirements.

To exempt the sessions from SSL proxy, you can create a whitelists by adding IP addresses or domain names of the servers. Whitelists include addresses that you want to exempt from undergoing SSL proxy processing.

Use the following steps to create whitelists:

• Specify IP addresses and domain name in your global address book.
• Refer the global address book in SSL proxy profile.

You can configure the following types of the IP addresses in global address book.

• IPv4 addresses (plain text). For example:

  ```
  set security address-book global address address-4 192.0.2.117
  ```

• IPv4 address range. For example:

  ```
  set security address-book global address address-2 range-address 192.0.2.117 to 192.0.2.199
  ```

• IPv4 wildcard. For example:

  ```
  set security address-book global address address-3 wildcard-address 203.0.113.0/24
  ```

• DNS name. For example:

  ```
  set security address-book global address address-1 dns-name www.abc.com
  ```

• IPv6 address. For example:

  ```
  set security address-book global address address-5 FE80::/10
  ```

Whitelists do not support the following types of IP addresses:
• Translated IP addresses. Sessions are whitelisted based on the actual IP address and not on the translated IP address. Because of this, in the whitelist configuration of the SSL proxy profile, the actual IP address should be provided and not the translated IP address.

• Noncontiguous netmasks. For example:
  • IP address -203.0.113.0 and mask 255.255.255.0 that is 203.0.113.0/24 is supported.
  • IP address - 203.0.113.9 and mask 255.0.255.0 is not supported.

Following example shows you how to use whitelists in SSL proxy profile.

In this example, you exempt all sessions to www.mycompany.com. For this, you first specify the domain in the address book and then configure the address in the SSL proxy profile.

1. Configure the domain in the address book.

   [edit]
   user@host# set security address-book global address address-1 dns-name www.mycompany.com

2. Specify the global address book address in the SSL proxy profile.

   [edit]
   user@host# set services ssl proxy profile profile-1 whitelist address-1

---

## Creating a Whitelist of Exempted URL Categories for SSL Proxy

You can configure the URL categories supported in UTM module to exempt from SSL inspection on SRX Series device. To use URL categories from UTM, SRX Series device integrates the SSL proxy profile with the EWF feature. With this now, you can configure a list of URL categories under an SSL proxy profile as whitelist along with address-books. You can configure the list from the predefined set of URL categories or custom URL categories supported by UTM.
The security device uses the Server Name Indication (SNI) field extracted by the UTM module to determine the URL category. The SSL proxy uses this information to determine whether to accept, and proxy, or to ignore the session.

This feature is supported on SRX340, SRX345, SRX5400, SRX5600, SRX5800 and vSRX instances.

Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, SSL proxy whitelisting feature includes URL categories supported by UTM.

Starting with Junos OS Release 17.4R1, SSL proxy whitelisting feature extends support to custom URL categories supported by UTM.

Following examples show how to configure the URL categories in SSL proxy profile:

Creating a Whitelist of Exempted URL Categories

Use the following steps to configure the predefined URL categories in an SSL proxy profile.

1. The predefined URL categories depend on UTM. To enable URL-based whitelisting in SSL proxy, the following basic URL configurations are required:

   ```
   [edit]
   user@host# set security utm utm-policy UTM-POLICY-1 web-filtering http-profile junos-wf-enhanced-default
   ```

2. Specify the predefined URL category in SSL proxy profile. In this example, you are using the URL category Enhanced_Financial_Data_and_Services.

   ```
   [edit]
   user@host# set services ssl proxy profile pr1 whitelist-url-categories Enhanced_Financial_Data_and_Services
   ```

3. Create the security policy by specifying the match conditions and attach the UTM policy to the security policy to use URL categories in SSL whitelist.

   ```
   user@host# set security policies from-zone trust to-zone untrust policy p1 match source-address any
   user@host# set security policies from-zone trust to-zone untrust policy p1 match destination-address any
   user@host# set security policies from-zone trust to-zone untrust policy p1 match application any
   user@host# set security policies from-zone trust to-zone untrust policy p1 permit application-services utm-policy UTM-POLICY-1
   user@host# set security policies from-zone trust to-zone untrust policy p1 permit application-services ssl-proxy profile-name pr1
   ```
Creating a Whitelist of Exempted Custom URL Categories

Use the following steps to configure custom URL categories in an SSL proxy profile.

1. Create a custom URL category.

   [edit]
   user@host# set security utm custom-objects url-pattern URL-1 value www.example.com
   user@host# set security utm custom-objects custom-url-category CATEGORY-1 value URL-1
   user@host# set security utm feature-profile web-filtering juniper-local profile PROFILE-1 category CATEGORY-1 action permit

2. Configure a UTM policy for the Web-filtering HTTP protocol and associate the profile you created in previous step to the the UTM policy.

   [edit]
   user@host# set security utm utm-policy UTM-POLICY-1 web-filtering http-profile PROFILE-1

3. Specify the custom URL category you created in previous step in SSL proxy profile.

   user@host# set services ssl proxy profile pr1 whitelist-url-categories CATEGORY-1

4. Create a security policy by specifying the match conditions and attach the UTM policy to the security policy to use URL categories in SSL whitelist.

   [edit]
   user@host# set security policies from-zone trust to-zone untrust policy p1 match source-address any
   user@host# set security policies from-zone trust to-zone untrust policy p1 match destination-address any
   user@host# set security policies from-zone trust to-zone untrust policy p1 match application any
   user@host# set security policies from-zone trust to-zone untrust policy p1 permit application-services utm-policy UTM-POLICY-1
   user@host# set security policies from-zone trust to-zone untrust policy p1 permit application-services ssl-proxy profile-name pr1
### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.4R1</td>
<td>Starting with Junos OS Release 17.4R1, SSL proxy whitelisting feature extends support to custom URL categories supported by UTM.</td>
</tr>
<tr>
<td>15.1X49-D80</td>
<td>Starting in Junos OS Release 15.1X49-D80 and 17.3R1, SSL reverse proxy is supported on SRX5000 Series, SRX4100, SRX4200, SRX1500 devices</td>
</tr>
<tr>
<td>15.1X49-D80</td>
<td>Starting in Junos OS Release 15.1X49-D80 and 17.3R1, we recommend using the SSL reverse proxy and Intrusion Detection and Prevention (IDP) instead of using the IDP SSL inspection functionality.</td>
</tr>
<tr>
<td>15.1X49-D80</td>
<td>Starting from Junos OS 15.1X49-D80 and 17.3R1, IDP SSL Inspection is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.</td>
</tr>
<tr>
<td>15.1X49-D80</td>
<td>Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, SSL proxy whitelisting feature includes URL categories supported by UTM.</td>
</tr>
</tbody>
</table>

### Related Documentation

- Example: Loading CA and Local Certificates Manually
- Example: Configuring a Device for Peer Certificate Chain Validation

### Unified Policies for SSL Proxy

**In This Section**

- Application Security Services with SSL Proxy | 406
- SSL Proxy Support for Unified Policies | 407
- Configuring Default SSL Proxy Profiles | 412
- Example: Configuring Default SSL Proxy Profile for Unified Policy | 414
Application Security Services with SSL Proxy

With the implementation of SSL proxy, AppID can identify applications encrypted in SSL. SSL proxy can be enabled as an application service in a regular firewall policy rule. Intrusion Detection and Prevention (IDP), application firewall (AppFW), application tracking (AppTrack), advanced policy-based routing (APBR) services, UTM, SKY ATP, and Security Intelligence (SecIntel) can use the decrypted content from SSL proxy.

To determine if a feature is supported by a specific platform or Junos OS release, refer Feature Explorer.

On the SSL payload, IDP can inspect attacks and anomalies; for example, HTTP chunk length overflow on HTTPS. On encrypted applications, such as Facebook, AppFW can enforce policies and AppTrack (when configured in the from and to zones) can report logging issues based on dynamic applications.

NOTE: If none of the services (AppFW, IDP, or AppTrack) are configured, then SSL proxy services are bypassed even if an SSL proxy is attached to a firewall policy.

NOTE: The IDP module will not perform an SSL inspection on a session if an SSL proxy is enabled for that session. That is, if both SSL inspection and SSL proxy are enabled on a session, SSL proxy will always take precedence.

Leveraging Dynamic Application Identification

SSL proxy uses application identification services to dynamically detect if a particular session is SSL encrypted. SSL proxies are allowed only if a session is SSL encrypted. The following rules apply for a session:

- Session is marked Encrypted=Yes in the application system cache. If the session is marked Encrypted=Yes, it indicates that the final match from application identification for that session is SSL encrypted, and SSL proxy transitions to a state where proxy functionality can be initiated.

- Session is marked Encrypted=No in the application system cache. If a non-SSL entry is found in the application system cache, it indicates that the final match from application identification for that session is non-SSL and SSL proxy ignores the session.

- An entry is not found in the application system cache. This can happen on the first session, or when the application system cache has been cleaned or has expired. In such a scenario, SSL proxy cannot wait for the final match (requires traffic in both directions). In SSL proxy, traffic in reverse direction happens only if SSL proxy has initiated an SSL handshake. Initially, for such a scenario SSL proxy tries to leverage
prematch or aggressive match results from application identification, and if the results indicate SSL, SSL proxy will go ahead with the handshake.

- Application identification fails due to resource constraints and other errors. Whenever the result from application identification is not available, SSL proxy will assume static port binding and will try to initiate SSL handshake on the session. This will succeed for actual SSL sessions, but it will result in dropped sessions for non SSL sessions.

**SEE ALSO**

| Example: Configuring Application Firewall When SSL Proxy Is Enabled | 163 |
| Example: Configuring Application Tracking When SSL Proxy Is Enabled | 183 |

### SSL Proxy Support for Unified Policies

Starting from Junos OS Release 18.2R1, unified policies are supported on SRX Series devices, allowing granular control and enforcement of dynamic Layer 7 applications, within the traditional security policy.

Unified policies are the security policies that enable you to use dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time.

SSL proxy functionality is supported when the device is configured with unified policies. As a part of this enhancement, you can configure a default SSL proxy profile.

During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different SSL proxy profiles, the SRX Series device applies the default SSL proxy profile until a more explicit match has occurred.

We recommend that you create a default SSL proxy profile. The sessions are dropped in case of policy conflicts, if there is no default SSL proxy profile available.

You can configure an SSL proxy profile under the [edit services ssl proxy] hierarchy level, and then apply it as a default SSL proxy profile under the [edit security ngfw] hierarchy level. This configuration does not impact the existing SSL service configuration.

Configuring a default SSL proxy profile is supported for both SSL forward and reverse proxy.

**Understanding How SSL Proxy Default Profile Works**

Table 40 on page 408 summarizes the default SSL proxy profile behavior in unified policies.
**Table 40: SSL Proxy Profile Usage in Unified Policies**

<table>
<thead>
<tr>
<th>Application Identification Status</th>
<th>SSL Proxy Profile Usage</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No security policy conflict</td>
<td>SSL proxy profile is applied when traffic matches the security policy.</td>
<td>SSL proxy profile is applied.</td>
</tr>
<tr>
<td>Security policy conflict (conflicting policies have distinct SSL proxy profiles)</td>
<td>Default SSL proxy profile is not configured or not found.</td>
<td>Session is terminated, because the default SSL proxy profile is not configured.</td>
</tr>
<tr>
<td></td>
<td>Default SSL proxy profile is configured.</td>
<td>Default SSL proxy profile is applied.</td>
</tr>
<tr>
<td>Final application is identified</td>
<td>Matching security policy has a SSL proxy profile that is same as default SSL proxy profile.</td>
<td>Default SSL proxy profile is applied.</td>
</tr>
<tr>
<td></td>
<td>Matching security policy does not have a SSL proxy profile.</td>
<td>Default SSL proxy profile is applied.</td>
</tr>
<tr>
<td></td>
<td>Matching security policy has a SSL proxy profile that is different from the default SSL proxy profile that is already applied.</td>
<td>Default SSL proxy profile that is already applied, continues remain as applied.</td>
</tr>
</tbody>
</table>

**NOTE:** A security policy can have either an SSL reverse proxy profile or an SSL forward proxy profile configured at a time.

If a security policy has an SSL forward proxy profile and another security policy has an SSL reverse proxy profile, in such case, a default profile—either from SSL reverse proxy profile or from SSL forward proxy profile is considered.

**CAUTION:** We recommend creating default SSL proxy profile because sessions are dropped in case of policy conflicts, when there is no default SSL proxy profile available. A system log message is generated to log the event.
TIP: Example of the system log message:

"<14>1 2018-03-07T03:18:33.374-08:00 4.0.0.254 kurinji junos-ssl-proxy -
SSL_PROXY_SSL_SESSION_DROP [junos@2636.1.1.2.105
logical-system-name="root-logical-system" session-id="15"
source-address="4.0.0.1" source-port="37010" destination-address="5.0.0.1"
destination-port="443" nat-source-address="4.0.0.1" nat-source-port="37010"
nat-destination-address="5.0.0.1" nat-destination-port="443"
profile-name="(null)" source-zone-name="untrust"
source-interface-name="xe-2/2/1.0" destination-zone-name="trust"
destination-interface-name="xe-2/2/2.0" message="default ssl-proxy profile
is not configured"]

Default SSL Proxy Profiles in Different Scenarios

IN THIS SECTION
- No Policy Conflict—All Policies Have Same SSL Proxy Profile | 409
- No Policy Conflict—All Policies Have Same SSL Proxy Profile and Final Policy Has No SSL Profile | 410
- Policy Conflict—No SSL Profile Configured for Final Policy | 410
- Policy Conflict—Default SSL Proxy Profile and Different SSL Proxy Profile for Final Policy | 411

Following examples discuss in detail about the default SSL proxy profile in different scenarios:

No Policy Conflict—All Policies Have Same SSL Proxy Profile
All matching policies have same SSL proxy profile as shown in Table 41 on page 409.

Table 41: No Policy Conflict—All Policies Have Same SSL Proxy Profile

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>Default SSL Proxy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>SSL Proxy</td>
<td>SSL-1</td>
</tr>
</tbody>
</table>
Table 41: No Policy Conflict—All Policies Have Same SSL Proxy Profile (continued)

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>Default SSL Proxy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>SSL Proxy</td>
<td>SSL-1</td>
</tr>
</tbody>
</table>

In this case, both Policy-P1 and Policy-P2 have the same SSL proxy profile (SSL-1). Because there is no conflict, the profile SSL-1 is applied.

If you have configured a default SSL proxy profile (SSL-2), it is not applied. Because there is no conflict in the policies (Policy-P1 and Policy-P2).

No Policy Conflict—All Policies Have Same SSL Proxy Profile and Final Policy Has No SSL Profile

Policy-P1 and Policy-P2 have same SSL proxy profile and the Policy-3 has no SSL profile as shown in Table 42 on page 410.

Table 42: No Policy Conflict—All Policies Have Same SSL Proxy Profile and Final Policy Has No SSL Profile Configured

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>Default SSL Proxy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>SSL Proxy</td>
<td>SSL-1</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>SSL Proxy</td>
<td>SSL-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>Any</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>Other</td>
<td>None</td>
</tr>
</tbody>
</table>

In this scenario, both Policy-P1 and Policy-P2 have the same SSL proxy profile (SSL-1). Because there is no conflict, the profile SSL-1 is applied before the final policy match.

When the final application is identified, the security policy matching with the final application, that is, Policy-P3 is applied. Because the Policy-P3 has no SSL proxy profile, the already applied profile SSL-1 remains applied. This is because, the SSL proxy profile is already applied on the traffic.

Policy Conflict—No SSL Profile Configured for Final Policy

The default SSL proxy profile is applied during potential match as shown in Table 43 on page 411. The final policy, Policy-P3 does not have any SSL proxy profile.
Table 43: Policy Conflict—No SSL Profile Configured for Final Policy

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>Default SSL Proxy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>SSL Proxy</td>
<td>SSL-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>SSL Proxy</td>
<td>SSL-2</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>Other</td>
<td>NA</td>
</tr>
</tbody>
</table>

In this example, SSL proxy profile SSL-1 is configured as default SSL proxy profile. During the policy conflict for Policy-P1 and Policy-P2, the default profile SSL-1 is applied.

When the final application is identified, the security policy matching with the final application, that is, Policy-P3 is applied. Because the Policy-P3 has no SSL proxy profile, the already applied profile SSL-1 continues to remain as applied. This is because, the SSL proxy profile is applied on the traffic.

Policy Conflict—Default SSL Proxy Profile and Different SSL Proxy Profile for Final Policy

The SSL proxy profile SSL-1 is configured as a default SSL proxy profile and is already applied before the final policy is matched. Refer Table 16 on page 207.

Table 44: Policy Conflict—Default SSL Proxy Profile and Different SSL Proxy Profile for Final Policy

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Source Zone</th>
<th>Source IP Address</th>
<th>Destination Zone</th>
<th>Destination IP Address</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Dynamic Application</th>
<th>Service</th>
<th>Default SSL Proxy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-P1</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Facebook</td>
<td>SSL Proxy</td>
<td>SSL-1</td>
</tr>
<tr>
<td>Policy-P2</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Google</td>
<td>SSL Proxy</td>
<td>SSL-2</td>
</tr>
<tr>
<td>Policy-P3</td>
<td>S1</td>
<td>50.1.1.1</td>
<td>D1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>YouTube</td>
<td>SSL Proxy</td>
<td>SSL-3</td>
</tr>
</tbody>
</table>

When the final application is identified, the security policy matching with the final application, that is, Policy-P3 is applied. The SSL profile for the Policy-P3, that is, SSL-3 is not applied. Instead, the SSL proxy profile SSL-2 configured and applied as default profile, continues to remain as applied.
Switching from the default SSL proxy profile that is already applied to the traffic, to another SSL proxy profile is not supported.

**Limitations of SSL Proxy with Unified Policies**

- When a default SSL proxy profile is enabled, it cannot be disabled even if the final security policy does not have SSL proxy configured.
- When a default SSL proxy profile is enabled and applied on the traffic and the final security policy has a different SSL proxy profile configured other than default profile, switching from the default SSL proxy profile to the SSL proxy profile in the security policy is not supported.

---

**Configuring Default SSL Proxy Profiles**

IN THIS SECTION

- Configuring Default Profile for SSL Forward Proxy | 412
- Configuring Default Profile for SSL Reverse Proxy | 413
- Configuring Default SSL Profiles for Logical System | 413

SSL proxy is enabled as an application service within a security policy. In a security policy, specify the match criteria for the traffic that must be SSL proxy enabled. Next, specify the SSL proxy profile to be applied to the traffic. When configuring unified policies, the steps include defining the SSL profile, then adding the SSL profile as default profile under the `edit security ngfw` hierarchy level, and then including it in the desired security policy.

**Configuring Default Profile for SSL Forward Proxy**

In this procedure, you configure an SSL forward proxy profile, and specify the profile as the default profile.

1. Create an SSL profile and attach the CA profile group to the SSL proxy profile.
   
   `user@host# set services ssl proxy profile profile-name trusted-ca all`

2. Apply the signing certificate as root-ca in the SSL proxy profile.
3. Define the SSL proxy profile as the default profile.

```
user@host# set security ngfw default-profile ssl-proxy profile-name
```

### Configuring Default Profile for SSL Reverse Proxy

In this procedure, you configure an SSL reverse proxy profile and specify the profile as the default profile.

1. Create an SSL profile and attach the CA profile group to the SSL proxy profile.

```
user@host# set services ssl proxy profile profile-name server-protection-profile server-certificate server1_certificate-id
```

2. Define the SSL reverse proxy profile as the default profile.

```
user@host# set security ngfw default-profile ssl-proxy profile-name server-protection-profile
```

### Configuring Default SSL Profiles for Logical System

In this procedure, you assign the SSL forward proxy profile or the SSL reverse proxy profile as the default profile in logical system configurations. In this case, one profile can be a default profile either from the SSL forward proxy or from the SSL reverse proxy.

- Define the SSL forward proxy profile as the default profile.

```
user@host# set logical-systems LSYS1 security ngfw default-profile ssl-proxy profile-name
```

- Define the SSL reverse proxy profile as the default profile.

```
user@host# set logical-systems LSYS1 security ngfw default-profile ssl-proxy profile-name
```
Example: Configuring Default SSL Proxy Profile for Unified Policy

This example shows how to configure a default SSL proxy profile and apply it in a unified policy.

Requirements

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 18.2R1 or later. This configuration example is tested for Junos OS Release 18.2R1.

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

Overview

In this example, you configure an SSL forward proxy profile by specifying the root CA certificate. Next, configure the profile as default SSL proxy profile. Now, you create a unified policy and invoke the SSL proxy as application services on the permitted traffic.

Configuration

To configure a default SSL proxy profile and apply it in a unified policy:

1. Create an SSL profile and attach the CA profile group to the SSL proxy profile.

   ```
   user@host# set services ssl proxy profile SSL-FP-PROFILE-1 trusted-ca all
   ```

2. Apply the signing certificate as root-ca in the SSL proxy profile.

   ```
   user@host# set services ssl proxy profile SSL-FP-PROFILE-1 root-ca ssl-inspect-ca
   ```
3. Define the SSL proxy profile as the default profile.

```
user@host# set security ngfw default-profile ssl-proxy profile-name SSL-FP-PROFILE-1
```

4. Create a unified policy and specify the dynamic application as the match criteria.

```
user@host# set security policies from-zone untrust to-zone trust policy from_internet match source-address any
user@host# set security policies from-zone untrust to-zone trust policy from_internet match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy from_internet match application any
user@host# set security policies from-zone untrust to-zone trust policy from_internet match dynamic-application junos:web
```

5. Apply the SSL proxy profile to the permitted traffic in the security policy.

```
user@host# set security policies from-zone untrust to-zone trust policy from_internet then permit application-services ssl-proxy profile-name SSL-FP-PROFILE-1
```

**Verification**

**Verify SSL Proxy Configuration**

**Purpose**
Confirm that the configuration is working properly by displaying the SSL proxy statistics.

**Action**
From operational mode, enter the `show services ssl proxy statistics` command.

```
user@host> show services ssl proxy statistics
```

```
PIC:fwdd0 fpc[0] pic[0]  sessions matched 0
sessions bypassed:non-ssl 0
sessions bypassed:mem overflow 0
sessions bypassed:low memory 0
sessions created 0
sessions ignored 0
sessions active 0
```
Meaning

The command output displays the following information:

- Details about the sessions matched for the SSL proxy.
- Details about the default SSL proxy profile such as the sessions where the default profile is applied and the sessions that are dropped due to the absence of the default profile.

SEE ALSO

ngfw | 577

ICAP Service Redirect

IN THIS SECTION

- Data Loss Prevention (DLP) Using ICAP Service Redirect | 417
- Example: Configuring ICAP Redirect Service on SRX Devices | 419

You can prevent data loss from your network by employing Internet Content Adaptation Protocol (ICAP) redirect services. SRX Series devices support ICAP redirect functionality to redirect HTTP or HTTPS traffic to any third-party server. For more information, read this topic.
Data Loss Prevention (DLP) Using ICAP Service Redirect

You can prevent data loss from your network by employing Internet Content Adaptation Protocol (ICAP) redirect services. ICAP is a lightweight HTTP-based remote procedure call protocol. ICAP allows its clients to pass HTTP-based content (HTML) to the ICAP servers for performing services such as virus scanning, content translation, or content filtering and so on for the associated client requests.

Junos OS ICAP Support for SRX Series Device

SRX Series devices support ICAP redirect functionality to redirect HTTP or HTTPS traffic to any third-party server. The SRX Series device acts as an SSL proxy server and decrypts the pass-through traffic with the proper SSL profile under a security policy. SRX Series device decrypts HTTPS traffic and redirects HTTP message to a third-party, on-premise server using an ICAP channel. After DLP processing, the traffic is redirected back to the SRX Series device and action is taken according to the results from the ICAP server. If any sensitive data is detected per the policies, the SRX Series device logs, redirects, or blocks the data traffic as configured in the profile.

The following sequences are involved in a typical ICAP redirect scenario:

1. The user opens a connection to a Website on the internet.
2. The request goes through the SRX Series device that is acting as a proxy server.
3. The SRX Series device receives information from the end-host, encapsulates the message and forwards the encapsulated ICAP message to the third-party on-premise ICAP server.
4. The ICAP server receives the ICAP request and analyzes it.
5. If the request does not contain any confidential information, the ICAP server sends it back to the proxy server, and directs the proxy server to send the HTTP to the internet.
6. If the request contains confidential information, you can choose to take action (block, permit, log) as per your requirement.

**NOTE:** The HTTP throughput depends on the connections between the SRX Series device and the ICAP channel.

Starting in Junos OS Release 19.3R1, ICAP redirect adds **X-Client-IP**, **X-Server-IP**, **X-Authenticated-User**, and **X-Authenticated-Groups** header extensions in an ICAP message to provide information about the source of the encapsulated HTTP message.
ICAP Profile

When you configure ICAP redirect service on SRX Series devices, you must configure the ICAP server information. This profile is applied to a security policy as application services for the permitted traffic. The ICAP profile defines the settings that allow the ICAP server to process request messages, response messages, fallback options (in case of a timeout), connectivity issues, too many requests, or any other conditions.

Service Redirect for Layer 7 Dynamic Applications with Unified Policies

Starting from Junos OS Release 18.2R1, SRX Series devices support ICAP service redirect feature when the device is configured with unified policies.

Unified policies are the security policies that enable you to use dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time.

In a unified policy with dynamic applications as a match condition, you configure an ICAP redirect profile and SSL proxy profile and apply these profiles as application services in the security policy for the permitted traffic. When the traffic matches the policy, the ICAP redirect service profile that is configured as application services is applied. The ICAP server profile defines the behavior of redirection and server specifications. The ICAP server performs the policy scan and the traffic is redirected to the SRX Series device, and the specified action is taken as per the ICAP redirect profile.

Note the following behavior while using ICAP redirect service with unified policy:

- When ICAP redirect is configured in a unified policy and the data that needs to be redirected has arrived and the final policy is not determined, the request is ignored by the ICAP redirect service.

- Because ICAP redirect is one of services located in the service chain, the data received by the ICAP redirect service might be different from the original data. The data sent by the ICAP redirect might affect downstream services.

Benefits of ICAP Redirect Service Support

- Keeps the sensitive data from leaving the network.

- Supports common on-premise server pool for redirection thereby improving management, security, and control of the content.

NOTE: The HTTP throughput depends on the connections between the SRX Series device and SRX ICAP.
Example: Configuring ICAP Redirect Service on SRX Devices

This example shows how to define an ICAP redirect profile for an SRX Series device.

**Requirements**

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 18.1R1 or later. This configuration example is tested for Junos OS Release 18.1R1.
- ICAP redirect profile for an SRX Series device with unified policies example is tested for Junos OS Release 18.2R1.

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

**Overview**

In this example, you configure an ICAP redirect profile and an SSL proxy profile and apply these profiles as application services in the security policy for the permitted traffic.

*Figure 23 on page 420* shows the topology used in this example.
To enable the service redirect using ICAP, you must configure an SSL profile to secure the connection to the ICAP server. Next, you configure a security policy to process the traffic, and specify the action for the permitted traffic.

Table 45 on page 420 lists the details of the parameters used in this example.

Table 45: ICAP Redirect Configuration Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>icap-pf1</td>
<td>The ICAP server profile allows the ICAP server to process request messages, response messages, fallback options and so on, for the permitted traffic. This profile is applied as an application service in the security policy.</td>
</tr>
<tr>
<td>Server name</td>
<td>icap-svr1 icap-svr2</td>
<td>The machine name of the remote ICAP host. Client's request is redirected to this ICAP server.</td>
</tr>
<tr>
<td>Server IP address</td>
<td>5.0.0.2 5.0.0.179</td>
<td>The IP address of the remote ICAP host. Client's request is redirected to this ICAP server.</td>
</tr>
<tr>
<td>SSL proxy profile</td>
<td>ssl-inspect-profile</td>
<td>An SSL proxy profile defines SSL behavior for the SRX Series device. The SSL proxy profile is applied to the security policy as an application service.</td>
</tr>
<tr>
<td>SSL profile</td>
<td>dlp_ssl</td>
<td>The SRX Series device that is acting as an SSL proxy client, initiates and maintains SSL sessions with an SSL server. This configuration enables you to secure the connection to the ICAP server.</td>
</tr>
<tr>
<td>Security policy</td>
<td>sp1</td>
<td>In a security policy, apply the SSL proxy profile and ICAP redirect profile, to the permitted traffic.</td>
</tr>
</tbody>
</table>
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.

```plaintext
set services ssl initiation profile dlp_ssl trusted-ca all
set services ssl initiation profile dlp_ssl actions ignore-server-auth-failure
set services icap-redirect profile icap-pf1 server icap-svr1 host 5.0.0.2
set services icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri echo
set services icap-redirect profile icap-pf1 server icap-svr1 respmod-uri echo
set services icap-redirect profile icap-pf1 server icap-svr1 sockets 64
set services icap-redirect profile icap-pf1 server icap-svr2 host 5.0.0.179
set services icap-redirect profile icap-pf1 server icap-svr2 reqmod-uri echo
set services icap-redirect profile icap-pf1 server icap-svr2 respmod-uri echo
set services icap-redirect profile icap-pf1 server icap-svr2 sockets 64
set services icap-redirect profile icap-pf1 server icap-svr2 tls-profile dlp_ssl
set services icap-redirect profile icap-pf1 http redirect-request
set services icap-redirect profile icap-pf1 http redirect-response
set security policies from-zone trust to-zone untrust policy sec_policy match source-address any
set security policies from-zone trust to-zone untrust policy sec_policy match destination-address any
set security policies from-zone trust to-zone untrust policy sec_policy match application any
set security policies from-zone trust to-zone untrust policy sec_policy then permit application-services ssl-proxy
  profile-name ssl-inspect-profile
set security policies from-zone trust to-zone untrust policy sec_policy then permit application-services
  icap-redirect icap-pf1
set security policies default-policy permit-all
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 xe-2/0/0.0
set security zones security-zone trust interfaces xe-2/0/2.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces xe-2/0/1.0
set interfaces xe-2/0/0 unit 0 family inet address 192.0.2.1/24
set interfaces xe-2/0/0 unit 0 family inet6 address 2001:db8::1/64
set interfaces xe-2/0/1 unit 0 family inet address 198.51.100.1/24
set interfaces xe-2/0/1 unit 0 family inet6 address 2001:db8::2/64
set interfaces xe-2/0/2 unit 0 family inet address 198.51.100.2/24
set interfaces xe-2/0/2 unit 0 family inet6 address 2001:db8::3/64
```

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 the CLI User Guide.

To configure the ICAP redirect service:

1. Configure the SSL profile for a secured connection with the ICAP server.

   ```
   [edit services]
   user@host# set ssl initiation profile dlp_ssl trusted-ca all
   user@host# set ssl initiation profile dlp_ssl actions ignore-server-auth-failure
   user@host# set ssl initiation profile dlp_ssl actions crl disable
   ```

2. Configure the ICAP redirect profile for the first server (icap-svr1).

   ```
   [edit services]
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 host 5.0.0.2
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri echo
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 respmod-uri echo
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 sockets 64
   ```

3. Configure the ICAP redirect profile for the second server (icap-svr2).

   ```
   [edit services]
   user@host# set icap-redirect profile icap-pf1 server icap-svr2 host 5.0.0.179
   user@host# set icap-redirect profile icap-pf1 server icap-svr2 reqmod-uri echo
   user@host# set icap-redirect profile icap-pf1 server icap-svr2 respmod-uri echo
   user@host# set icap-redirect profile icap-pf1 server icap-svr2 sockets 64
   user@host# set icap-redirect profile icap-pf1 server icap-svr2 tls-profile dlp_ssl
   ```

4. Configure the redirect request and the redirect response for the HTTP traffic.

   ```
   [edit services]
   user@host# set icap-redirect profile icap-pf1 http redirect-request
   user@host# set icap-redirect profile icap-pf1 http redirect-response
   ```

5. Configure a security policy to apply application services for the ICAP redirect to the permitted traffic.

   ```
   [edit security]
   user@host# set policies from-zone trust to-zone untrust policy sec_policy match source-address any
   user@host# set policies from-zone trust to-zone untrust policy sec_policy match destination-address any
   user@host# set policies from-zone trust to-zone untrust policy sec_policy match application any
   ```
6. Configure interfaces and zones.

```
[edit]
user@host# set interfaces xe-2/0/0 unit 0 family inet address 192.0.2.1/24
user@host# set interfaces xe-2/0/0 unit 0 family inet6 address 2001:db8::1/64
user@host# set interfaces xe-2/0/1 unit 0 family inet address 198.51.100.1/24
user@host# set interfaces xe-2/0/1 unit 0 family inet6 address 2001:db8::2/64
user@host# set interfaces xe-2/0/2 unit 0 family inet address 198.51.100.2/24
user@host# set interfaces xe-2/0/2 unit 0 family inet6 address 2001:db8::3/64
user@host# set zones security-zone trust host-inbound-traffic system-services all
user@host# set zones security-zone trust host-inbound-traffic protocols all
user@host# set zones security-zone trust interfaces xe-2/0/0.0
user@host# set zones security-zone trust interfaces xe-2/0/2.0
user@host# set zones security-zone untrust host-inbound-traffic system-services all
user@host# set zones security-zone untrust host-inbound-traffic protocols all
user@host# set zones security-zone untrust interfaces xe-2/0/1.0
```

Results
From configuration mode, confirm your configuration by entering the `show services ssl`, `show services icap-redirect`, `show security policies`, `show security zones`, and `show interfaces` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show services ssl
initiation {
  profile dlp_ssl {
    trusted-ca all;
    actions {
      ignore-server-auth-failure;
      crl {
        disable;
      }
    }
  }
}
```
user@host# show services icap-redirect
profile icap-pf1 {
  server icap-svr1 {
    host 5.0.0.2;
    reqmod-uri echo;
    respmod-uri echo;
    sockets 64;
  }
  server icap-svr2 {
    host 5.0.0.179;
    reqmod-uri echo;
    respmod-uri echo;
    sockets 10;
    tls-profile dlp_ssl;
  }
  http {
    redirect-request;
    redirect-response;
  }
}

user@host# show security policies
from-zone trust to-zone untrust {
  policy sec_policy {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          ssl-proxy {
            profile-name ssl-inspect-profile;
          }
          icap-redirect icap-pf1;
        }
      }
    }
  }
  default-policy {
    permit-all;
  }
user@host# show security zones
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    xe-2/0/0.0;
    xe-2/0/2.0;
  }
}
security-zone untrust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    xe-2/0/1.0;
  }
}

user@host# show interfaces
xe-2/0/0 {
  unit 0 {
    family inet {
      address 192.0.2.1/24;
    }
    family inet6 {
      address 2001:db8::1/64;
    }
  }
}
xе-2/0/1 {
  unit 0 {
    family inet {
      address 198.51.100.1/24;
    }
  }
}
If you are done configuring the device, enter \texttt{commit} from configuration mode.

**Configuring ICAP Service Redirect for Unified Policy**

**Step-by-Step Procedure**

You can follow the procedure below if you have configured a unified policy (supported from Junos OS Release 18.2R1).

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

To configure the ICAP redirect service:

1. Configure the SSL profile for secured connection with the ICAP server.

   ```
   [edit services]
   user@host# set ssl initiation profile dlp_ssl trusted-ca all
   user@host# set ssl initiation profile dlp_ssl actions ignore-server-auth-failure
   user@host# set ssl initiation profile dlp_ssl actions crl disable
   ```

2. Configure the ICAP redirect profile for the first server (icap-svr1).

   ```
   [edit services]
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 host 5.0.0.2
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri echo
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 respmod-uri echo
   user@host# set icap-redirect profile icap-pf1 server icap-svr1 sockets 64
   ```
3. Configure the ICAP redirect profile for the second server (icap-svr2).

```
[edit services]
user@host# set icap-redirect profile icap-pf1 server icap-svr2 host 5.0.0.179
user@host# set icap-redirect profile icap-pf1 server icap-svr2 reqmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr2 respsmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr2 sockets 64
user@host# set icap-redirect profile icap-pf1 server icap-svr2 tls-profile dlp_ssl
```

4. Configure the redirect request for HTTP traffic.

```
[edit services]
user@host# set icap-redirect profile icap-pf1 http redirect-request
user@host# set icap-redirect profile icap-pf1 http redirect-response
```

5. Configure a security policy to apply application services for the ICAP redirect to the permitted traffic.

```
[edit security]
user@host# set policies from-zone trust to-zone untrust policy sec_policy match source-address any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match destination-address any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match application any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match dynamic-application
  junos:HTTP
user@host# set policies from-zone trust to-zone untrust policy sec_policy then permit application-services
  ssl-proxy profile-name ssl-inspect-profile
user@host# set policies from-zone trust to-zone untrust policy sec_policy then permit application-services
  icap-redirect icap-pf1
user@host# set policies default-policy permit-all
```

**Verification**

**Verifying ICAP Redirect Configuration**

**Purpose**
Verify that the ICAP redirect service is configured on the device.

**Action**
From operational mode, enter the `show services icap-redirect status` and `show services icap-redirect statistic` commands.

```
user@host> show services icap-redirect 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

user@host> show services icap-redirect statistic

ICAP Redirect statistic:
  Message Redirected            : 2
  Message REQMOD Redirected     : 1
  Message RESPMOD Redirected    : 1
  Message Received              : 2
  Message REQMOD Received       : 1
  Message RESPMOD Received      : 1

Fallback:    permit          log-permit  reject
  Timeout     0               0          0
  Connectivity 0               0         0
  Default     0               0          0
```

**Meaning**

The status **Up** indicates that the ICAP redirect service is enabled. The **Message Redirected** and the **Message Received** fields show the number of HTTP requests that have passed through the ICAP channel.
SSL Decryption Mirroring

IN THIS SECTION

- Understanding SSL Decryption Mirroring Functionality | 429
- Configuring SSL Decryption Mirroring | 431

SSL decryption mirroring feature enables you to monitor SSL decrypted application traffic entering and exiting the SRX Series device. For more information on SSL decryption mirroring, read this topic.

**Understanding SSL Decryption Mirroring Functionality**

Starting in Junos OS Release 18.4R1, SSL decryption mirroring functionality for SSL forward proxy and for SSL reverse proxy is introduced.

SSL decryption mirroring feature enables you to monitor SSL decrypted application traffic entering and exiting the SRX Series device. When you enable this feature, the SRX Series device uses an Ethernet interface—the configured SSL decryption mirroring interface—to forward a copy of the decrypted SSL traffic to a trusted traffic collection tool or a network analyzer for inspection and analysis. Typically, you connect this external monitoring device to the SSL decryption mirroring interface through a switching device. The external mirror traffic collector port is the port (or interface) that receives the copy of the decrypted traffic from the SSL decryption mirroring interface on the SRX Series device.
To use the SSL decryption mirroring feature, you define an SSL proxy profile, and apply it to the security policy. The security policy rule allows you to define traffic that you want the device to decrypt. When you attach the SSL proxy profile to the security policy rule, the traffic matching the security policy rule is decrypted. The SSL decryption mirroring interface delivers a copy of decrypted HTTPS and STARTTLS (POP3S/SMTPS/IMAPS) traffic to a trusted external device or traffic collection tool for inspection and analysis.

The embedded 5-tuple data of the decrypted IP packet includes the same following values as the encrypted IP packets:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol number

Retaining the same 5-tuple data without reconfiguration ensures that the decrypted traffic is saved in packet-capturing format (Wireshark) and you can replay the data later.

Only TCP sequence numbers and ACK numbers are constructed based on the actual decrypted payload forwarded on the SSL decryption mirroring port. If the decrypted packet size exceeds the maximum transmission unit (MTU) size of the SSL decryption mirroring port, then the decrypted payload is divided into multiple TCP segments based on the MTU size requirements.

**SSL Decryption Mirroring Before or After Policy Enforcement**

By default, the SRX Series device forwards the SSL decrypted payload to the mirror port before Junos OS enforces Layer 7 security services, including IDP, Juniper SKY ATP, and UTM. This option allows you to replay events and analyze traffic that generates a threat or triggers a drop action.

You can also configure mirroring of the decrypted traffic after enforcing the security policy. With this option, only traffic that is forwarded through the security policy is mirrored. However, if the decrypted payload is modified while enforcing the security policy, the modified decrypted payload is forwarded on the mirror port. Similarly, if the decrypted traffic is dropped because of policy enforcement (for example, when a threat is detected in the decrypted traffic), that particular decrypted traffic is not forwarded on the mirror port.

**SSL Decryption Mirroring Support**

- Supported for SSL forward proxy and SSL reverse proxy.
- Supported for both IPv4 and IPv6 traffic.
The SSL decrypted traffic available on the mirror port is in cleartext format. All the cipher suites that are supported by SSL proxy support SSL decryption mirroring functionality. For the list of supported cipher suites, see SSL Proxy Overview.

Benefits of SSL Decryption Mirroring

- Enables comprehensive data capture for auditing, forensic investigations, and historical purposes.
- Provides data leak prevention.
- Enables additional security processing done by third-party appliances for IDP, UTM, and so on.
- Provides insight about the threats involved.

Limitations

- SSL decryption mirroring cannot be configured on the st0 tunnel interface.

SSL Decryption Mirroring Support in Chassis Cluster

Starting in Junos OS Release 18.4R1-S2 and Junos OS Release 19.2R1, the SSL decryption mirroring feature is supported on redundant Ethernet (reth) interface on SRX Series devices operating in a chassis cluster.

```
set interfaces reth20 redundant-ether-options redundancy-group 1
set interfaces reth20 unit 0 family inet
```

Configuring SSL Decryption Mirroring

This example shows how to enable mirroring of SSL decrypted traffic on an SRX Series device.
Requirements

This example uses the following hardware and software components:

- Any SRX Series device with Junos OS Release 18.4R1 or later. This configuration example is tested for Junos OS Release 18.4R1.

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

Before you begin:

- Configure SSL proxy. See SSL Proxy Overview.
- The SSL decryption mirroring interface that you configure doesn’t need to be part of any security zones.
- Ensure that SSL decryption mirroring interface and the actual client-server SSL traffic processing interfaces are part of the same routing instance.
- Ensure that the SSL decryption mirroring interface on the SRX Series device and the external mirror traffic collector port must be part of the same broadcast domain.

**NOTE:** You don’t need to configure a separate security policy to allow traffic from SRX Series device to the SSL decryption mirroring interface.

Overview

In this example, configure an SSL forward proxy profile by specifying the name of the SSL decryption mirroring interface and the MAC address of the external mirror traffic collector port. Next, create a security policy and invoke the SSL proxy as application service on the permitted traffic. The traffic matching the security policy rule is decrypted. A copy of the decrypted SSL payload is then encapsulated into an IP packet and forwarded to the on the external mirror traffic collector port through SSL decryption mirroring interface.

**Figure 24 on page 433** illustrates the topology used in this example.
Figure 24: SSL Decryption Mirroring

Table 46 on page 433 provides the details of the parameters used in this example.

Table 46: Parameters Used in SSL Decryption Mirroring Example

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL decryption mirroring interface on SRX Series device</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>MAC address of the external mirror traffic collector port</td>
<td>00:50:56:a6:5f:1f</td>
</tr>
<tr>
<td>SSL proxy profile</td>
<td>profile-1</td>
</tr>
<tr>
<td>Security policy</td>
<td>policy 1</td>
</tr>
</tbody>
</table>

Configuration

Use the following steps to configure the SSL decryption mirroring.

1. Define the SSL decryption mirroring interface with logical unit number 0.

   ```
   user@host# set interfaces ge-0/0/2 unit 0
   ```

2. Specify the SSL decryption mirroring interface in the SSL proxy profile.

   ```
   user@host# set services ssl proxy profile profile-1 mirror-decrypt-traffic interface ge-0/0/2.0
   ```

Ge-0/0/2.0 is configured as designated SSL decryption mirroring interface.
3. Specify the MAC address of the external mirror traffic collector port.

```bash
user@host# set services ssl proxy profile profile-1 mirror-decrypt-traffic destination-mac-address 00:50:56:a6:5f:1f
```

4. Create a security policy by specifying the match criteria for the traffic.

```bash
user@host# set security policies from-zone trust to-zone untrust policy policy-1 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy policy-1 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy policy-1 match application any
```

5. Attach the SSL proxy profile to the security policy rule.

```bash
user@host# set security policies from-zone trust to-zone untrust policy policy-1 then permit application-services ssl-proxy profile-name profile-1
```

This configuration enables the external mirror traffic collector port (or interface) to receive the copy of the decrypted traffic from the SSL decryption mirroring interface on the SRX Series device.

**Results**

From configuration mode, confirm your configuration by entering the `show services ssl proxy profile` and `show security policies from-zone trust to-zone untrust policy` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services ssl proxy profile profile-1
server-certificate Email_server_cert;
mirror-decrypt-traffic {
    interface ge-0/0/2.0;
destination-mac-address 00:50:56:a6:5f:1f;
}
```

```
[edit]
user@host# show security policies from-zone trust to-zone untrust policy policy-1
match {
    source-address any;
}
```
destination-address any;
application any;
}
then {
permit {
application-services {
ssl-proxy {
profile-name profile-1;
}
}
}
}

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

Verification

*Verify SSL Proxy Configuration*

**Purpose**

Confirm that the configuration is working properly by displaying the SSL proxy statistics.

**Action**

From operational mode, enter the `show services ssl proxy statistics` command.

```
user@host> show services ssl proxy statistics
```

PIC:fwdd0 fpc[0] pic[0]
sessions matched 30647
sessions bypassed:non-ssl 0
sessions bypassed:mem overflow 0
sessions bypassed:low memory 0
sessions created 25665
sessions ignored 0
sessions active 0
sessions dropped 0
sessions whitelisted 0
whitelisted url category match 0
default profile hit 0
session dropped no default profile 0
policy hit no profile configured 0
SSL Proxy Logs

When logging is enabled in an SSalpha, Table 47 on page 436.

Table 47: SSL Proxy Logs

<table>
<thead>
<tr>
<th>Syslog Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_PROXY_SSL_SESSION_DROP</td>
<td>Logs generated when a session is dropped by SSL proxy.</td>
</tr>
<tr>
<td>SSL_PROXY_SSL_SESSION_ALLOW</td>
<td>Logs generated when a session is processed by SSL proxy even after</td>
</tr>
<tr>
<td></td>
<td>encountering some minor errors.</td>
</tr>
<tr>
<td>SSL_PROXY_SESSION_IGNORE</td>
<td>Logs generated if non-SSL sessions are initially mistaken as SSL sessions.</td>
</tr>
<tr>
<td>SSL_PROXY_SESSION_WHITELIST</td>
<td>Logs generated when a session is whitelisted.</td>
</tr>
<tr>
<td>SSL_PROXY_ERROR</td>
<td>Logs used for reporting errors.</td>
</tr>
<tr>
<td>SSL_PROXY_WARNING</td>
<td>Logs used for reporting warnings.</td>
</tr>
<tr>
<td>SSL_PROXY_INFO</td>
<td>Logs used for reporting general information.</td>
</tr>
</tbody>
</table>
All logs contain similar information as shown in the following example (actual order of appearance):

```plaintext
logical-system-name, session-id, source-ip-address, source-port,
destination-ip-address, destination-port,
nat-source-ip-address, nat-source-port, nat-destination-ip-address,
nat-destination-port, proxy profile name, source-zone-name,
source-interface-name, destination-zone-name, destination-interface-name, message
```

The **message** field contains the reason for the log generation. One of three prefixes shown in [Table 48 on page 437](#) identifies the source of the message. Other fields are descriptively labeled.

**Table 48: SSL Proxy Log Prefixes**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>Logs generated due to errors related to the device or an action taken as part of the SSL proxy profile. Most logs fall into this category.</td>
</tr>
<tr>
<td>openssl error</td>
<td>Logs generated during the handshaking process if an error is detected by the openssl library.</td>
</tr>
<tr>
<td>certificate error</td>
<td>Logs generated during the handshaking process if an error is detected in the certificate (x509 related errors).</td>
</tr>
</tbody>
</table>

**Sample logs:**

```plaintext
Jun 1 05:11:13 4.0.0.254 junos-ssl-proxy: SSL_PROXY_SSL_SESSION_DROP: lsys:root
    23 < 203.0.113.1/35090->192.0.2.1/443> NAT:< 203.0.113.1/35090->192.0.2.1/443>
    ssl-inspect-profile <untrust:ge-0/0/0.0->trust:ge-0/0/1.0> message:certificate error: self signed certificate
```

**NOTE:** These logs capture sessions that are dropped by SSL proxy, not sessions that are marked by other modules that also use SSL proxy services.

For SSL_PROXY_SESSION_WHITELIST messages, an additional **host** field is included after the **session-id** and contains the IP address of the server or domain that has been whitelisted.

```plaintext
Jun 1 05:25:36 4.0.0.254 junos-ssl-proxy: SSL_PROXY_SESSION_WHITELIST: lsys:root
    24 host:192.0.2.1/443<203.0.113.1/35090->192.0.2.1/443> NAT:<
```
Enabling Debugging and Tracing for SSL Proxy

Debug tracing on both Routing Engine and the Packet Forwarding Engine can be enabled for SSL proxy by setting the following configuration:

```
user@host# set services ssl traceoptions file file-name
```

SSL proxy is supported on SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 devices and vSRX instances. Table 49 on page 438 shows the supported levels for trace options.

**Table 49: Trace Levels**

<table>
<thead>
<tr>
<th>Cause Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief</td>
<td>Only error traces on both the Routing Engine and the Packet Forwarding Engine.</td>
</tr>
<tr>
<td>Detail</td>
<td>Packet Forwarding Engine–Only event details up to the handshake should be traced. Routing Engine–Traces related to commit. No periodic traces on the Routing Engine will be available.</td>
</tr>
<tr>
<td>Extensive</td>
<td>Packet Forwarding Engine–Data transfer summary available. Routing Engine–Traces related to commit (more extensive). No periodic traces on the Routing Engine will be available.</td>
</tr>
<tr>
<td>Verbose</td>
<td>All traces are available.</td>
</tr>
</tbody>
</table>

Table 50 on page 438 shows the flags that are supported.

**Table 50: Supported Flags in Trace**

<table>
<thead>
<tr>
<th>Cause Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli-configuration</td>
<td>Configuration-related traces only.</td>
</tr>
</tbody>
</table>
Table 50: Supported Flags in Trace (continued)

<table>
<thead>
<tr>
<th>Cause Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>initiation</td>
<td>Enable tracing on the SSL-I plug-in.</td>
</tr>
<tr>
<td>proxy</td>
<td>Enable tracing on the SSL-Proxy-Policy plug-in.</td>
</tr>
<tr>
<td>termination</td>
<td>Enable tracing on the SSL-T plug-in.</td>
</tr>
<tr>
<td>selected-profile</td>
<td>Enable tracing only for profiles that have <code>enable-flow-tracing</code> set.</td>
</tr>
</tbody>
</table>

You can enable logs in the SSL proxy profile to get to the root cause for the drop. The following errors are some of the most common:

- Server certification validation error. Check the trusted CA configuration to verify your configuration.
- System failures such as memory allocation failures.
- Ciphers do not match.
- SSL versions do not match.
- SSL options are not supported.
- Root CA has expired. You need to load a new root CA.

You can enable the `ignore-server-auth-failure` option in the SSL proxy profile to ensure that certificate validation, root CA expiration dates, and other such issues are ignored. If sessions are inspected after the `ignore-server-auth-failure` option is enabled, the problem is localized.

SEE ALSO
- traceoptions (Services SSL) | 650

Operational Commands to Troubleshoot SSL Sessions
In the CLI, the operational commands provide information that can help with troubleshooting. You can use show commands to determine and analyze the statistical counters and metrics related to any traffic loss and take an appropriate corrective measure. This topic covers information for monitoring, displaying, and verifying of SSL-related issues using the operational mode commands.
Displaying Active SSL Sessions

**Purpose**
Display information about all the active SSL sessions on the device.

**Action**
Use the `show security flow session ssl` command.

user@host > show security flow session ssl

```
Session ID: 1, Policy name: default-permit, Timeout: 1746, Valid
In: 4.0.0.1/37369 --> 5.0.0.1/4433; tcp, Conn Tag: 0x0, If: xe-0/0/0.0, Pkts: 6, Bytes: 671,
Out: 5.0.0.1/4433 --> 4.0.0.1/37369; tcp, Conn Tag: 0x0, If: xe-0/0/1.0, Pkts: 7, Bytes: 1635,
```

**Meaning**
The output shows all standard flow information including the session ID, timeout value for the session, the direction of the flow, the source address and port, the destination address and port, the IP protocol, and the interface used for the session. Example:

- The policy name that allowed this traffic is default-permit.
- The timeout value.
- Both the source IP and the destination IP are displayed with their respective source/destination ports.
- Session type.
- The source interface and the destination interface for this session.

For details about the output fields of the command, see `show security flow session ssl`.

Displaying Active SSL Sessions Details

**Purpose**
Display detail information about the active SSL sessions on the device.

**Action**
From the operational mode, use the `show security flow session extensive ssl` command.

```
user@host > show security flow session extensive ssl
```

| Output:                                                                 |
|---|---|
| Session ID: 1, Status: Normal                                          |
| Flags: 0x42/0x20000000/0x2/0x10103                                      |
| Policy name: 1/5                                                        |
| Source NAT pool: Null                                                   |
| Dynamic application: junos:UNKNOWN,                                    |
| Encryption: Unknown                                                    |
| Application traffic control rule-set: INVALID, Rule: INVALID            |
| Maximum timeout: 1800, Current timeout: 1636                           |
| Session State: Valid                                                    |
| Start time: 587131, Duration: 163                                      |
| In: 4.0.0.1/37369 --> 5.0.0.1/4433;tcp,                                |
| Conn Tag: 0x0, Interface: xe-0/0/0.0,                                  |
| Session token: 0x7, Flag: 0x2621                                       |
| Route: 0xa0010, Gateway: 4.0.0.1, Tunnel: 0                            |
| Port sequence: 0, FIN sequence: 0,                                    |
| FIN state: 0,                                                          |
| Pkts: 6, Bytes: 671                                                    |
| Out: 5.0.0.1/4433 --> 4.0.0.1/37369;tcp,                               |
| Conn Tag: 0x0, Interface: xe-0/0/1.0,                                  |
| Session token: 0x8, Flag: 0x2620                                       |
| Route: 0xb0010, Gateway: 5.0.0.1, Tunnel: 0                            |
| Port sequence: 0, FIN sequence: 0,                                    |
| FIN state: 0,                                                          |
| Pkts: 7, Bytes: 1635                                                   |
| Total sessions: 1                                                      |

**Meaning**

The output of the command displays extensive information about all the active sessions on the device. Display information includes the session ID, the Network Address Translation (NAT) source pool (if source NAT is used), the configured timeout value for the session and its standard timeout, and the session start time and how long the session has been active, direction of the flow, the source address and port, the destination address and port, the IP protocol, and the interface used for the session.

**Example:**

- The policy name that allowed this traffic is default-permit.
- The maximum timeout and current timeout values.
- Session type.
- The source interface and the destination interface for the session
- The next-hop gateway IP address
- AppQoS rule set details.

For details about the output fields of the command, see `show services ssl session`.

## Displaying Specific SSL Session Details

### Purpose
Display information about the specific SSL session.

### Action
Use the `show services ssl session 56` command.

```plaintext
Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

Session ID          : 56
Connection Type     : PROXY
SSL Profile         : SSL_PROFILE
Resumed Session     : No
One-crypto          : Disabled
Async-crypto        : Enabled
Renegotiation count : 0
Server Certificate Subject Name    :
/C=IN/ST=KA/L=BNG/O=JN/OU=XYZ/CN=server/emailAddress=ser
Server Cert verification status : OK
CRL check            : Enabled
Action               : Allow
SSL_T Details :
  Key size      : 2048
cipher        : ECDHE-RSA-AES256-GCM-SHA384
  TLS version   : 1.2
SSL_I Details :
  Key size      : 2048
Cipher        : ECDHE-RSA-AES256-GCM-SHA384
  TLS version   : 1.2
```
Meaning
You can get the detail information about the specific SSL session with this command. Example:

- Session ID, connection type and SSL profile used for the session.
- Server certificate subject name and verification status.
- CRL check status and action.
- SSL Initiation and termination details.
- The source interface and the destination interface for this session.

For details about the output fields of the command, see `show security flow session ssl`.

Display SSL Certificates

Purpose
Display the digital certificates available on the device.

Action
From the operational mode, use the `show services ssl certificate all` command.

```
user@host > show services ssl certificate all
```

Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------
CertId
-----------------------------
ssl-inspect-ca
ssl-cert-4k

Meaning
Display the list of all SSL certificates active on the device. SSL sessions use these certificates to establish a secure communication between a client and a server.

For details about the output fields of the command, see `show services ssl certificate`.

Display SSL Certificate Information

Purpose
Display brief information about the SSL certificate.

**Action**

From the operational mode, use the `show services ssl certificate brief certificate-id` command. Following samples show command outputs for CA certificate and local certificates.

```
user@host > show services ssl certificate brief certificate-id

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

CertID : trusted-ca
Certificate Type : CA-CERT
Issuer : /C=IN/ST=KA/L=BNG/O=XYZ/OU=ABC/CN=5.0.0.1/emailAddress=newca@test.com
Subject : /C=IN/ST=KA/L=BNG/O=XYZ/OU=ABC/CN=5.0.0.1/emailAddress=newca@test.com
Public Key algorithm : rsaEncryption

user@host> show services ssl certificate brief certificate-id

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

CertID : ssl-inspect-ca
Certificate Type : LOCAL-CERT
Issuer : /DC=dc/CN=xyz.com/OU=IT/O=abc/L=bng/ST=KA/C=IN
Subject : /DC=dc/CN=xyz.com/OU=IT/O=abc/L=bng/ST=KA/C=IN
Validity :
Not before : Mon 02/18/2019 07:30:37 AM
Not after : Sat 02/17/2024 07:30:37 AM
Public Key algorithm : rsaEncryption
```

**Meaning**

Displays details about the certificate including certificate ID, type, issuer of the certificate, and encryption algorithm used. The **type** field displays the type of the certificate—That is—CA-CERT or LOCAL-CERT. CA-Cert certificate is an authorized certificate issued by trusted certificate authority and LOCAL-CERT is a self-signed certificate.

Note that the output of the commands vary depending on the type of certificate.

For details about the output fields of the command, see `show services ssl certificate`. 
Display SSL Certificate Details

Purpose
Display detail information about the SSL certificate.

Action
From the operational mode, use the `show services ssl detail certificate-id` command.

user@host > show services ssl detail certificate-id

```
Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

CertID : ssl-inspect-ca
Certificate Type : LOCAL-CERT
cert modify time : Mon 02/18/2019 07:30:37 AM
key modify time : Mon 02/18/2019 07:30:23 AM
certificate version : 3
serial number : 72 a4 a8 12 0e a0 da 5f ee 27 47 d8 19 7c 76 b5
Issuer : /DC=dc/CN=xyz.com/OU=IT/O=xyz/L=blr/ST=KA/C=IN
Subject : /DC=dc/CN=xyz.com/OU=IT/O=xyz/L=blr/ST=KA/C=IN
Validity :
   Not before : Mon 02/18/2019 07:30:37 AM
   Not after : Sat 02/17/2024 07:30:37 AM
Public Key algorithm : rsaEncryption
Signature Algorithm : sha256WithRSAEncryption
```

```
Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

CertID : test
Certificate Type : CA-CERT
cert modify time : Mon 09/02/2019 09:47:48 PM
certificate version : 1
serial number : 21 a8 d6 00 eb 24 1f 78 9a e5 0e ec 6a 39 ce 65 66 42 8c 0a
Issuer : /C=IN/ST=KA/L=BLR/O=XYZ/OU=ABC/CN=5.0.0.1/emailAddress=newca@test.com
Subject : /C=IN/ST=KA/L=BLR/O=XYZ/OU=ABC/CN=5.0.0.1/emailAddress=newca@test.com
```
Public Key algorithm : rsaEncryption
Signature Algorithm   : sha256WithRSAEncryption
CRL :
  present            : no
  check              : enabled
  download-failed    : true
  check-on-download-fail : enabled

**Meaning**
Displays details about the certificate including certificate ID, type, last modified date, version, serial number, issuer, subject, validity, and encryption algorithm used.

**Example:**

- **Type of the certificate.** The *type* field displays the type of the certificate—That is—CA-CERT or LOCAL-CERT. CA-Cert certificate is an authorized certificate issued by trusted certificate authority and LOCAL-CERT is a self-signed certificate.
- **Subject and issuer of the certificate.**
- **Certificate validity from-date and to-date.**
- **Public key algorithms used.**
- **Algorithm used by the certificate authority to sign the certificate.**
- **CRL-related updates (CA certificates only)**

For details about the output fields of the command, see `show services ssl certificate`.

### SSL Proxy Counters All

**Purpose**
Display all the statistical counters for the SSL proxy sessions.

**Action**
From the operational mode, use the `show services ssl proxy counters all` command.

```bash
user@host > show services ssl proxy counters all
```

```
Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------
```
Meaning
The output display the counters details related to SSL proxy sessions. These counters generally increment whenever there is some activity such as session matched, session created, and so on.

Example:

- Count of sessions created, matched, ignored or destroyed.
- Number of sessions whitelisted based on IP address and URL categories.
- Session counts based on CRL-related information such as new updates done or certificates revoked, no CRL present, or no CA certificate present.
- Number of sessions matching default SSL proxy profile in unified policy.
- Number of sessions dropped because of absence of default SSL proxy profile.

For details about the output fields of the command, see `show services ssl proxy counters`.  

<table>
<thead>
<tr>
<th>Counter</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>session create failed</td>
<td>0</td>
</tr>
<tr>
<td>non SSL sessions received</td>
<td>0</td>
</tr>
<tr>
<td>Memory failures</td>
<td>0</td>
</tr>
<tr>
<td>session dropped</td>
<td>0</td>
</tr>
<tr>
<td>sessions matched</td>
<td>0</td>
</tr>
<tr>
<td>sessions created</td>
<td>0</td>
</tr>
<tr>
<td>sessions destroyed</td>
<td>0</td>
</tr>
<tr>
<td>sessions ignored</td>
<td>0</td>
</tr>
<tr>
<td>sessions ignored : backup only</td>
<td>0</td>
</tr>
<tr>
<td>sessions whitelisted : IP based</td>
<td>0</td>
</tr>
<tr>
<td>sessions whitelisted : url based</td>
<td>0</td>
</tr>
<tr>
<td>crl : data added</td>
<td>0</td>
</tr>
<tr>
<td>crl : certificate revoked</td>
<td>0</td>
</tr>
<tr>
<td>crl : no crl info present</td>
<td>0</td>
</tr>
<tr>
<td>crl : no CA certificate</td>
<td>0</td>
</tr>
<tr>
<td>SSL sessions</td>
<td>0</td>
</tr>
<tr>
<td>SMTP over STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>IMAP over STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>POP3 over STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>SMTP sessions</td>
<td>0</td>
</tr>
<tr>
<td>IMAP sessions</td>
<td>0</td>
</tr>
<tr>
<td>POP3 sessions</td>
<td>0</td>
</tr>
<tr>
<td>Server not supporting STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>Client not supporting STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>Unified policy : default profile hit</td>
<td>0</td>
</tr>
<tr>
<td>Unified policy : no default profile</td>
<td>0</td>
</tr>
</tbody>
</table>
SSL Proxy Counters Information

Purpose
Display statistical counters for the SSL proxy session to provide information about the sessions.

Action
From the operational mode, use the `show services ssl proxy counters info` command.

user@host > show services ssl proxy counters info

Lsys Name : root-logical-system
PIC:fpc0 ------

sessions matched 0
sessions created 0
sessions destroyed 0
sessions ignored 0
sessions ignored : backup only 0
sessions whitelisted : IP based 0
sessions whitelisted : url based 0
crl : data added 1
crl : certificate revoked 0
crl : no crl info present 0
crl : no CA certificate 0
SSL sessions 0
SMTP over STARTTLS 0
IMAP over STARTTLS 0
POP3 over STARTTLS 0
SMTP sessions 0
IMAP sessions 0
POP3 sessions 0
Server not supporting STARTTLS 0
Client not supporting STARTTLS 0
Unified policy : default profile hit 0
Unified policy : no default profile 0

Meaning
The output display the counters details related SSL proxy session. These counters generally increment whenever there is some activity such as session matched, session created, and so on.
Example:

- Count of sessions created, matched, ignored or destroyed.
- Number of sessions whitelisted.
- Session counts based on CRL-related information such as new updates done, certificates revoked, no CRL present, or no CA certificate present.
- Number of sessions matching default SSL proxy profile in unified policy.
- Number of sessions dropped because of absence of default SSL proxy profile.

For details about the output fields of the command, see `show services ssl proxy counters`.

### SSL Proxy Counters Errors

**Purpose**
Display statistical counters for the errors encountered in SSL proxy session.

**Action**
From the operational mode, use the `show services ssl proxy counters errors` command.

```
user@host > show services ssl proxy counters errors
```

<table>
<thead>
<tr>
<th>Lsys Name</th>
<th>root-logical-system</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC</td>
<td>fpc0</td>
</tr>
</tbody>
</table>

Session create failed 0
non SSL sessions received 0
memory failures 0
session dropped 7

**Meaning**
The output display the counters details for the errors encountered in an SSL proxy session. Example:

- Number of failed sessions.
- Number of non-SSL sessions received on the system.
- Number of dropped sessions.

For details about the output fields of the command, see `show services ssl proxy counters`. 
Display SSL Proxy Profile Details

Purpose
Display information about the SSL proxy profile.

Action
From the operational mode, use the `show services ssl proxy profile profile-name` command.

```
user@host > show services ssl proxy profile profile-name
```

<table>
<thead>
<tr>
<th>Lsys Name</th>
<th>root-logical-system</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC:</td>
<td>fwdd0 fpc[0] pic[0]</td>
</tr>
</tbody>
</table>
| PIC:               | -----
| Profile:           | ssl-proxy          |
| enable-tracing:    | false              |
| root-ca expired:   | false              |
| allow non-ssl session: | true        |
| ssl-termination-id: | 65537             |
| ssl-initiation-id: | 65537              |
| Number of whitelist entries: | 0            |

Meaning
Output of the command displays the details of the SSL proxy profile. Example:

- The number of sessions that are whitelisted.
- Whether the non SSL sessions are allowed.
- Whether the root certificate is active or expired.

For details about the output fields of the command, see `show services ssl proxy profile`.

Display SSL Proxy Profiles

Purpose
Display all the SSL proxy profiles configured on the device.

Action
From the operational mode, use the `show services ssl proxy profile all` command.

```
user@host > show services ssl proxy profile all
```
The output displays the list of SSL proxy profiles available on the device.

For details about the output fields of the command, see `show services ssl proxy profile`.

### Display SSL Proxy Session Cache Statistics

#### Purpose
Display the data for the SSL proxy session cache.

#### Action
From the operational mode, use the `show services ssl proxy session-cache statistics` command.

```
user@host > show services ssl proxy session-cache statistics
```

#### Meaning
Command output displays SSL proxy session cache statistics. You can get the details such as number of times the information related to an SSL session is found in the cache or the number of times the information related to an SSL session is missing in the cache, and number of times the session cache limit is reached.

For details about the output fields of the command, see `show services ssl proxy session-cache statistics`. 
Display SSL Proxy Session Cache Summary

Purpose
Display brief information about the entries stored in the SSL proxy session cache.

Action
From the operational mode, use the `show services ssl proxy session-cache entries summary` command.

```
user@host> show services ssl proxy session-cache entries summary
```

```
Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------
Hash Entry 1
  Status: ACTIVE, Time to expire 294 seconds
  Session Id Length: 32
  Session Id: 1b 2a 9f 5f d8 6e d2 cd 6b b8 89 e8 88 07 75 80 32 c2 54 5a c7 9b 12
  a2 e6 5c f0 6d 85 c5 40 4b
  Dst IP: 5.0.0.1, Dst Port: 20753
  SSL-T Profile Id: 2, SSL-I Profile Id: 2
```

Meaning
Command output displays SSL proxy session cache entries details such as session information saved in the cache, session status, session ID, and length of the session ID, destination IP address and port details, and SSL initiation and SSL termination profile IDs.

For details about the output fields of the command, see `show services ssl proxy session-cache entries`.

Display SSL Proxy Session Cache Details

Purpose
Display detail information about the entries stored in the SSL proxy session cache.

Action
From the operational mode, use the `show services ssl proxy session-cache entries detail` command.

```
user@host> show services ssl proxy session-cache entries detail
```

```
Lsys Name : root-logical-system
PIC: fpc0 fpc[0] pic[0]
```
Hash Entry: 1
Status: ACTIVE, Time to expire 294 seconds
Session Id Length: 32
Session Id: c1 6e 88 65 43 9f 57 2f 0f 06 f7 4b 03 c5 38 58 74 b4 4f 43 66 9a 6f
c7 a6 2a ae 22 ab f8 b4 ce
Dst IP: 5.0.0.1, Dst Port: 4433
SSL-T Profile Id: 2, SSL-I Profile Id: 2
Session Info:
Interdicted cert type [0x0]: CA issued, Authentication failed
Server cert verification result: unable to get local issuer certificate [0x14]
Server name extn len: 0, name: None
Server cert chain hash: b5 3d cd cb ca 35 81 5a db 6f 83 ab 5e a0 19 73

SSL-TERM session:
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

SSL-INIT session:
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

Hash Entry:2
Status: EXPIRED
Session Id Length: 32
Session Id: 1b 2a 9f 5f d8 6e d2 cd 6b b8 89 e8 88 07 75 80 32 c2 54 5a c7 9b 12
a2 e6 5c f0 6d 85 c5 40 4b
Dst IP: 5.0.0.1, Dst Port: 4433,
SSL-T Profile Id: 2, SSL-I Profile Id: 2
Session Info:
-----------------
Interdicted cert type [0x0]: CA issued, Authentication failed
Server cert verification result: unable to get local issuer certificate [0x14]
Server name extn len: 0, name: None
Server cert chain hash: b5 3d cd cb ca 35 81 5a db 6f 83 ab 5e a0 19 73

SSL-TERM session:
-----------------
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

SSL-INIT session:
----------------
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

Stale entry in cache: 1

Meaning
Command output displays cached SSL proxy session entries details. Example:

- Status of the cache entry with time to expire. Because the cache entries are valid only for short interval.
- Session ID, and length of the session ID.
- Destination IP address and destination port details.
- SSL initiation and SSL termination session details.
- Server certificate validation, interdicted certificate details.

For details about the output fields of the command, see show services ssl proxy session-cache entries.

Display SSL Proxy Certificate Cache Entry Statistics

Purpose
Display data for the SSL proxy certificate cache.

Action
From operational mode, use the show services ssl proxy certificate-cache statistics command.

user@host > show services ssl proxy certificate-cache statistics

Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------
cert cache hit 0
cert cache miss 0
cert cache full
Meaning
Command output displays SSL proxy certificate cache statistics such as number of times the match is available in cache, number of times an entry is not found in cache, or the number of times that cache was full.

For details about the output fields of the command, see show services ssl proxy certificate-cache statistics.

Display SSL Proxy Certificate Cache Entry Summary

Purpose
Display brief information about the entries stored in the SSL proxy certificate cache.

Action
From operational mode, use the show services ssl proxy certificate-cache entries summary command.

user@host > show services ssl proxy certificate-cache entries summary

Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------
Cache Entries : 1
Serial number : 0x12345678
SSL-I Profile Id: 1
Num of CRL updates: 0

Meaning
Command output displays certificate cache statistics such number of cache entries, serial number, profile ID, and CRL updates.

For details about the output fields of the command, see show services ssl proxy certificate-cache entries.

Display SSL Proxy Certificate Cache Entry Details

Purpose
Display detail information about the entries stored in the SSL proxy certificate cache.

Action
From operational mode, use the show services ssl proxy certificate-cache entries detail command.

user@host > show services ssl proxy certificate-cache entries detail
Lsys Name: root-logical-system
PIC: fwdd0 fpc[0] pic[0] ------
Cache entry: 1
Serial number: 0x12345678
SSL-I Profile Id: 1
Num of CRL updates: 0
Status: Active: Time to expire 570 seconds

Cert Info:
-------------
Interdicted cert type [0x0]: CA issued, Authentication failed
Server cert verification result: unable to get local issuer certificate [0x14]
Cert reference count: 2
Subject: /C=IN/ST=KA/O=XYZ Inc/CN=ABC Inc Root CA/emailAddress=newca@test.com
Issuer: /CN=SSL-PROXY:DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE

Meaning
You can get the detail information about the cached SSL proxy certificate entries with this command.
Example:

- Number of entries present in the certificate-cache.
- Number of times the CRL updates done till the interdicted certificate was added to the certificate-cache.
- Cached interdicted certificate and the server certificate verification results.
- Subject and issuer of the interdicted certificate.

For details about the output fields of the command, see show services ssl proxy certificate-cache entries.

Display SSL Proxy Status

Purpose
Display the status of the SSL proxy session.

Action
From operational mode, use the show services ssl proxy status command.

user@host > show services ssl proxy status

PIC: fwdd0 fpc[0] pic[0] ------
One-Crypto: Enable
Meaning
The command displays the overall status of the SSL proxy. Example:

- Crypto status, proxy activation status.
- Certificate cache details such as whether certificate cache is activated, CRL configuration, certificate cache size, number of certificates in certificate cache currently used.
- Session cache details such as whether session cache is activated, size of the session cache, number of sessions in session cache currently used.

For details about the output fields of the command, see `show services ssl proxy status`.

Display SSL Termination Counter Details

**Purpose**
Display statistical counter details for the SSL termination sessions.

**Action**
From operational mode, use the `show services ssl termination counters all` command.

`user@host > show services ssl termination counters all`

```
Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0] ------

Memory errors 0
```
<table>
<thead>
<tr>
<th>Error Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handshake errors</td>
<td>0</td>
</tr>
<tr>
<td>Cert Cache errors</td>
<td>0</td>
</tr>
<tr>
<td>Server Protection errors</td>
<td>0</td>
</tr>
<tr>
<td>Proxy errors</td>
<td>0</td>
</tr>
<tr>
<td>Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Certificate errors</td>
<td>0</td>
</tr>
<tr>
<td>One-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Async-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Mirror errors</td>
<td>0</td>
</tr>
<tr>
<td>handshakes started</td>
<td>0</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>0</td>
</tr>
<tr>
<td>active sessions</td>
<td>0</td>
</tr>
<tr>
<td>Interdicted cert generated</td>
<td>0</td>
</tr>
<tr>
<td>proxy: sessions created</td>
<td>0</td>
</tr>
<tr>
<td>proxy: sessions active</td>
<td>0</td>
</tr>
<tr>
<td>proxy: sessions ignored</td>
<td>0</td>
</tr>
<tr>
<td>proxy: renegotiation ignored</td>
<td>0</td>
</tr>
<tr>
<td>proxy: session resumption</td>
<td>0</td>
</tr>
<tr>
<td>proxy: secure renegotation</td>
<td>0</td>
</tr>
<tr>
<td>proxy: insecure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>proxy: multiple renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>proxy: reneg after resumption</td>
<td>0</td>
</tr>
<tr>
<td>init: passthrough requests</td>
<td>0</td>
</tr>
<tr>
<td>init: start requests</td>
<td>0</td>
</tr>
<tr>
<td>proxy: ECDSA based srvr auth</td>
<td>0</td>
</tr>
<tr>
<td>proxy: RSA based srvr auth</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**

You can get useful information about the SSL termination counters with this command. Example:

- Number of errors related to memory, handshake, certificate, server protection, proxy and crypto
- Number of sessions initiated handshake and completed handshake.
- Number of active sessions.
- Number of SSL proxy sessions such as sessions created, active sessions, ignored sessions, renegotiated sessions, sessions with different authentication methods and so on.

For details about the output fields of the command, see `show services ssl termination counters`.

**Display SSL Termination Counters Errors**

**Purpose**
Display statistical counters for the errors encountered in SSL termination session.

**Action**
From operational mode, use the `show services ssl termination counters error` command.

```
user@host > show services ssl termination counters error
```

<table>
<thead>
<tr>
<th>Lsys Name</th>
<th>root-logical-system</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC</td>
<td>fpc0</td>
</tr>
<tr>
<td>Memory errors</td>
<td>0</td>
</tr>
<tr>
<td>Handshake errors</td>
<td>0</td>
</tr>
<tr>
<td>Cert Cache errors</td>
<td>0</td>
</tr>
<tr>
<td>Server Protection errors</td>
<td>0</td>
</tr>
<tr>
<td>Proxy errors</td>
<td>0</td>
</tr>
<tr>
<td>Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Certificate errors</td>
<td>0</td>
</tr>
<tr>
<td>One-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Async-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Mirror errors</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**
The output of the command displays number of errors related to memory, handshake, certificate, server protection, proxy and crypto, and SSL decryption mirroring functionality.

For details about the output fields of the command, see `show services ssl termination counters`.

---

**Display SSL Termination Counters Handshake**

**Purpose**
Display statistical counters for the SSL termination handshake.

**Action**
From operational mode, use the `show services ssl termination counters handshake` command.

```
user@host > show services ssl termination counters handshake
```

<table>
<thead>
<tr>
<th>Lsys Name</th>
<th>root-logical-system</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC</td>
<td>fpc0 fpc[0] pic[0]</td>
</tr>
<tr>
<td>Memory errors</td>
<td>0</td>
</tr>
<tr>
<td>Handshake errors</td>
<td>0</td>
</tr>
<tr>
<td>Cert Cache errors</td>
<td>0</td>
</tr>
<tr>
<td>Server Protection errors</td>
<td>0</td>
</tr>
<tr>
<td>Proxy errors</td>
<td>0</td>
</tr>
<tr>
<td>Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Certificate errors</td>
<td>0</td>
</tr>
<tr>
<td>One-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Async-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Mirror errors</td>
<td>0</td>
</tr>
</tbody>
</table>
handshakes started 0
handshakes completed 0
active sessions 0
Interdicted cert generated 0
proxy: sessions created 0
proxy: sessions active 0
proxy: sessions ignored 0
proxy: renegotiation ignored 0
proxy: session resumption 0
proxy: secure renegotiation 0
proxy: insecure renegotiation 0
proxy: multiple renegotiation 0
proxy: reneg after resumption 0
init: passthrough requests 0
init: start requests 0
proxy: ECDSA based srvr auth 0
proxy: RSA based srvr auth 0

Meaning
You can get useful information about the SSL termination counters with this command. Example:

- Number of sessions initiated handshake and completed handshake.
- Number of active sessions
- Number of SSL proxy sessions such as sessions created, active sessions, ignored sessions, renegotiated sessions, sessions with different authentication methods and so on.

For details about the output fields of the command, see show services ssl termination counters.

Display SSL Termination Profile

Purpose
Display all SSL termination profiles available on the device.

Action
From operational mode, use the show services ssl termination profile all command.

user@host > show services ssl termination profile all
Meaning
The output of the command displays the list of all SSL termination profiles available on the device.

For details about the output fields of the command, see `show services ssl termination profile`.

Display SSL Termination Profile Summary

Purpose
Display the brief information about the SSL termination profiles.

Action
From operational mode, use the `show services ssl termination profile brief profile-name` command.

```
user@host > show services ssl termination profile brief profile-name
```

Meaning
Displays the details of the SSL termination profile.

You can get useful information about the SSL initiation profile with this command. Example:

- Whether the root certificate is active or expired.
- Preferred SSL cipher with key strength.
- Whether the non SSL sessions are allowed.
• Number of URL categories configured.
• Number of whitelisted sessions.

For details about the output fields of the command, see `show services ssl termination profile`.

## Display SSL Termination Profile Details

### Purpose
Display the detail information about the SSL termination profile.

### Action
From operational mode, use the `show services ssl termination profile detail profile-name` command.

```
user@host > show services ssl termination profile detail profile-name
```

```
Lsys Name : root-logical-system

PIC: fwdd0 fpc[0] pic[0] ----------

Profile                          : p1_65536_proxy_t
allow non-ssl session            : true
preferred-ciphers                : medium
Num of url categories configured : 0
Protocol version                 : all
Client Authentication            : notset
Server Authentication            : Required
Crypto Mode                      : hw-sync
Session Resumption               : Enabled
CRL check                        : Enabled
Certificate RSA : p_5
Renegotiation                    : only secure allowed
Custom ciphers                   : 0
Server cert                       : 0
Decrypt Mirror                    : Disabled
Trusted CA                       : 0

  handshakes started  0
  handshakes completed 0
  active sessions 0
  total handshake errors 0
  Data Errors 0
  session resumption 0
  secure renegotiation 0
```
Meaning
You can get useful information about the SSL termination profile with this command. Example:

- Profile name.
- Whether the non-SSL sessions are allowed.
- Category of the preferred cipher.
- Number of URL categories configured.
- Protocol version.
- Status of the various functionality such as client and server authentication, certificate revocation actions, session resumption, session renegotiation.
- Trusted CA and custom cipher details.
- SSL decryption mirror status.
- SSL termination per profile statistics or counters.

For details about the output fields of the command, see `show services ssl termination profile`.

Display SSL Initiation Counter Details

Purpose
Display statistical counters for the SSL initiation session.

Action
From operational mode, use the `show services ssl initiation counters all` command.

```
user@host > show services ssl initiation counters all

Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0] -------
Memory errors 0
```
<table>
<thead>
<tr>
<th>Error Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handshake errors</td>
<td>0</td>
</tr>
<tr>
<td>Cert Cache errors</td>
<td>0</td>
</tr>
<tr>
<td>Server Protection errors</td>
<td>0</td>
</tr>
<tr>
<td>Proxy errors</td>
<td>0</td>
</tr>
<tr>
<td>Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Certificate errors</td>
<td>0</td>
</tr>
<tr>
<td>One-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Async-Crypto errors</td>
<td>0</td>
</tr>
<tr>
<td>Mirror errors</td>
<td>0</td>
</tr>
<tr>
<td>Handshakes started</td>
<td>0</td>
</tr>
<tr>
<td>Handshakes completed</td>
<td>0</td>
</tr>
<tr>
<td>Active sessions</td>
<td>0</td>
</tr>
<tr>
<td>Interdicted cert generated</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: sessions created</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: sessions active</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: sessions ignored</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: renegotiation ignored</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: session resumption</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: secure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: insecure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: multiple renegotation</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: reneg after resumption</td>
<td>0</td>
</tr>
<tr>
<td>Init: passthrough requests</td>
<td>0</td>
</tr>
<tr>
<td>Init: start requests</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: ECDSA based srvr auth</td>
<td>0</td>
</tr>
<tr>
<td>Proxy: RSA based srvr auth</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**

You can get useful information about the SSL initiation counters with this command. Example:

- Number of errors related to memory, handshake, certificate, server protection, proxy and crypto.
- Number of sessions initiated handshake and completed the handshake.
- Number of active sessions.
- Number of SSL proxy sessions such as sessions created, active sessions, ignored sessions, renegotiated sessions, sessions with different authentication methods and so on.

For details about the output fields of the command, see `show services ssl initiation counters`.

---

**Display SSL initiation Counter Handshake**

**Purpose**
Display statistical counters for the SSL initiation handshake.

**Action**

From operational mode, use the `show services ssl initiation counters handshake` command.

```
user@host > show services ssl initiation counters handshake
```

```
Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0] -------
handshakes started 0
handshakes completed 0
active sessions 0
Interdicted cert generated 0
proxy: sessions created 0
proxy: sessions active 0
proxy: sessions ignored 0
proxy: renegotiation ignored 0
proxy: session resumption 0
proxy: secure renegotiation 0
proxy: insecure renegotiation 0
proxy: multiple renegotiation 0
proxy: reneg after resumption 0
init: passthrough requests 0
init: start requests 0
proxy: ECDSA based srvr auth 0
proxy: RSA based srvr auth 0
```

**Meaning**

You can get useful information about the SSL initiation counters with this command. Example:

- Number of sessions initiated handshake and completed handshake.
- Number of active sessions.
- Number of SSL proxy sessions such as sessions created, active sessions, ignored sessions, renegotiated sessions, sessions with different authentication methods and so on.

For details about the output fields of the command, see `show services ssl initiation counters`.

---

**Display SSL Initiation Counter Errors**

**Purpose**
Display statistical counters for the errors encountered in SSL initiation session.

**Action**
From operational mode, use the `show services ssl initiation counters error` command.

```
user@host > show services ssl initiation counters error
```

### Meaning
The output of the command displays number of errors related to memory, handshake, certificate, server protection, proxy and crypto, and SSL decryption mirroring functionality.

For details about the output fields of the command, see `show services ssl initiation counters`.

---

**Display SSL Initiation Profile**

**Purpose**
Display all SSL initiation profiles available on the device.

**Action**
From operational mode, use the `show services ssl initiation profile all` command.

```
user@host > show services ssl initiation profile all
```

```
Lsys Name : root-logical-system
```

Meaning
The output of the command displays the list of all SSL initiation profiles available on the device.

For details about the output fields of the command, see `show services ssl initiation profile`.

Display SSL Initiation Profile Summary

Purpose
Display the summary of the SSL initiation profile.

Action
From operational mode, use the `show services ssl initiation profile brief profile-name` command.

```
user@host > show services ssl initiation profile brief profile-name
```

Meaning
Displays the details of the SSL initiation profile such as profile name, whether the non-SSL sessions are allowed, preferred-ciphers, and number of URL categories configured.

For details about the output fields of the command, see `show services ssl initiation profile`. 
Display SSL Initiation Profile Details

**Purpose**
Display the detail information about the SSL initiation profile.

**Action**
From operational mode, use the `show services ssl initiation profile detail profile-name` command.

```
user@host > show services ssl initiation profile detail profile-name
```

<table>
<thead>
<tr>
<th>Lsys Name</th>
<th>root-logical-system</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC</td>
<td>fpc0 fpc[0] pic[0] -------</td>
</tr>
<tr>
<td>Profile</td>
<td>SSL_PROFILE_65536_proxy_i</td>
</tr>
<tr>
<td>allow non-ssl session</td>
<td>true</td>
</tr>
<tr>
<td>preferred-ciphers</td>
<td>medium</td>
</tr>
<tr>
<td>Num of url categories configured</td>
<td>0</td>
</tr>
<tr>
<td>Protocol version</td>
<td>all</td>
</tr>
<tr>
<td>Client Authentication</td>
<td>notset</td>
</tr>
<tr>
<td>Server Authentication</td>
<td>Ignore Failure</td>
</tr>
<tr>
<td>Crypto Mode</td>
<td>sw</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>Enabled</td>
</tr>
<tr>
<td>CRL check</td>
<td>Enabled</td>
</tr>
<tr>
<td>Certificate RSA</td>
<td>ssl-inspect-ca</td>
</tr>
<tr>
<td>Renegotiation</td>
<td>only secure allowed</td>
</tr>
<tr>
<td>Custom ciphers</td>
<td>0</td>
</tr>
<tr>
<td>Server cert</td>
<td>0</td>
</tr>
<tr>
<td>Decrypt Mirror</td>
<td>Disabled</td>
</tr>
<tr>
<td>Trusted CA</td>
<td>1</td>
</tr>
<tr>
<td>handshakes started</td>
<td>8</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>8</td>
</tr>
<tr>
<td>active sessions</td>
<td>0</td>
</tr>
<tr>
<td>total handshake errors</td>
<td>0</td>
</tr>
<tr>
<td>Data Errors</td>
<td>0</td>
</tr>
<tr>
<td>session resumption</td>
<td>5</td>
</tr>
<tr>
<td>secure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>insecure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>multiple renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>reneg after resumption</td>
<td>0</td>
</tr>
<tr>
<td>no_reneg alert by peer</td>
<td>0</td>
</tr>
<tr>
<td>drop on reneg</td>
<td>0</td>
</tr>
</tbody>
</table>
Meaning
You can get useful information about the SSL initiation profile with this command. Example:

- Whether the non SSL sessions are allowed.
- Preferred SSL cipher
- Number of URL categories configured.
- Status of the various functionality such as client and server authentication, certificate revocation actions, session resumption, session renegotiation.
- Trusted CA, chain certificates details.
- SSL decryption mirror status
- SSL initiation session counters

For details about the output fields of the command, see `show services ssl initiation profile`.

Display SSL Drop Log Details

Purpose
Display information about SSL drop logs.

Action
From operational mode, use the `show services ssl droplogs` command.

user@host > show services ssl droplogs

```plaintext
Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0]------

==========log msg for cpu 0

==========log msg for cpu 1

```
Meaning
Output of the command displays the denied/dropped session details. You can use the command output to understand the issue why session was dropped.
CHAPTER

Configuration Statements

active-probe-params | 476
actions (Services SSL Proxy) | 480
actions (Services SSL Initiation) | 483
address-mapping (Application Identification) | 485
advance-policy-based-routing | 487
advance-policy-based-routing (Security Zones) | 492
appfw-profile (System) | 493
appfw-rule | 494
appfw-rule-set | 496
application-firewall | 498
application (Application Identification) | 500
application-firewall (Application Services) | 504
application-identification | 505
application-group (Services) | 511
application-services (Security Policies) | 513
ip-protocol-mapping (Application Identification) | 564
initiation (Services) | 565
level (Services) | 567
log (Services) | 568
maximum-transactions | 570
metrics-profile | 571
mirror-decrypt-traffic | 573
no-application-identification (Services) | 575
no-application-system-cache (Services) | 576
ngfw | 577
over (Application Identification) | 579
overlay-path | 581
packet-capture | 583
passive-probe-params | 586
policy (advanced-policy-based-routing) | 588
policy (Security Policies) | 590
port-range (Application Identification) | 594
preferred-ciphers | 595
profile (icap-redirect) | 596
profile (Rule Sets) | 598
profile (Services SSL Proxy) | 599
profile (Services Proxy) | 603
protocol (Services Proxy) | 605
profile (SSL Initiation) | 606
profile (SSL Termination) | 609
protocol-version | 611
proxy (Services) | 612
rate-limiters | 614
renegotiation (Services) | 616
active-probe-params

Syntax

```
active-probe-params probe-name {
    settings {
        burst-size {
            size;
        }
        data-fill {
            string;
        }
        data-size {
            size;
        }
        dscp-code-points {
            dscp;
        }
        enable-sla-export {
            interval;
        }
        forwarding-class {
            forwarding-class-name;
        }
        loss-priority (low | high | medium-high | medium-low) {
        }
        probe-count {
            count;
        }
        probe-interval {
            interval;
        }
    }
}
```

Hierarchy Level
[edit security advance-policy-based-routing]

Release Information
Statement introduced in Junos OS Release 18.2R1. The options forwarding-class and loss-priority are introduced in Junos OS Release 19.2R1.

Description
Specify parameter settings for an active probe.
Application performance is monitored and measured using active probes.

In active probing, custom packets are sent between a spoke device and a hub device on multiple routes to measure RTT, jitter, and packet loss between the book-ended points. You can configure to send active probes periodically on all the active and passive links.

Active probing starts after the configuration is committed. A configured number of samples are collected and used for measuring the SLA. If there is a violation detected for any application, the probe metrics are evaluated to determine the best possible link for that application traffic in order to meet performance requirements as in the SLA.

Consider the example, where you configure the probe count as 1000, probe interval as 10 seconds, and burst size as 100. Burst count is calculated as probe count/burst size (1000/100 = 10). Burst-count is 10. So, probes are sent in sets of 10 bursts each containing 100 packets.

Burst interval is calculated as probe interval/burst-count (10/10 = 1). Burst interval is 1 second. So, a burst is sent every 1 second. The active probe is initiated from the spoke device to the hub device on each of the overlay path.
Options

probe-name—Active probe identifier.

burst-size—Number of probes sent as a burst. This value should be less than or equal to probe-count.
    Range: 1–100
    Default: 10

data-fill string—Data payload for a probe packet. This is a hexadecimal string, which is used the payload for probe.

data-size size—Size of the data portion.

dscp-code-points dscp—DiffServ code point (DSCP) bits value.

enable-sla-export—Time Interval (in seconds) at which the active probe data to be exported to controller. This option is disabled by default.
    Range: 60-600

forwarding-class forwarding-class-name—Name of the forwarding class
    Default: network-control

loss-priority level—Map packet values to a loss priority. Loss priority allows you to set the priority for dropping packets. Typically, you mark packets exceeding some service level with a high loss priority—that is, a greater likelihood of being dropped. Level can be one of the following:
    • high—Packet has high loss priority.
    • medium-high—Packet has medium-high loss priority.
    • medium-low—Packet has medium-low loss priority.
    • low—Packet has low loss priority.

probe-count count—Number of samples required to be collected for an SLA measurement.
    Range: 10-1000
    Default: 100

probe-interval interval—Time interval (in seconds) between successive probes in seconds.
    Range: 1-30
    Default: 5 seconds

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  | 283
- Advanced Policy-Based Routing  | 213
actions (Services SSL Proxy)

Syntax

```
actions {
    allow-strong-certificate;
    crl {
        disable;
        if-not-present (allow | drop);
        ignore-hold-instruction-code;
    }
    disable-session-resumption;
    ignore-server-auth-failure;
    log {
        all;
        errors;
        info;
        sessions-allowed;
        sessions-dropped;
        sessions-ignored;
        sessions-whitelisted;
        warning;
    }
    renegotiation {
        (allow | allow-secure | drop);
    }
}
```

Hierarchy Level

```
[edit services ssl proxy profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10. The `crl` statement is supported from Junos OS Release 15.1X49-D30.

Description

Specify the logging and traffic related actions for a SSL proxy profile.

An SSL proxy profile is required to configure SSL proxy on your SRX Series device. As a part of the proxy profile configuration, you can configure actions related to certification revocations checks, options to specify if a change in SSL parameters requires renegotiation for a session, option to disable session
resumption, option to ignore certificate validation, root CA expiration dates, and other such issues based on your requirements.

Options
• allow-strong-certificate—Enable devices to use the RSA certificates with key size 4,096 bits. By default, this option is disabled. Option is available on SRX300, SRX320, and SRX380 devices in standalone mode.
  Default - Not configured.
• crl—Specify the certificate revocation actions.
  • disable—Disable CRL verification.
  • if-not-present—Specify actions for sessions.
    • allow—Allow sessions when CRL information is not available.
    • drop—Drop sessions when CRL information is not available.
  • ignore-hold-instruction-code—Ignore the unconfirmed (on hold) revocation status, and accept a certificate.
• disable-session-resumption—Disable session resumption.
• ignore-server-auth-failure—Ignore server authentication failure.
• log—Specify the logging actions.
  • 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.
• renegotiation—Specify the renegotiation 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

SSL Proxy Overview | 351
Configuring SSL Forward Proxy | 382
Enabling Debugging and Tracing for SSL Proxy | 438
actions (Services SSL Initiation)

Syntax

```
actions {
    crl {
        disable;
        if-not-present (allow | drop);
        ignore-hold-instruction-code;
    }
    ignore-server-auth-failure;
}
```

Hierarchy Level

```
[edit services ssl initiation profile profile-name]
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10.

Description
Specify the certification revocation checks and traffic related actions for configuring SSL initiation support service. As a part of SSL initiation profile, you can specify actions related to certification revocations checks and chose an option to ignore certificate validation, root CA expiration dates, and other such issues based on your requirements. Commonly ignored errors include the inability to verify CA signature, incorrect certificate expiration dates, and so forth. We do not recommend using this option for authentication because configuring it results in websites not being authenticated at all.

Options
- **crl**—Specify the certificate revocation actions.
  - **disable**—Disable CRL verification.
  - **if-not-present**—Specify actions for sessions.
    - **allow**—Allow sessions when CRL information is not available.
    - **drop**—Drop sessions when CRL information is not available.
  - **ignore-hold-instruction-code**—Ignore the unconfirmed (on hold) revocation status, and accept a certificate.
  - **ignore-server-auth-failure**—Ignore server authentication failure.

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 | 351
Configuring SSL Forward Proxy | 382
Enabling Debugging and Tracing for SSL Proxy | 438
address-mapping (Application Identification)

Syntax

```plaintext
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 | 86 |
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;

**source-identity**
  [user-or-role-name];
  any;
  authenticated-user;
  unauthenticated-user;
  unknown-user;

} } }

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 {
        disable-midstream-routing;
        match {
            category (juniper-enhanced-category | custom-category);
            dynamic-application [system-application];
            dynamic-application-group [system-application-group];
            dscp dscp-value;
        }
        then {
            routing-instance name;
            application-services-bypass;
        }
    }
}
sla-options {
    local-route-switch {
        [enabled | disabled];
    }
    logging {
        syslog;
    }
}
sla-rule sla-rule-name {
  active-probe-params {
    probe-params-name;
  }
  link-type-affinity strict;
  metrics-profile {
    metric-profile-name;
  }
  passive-probe-params {
    sampling-percentage {
      percentage;
    }
    sampling-period {
      period;
    }
    sla-export-factor {
      value;
    }
    type {
      book-ended;
    }
    violation-count {
      count;
    }
    preferred-link-type (Any | IP | MPLS);
    switch-idle-time {
      period;
    }
  }
}
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;
}

underlay-interfaces interface-name {
  unit unit-number {
    link-type (IP | MPLS)
    priority priority-number;
  }
}

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.
**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 | 222
- Understanding Advanced Policy-Based Routing | 213
appfw-profile (System)

Syntax

appfw-profile {
  maximum amount;
  reserved amount;
}

Hierarchy Level

[edit security application-firewall profile profile-name]
[edit tenants tenant-name security application-firewall]

Release Information

Statement introduced in Junos OS Release 11.4.
The edit tenant tenant-name security application-firewall level is introduced in Junos OS Release 18.4R1.

Description

Specify the application firewall profile quota of a logical system and tenant systems.

As a master administrator, you can create a security profile and specify the kinds and amounts of resources that are to be allocated to a logical system to which the security profile is bound. A security profile is used for share the device resources, including policies, zones, addresses and address books, flow sessions, and various forms of NAT, among all the logical systems appropriately. You can dedicate various amounts of a resource to the logical systems and also allow the logical systems 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

Traditional Application Firewall | 145
appfw-rule

Syntax

```plaintext
appfw-rule {
    maximum amount;
    reserved amount;
}
```

Hierarchy Level

```
[edit system security-profile security-profile-name ]
[edit tenants tenant-name security application-firewall ]
```

Release Information

Statement introduced in Junos OS Release 11.4.
The `edit tenant tenant-name security application-firewall` level is introduced in Junos OS Release 18.4R1.

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 and tenant systems.

Tasks performed by the master administrator are:

- Uses security profiles to provision logical systems with resources.
- Binds security profiles to the master logical system and the user logical systems.
- Configures more than one security profile, and 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 ]
[edit tenants tenant-name security application-firewall]
```

Release Information

Statement introduced in Junos OS Release 11.4.
The `edit tenant tenant-name security application-firewall` level is introduced in Junos OS Release 18.4R1.

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 and tenant 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

| Traditional Application Firewall | 145 |
application-firewall

Syntax

```plaintext
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

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

| Traditional Application Firewall | 145 |
application (Application Identification)

Syntax

```plaintext
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;
}

priority high;
order;
over protocol-type {
    signature name {
        member name {
            context {
                context;
            }
            direction {
                any;
                client-to-server;
                server-to-client;
            }
            pattern pattern;
            depth byte-number;
        }
        port-range value;
    }
    priority [high | low];
type;
risk;
}
```
Hierarchy Level
[edit services application-identification]

Release Information
Statement introduced in Junos OS Release 15.1X49-D40.
Risk option introduced in Junos OS Release 19.1R1.

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 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.

priority—Priority of custom applications over the predefined applications.

Values: high

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.

risk—Custom application risk value should range from 1 to 5 to keep in sync with the predefined applications. The default value is 1 when the risk is not configured. Configuring risk value for custom application signatures is not supported.

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

<table>
<thead>
<tr>
<th>Example: Configuring Junos OS Application Identification Custom Application Signatures</th>
<th>91</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-mapping (Application Identification)</td>
<td>485</td>
</tr>
<tr>
<td>icmp-mapping (Application Identification)</td>
<td>563</td>
</tr>
<tr>
<td>ip-protocol-mapping (Application Identification)</td>
<td>564</td>
</tr>
<tr>
<td>over (Application Identification)</td>
<td>579</td>
</tr>
</tbody>
</table>
application-firewall (Application Services)

Syntax

```plaintext
application-firewall {
  rule-set rule-set-name;
}
```

Hierarchy Level

```plaintext
[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

- Traditional Application Firewall | 145
- rule-sets (Security Application Firewall) | 662
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;
risk;
} application-group group-name {
    application-groups application-group-name;
    applications application-name;
}
} application-system-cache-timeout value;
download (Services) {
    automatic {
        interval hours;
        start-time MM-DD.hh:mm;
    }
    url url;
}
enable-cdn-application-detection
enable-performance-mode max-packet-threshold number;
global-offload-byte-limit byte-limit-number;
imap-cache-size number;
imap-cache-timeout number;
inspection-limit {
    tcp {
        byte-limit byte-limit-number;
        packet-limit packet-limit-number;
    }
    udp {
        byte-limit byte-limit-number;
        packet-limit packet-limit-number;
    }
}
max-memory memory-value
maximum-transactions transactions-number;
micro-apps;
no-application-identification;
no-application-system-cache;
packet-capture {
  aggressive-mode;
  buffer-packets-limit bytes;
  capture-interval capture-interval;
  capture-limit capture-limit;
  global;
  max-bytes bytes;
  max-files max-files;
  max-packets max-packets;
  no-inconclusive;
  storage-limit bytes;
}

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.
Risk option introduced in Junos OS Release 19.1R1.
micro-app option introduced in Junos OS Release 19.2R1.
global-offload-byte-limit and inspection-limit options are introduced in Junos OS Release 19.4R1 and 15.1X49-D200.
Description
Configure application identification to identify applications regardless of the application port or protocol that is used to transmit the application.

Use this option to configure various options for the application identification such as application signatures, application groups, signature package download option, enable and deactivating application system cache, application traffic throughput, micro applications, application identification inspection limit, trace options and so on to use the application identification functionality.

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

**application application-name**—Configure application definition. You can create custom application signatures by specifying a name, protocol, port where the application runs, and match criteria.

**application-group group-name**—Configure a custom application group for application identification.

**application-system-cache-timeout value**—Specify the timeout value in seconds for the application system cache (ASC) entries.

**download**—Configure automatic download for the application identification services application package.

**enable-cdn-application-detection**—Enable application identification (ApplID) to classify a web application hosted on a content delivery network (CDN).

**enable-performance-mode max-packet-threshold number**—Set the deep packet inspection (DPI) in performance mode for application identification.

**global-offload-byte-limit byte-limit-number**—Specify the maximum number of byte limit before concluding the classification for identifying an application.

NOTE: The byte limit excludes the IP header and the TCP/UDP header lengths.

Range: 0 through 4294967295
Default: 10000

**imap-cache-size number**—Configure to limit the maximum number of entries in the IMAP cache.

**imap-cache-timeout time-period**—Specify the timeout value for the entries in the IMAP cache cache.

**inspection-limit**—Specify the maximum number of byte limit before concluding the classification for identifying an application in TCP and UDP sessions.

NOTE: The byte limit excludes the IP header and the TCP/UDP header lengths.

**tcp byte-limit byte-limit-number** —Specify the byte limit.

Range: 0 through 4294967295
Default: 6000

Default: For Junos OS Release 15.1X49-D200, the default value is 10000.

**tcp packet-limit packet-limit-number**—Specify the packet limit.

Range: 0 through 4294967295
Default: 0
udp byte-limit byte-limit-number — Specify the byte limit.
  Range: 0 through 4294967295
  Default: 0

udp packet-limit packet-limit-number — Specify the packet limit.
  Range: 0 through 4294967295
  Default: 10
  Default: For Junos OS Release 15.1X49-D200, the default value is 20.

max-memory value — Specify maximum memory limit for the deep packet inspection (DPI).
  Range: 1 through 200000 MB

micro-apps — Enable micro-application detection with application identification feature.

no-application-identification; — Disable the application identification of applications running on nonstandard ports. By default, application identification is enabled on the device.

no-application-system-cache — Disable application system cache. ASC is enabled by default when a session is created

interval interval-number; — Specify the interval, in minutes, for statistics collection.

traceoptions — Specify the trace file information.

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  |  32
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 | 98
application-services (Security Policies)

Syntax

```plaintext
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;
  packet-capture;
  (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;
  web-proxy {
    profile-name profile-name;
  }
}
```

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. The **web-proxy** option is introduced in Junos OS Release 19.2R1.

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.

web-proxy profile-name—Specify secure Web proxy profile name. The secure Web proxy profile is configured with dynamic application and external proxy server details. This profile is attached to the security policy and applied on 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

| Traditional Application Firewall | 145 |
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 including security policies, application firewall (AppFW), application tracking (AppTrack), application quality of service (AppQoS), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services including advanced policy-based routing (APBR) 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 | 37
application-system-cache-timeout (Services)

Syntax

```
application-system-cache-timeout value;
```

Hierarchy Level

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

Release Information


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 | 37
application-tracking

Syntax

```
application-tracking {
   (first-update | first-update-interval minutes);
   disable [Application Tracking];
   session-update-interval minutes;
}
```

Hierarchy Level

```
[edit security]
```

Release Information


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 Application Tracking | 177 |

---

**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 Application Tracking | 177 |
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 Application Tracking | 177
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]
[edit logical-systems logical-system-name security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services]
[edit tenants tenant-name 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.
Support at the following hierarchy levels introduced in Junos OS Release 19.3R1: [edit logical-systems logical-system-name security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services], and [edit tenants tenant-name security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services].

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 Application Quality of Service | 196
- Security Policies Overview
authorization (icap-redirect profile)

Syntax

```yaml
authorization {
  authorization-type authorization-type;
  credentials (ascii | base64);
}
```

Hierarchy Level

```text
[edit services icap-redirect profile name server name]
```

Release Information

Statement introduced in Junos OS Release 18.1R1.

Description

User authentication for the ICAP server if the request needs to be authorized.

Options

- **authorization-type**—Authentication type for the ICAP server. Authorization type is basic by default.
- **credentials**—Credentials (user name and password) for authentication to ICAP server.
  - **Values:**
    - ascii ascii—ASCII string.
    - base64 base64—bBase64 encoded string.

Required Privilege Level

system

RELATED DOCUMENTATION

- Example: Configuring ICAP Redirect Service on SRX Devices | 419
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 Application Quality of Service | 196
**context (Application Identification)**

**Syntax**

```plaintext
class context {
    context;
}
```

**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**

- **context**—Specify the context type. For example, Following options are available in application signature package version 3284.
  - `ftp-content-type`—Content type of the transferred file.
  - `ftp-file-name`—Filename being transferred.
  - `ftp-greeting-message`—First line of the server banner.
  - `ftp-load-way`—File transfer way—upload or download.
  - `ftp-method`—FTP command sent.
  - `http-filename`—The name of the file being fetched or posted. Extracted if content-disposition field has a filename.
  - `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 — Content-type header in an HTTP transaction.

http-header-cookie — Cookie header in an HTTP transaction.

http-header-host — Host header in an HTTP transaction.


http-post-url-parsed-param-parsed — Decoded, normalized POST URL in an HTTP request along with the decoded CGI parameters (if any).

http-post-variable-parsed — Decoded POST URL or form data variables.

http-url-parsed — Decoded, normalized URL in an HTTP request.

http-url-parsed-param-parsed — Decoded, normalized URL in an HTTP request along with the decoded CGI parameters (if any).

imap-attach-filename — Name of the file attached.

imap-attach-transfer-encoding — Encoding of the attached content.

imap-attach-type — Content type of the sent attached file

imap-auth-type — Used authentication type.

imap-content-language — Language of the message content.

imap-content-transfer-encoding — The encoding of the content

imap-content-type — Content type of the transferred file.

imap-greeting-message — Greeting message of the server

imap-method — Command sent by the client.

imap-mime-version — Version of the message body format standard used in the mail protocol.

imap-received-by-name — Receiving host name.

imap-received-from-name — Sending host name.

smtp-attach-filename — Attachment file name.

smtp-attach-transfer-encoding — Encoding of the attached content.

smtp-attach-type — Content type of the sent attached file.

smtp-content-language — Language of the message content.

smtp-content-transfer-encoding — Encoding of the content

smtp-content-type — Content type of transferred file
smtp-greeting-message—Greeting message of the server

smtp-method—Command sent by the client.

smtp-mime-version—Version of the message body format standard.

smtp-received-by-name—Name of the receiving host.

smtp-received-from-name—Name of the sending host.

smtp-server—The SMTP server name

ssl-common-name—Domain name in the certificate.

ssl-issuer—Certificate Authority.

ssl-organization-name—Organisation name in the certificate.

ssl-protocol-version—SSL/TLS protocol version chosen by the server.

ssl-server-name—Server name in TLS server name extension or SSL server certificate.

ssl-version—SSL major version in the handshake.

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.

Examples of context types with direction. When configuring custom application signatures, the context-direction combinations as mentioned in Table 51 on page 532 is supported. Any other combination other than this is not supported.
<table>
<thead>
<tr>
<th>Context</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-get-url-parsed-param-parsed</td>
<td>client-to-server</td>
</tr>
<tr>
<td>http-header-host</td>
<td>client-to-server</td>
</tr>
<tr>
<td>http-header-user-agent</td>
<td>client-to-server</td>
</tr>
<tr>
<td>http-post-url-parsed-param-parsed</td>
<td>client-to-server</td>
</tr>
<tr>
<td>http-post-variable-parsed</td>
<td>client-to-server</td>
</tr>
<tr>
<td>http-url-parsed</td>
<td>client-to-server</td>
</tr>
<tr>
<td>http-url-parsed-param-parsed</td>
<td>client-to-server</td>
</tr>
<tr>
<td>ssl-server-name</td>
<td>client-to-server</td>
</tr>
<tr>
<td>stream</td>
<td>any/client-to-server/server-to-client</td>
</tr>
<tr>
<td>http-header-content-type</td>
<td>any/client-to-server/server-to-client</td>
</tr>
<tr>
<td>http-header-cookie</td>
<td>any/client-to-server/server-to-client</td>
</tr>
</tbody>
</table>

**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 51 on page 532 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 | 86 |
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 profile-name actions]
[edit services ssl proxy profile 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**

```plaintext
rsa-rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-rsa-with-rc4-128-sha RSA | 128bit rc4 | sha hash |
rsa-with-rc4-128-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-md5 RSA | no |
rsa-with-rc4-128-md5 RSA export | 40 bit rc4 | md5 hash rsa-export-with-des40-cbc-sha RSA export |
no symmetric cipher | sha hash | ecdhe-ecdsa-with-aes-256-gcm-sha384 RSA |
ecdhe-ecdsa-with-aes-256-cbc-sha256 RSA |
ecdhe-ecdsa-with-aes-256-cbc-sha256 RSA |
ecdhe-ecdsa-with-aes-128-cbc-sha256 RSA |
ecdhe-ecdsa-with-aes-128-cbc-sha256 RSA |
ecdhe-ecdsa-with-3des-ede-cbc-sha RSA |
ecdhe-ecdsa-with-aes-256-cbc-sha RSA ];
```

**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, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances. Options to support Elliptic Curve Digital Signature Algorithm (ECDSA) added in Junos OS Release 18.3R1.

**Description**

Configure custom cipher for an SSL profile.

Custom ciphers allow you to define your own cipher list. If you do not want to use one of the three categories (strong, medium, or week) of preferred ciphers, 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, 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-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-rc4-1024-md5—RSA, 1024-bit RC4, MD5 hash
rsa-with-rc4-128-sha—RSA, 128-bit RC4, SHA hash
ecdhe-ecdsa-with-aes-256-gcm-sha384—ECDHE,ECDSA, 256 bit aes/gcm, sha384 hash
ecdhe-ecdsa-with-aes-256-cbc-sha384—ECDHE,ECDSA, 256 bit aes/cbc, sha384 hash
ecdhe-ecdsa-with-aes-256-cbc-sha—ECDHE,ECDSA, 256 bit aes/cbc, sha hash
ecdhe-ecdsa-with-aes-128-gcm-sha256—ECDHE,ECDSA, 128 bit aes/gcm, sha256 hash
ecdhe-ecdsa-with-aes-128-cbc-sha256—ECDHE,ECDSA, 128 bit aes/cbc, sha256 hash
**ecdhe-ecdsa-with-aes-128-cbc-sha**—ECDHE,ECDSA, 128 bit aes/cbc, sha hash

**ecdhe-ecdsa-with-3des-ede-cbc-sha**—ECDHE,ECDSA, 3des ede/cbc, sha hash

**Required Privilege Level**
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>SSL Proxy Overview</th>
<th>351</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SSL Forward Proxy</td>
<td>382</td>
</tr>
<tr>
<td>Enabling Debugging and Tracing for SSL Proxy</td>
<td>438</td>
</tr>
</tbody>
</table>
default-rule

Syntax

```plaintext
default-rule {
    (deny [block-message] | permit | reject [block-message]);
}
```

Hierarchy Level

```
[edit security application-firewall rule-sets rule-set-name]
```

Release Information


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](#)
**destination-path-group**

**Syntax**

```plaintext
destination-path-group group-name {
  active-probe-properties {
    active-probe-only;
  }
  inline-gre-encap
  overlay-path {
    overlay-path-name;
  }
  probe-routing-instance {
    routing-instance-name;
  }
}
```

**Hierarchy Level**

[edit security advance-policy-based-routing]

**Release Information**

Statement introduced in Junos OS Release 18.2R1.

**Description**

Define a group containing multiple overlay paths terminating at a same destination.

In releases prior to Junos OS release 20.2R1, AppQoE determines the applicable destination path group and binds the application sessions to that particular destination-path-group. Based on the application’s SLA requirements and link preferences, AppQoE determines the best link among all the links in that destination-path-group. All the instances of the applications use the same best path in the chosen DPG. If there is SLA violation on the current link, then AppQoE determines a new best-link only among all the links in the chosen destination-path-group. In the case of primary hub failover or routing change, AppQoE selects another DPG and then binds the session to the new destination-path-group.

Starting in Junos OS release 20.2R1, with support for the active-active deployment, you can select the links across the destination path groups if an end-point is reachable through them. The best link selected among all the links in the selected destination path group sends the application traffic.

**Options**

- **group-name**—Name that identifies the destination path group.
- **active-probe-properties**—Specify additional active probe property.
  - **active-probe-only**—Enable active probing only to the destination path group
**inline-gre-encap** — Enable inline GRE encapsulation.

**overlay-path overlay-path-name** — Overlay path name.

**probe-routing-instance routing-instance-name** — Routing instance for the probe path.

**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 | 283
- Advanced Policy-Based Routing | 213
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 | 86
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 Application Tracking | 177
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 | 73 |
**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

Traditional Application Firewall  |  145
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

| Traditional Application Firewall | 145 |
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 | 351
- Configuring SSL Forward Proxy | 382
- Enabling Debugging and Tracing for SSL Proxy | 438
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.

Starting in Junos OS Release 15.1X49-D210R1 and Junos OS Release 19.4R1, the maximum packet threshold for DPI performance mode option is deprecated—rather than immediately removed—to provide backward compatibility and an 6 opportunity to bring your configuration into compliance with the new configuration.

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 | 46
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 | 213
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 | 351
- Configuring SSL Forward Proxy | 382
- Enabling Debugging and Tracing for SSL Proxy | 438
fallback-option (ICAP Redirect Service)

Syntax

```bash
fallback-option {
    connectivity (block | log-permit | permit);
    default-action (block | log-permit | permit);
    timeout (block | log-permit | permit);
}
```

Hierarchy Level

```bash
[edit services icap-redirect profile name]
[edit logical-system logical-system-name services icap-redirect profile name]
```

Release Information

Statement introduced in Junos OS Release 18.1R1.
The logical system option is introduced in Junos OS Release 18.3R1.

Description

Specify fallback options for the device. Fallback settings enable the device to handle errors.

The fallback option is used to define the actions such as permit, log-and-permit, or block. This is the action that occurs when a request fails due to conditions such as too many requests, or a timeout occurred, or connectivity issues.

Options

**connectivity**—Fallback settings when connection-related failures occur.

Values:

- block—Log the error and deny the requests.
- log-permit—Log the error and permit the requests.
- permit—Permit the requests.

**default-action**—Default failure action.

Values:

- block—Log the error and deny the requests.
- log-permit—Log the error and permit the requests.
- permit—Permit the requests.
**throttle**—Fallback action when the total number of requests received concurrently exceeds the devices limit.

**Values:**
- block—Log the error and deny the requests.
- log-permit—Log the error and permit the requests.
- permit—Permit the requests.

**timeout**—Fallback action when there is a timeout occurrence.

**Values:**
- block—Log the error and deny the requests.
- log-permit—Log the error and permit the requests.
- permit—Permit the requests.

**Required Privilege Level**
system

**RELATED DOCUMENTATION**
- Example: Configuring ICAP Redirect Service on SRX Devices | 419
file (System Logging)

Syntax

```
file name {
    allow-duplicates;
    archive name password password routing-instance routing-instance <(binary-data | no-binary-data)> <files files>
      <size bytes> <start-time start-time> <transfer-interval minutes> <(world-readable | no-world-readable)>;
    contents (any | authorization | change-log | conflict-log | daemon | dfc | external | firewall | ftp | interactive-commands | kernel | local0 | lpr | mail | news | ntp | pfe | privileged | security | syslog | user | uucp) {
    }
    explicit-priority;
    match match;
    match-strings [ match-strings ... ];
    structured-data (brief | detail);
}
```

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 | 382 |
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


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

<table>
<thead>
<tr>
<th>SSL Proxy Overview</th>
<th>351</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SSL Forward Proxy</td>
<td>382</td>
</tr>
</tbody>
</table>
http (icap-redirect profile)

Syntax

```plaintext
http {
    redirect-request;
    redirect-response;
}
```

Hierarchy Level

```plaintext
[edit services icap-redirect profile name]
[edit logical system logical-system-name services icap-redirect profile name]
```

Release Information

Statement introduced in Junos OS Release 18.1R1.
The logical system option is introduced in Junos OS Release 18.3R1.

Description

Enable the redirect request and the redirect response for the HTTP traffic.

You can forward HTTP requests and HTTP responses to an Internet Content Adaptation Protocol (ICAP) server before sending a request to a Web server or returning a response to the client system.

The SRX Series device decrypts the HTTPS traffic and redirects the HTTP message to a third-party, on-premise, DLP server using the ICAP channel. After DLP processing, the traffic is reflected back to the SRX Series device.

Options

- `redirect-request`—Enable the redirect service on HTTP request
- `redirect-response`—Enable the redirect service on HTTP response

Required Privilege Level

- `system`

RELATED DOCUMENTATION

- Example: Configuring ICAP Redirect Service on SRX Devices | 419
icap-redirection

Syntax

```plaintext
icap-redirection {
  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 | 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> <match match> <size size> (world-readable | no-world-readable);
    flag name;
    no-remote-trace no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit services]
[edit logical-system logical-system-name services]
[edit tenants tenants_name services]
```

Release Information
Statement introduced in Junos OS Release 18.1 R1.
Support at the [edit logical-system logical-system-name services] hierarchy level introduced in Junos OS Release 18.3R1.
Support at the [edit tenants tenants_name services] hierarchy level introduced in Junos OS Release 20.1R1.

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.

Starting in Junos OS Release 20.1R1, you can enable ICAP redirect service at the tenant system level, and you can view/clear the ICAP redirect services status and statistics at the tenant systems level. The ICAP service redirect configuration for tenant system is implemented under profile and the ICAP redirect profile capacity is 64 globally. All tenant systems need to share this profile capacity. If 64 tenant systems used the maximum tenants profile capacity, the remaining tenant systems will not be not able to configure the ICAP redirect profile. Tenant systems can reserve the required or the maximum ICAP redirect profile capacity in their security-profiles using the following CLI commands respectively:

- `edit system security-profile security-profile-name icap-redirect-profile reserved quota`
- `edit system security-profile security-profile-name icap-redirect-profile maximum quota`

In addition, we’ve introduced the X-Client-IP, X-Server-IP, X-Authenticated-User, and X-Authenticated-Groups header extensions in an ICAP message to provide information about the source of the encapsulated HTTP message.

Options
The 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.
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 | 86
ip-protocol-mapping (Application Identification)

Syntax

```plaintext
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 | 86
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;
            rsa-with-null-sha | rsa-with-rc4-128-md5 | rsa-with-rc4-128-sha); 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 | 382 |
| Firewall User Authentication Overview |
level (Services)

Syntax

```plaintext
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 | 382
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 | 382 |
maximum-transactions

Syntax

maximum-transactions transactions-number;

Hierarchy Level

[edit services application-identification]

Release Information

Statement introduced in Junos OS Release 18.2R1

Description

Configure the maximum number of transactions matched by application identification for finalizing the application.

Application classification does not terminate for applications that are transaction based such as Facebook applications. To terminate the application classifications for such applications, you can choose to consider the results from multiple transactions as the final classification. You can configure the number of transactions before concluding the final result for the identified application.

For example, when you configure the maximum number of transactions as 10, the following sequence is applied for identifying the final application:

- In the first and second transactions, application-1 and application-2 are identified respectively.
- The identification process continues till the 10th transaction is reached.
- Since 10th transaction is equal to the configured value of the maximum number of transactions, the application identified in this transaction is considered as the final match.

Options

maximum-transactions transactions-number—Number of transaction results that can be considered before concluding the final result for application identification.

- Range: 0 through 25
- Default: 5

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.
metrics-profile

Syntax

```text
metrics-profile metrics-profile-name {
  sla-threshold {
    delay-round-trip {
      delay-value;
    }
    jitter {
      jitter-value;
    }
    jitter-type {
      egress-jitter ;
      ingress-jitter;
      two-way-jitter;
    }
    match {
      [all | any];
    }
    packet-loss {
      loss-value;
    }
  }
}
```

Hierarchy Level
[edit security advance-policy-based-routing]

Release Information
Statement introduced in Junos OS Release 18.2R1.

Description
Create a set of metrics, which can be used by AppQoE to evaluate the SLA of the link.

A metrics profile defines the performance metrics for delay round trip, one-way jitter or two-way jitter, and packet loss.

To ensure compliance with the SLA, metrics are required to measure and monitor the network performance. This measurement capability provides a greater visibility into the performance characteristics of the links and helps in network performance evaluation.

Options

`metrics-profile-name`—Metrics profile name.
**delay-round-trip delay-value**—Sets the total round-trip time (in microseconds), from the device to the remote server, that triggers a probe failure.

**jitter jitter-value**—Total jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure

**jitter-type**—Jitter type.

  Values: Ingress jitter, egress jitter, and two-way jitter.

  Default: Two-way jitter

**match**—Matching SLA metrics.

  **all**—The path selection mechanism attempts to find a path that satisfies all the 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 satisfy the metric, a random path among the available paths will be selected. Also, SLA violation will be detected and raised even if any one of the metrics is violated.

  This is the default match option.

  **any**—Path selection mechanism attempts to find a path which satisfies the maximum number of metrics. For example, if there is a path available that conforms to more than one metric, then the path is chosen over another path which satisfies less number of metrics. In this case, SLA violation is detected only when none of the metrics meets the requirement. If either one of the metric is meets the requirement, then violation is not triggered.

**packet-loss loss-value**—Percentage of number of packets that must be lost successively to trigger a probe failure.

**Required Privilege Level**

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

---

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Application Quality of Experience</th>
<th>283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Policy-Based Routing</td>
<td>213</td>
</tr>
</tbody>
</table>
mirror-decrypt-traffic

Syntax

```
mirror-decrypt-traffic {
    interface interface-name;
    only-after-security-policies-enforcement;
    destination-mac-address mac-address;
}
```

Hierarchy Level

```
[edit services ssl proxy profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 18.4R1

Description

Specify SSL decryption mirroring options to forward the copy of SSL decrypted traffic to an external traffic collection device.

To use SSL decryption mirroring, configure the SSL decryption port mirroring interface on SRX Series device and MAC address of the of the external mirror traffic collector port in an SSL proxy profile. Next, apply the SSL proxy profile as application services in the security policy. The SSL traffic matching the security policy rule is decrypted and a copy of the decrypted traffic is forwarded to an external traffic collection device through the SSL decryption port mirroring interface.

Options

- **interface**—SSL decryption port mirroring interface on SRX Series device. This is an Ethernet interface on SRX Series device through which the copy of the SSL decrypted traffic is forwarded to a mirror port.

- **only-after-security-policies-enforcement**—Enables forwarding the copy of the decrypted traffic to the external mirror traffic collector after enforcing the Layer 7 security services through a security policy.

  By default, forwarding of the SSL decrypted payload to the external mirror traffic collector port occurs before enforcing Layer 7 security services including IDP, Juniper SKY ATP, and UTM. When you select to forward the copy of the decrypted traffic after security policies enforcement, and if the decrypted payload is modified while enforcing the security policy, the modified decrypted payload is forwarded to external traffic collection device. Similarly, if the decrypted traffic is dropped because of policy enforcement (for example, a threat is detected in the decrypted traffic), that particular decrypted traffic is not forwarded.

- **destination-mac-address**—MAC address of the of the external mirror traffic collector port.
**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** | 382
- *Firewall User Authentication Overview*
**no-application-identification (Services)**

**Syntax**

```plaintext
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:

```plaintext
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:

```plaintext
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 | 37 |
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

| Enabling or Disabling Application System Cache for Application Services | 38 |
**ngfw**

**Syntax**

```
ngfw {
    default-profile {
        application-traffic-control {
            rule-set rule-set;
        }
        ssl-proxy {
            profile-name profile-name;
        }
    }
}
```

**Hierarchy Level**

- [edit security]
- [edit security logical-systems logical-system-name]

**Release Information**

Statement introduced in Junos OS Release 18.2R1

**Description**

Specify a default profile to manage conflicts when a security policy lookup returns a list of policies before the final application is identified.

The initial policy lookup phase occurs prior to identifying a dynamic application. If there are multiple policies present in the potential policy list that contain different SSL proxy profiles, then the SRX Series device applies the default profile until a more explicit match has occurred.

You can configure a default profile for an SSL proxy and for an application quality of service (AppQoS) under the [edit security ngfw] hierarchy level.

You can configure an SSL proxy profile under the [edit services ssl proxy] hierarchy level, which can be applied as the default SSL proxy profile under the [edit security ngfw] hierarchy level. Similarly, you can configure application traffic rule sets under the [edit class-of-service] hierarchy level, and apply the rule set under the [edit security ngfw] hierarchy level as the default AppQoS rule set.

**Options**

- **application-traffic-control**—Specify the application traffic control rule as the default rule.
  
  `rule-set rule-set`—Rule set name of the application traffic control.
ssl-proxy—Specify the SSL forward proxy profile or the SSL reverse proxy profile as the default profile.

profile-name profile-name—Name of the SSL forward proxy profile or the SSL reverse proxy profile.

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 | 382 |
| Firewall User Authentication Overview |
over (Application Identification)

Syntax

```
over protocol-type { 
  signature name { 
    member name { 
      context { 
        context; 
      } 
      direction { 
        any; 
        client-to-server; 
        server-to-client; 
      } 
      pattern pattern; 
      depth byte-number; 
    } 
    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.

**depth** — Maximum number of bytes to check for context match. Use the byte limit for AppID to identify custom application pattern for applications running over TCP or UDP or Layer 7 applications.

**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 | 86
overlay-path

Syntax

```plaintext
overlay-path overlay-path-name {
    probe-path {
        local ip-address;
        remote ip-address
    }
    tunnel-path {
        local ip-address;
        remote ip-address
    }
}
```

Hierarchy Level

[edit security advance-policy-based-routing]

Release Information

Statement introduced in Junos OS Release 18.2R1.

Description

Configure overlay path 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 and probe IP addresses.

You need to create the overlay setup between local and remote endpoints on both ends of the overlay (spoke device and hub device).

Options

- **overlay-path-name**—Overlay path name.
- **probe-path**—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.
  - **local ip-address**—IP address of the local device.
  - **remote ip-address**—IP address of the remote device.
- **tunnel-path**—Start and end IP addresses of a tunnel. Tunnel IP addresses must be unique across individual overlay paths.
  - **local ip-address**—IP address of the local device.
  - **remote ip-address**—IP address of the remote device.
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 | 283 |
| Advanced Policy-Based Routing     | 213 |
**packet-capture**

**Syntax**

```bash
packet-capture {
  aggressive-mode;
  buffer-packets-limit bytes;
  capture-interval capture-interval;
  capture-limit capture-limit;
  global;
  max-bytes bytes;
  max-files max-files;
  max-packets max-packets;
  no-inconclusive;
  storage-limit bytes;
}
```

**Hierarchy Level**

[edit services application-identification]

**Release Information**

Statement introduced in Junos OS Release 20.2R1.

**Description**

Specify packet capture options to capture unknown application traffic.

You can use the packet capture of unknown applications functionality to gather more details about an unknown application on your security device. Once you've configured packet capture options on your security device, the unknown application traffic is gathered and stored on the device in a packet capture file (.pcap) at /var/log/pcap/ location.

**Options**

- **aggressive-mode**—Capture all traffic before ApplID classifies the applications. In this mode, the system captures all application traffic irrespective of the application system cache (ASC) entry. Packet capture starts for the first packet of the first session.

- **buffer-packets-limit**—Maximum memory to buffer packets (bytes). Use this option to limit the memory available in the Packet Forwarding Engine for packet capture functionality.
  - **Default:** 1% of available data in shared memory
  - **Range:** 0% through 5% of available data in shared memory
  - **Default:** 1 MB (for cSRX)
  - **Range:** 0 through 5 MB
**capture-interval**—Timeout value in minutes to avoid repetitive capture of the same traffic. After this interval, the system continues to capture newer packet details for unknown applications until the capture limit is reached.

   **Default:** 1440 minutes (24 hours).
   **Range:** 1 through 525,600 seconds

**capture-limit**—Number of repetitive captures of the same traffic. Use this option to limit the number of times the same traffic can be repeatedly captured before the cache entry times out.

   **Default:** 4
   **Range:** 1 through 1000

**global**—Enable packet capture globally to capture all unknown application traffic. Another option is to enable capturing of unknown application traffic specific to a security policy.

**max-bytes**—Maximum number of TCP bytes per session (bytes). For TCP sessions, the count includes the actual payload data length and excludes IP/TCP headers for the maximum bytes limit.

   If you are setting the packet capture at the security policy level, the packet capture concludes only after the final policy is applied even if the configured limit is reached.

   **Limitation**—Jumbo frames can have up to 1500 bytes of the payload saved in the capture file.

   **Default:** 6000 bytes
   **Range:** 40 through 1,073,741,824

**max-files**—Maximum number of unique packet capture files to create before the oldest file is overwritten by a new file created.

   **Default:** 25
   **Range:** 1 through 2500

**max-packets**—Maximum number of UDP packets per session.

   **Default:** 10 packets
   **Range:** 1 through 1000

**no-inconclusive**—Disable packet capturing of inconclusive traffic. This option disables the packet capture for the following sessions:

   - **Sessions** that are closed before the application identification or classification completes.
   - **Sessions** that are not getting classified even when they reach the maximum packet capture limit.

   If you do not configure this option, by default, the system captures packets for inconclusive sessions.

**storage-limit**—Maximum disk space (bytes) that can be used in the Routing Engine for packet capture files.

   **Default:** 50 MB
   **Range:** 1,048,576 through 4,294,967,295 bytes
Required Privilege Level
system

RELATED DOCUMENTATION
- Configure Packet Capture of Unknown Application Traffic | 49
- show services application-identification packet-capture counters | 850
passive-probe-params

Syntax

```plaintext
passive-probe-params {
    sampling-percentage {
        percentage;
    }
    sampling-period {
        period;
    }
    type {
        book-ended;
    }
}
```

Hierarchy Level
[edit security advance-policy-based-routing]

Release Information
Statement introduced in Junos OS Release 18.2R1.

Description
Configure the passive probe parameters with the SLA rule.

Passive probes measure the service quality of an application by inserting a custom probe header in the live traffic between the spoke and hub points and measuring the RTT, jitter and packet loss between the points of installation of the probes.

SLA violation is determined through passive probing of live application or application group traffic.

Options

**sampling-percentage percentage**—Indicates the percentage of sessions that are selected for a book-ended SLA measurement.

Example: If 18 sessions are available for a particular application are available, and if you have configured 25%, then 25% of the 18 sessions—that is 5 sessions out of 18 sessions, are evaluated.

Range: 1-100

**sampling-period period**—Indicates a defined sampling period (in milliseconds) in which the number of violations are collected. Once this period is expired, the collected sampling data is purged and a new data is collected.

Range: 2000-60,000

Default: 5000 milliseconds
**type**—Indicates the type of probe measurement, only p-encap or book-ended supported.

**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 | 283
- Advanced Policy-Based Routing | 213
policy (advanced-policy-based-routing)

Syntax

```plaintext
policy policy-name {
  match {
    application;
    destination-address;
    destination-address-excluded;
    source-address;
    source-address-excluded;
    source-identity {
      [user-or-role-name];
      any;
      authenticated-user;
      unauthenticated-user;
      unknown-user;
    }
  }
  then {
    application-services {
      advance-policy-based-routing-profile apbr-profile-name;
    }
  }
}
```

Hierarchy Level

```
[edit security advanced-policy-based-routing from-zone name]
```

Release Information
Statement introduced in Junos OS Release 18.2R1

Description
Configure advanced policy-based routing (APBR) policies.

You can create APBR policies for a security zone and apply advanced policy-based routing (APBR) profiles on the traffic that matches the policy.

In the APBR policy, you can define 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.
The routing instance associated with APBR profile includes a static route and next hop configured. The matching traffic arriving at the trust zone is forwarded to a specific device or interface as specified by the next-hop IP address.

**NOTE:** 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.

**Options**

- **policy policy-name**—Specify the name of the APBR policy.

- **description**—Specify descriptive text for the APBR policy.

- **match**—Specify an APBR policy match-criteria.
  - **source-address**—Define the source address as the matching criteria.
  - **destination-address**—Define the destination address as the matching criteria.
  - **application**—Name of the predefined or custom application or application set used as match criteria.
  - **destination-address-excluded**—Exclude destination addresses.
  - **source-address-excluded**—Exclude source addresses.
  - **source-identity**—Specify users and roles to be used as the match criteria.

- **then**—Specify the policy action to be performed when packets match the defined criteria.
  - **application-services**—Enable application services within a security policy. the following application services is supported:
    - advance-policy-based-routing-profile *apbr-profile-name*—Specify the advanced policy-based routing (APBR) profile.

**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*
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;
  }
}
Hierarchy Level

[edit security policies from-zone zone-name to-zone zone-name]

Release Information

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

<table>
<thead>
<tr>
<th>Configuring SSL Forward Proxy</th>
<th>382</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policies Overview</td>
<td></td>
</tr>
</tbody>
</table>
port-range (Application Identification)

Syntax

```plaintext
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 | 86 |
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 | 351
profile (icap-redirect)

Syntax

```
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;
}
```

Hierarchy Level

[edit services]

Release Information

Statement introduced in Junos OS Release 18.1 R1.

Description

Configure the ICAP redirect profile.

The ICAP server profile allows the ICAP server to process request messages, response messages, fallback options, and so on, for the permitted traffic.
When you configure an ICAP redirect service on SRX Series devices, you must configure the ICAP redirect profile. The ICAP redirect profile defines the settings for ICAP server to process request messages, response messages, fallback options in case of a timeout, connectivity issues, too many requests, or other conditions.

This profile is applied to a security policy as an application service when the traffic is permitted by the security policy.

**Options**

- **profile name**—ICAP redirect profile name.
- **fallback-option**—Fallback options to specify the actions the device applies if the ICAP server is unavailable.
- **http**—Redirect request and redirect response for HTTP traffic.
  - **Values:**
    - redirect-request—Enable the redirect service on HTTP request
    - redirect-response—Enable the redirect service on HTTP response
- **timeout**—Server response timeout in milliseconds. Timeout is the interval after which the server is considered inactive if there is no response from the server. A new incoming requests can bypass inactive status server.
  - **Default:** 500
  - **Range:** 100 through 50000

**Required Privilege Level**

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**RELATED DOCUMENTATION**

- Example: Configuring ICAP Redirect Service on SRX Devices | 419
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

- Traditional Application Firewall | 145
profile (Services SSL Proxy)

Syntax

```plaintext
profile name {
    (root-ca root-ca | server-certificate[ server-certificate ... ]); 
actions {
    allow-strong-certificate;
    crl {
        disable;
        if-not-present (allow | drop);
        ignore-hold-instruction-code;
    }
    disable-session-resumption;
    ignore-server-auth-failure;
    log {
        all;
        errors;
        info;
        sessions-allowed;
        sessions-dropped;
        sessions-ignored;
        sessions-whitelisted;
        warning;
    }
    renegotiation {
        (allow | allow-secure | drop);
    }
    }
    custom-ciphers ;
    enable-flow-tracing enable-flow-tracing;
    mirror-decrypt-traffic {
        interface interface-name;
        only-after-security-policies-enforcement;
        destination-mac-address mac-address;
    }
    preferred-ciphers (custom | medium | strong | weak);
    trusted-ca ;
    whitelist [ whitelist ... ];
    whitelist-url-categories [ whitelist-url-categories ... ];
}```

Hierarchy Level
[edit services ssl proxy]
[edit logical-system logical-system-name services ssl proxy]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10.
The crl statement is supported from 15.1X49-D30.
The **logical system** option is introduced in Junos OS Release 19.1R1.

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-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**

<table>
<thead>
<tr>
<th>SSL Proxy Overview</th>
<th>351</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SSL Forward Proxy</td>
<td>382</td>
</tr>
<tr>
<td>Enabling Debugging and Tracing for SSL Proxy</td>
<td>438</td>
</tr>
</tbody>
</table>
profile (Services Proxy)

Syntax

```
profile name {
  profile (Services Proxy) {
    http {
      host host;
      port port;
    }
  }
}
```

Hierarchy Level

```
[edit services proxy]
```

Release Information

Statement introduced in Junos OS Release 18.3R1.

Description

Define the proxy profile settings for application signature package download.

You can download the application signature package hosted on an external server, using a proxy server. To use the proxy server for downloading, you must configure a profile with host and port details of the proxy server, and apply the proxy profile in the `set services application-identification download` command.

This configuration enables you to download the signature package when you have already deployed a web proxy on your device as part of your overall security solution.

Options

- **name**—Proxy profile name.
- **protocol**—Protocol type for the profile. Support is available for only HTTP connections.
- **host**—IP address of the proxy server.
- **port**—Port number used by the proxy server.

Required Privilege Level

```
system
```
protocol (Services Proxy)

Syntax

```plaintext
protocol {
  http {
    host host;
    port port;
  }
}
```

Hierarchy Level

[edit services proxy]

Release Information
Statement introduced in Junos OS Release 18.3R1.

Description
Define the proxy profile settings for application signature package download.

You can download the application signature package hosted on an external server, using a proxy sever. To use the proxy server for downloading, you must configure a profile with host and port details of the proxy server, and apply the proxy profile in the `set services application-identification download` command.

This configuration enables you to download the signature package when you have already deployed a web proxy on your device as part of your overall security solution.

Options

- `name`—Proxy profile name.
- `protocol`—Protocol type for the profile. Support is available for only HTTP connections.
- `host`—IP address of the proxy server.
- `port`—Port number used by the proxy server.

Required Privilege Level
- `system`
profile (SSL Initiation)

Syntax

```
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 ;
    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 initiation]
```

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 name of the profile for SSL initiation support service.

SSL initiation is a process where the SRX Series device acts as in SSL proxy client, initiates the SSL sessions with an SSL server. The SRX Series device receives clear text from an HTTP client. It encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the SRX Series decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.

The profile contains the settings for the SSL-initiated connections. This includes the list of supported ciphers and their priority, the supported versions of SSL/TLS, and a few other options.

Options
**actions**—Specify the certification revocation checks and traffic related actions for configuring SSL initiation support service.

**crl**—Specify certificate revocation actions. The certificate revocation list (CRL) contains the list of digital certificates that have been canceled before their expiration date. When a participating device uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL. By default, CRL verification is enabled on SSL profile.

**ignore-hold-instruction-code**—Ignore server authentication failure. By selecting this option, you can choose to ignore certificate validation, root CA expiration dates, and other such issues based on your requirements.

**client-certificate**—Local certificate. It is a certificate that client connects to server with. It is usually signed by a CA that the SRX Series device trusts.

**custom-ciphers**—Configure custom cipher for an SSL profile.

Custom ciphers allow you to define your own cipher list. If you do not want to use one of the three categories (strong, medium, or week) of preferred ciphers, 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.

**enable-flow-tracing**—Enable flow tracing to enable debug tracing.

**enable-session-cache**—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.

**ignore-server-auth-failure**—Ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

**preferred-ciphers**—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.

**protocol-version**—Specify the accepted SSL protocol version. You can specify the SSL/TLS protocol version the security device uses to negotiate in SSL connections.

**trusted-ca**—List of trusted certificate authority profiles. SSL forward proxy uses trusted CA certificates for server authentication. Junos OS provides a default list of trusted CA certificates that you can easily load on to your system using a default command option.

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 | 382 |
profile (SSL Termination)

Syntax

```
profile name {
  custom-ciphers;
  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);
  server-certificate server-certificate;
  trusted-ca ;
}
```

Hierarchy Level

```
[edit services ssl termination]
```

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 name of the profile for SSL termination support service.

Traffic from the client to SRX Series is encrypted and terminated at SRX Series, which then re-encrypts traffic to the back-end server.

SSL termination is a process where the SRX Series device acts as an SSL proxy server, terminates the SSL session from the client. The SRX Series device receives encrypted data from the HTTP client. It decrypts and transmits the data as unencrypted request to the other servers (HTTP server).

The profile contains the settings for the SSL-terminated connections. This includes the list of supported ciphers and their priority, the supported versions of SSL/TLS, and a few other options.

Options

- **custom-ciphers**—Configure custom cipher for an SSL profile.

  Custom ciphers allow you to define your own cipher list. If you do not want to use one of the three categories (strong, medium, or weak) of preferred ciphers, 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.
enable-flow-tracing—Enable flow tracing to enable debug tracing.

enable-session-cache—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.

preferred-ciphers—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.

protocol-version—Specify the accepted SSL protocol version. You can specify the SSL/TLS protocol version the security device uses to negotiate in SSL connections.

server-certificate—Local certificate identifier. Server certificates are used to authenticate the identity of a server. A server is required to present a certificate as part of the initial connection setup. SSL proxy generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration).

trusted-ca—List of trusted certificate authority profiles. SSL forward proxy uses trusted CA certificates for server authentication. Junos OS provides a default list of trusted CA certificates that you can easily load on to your system using a default command option.

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 | 382 |
| Firewall User Authentication Overview |
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 | 351
proxy (Services)

Syntax

```plaintext
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

<table>
<thead>
<tr>
<th>SSL Proxy Overview</th>
<th>351</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SSL Forward Proxy</td>
<td>382</td>
</tr>
<tr>
<td>Enabling Debugging and Tracing for SSL Proxy</td>
<td>438</td>
</tr>
</tbody>
</table>
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]
[edit logical-systems logical-system-name class-of-service application-traffic-control]
[edit tenants tenant-name class-of-service application-traffic-control]

Release Information

Statement introduced in Junos OS Release 11.4.
Support at the following hierarchy levels introduced in Junos OS Release 19.3R1: [edit logical-systems logical-system-name class-of-service application-traffic-control], and [edit tenants tenant-name class-of-service application-traffic-control].

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 Application Quality of Service  | 196
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 | 382 |
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 | 382
- 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 | 222
- Understanding Advanced Policy-Based Routing | 213
rule (Advanced Policy-Based Routing)

Syntax

```plaintext
rule rule-name {
    disable-midstream-routing;
    match {
        category (juniper-enhanced-category | custom-category);
        dynamic-application [system-application | any];
        dynamic-application-group [system-application-group];
        dscp dscp-value;
    }
    then {
        routing-instance name ;
        application-services-bypass;
    }
}
```

Hierarchy Level

[edit security advance-policy-based-routing profile profile-name]

Release Information

Statement introduced in Junos OS Release 15.1X49-D60. The option `category` is introduced in Junos OS Release 18.3R1. Junos OS Release 19.3R1 supports the option `dscp`. Junos OS Release 20.1R1 supports the option `any` for `dynamic-application`.

Description

Configure rules for the advanced policy-based routing (APBR) profile (application profile). Associate the rule with one or more than one dynamic applications or application groups or URL categories as follows:

- For matching the dynamic applications, APBR consults the application identification (AppID) and application system cache (ASC) to get the application type. 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, and the traffic is redirected to the defined routing instance for the route lookup.

- You can use a DSCP value in an APBR rule as a matching criteria to perform advanced policy-based routing on the traffic with DSCP markings. You can use the DSCP value in addition to the dynamic applications in an APBR rule.

- For matching the URL categories, APBR leverages category identification from the Enhanced Web Filtering (EWF) and local Web filtering results obtained from the unified threat management (UTM) module. Web filtering classifies websites into categories. If the traffic matches the URL categories specified in the rule of the APBR profile, it is redirected to the defined routing instance.
Options

disable-midstream-routing—Selectively disable APBR in the middle of a session for a specific APBR rule.

match—Define a match criteria for matching the traffic in APBR profile rule.

category (juniper-enhanced-category | custom-category)—Define the category type as the Juniper Enhanced Web Filtering (EWF) or a custom category if you are using local Web filtering.

juniper-enhanced-category—Define URL categories such as Enhanced_Social_Web_Facebook, Enhanced_Social_Web_Linkedin, Enhanced_Social_Web_Twitter or Enhanced_Social_Web_Youtube as match criteria in APBR profile rule.

custom-category—Define either custom URL or IP address of a site as match criteria in APBR profile rule.

dynamic-application [system-application | any]—Specify the dynamic application names for match criteria in APBR rule.

dynamic-application-group [system-application-group]—Dynamic application groups for match criteria in APBR rule.

dscp [dscp-value]—Specify DSCP value as match criteria in APBR rule.

Range: 0-63

then—Define the action for the match condition by specifying the routing instance name.

application-services-bypass—Bypass applying the application services on the traffic matching the APBR rule. As URL category-based routing enables you to identify and selectively route Web traffic (HTTP and HTTPS) to a specified destination or to another device where further inspection, you can select not to apply or bypass application services on the same session. You can select to exclude traffic from security services when additional throughput is required, or traffic is going from trusted device to another trusted device.

routing-instance name—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 | 222

Understanding Advanced Policy-Based Routing | 213
rule-sets (CoS AppQoS)

Syntax

```plaintext
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]
- [edit logical-systems logical-system-name class-of-service application-traffic-control]
- [edit tenants tenant-name class-of-service application-traffic-control]

Release Information

Statement introduced in Junos OS Release 11.4.
Support at the following hierarchy levels introduced in Junos OS Release 19.3R1: [edit logical-systems logical-system-name class-of-service application-traffic-control], and [edit tenants tenant-name class-of-service application-traffic-control].

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 Application Quality of Service | 196
server (icap-redirect profile)

Syntax

```
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;
}
```

Hierarchy Level

```
[edit services icap-redirect profile name]
[edit logical-system logical-system-name services icap-redirect profile name]
```

Release Information

Statement introduced in Junos OS Release 18.1R1.
The logical system option is introduced in Junos OS Release 18.3R1.

Description

Configure the ICAP server details.

When you configure the ICAP redirect service on SRX Series devices, you must configure the ICAP server details. ICAP server configuration allows you to define the settings required to process request messages, response messages, authorization, and so on. You can also specify an SSL profile in the ICAP server configuration that enables you to secure the connection to the ICAP server.

You can configure up to two ICAP servers.

Options

**name**—ICAP server name.

**host**—ICAP server hostname or IP address.

**port**—ICAP server listening port, default port is reached according to the protocol defined.

Default: 1344
Range: 1025 through 65535

**route-instance**—Virtual router that is used for launching the service.

**reqmod-uri**—Path to the service that handles Request Modification (REQMOD) requests.

**respmod-uri**—Path to the service that handles Response Modification (RESPMOD) requests.

**sockets**—Number of connections to create the ICAP service.

  Default: 8
  Range: 1 through 64

**tls-profile**—SSL profile configured to provide a secure connection to the ICAP server.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

system

**RELATED DOCUMENTATION**

  Example: Configuring ICAP Redirect Service on SRX Devices | 419
secure-proxy

Syntax

secure-proxy {
    profile name {
        drop-on-dns-error;
        dynamic-web-application;
        dynamic-web-application-group;
        proxy-address name {
            ip ip-address;
            port port-number;
        }
    }
}

Hierarchy Level

[edit services web-proxy]

Release Information
Statement introduced in Junos OS Release 19.2R1.

Description
Configure secure Web proxy profile.

When you configure secure Web proxy on SRX series device, it intercepts the session and allows sessions that are interested in specific application and are destined to a configured external web-proxy. The device connects sessions directly to the Web server bypassing the external proxy server. Connections that do not match the applications are routed to the external proxy server.

Since the Secure Web proxy forwards traffic based on applications either to the external proxy server or to the Web server, you can define the routing behavior based on applications. For example, you can specify Office 365 application group in secure Web proxy profile to bypass the external proxy server for connections to Office 365.

To configure secure Web proxy on the SRX Series device, you must define a Web proxy profile by specifying external proxy server details and dynamic application. You can associate this secure Web proxy profile with security policy. The secure Web profile is applied on the traffic matching the application and security policy. The session is now allowed to bypass the external proxy server and connect to the Web server directly.

Options
profile name—Name of the secure Web proxy profile.
drop-on-dns-error—Drop the Web proxy session on DNS error.
dynamic-web-application—Dynamic web application.
dynamic-web-application-group—Dynamic web application group.
proxy-address name—Name of the external proxy server.
ip ip-address—IP address of the external proxy server.
port port-number—Port number of the external proxy server.

Required Privilege Level
flow-tap

**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 Application Tracking  |  177
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
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 | 382
  - Firewall User Authentication Overview
ssl (Services)

Syntax

ssl {
  initiation {
    profile profile-name {
      actions {
        crl {
          disable;
          if-not-present (allow | drop);
          ignore-hold-instruction-code;
        }
        ignore-server-auth-failure;
      }
      client-certificate;
      custom-ciphers [cipher];
      enable-flow-tracing;
      enable-session-cache;
      preferred-ciphers (custom | medium | strong | weak);
      protocol-version (all | tls1 | tls11 | tls12);
      trusted-ca (all | [ca-profile] );
    }
  }
}
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;
      log {
        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];
}
}
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;
  }
}
}
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  flag flag;
  level [brief | detail | extensive | verbose];
  no-remote-trace;
}
}

Hierarchy Level

[edit services]
Release Information
Statement introduced in Junos OS Release 12.1X44-D10. The `crl` statement is supported from 15.1X49-D30. 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) support service. This statement is supported on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

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

- Configuring SSL Forward Proxy | 382
- Firewall User Authentication Overview
ssl-proxy (Application Services)

Syntax

ssl-proxy { profile-name profile-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 12.1.

Description

Enable SSL proxy and identify the name of the SSL proxy profile to be used. This option is supported on
SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

Options

profile-name—SSL proxy profile.

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 | 382
statistics (Services)

Syntax

```plaintext
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 | 41 |
sla-options

Syntax

```
sla-options {
  log {
    syslog:
    disabled;
  }
}
```

Hierarchy Level
[edit security advance-policy-based-routing]

Release Information
Statement introduced in Junos OS Release 18.2R1.

Description
Enable or disable switching of the application traffic to another route (local to the device) during an SLA violation.

The configuration by default uses the log-type as syslog to support application-level logging. If AppQoE logging needs to be turned off, then log-type needs to be set to disabled.

Options

logging—Configure AppQoE logging

  disabled—Disable logging

  syslog—Enable logging.

Default: syslog

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 | 283 |
| Advanced Policy-Based Routing     | 213 |
sla-rule

Syntax

```
sla-rule sla-rule-name {
  active-probe-params {
    probe-params-name;
  }
  link-type-affinity strict;
  metrics-profile {
    metric-profile-name;
  }
  passive-probe-params {
    sampling-percentage {
      percentage;
    }
    sampling-period {
      period;
    }
    type {
      book-ended;
    }
    preferred-link-type (Any | IP | MPLS);
    sla-export-factor {
      value;
    }
    switch-idle-time {
      period;
    }
    violation-count {
      count;
    }
  }]
```

Hierarchy Level

[edit security advance-policy-based-routing]

Release Information

Statement introduced in Junos OS Release 18.2R1. The options preferred-link-type and link-type-affinity are introduced in Junos OS Release 18.4R1.


Description
Configure an SLA rule.

An SLA rule includes all information required to measure the SLA and to identify whether any SLA violation has occurred or not. It contains the complete probe profiles, time interval which the profiles need to be sent, preferred SLA configuration, and so on.

When you configure an APBR rule, you must associate the corresponding SLA rule for the application.

The presence of SLA rule in the APBR configuration triggers the AppQoE functionality; If there are no SLA profiles available, APBR operates without AppQoE.
Options

**active-probe-params probe-params-name**—Name of the active probe parameter. Associate the active probe parameter with the SLA rule.

**link-type-affinity (strict);**—(optional) Configure the link-type affinity as strict for the preferred link type. For strict affinity, AppQoE ensures that the path selected is always of the preferred link type. When the default affinity (loose) is configured and if there are no SLA meeting links belonging to the preferred link type available, then AppQoE selects a link outside the preferred link type that meets the SLA requirements.

**metrics-profile profile-name**—Metric profile name. The SLA rule contains metric profiles that provide the acceptable threshold. If the violation goes beyond the threshold, an alternate path is identified and then traffic is rerouted.

**passive-probe-params**—Active probe parameter name. Associate the active probe parameter with the SLA rule.

**preferred-link-type (IP | MPLS | Any)**—Select an MPLS or Internet link as the preferred path. If you do not select IP or MPLS, the preferred link type Any is selected when the link-type affinity is configured as loose (default link type affinity). Configuring the link type as Any when the link-type affinity is configured as strict is not supported.

*Default: Any*

**sla-export-factor value**—Set interval to report passive probe report metrics at the application level.

Example: When you configure the sla-export-factor as 5, passive probe results are exported once at the end of the 5th, 10th, and 15th probe interval. You can use a passive probe report to report any data that remains unreported in the probe interval at the end of a session.

With application-level summarization, each probe candidate session must send data to central location where the metrics are aggregated. The data thus aggregated is sent out once the configured SLA export factor is met.

*Range: 5-1000*

*Default: 500*

**switch-idle-time period**—Path switch idle time in seconds. This is the period during which no subsequent switching of application traffic path occurs until the switch idle time expires. This idle time starts when application traffic switches the path.

*Range: 5-300 seconds*

*Default: 15 seconds*

**violation-countnumber**—Indicates the number of violations that must occur in a sampling-period for a given session before a link is marked as having violated the SLA.

*Range: 1-32 seconds*

*Default: 5*
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**

<table>
<thead>
<tr>
<th>Application Quality of Experience</th>
<th>283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Policy-Based Routing</td>
<td>213</td>
</tr>
</tbody>
</table>
source-identity

Syntax

```plaintext
source-identity {
    [user-or-role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
}
```

Hierarchy Level

```plaintext
[edit security policies from-zone zone-name to-zone zone-name policy policy-name match]

[edit security policies global policy policy-name match]

[edit security advance-policy-based-routing from-zone zone-name policy policy-name match]
```

Release Information


Description

Identifies users and roles to be used as match criteria for a policy. If a value other than any is specified as match criteria for a policy within a zone pair, the traffic is matched to table entries to retrieve associated user and roles before policy lookup occurs. Users and roles are retrieved from the local authentication table or from a UAC pushed to the SRX Series device from an access control service when a user is authenticated.

Options

The following entries specify the source identities that match a policy:

- **user-or-role-name**—A list of specific users and roles.
  
  **Range:** 0 through 39 characters

  **NOTE:** SRX Series devices truncate imported roles to 39 characters. You need to ensure that all of your roles are 39 characters or less.
any—Any user or role, as well as the keywords authenticated-user, unauthenticated-user, and unknown-user.

authenticated-user—All users and roles that have been authenticated.

unauthenticated-user—Any user or role that does not have an IP-address mapped to authentication sources and the authentication source is up and running.

unknown-user—Any user or role that does not have an IP address mapped to authentication sources, because the authentication source is disconnected from the SRX Series device. In this case, users are unable to be authenticated due to an authentication server disconnection, such as a power outage.

Unknown-user must be configured for non-domain users to be able to authenticate and log in.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Understanding User Role Firewalls
- Understanding the User Identification Table
- Security Policies Overview
termination (Services)

Syntax

```plaintext
termination {
  profile name {
    custom-ciphers;
    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);
    server-certificate server-certificate;
    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) 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, acting 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.
traceoptions (advanced policy-based routing)

Syntax

```bash
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 intercommunication 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 | 222**
- **Understanding Advanced Policy-Based Routing | 213**
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]
[edit services icap-redirect]
```

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 | 32 |
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 | 382
Firewall User Authentication Overview
traceoptions (Services SSL)

Syntax

```plaintext
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size (Services) maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level [brief | detail | extensive | verbose];
  no-remote-trace;
  packet-filter {
    destination-ip;
    destination-port;
    source-ip;
    source-port;
  }
}
```

Hierarchy Level

```
[edit services ssl]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10. This statement is supported on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX. Junos OS Release 19.3R1 introduces `packet-filter` statement.

Description

Specify the trace file information.

Debug tracing on both Routing Engine and the Packet Forwarding Engine can be enabled for SSL proxy by using `[edit services ssl traceoptions]` command.

Options

- **file-name**—Specify the name of file in which to write trace information.
  - **files**—Specify the maximum number of trace files. Range: 2 to 1000.
• **match**—Specify the regular expression for lines to be logged. This statement is supported on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

• **no-world-readable size**—Do not allow any user to read the log file.

• **size**—Specify the maximum trace file size. Range: 10,240 to 1,073,741,824.

• **world-readable**—Allow any user to read the log file.

• **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **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.

• **level**—Set the level of debugging the output option.
  - **brief**—Match brief messages.
  - **detail**—Match detail messages.
  - **extensive**—Match extensive messages.
  - **verbose**—Match verbose messages.

• **no-remote-trace**—Set remote tracing as disabled.

• **packet-filter**—Set packet filter to capture the traffic details.
  - **destination-ip ipvaddress**—Specify a destination IP address.
    Range—1 through 65535
  - **destination-port port-number**—Specify a destination port.
  - **source-ip ip-address**—Specify a source IP address.
  - **source-port port-number**—Specify a source IP port.
    Range—1 through 65535

**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  |  382

Firewall User Authentication Overview
tunables

Syntax

tunables {
  drop-on-zone-mismatch;
  enable-logging;
  max-route-change \textit{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 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 \textit{value}—Configure the threshold for limiting the number of times a route can change for a session.

\textbf{Range:} 0-5
\textbf{Default:} 1

Required Privilege Level
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

RELATED DOCUMENTATION
underlay-interfaces

Syntax

underlay-interfaces interface-name {
    unit unit-number {
        link-type (IP | MPLS)
        priority priority-number;
    }
}

Hierarchy Level

[edit security advance-policy-based-routing]

Release Information
Statement introduced in Junos OS Release 18.4R1

Description
Configure the link priority and link type for the underlay interface in an APBR profile.

When a list of best paths that meet the SLA requirements are available for the application path, the path selection mechanism selects a path that matches the configured link preference (link type and priority). Paths are the WAN links that are used for forwarding the application traffic.

You can define the link type and priority for the underlay links in the APBR profile. Because the APBR rule is defined for an application or a group of applications, you can enforce the link preference at the application or application group level.

The link preference configuration is applied for the application traffic matching the APBR rule.

NOTE: If any of the parameters are not configured (link-type or priority) then the path selection mechanism follows the existing behavior. That is, applications traffic is assigned to a particular overlay link based on the SLA metrics of that overlay link only.

Options

link-type (IP | MPLS)—Select an MPLS or Internet link as the preferred path.

priority—Assign the priority for the link. If there are multiple paths available, the path that has the highest priority is selected.

Range: 1 through 255
**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 | 382
- *Firewall User Authentication Overview*
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 whitelist, 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  |  382

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

Configure the predefined URL categories in SSL proxy profile to exempt from SSL inspection. The URL category identification is leveraged from the Web filtering categories obtained from the unified threat management (UTM) module.

Before you specify URL category list, you must create a web filtering profile with custom objects using custom URL category or use predefined list. Next apply the feature profile to the UTM policy.

The following example uses a predefined profile, junos-wf-enhanced-default.

[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

Starting in Junos OS Release 17.4R1, you can use custom URL categories in SSL proxy profile.

Options

url-category-list—List of predefined or custom URL category.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Creating a Whitelist of Exempted URL Categories for SSL Proxy
Configuration Statements (Legacy Application Firewall)

rule (Application Firewall) | 660
rule-sets (Security Application Firewall) | 662
ssl-encryption | 664
then (Security Application Firewall) | 665
traceoptions (Security Application Firewall) | 667
profile (Application Firewall) | 669
rule (Application Firewall)

Syntax

```plaintext
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


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**

<table>
<thead>
<tr>
<th>Traditional Application Firewall</th>
<th>145</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule-sets (Security Application Firewall)</td>
<td>662</td>
</tr>
<tr>
<td>application-firewall (Application Services)</td>
<td>504</td>
</tr>
</tbody>
</table>
rule-sets (Security Application Firewall)

Syntax

```plaintext
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


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 Application Firewall with Application Groups | 158
ssl-encryption

Syntax

ssl-encryption (any | no | yes);

Hierarchy Level

[edit security application-firewall rule-sets rule-set-name rule rule-name match]

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Description

Distinguishes between encrypted and unencrypted SSL traffic as match criteria for the rule. In application firewall usage, this option lets you specify different actions for encrypted and unencrypted SSL traffic.

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

• any—Matches both encrypted and unencrypted SSL traffic.
• no—Matches unencrypted SSL traffic only.
• yes—Matches encrypted SSL traffic only.

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 | 382
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


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 Application Firewall with Application Groups | 158
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]
[edit tenants tenant-name security application-firewall]

Release Information

Statement introduced in Junos OS Release 11.1.
The statement `set tenant tenant-name security application-firewall` is introduced in Junos OS Release 18.4R1.

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 intercommunication 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**

- Traditional Application Firewall | 145
profile (Application Firewall)

Syntax

```bash
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**
- Traditional Application Firewall | 145
 Operational Commands

clear security advance-policy-based-routing sla statistics  | 675

clear security application-firewall rule-set statistics  | 676

clear security application-firewall rule-set statistics logical-system  | 677

clear services application-identification application-statistics  | 679

clear services application-identification application-statistics cumulative  | 680

clear services application-identification application-statistics interval  | 681

clear services application-identification application-system-cache (Junos OS)  | 682

clear services application-identification counter (Values)  | 684

clear services application-identification packet-capture counters  | 686

clear services icap-redirect statistic  | 687

clear services ssl proxy statistics  | 689

request security pki ca-certificate ca-profile-group load  | 690

request security pki local-certificate export  | 692

request security pki local-certificate generate-self-signed  | 693

request security pki local-certificate load  | 695
request services application-identification application | 696
request services application-identification clear packet-capture all | 698
request services application-identification download | 699
request services application-identification download status | 701
request services application-identification group | 702
request services application-identification install | 704
request services application-identification install status | 705
request services application-identification proto-bundle-status | 706
request services application-identification uninstall | 707
request services application-identification uninstall status | 708
show class-of-service application-traffic-control counter | 709
show class-of-service application-traffic-control statistics rate-limiter | 715
show class-of-service application-traffic-control statistics rule | 719
show security advance-policy-based-routing detail | 722
show security advanced-policy-based-routing policy-name | 726
show security advance-policy-based-routing profile | 731
show security advance-policy-based-routing statistics | 733
show security advance-policy-based-routing status | 739
show security advance-policy-based-routing sla active-probe-statistics | 740
show security advance-policy-based-routing sla profile (Application Name) | 742
show security advance-policy-based-routing sla profile (Application Name) | 744
show security advance-policy-based-routing sla profile (Next-Hop) | 746
show security advance-policy-based-routing sla profile (Status) | 751
show security advance-policy-based-routing sla statistics | 753
show security advance-policy-based-routing sla status | 755
show security advance-policy-based-routing sla version | 756
show security application-firewall rule-set | 757
show security application-firewall rule-set logical-system | 762
show security application-tracking counters | 766
show security flow session | 768
show security flow session ssl | 778
show security flow session application-firewall | 782
show security pki ca-certificate | 790
show security pki local-certificate (View) | 795
show security policies | 803
show services application-identification application | 820
show services application-identification application-system-cache (View) | 829
show services application-identification commit-status | 834
show services application-identification counter (AppSecure) | 836
show services application-identification entries | 844
show services application-identification group | 847
show services application-identification packet-capture counters | 850
show services application-identification statistics applications | 852
show services application-identification statistics application-groups | 856
show services application-identification status | 860
show services application-identification version | 869
show services icap-redirect server status | 871
show services icap-redirect statistic | 873
show services icap-redirect status | 877
show services service-redirect statistic | 880
show services ssl droplogs | 882
show services ssl initiation counters | 884
show services ssl initiation profile | 889
show services ssl proxy certificate-cache entries | 893
show services ssl proxy certificate-cache statistics | 896
show services ssl proxy counters | 898
show services ssl proxy profile | 903
show services ssl proxy statistics | 906
show services ssl proxy status | 909
show services ssl proxy session-cache entries | 911
show services ssl proxy session-cache statistics | 916
show services ssl proxy statistics | 918
show services ssl certificate | 921
show services ssl session | 926
show services ssl termination counters | 929
show services ssl termination profile | 934
show services web-proxy dns forwarding-cache | 939
show services web-proxy dns global-cache statistics | 941
show services web-proxy session | 943
clear security advance-policy-based-routing sla statistics

Syntax

```
clear security advance-policy-based-routing sla statistics
```

Release Information
Command introduced in Junos OS Release 15.1X49-D130.

Description
Clears SLA rule-specific statistics and counters.

Required Privilege Level
view

RELATED DOCUMENTATION

- Application Quality of Experience | 283
- Advanced Policy-Based Routing | 213

Output Fields
This command produces no output.

Sample Output
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` | 757 |

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 Systems 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` | 762

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show services application-identification statistics applications</td>
<td>852</td>
</tr>
<tr>
<td>show services application-identification statistics application-groups</td>
<td>856</td>
</tr>
<tr>
<td>clear services application-identification application-statistics interval</td>
<td>681</td>
</tr>
<tr>
<td>clear services application-identification application-statistics cumulative</td>
<td>680</td>
</tr>
</tbody>
</table>

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 | 852 |
| show services application-identification statistics application-groups | 856 |
| clear services application-identification application-statistics | 679 |
| clear services application-identification application-statistics interval | 681 |

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 | 852
- show services application-identification statistics application-groups | 856
- clear services application-identification application-statistics | 679
- clear services application-identification application-statistics cumulative | 680

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 ) >
   <logical-system (logical-system-name | all | root-logical-system)>
   <tenant (tenant-name | all)>
```

Release Information

Command introduced in Junos OS Release 10.2.
logical-system option introduced in Junos OS Release 18.3R1.
tenant option introduced in Junos OS Release 19.4R1.

Description

Clear Junos OS application identification application system cache.

Options

none—Clears 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

logical-system logical-system-name—(Optional) Clears the application system cache of the specified logical system.

logical-system all—(Optional) Clears the application system cache of all the logical systems.

root-logical-system—(Optional) Clears the application system cache of the root logical system.

tenant tenant-name—(Optional) Clears the application system cache of the specified tenant system.

tenant all—(Optional) Clears the application system cache of all the tenant systems.

Required Privilege Level

clear
RELATED DOCUMENTATION

show services application-identification application-system-cache (View) | 829

Output Fields
This command produces no output.
clear services application-identification counter (Values)

Syntax

```
clear services application-identification counter
<ssl-encrypted-sessions>
<logical-system (logical-system-name | all | root-logical-system)>
<tenant (tenant-name | all)>
```

Release Information


`logical-system` option introduced in Junos OS Release 18.3R1.

`tenant` option introduced in Junos OS Release 19.4R1.

Description

Resets all the Junos OS application identification counter values.

Options

- `ssl-encrypted-sessions`—(Optional) Resets application identification counter values for SSL encrypted sessions.
- `logical-system logical-system-name`—(Optional) Resets application identification counter values of the specified logical system.
- `logical-system all`—(Optional) Resets application identification counter values of all the logical systems.
- `root-logical-system`—(Optional) Resets application identification counter values of the root logical system.
- `tenant tenant-name`—(Optional) Resets application identification counter values of the specified tenant system.
- `tenant all`—(Optional) Resets application identification counter values of all the tenant systems.

Required Privilege Level

clear

RELATED DOCUMENTATION

- show services application-identification counter (AppSecure) | 836

List of Sample Output

`clear services application-identification counter on page 685`
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

```

```
clear services application-identification counter logical-system all
user@host> clear services application-identification counter logical-system all

  appid counter cleared

```

```
clear services application-identification counter
user@host:TSYS1> clear services application-identification counter

  appid counter cleared

```

```
clear services application-identification counter tenant all
user@host> clear services application-identification counter tenant all

  appid counter cleared

```
clear services application-identification packet-capture counters

Syntax

```
clear services application-identification packet-capture counters
```

Release Information

Statement introduced in Junos OS Release 20.2R1.

Description

Clear all packet capture counters generated for unknown application traffic.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

- Configure Packet Capture of Unknown Application Traffic | 49
- packet-capture | 583
- show services application-identification packet-capture counters | 850
- request services application-identification clear packet-capture all | 698

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

```
user@host> clear services application-identification packet-capture counters
Packet-capture counters cleared
```
clear services icap-redirect statistic

Syntax

```
clear services icap-redirect statistic
<all-logical-systems-tenants>
<root-logical-system>
<logical-system (logical-system-name | all)>
<tenant (tenant-name | all)>
```

Release Information

Command introduced in Junos OS Release 18.3R1.
tenant option introduced in Junos OS Release 20.1R1.

Description

Clears the ICAP services redirects statistic. ICAP services redirect redirects the HTTP or HTTPS traffic to any third-party server. The security device acts as an SSL proxy server and decrypts the pass-through traffic with the proper SSL profile under a security policy.

Options

- **all-logical-systems-tenants**—(Optional) Clears the ICAP services redirects statistic for the root logical system, all logical systems, and all tenant systems.

- **logical-system logical-system-name**—(Optional) Clears the ICAP services redirects statistic for the specified logical system.

- **logical-system all**—(Optional) Clears the ICAP services redirects statistic for all the logical systems.

- **root-logical-system**—(Optional) Clears the ICAP services redirects statistic for the root logical system.

- **tenant tenant-name**—(Optional) Clears the ICAP services redirects statistic for the specified tenant system.

- **tenant all**—(Optional) Clears the ICAP services redirects statistic for all the tenant systems.

Required Privilege Level

clear

RELATED DOCUMENTATION

- ICAP Service Redirect | 416

List of Sample Output

clear services icap-redirect statistic root-logical-system on page 688
clear services icap-redirect statistic all-logical-systems-tenants on page 688
clear services icap-redirect statistic logical-system LSYS1 on page 688
clear services icap-redirect statistic tenant TSYS1 on page 688
clear services icap-redirect statistic on page 688

## Sample Output

**clear services icap-redirect statistic root-logical-system**

```
user@host>  clear services icap-redirect statistic root-logical-system

STATISTICS CLEARED
```

**clear services icap-redirect statistic all-logical-systems-tenants**

```
user@host>  clear services icap-redirect statistic all-logical-systems-tenants

STATISTICS CLEARED
```

**clear services icap-redirect statistic logical-system LSYS1**

```
user@host>  clear services icap-redirect statistic logical-system LSYS1

STATISTICS CLEARED
```

**clear services icap-redirect statistic tenant TSYS1**

```
user@host>  clear services icap-redirect statistic tenant TSYS1

STATISTICS CLEARED
```

**clear services icap-redirect statistic**

```
user@host:TSYS1>  clear services icap-redirect statistic

STATISTICS CLEARED
```
clear services ssl proxy statistics

Syntax

```plaintext
clear services ssl proxy statistics
```

Release Information
Command introduced in Junos OS Release 12.1.
The `logical system` option is introduced in Junos OS Release 19.1R1.

Description
Clear services SSL proxy statistics. An SSL proxy profile defines SSL behavior for the SRX Series device.

Options
`logical-system`—Clear the ssl proxy statistics.

Required Privilege Level
clear

RELATED DOCUMENTATION

| show services ssl proxy statistics | 906 |

Output Fields
This command produces no output.
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 | 790 |
| Understanding Certificates and PKI |

List of Sample Output

request security pki ca-certificate ca-profile-group load (default) on page 691
request security pki ca-certificate ca-profile-group load (path/filename) on page 691

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.
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 692

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.

e-mail 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
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=abcd 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 695

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.

disable—(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 | 820

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 clear packet-capture all

Syntax

```
request services application-identification clear packet-capture all
```

Release Information
Statement introduced in Junos OS Release 20.2R1.

Description
Clear all packet capture files generated for unknown application traffic.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

- Configure Packet Capture of Unknown Application Traffic | 49
- packet-capture | 583
- show services application-identification packet-capture counters | 850
- clear services application-identification packet-capture counters | 686

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 clear packet-capture all
Packet-capture file(s) deleted
```
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 | 701 |
| request services application-identification install | 704 |

List of Sample Output
request services application-identification download on page 699

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 | 699 |

List of Sample Output
request services application-identification download status on page 701

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.

**disable**—(Optional) Disable a predefined 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

NOTE: In configuration mode, if an uncommitted action is pending, the `request services application-identification group copy` command fails.

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.

RELATED DOCUMENTATION
Output Fields
When you enter this command, the system provides feedback on the status of your request.

Sample Output

```bash
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 | 705
- request services application-identification download | 699

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 | 704

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 | 704

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


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` | 704

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 | 707 |

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 Application Quality of Service | 196 |

List of Sample Output

- `show class-of-service application-traffic-control counter on page 710`
- `show class-of-service application-traffic-control counter (Unified Policies) on page 710`
- `show class-of-service application-traffic-control counter logical-system LSYS1 on page 711`
- `show class-of-service application-traffic-control counter logical-system all on page 711`
- `show class-of-service application-traffic-control counter tenant TSYS1 on page 712`
- `show class-of-service application-traffic-control counter tenant all on page 713`

Output Fields

Table 52 on page 709 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 52: show class-of-service application-traffic-control counter Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pic</td>
<td>PIC number of the accumulated statistics.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.</td>
</tr>
<tr>
<td>Sessions processed</td>
<td>The number of sessions where the class of service was checked.</td>
</tr>
</tbody>
</table>
### Table 52: show class-of-service application-traffic-control counter Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sessions marked</strong></td>
<td>The number of sessions marked based on application-aware DSCP marking.</td>
</tr>
<tr>
<td><strong>Sessions honored</strong></td>
<td>The number of sessions honored based on application-aware traffic honoring.</td>
</tr>
<tr>
<td><strong>Sessions rate limited</strong></td>
<td>The number of sessions that have been rate limited.</td>
</tr>
<tr>
<td><strong>Client-to-server flows rate limited</strong></td>
<td>The number of client-to-server flows that have been rate limited.</td>
</tr>
<tr>
<td><strong>Server-to-client flows rate limited</strong></td>
<td>The number of server-to-client flows that have been rate limited.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show class-of-service application-traffic-control counter

user@host> show class-of-service application-traffic-control counter

pic: 2/1

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>300</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>200</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>100</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>100</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>70</td>
</tr>
</tbody>
</table>

pic: 2/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>400</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>300</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>200</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>200</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>100</td>
</tr>
</tbody>
</table>
```

show class-of-service application-traffic-control counter (Unified Policies)

User@host> show class-of-service application-traffic-control counter
<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>2</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>1</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>1</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>1</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>1</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>1</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>1</td>
</tr>
</tbody>
</table>

**show class-of-service application-traffic-control counter logical-system LSYS1**

user@host>**show class-of-service application-traffic-control counter logical-system LSYS1**

Logical System: LSYS1

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>1</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

**show class-of-service application-traffic-control counter logical-system all**

user@host>**show class-of-service application-traffic-control counter logical-system all**

Logical System: root-logical-system

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>
### Logical System: LSYS0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

### Logical System: LSYS1

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>1</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

### Logical System: LSYS2

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

**show class-of-service application-traffic-control counter tenant TSYS1**

```bash
user@host> show class-of-service application-traffic-control counter tenant TSYS1
```
Tenant System: TSYS1

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>1</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

show class-of-service application-traffic-control counter tenant all

user@host> show class-of-service application-traffic-control counter tenant all

Tenant System: root-logical-system

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

Tenant System: TSYS0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

Tenant System: TSYS1
<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>1</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>

Tenant System: TSYS2

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions marked</td>
<td>0</td>
</tr>
<tr>
<td>Sessions honored</td>
<td>0</td>
</tr>
<tr>
<td>Sessions rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client flows rate limited</td>
<td>0</td>
</tr>
<tr>
<td>Session default ruleset hit</td>
<td>0</td>
</tr>
<tr>
<td>Session ignored no default ruleset</td>
<td>0</td>
</tr>
</tbody>
</table>
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 Application Quality of Service | 196 |

List of Sample Output

- show class-of-service application-traffic-control statistics rate-limiter on page 716
- show class-of-service application-traffic-control statistics rate-limiter logical-system LSYS1 on page 717
- show class-of-service application-traffic-control statistics rate-limiter logical-system all on page 717
- show class-of-service application-traffic-control statistics rate-limiter tenant TSYS1 on page 717
- show class-of-service application-traffic-control statistics rate-limiter tenant all on page 717

Output Fields

Table 53 on page 715 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 53: show class-of-service application-traffic-control statistics rate-limiter Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pic</td>
<td>PIC number.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.</td>
</tr>
<tr>
<td>Ruleset</td>
<td>The rule set applied on the session.</td>
</tr>
</tbody>
</table>
### Table 53: show class-of-service application-traffic-control statistics rate-limiter Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>The application match for applying the rule set.</td>
</tr>
<tr>
<td><strong>Client-to-server</strong></td>
<td>The rate limiter applied from client to server.</td>
</tr>
<tr>
<td><strong>Rate(kbps)</strong></td>
<td>The rate in the client-to-server direction</td>
</tr>
<tr>
<td><strong>Server-to-client</strong></td>
<td>The rate limiter applied from server to client.</td>
</tr>
<tr>
<td><strong>Rate(kbps)</strong></td>
<td>The rate in the server-to-client direction.</td>
</tr>
</tbody>
</table>

---

**Sample Output**

```bash
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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
</table>
| show class-of-service application-traffic-control statistics rate-limiter logical-system LSYS1 | Logical System: LSYS1  
        pic: 0/0                                                                 |
| user@host> show class-of-service application-traffic-control statistics rate-limiter logical-system LSYS1 | Logical System: LSYS1  
        pic: 0/0                                                                 |
| show class-of-service application-traffic-control statistics rate-limiter logical-system all | Logical System: root-logical-system  
        pic: 0/0  
        Logical System: LSYS0  
        pic: 0/0  
        Logical System: LSYS1  
        pic: 0/0  
        Logical System: LSYS2  
        pic: 0/0                                                                 |
| user@host> show class-of-service application-traffic-control statistics rate-limiter logical-system all | Logical System: root-logical-system  
        pic: 0/0                                                                 |
| show class-of-service application-traffic-control statistics rate-limiter tenant TSYS1 | Tenant System: LSYS1  
        pic: 0/0                                                                 |
| user@host> show class-of-service application-traffic-control statistics rate-limiter tenant TSYS1 | Tenant System: LSYS1  
        pic: 0/0                                                                 |
| show class-of-service application-traffic-control statistics rate-limiter tenant all | Tenant System: root-logical-system  
        pic: 0/0                                                                 |
| user@host> show class-of-service application-traffic-control statistics rate-limiter tenant all | Tenant System: root-logical-system  
        pic: 0/0                                                                 |
Tenant System: TSYS0
pic: 0/0
Tenant System: TSYS1
pic: 0/0
Tenant System: TSYS2
pic: 0/0
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 Application Quality of Service | 196

List of Sample Output

- show class-of-service application-traffic-control statistics rule on page 720
- show class-of-service application-traffic-control statistics rule logical-system LSYS1 on page 720
- show class-of-service application-traffic-control statistics rule logical-system all on page 720
- show class-of-service application-traffic-control statistics rule tenant TSYS1 on page 721
- show class-of-service application-traffic-control statistics rule tenant all on page 721

Output Fields

Table 54 on page 719 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 54: show class-of-service application-traffic-control statistics rule Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| pic        | PIC number where the rule is applied.  
  NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices. |
| Ruleset    | The rule set containing the rule. |
Table 54: show class-of-service application-traffic-control statistics rule Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>The rule to which the statistic applies.</td>
</tr>
<tr>
<td>Hits</td>
<td>The number of times a match for the rule was encountered.</td>
</tr>
</tbody>
</table>

**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     https-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     https-rule     300
my-ruleset-2     telnet-rule    400
my-ruleset-2     smtp-rule      500

show class-of-service application-traffic-control statistics rule logical-system LSYS1

user@host>show class-of-service application-traffic-control statistics rule logical-system LSYS1

Logical System: LSYS1

pic: 0/0

show class-of-service application-traffic-control statistics rule logical-system all

user@host>show class-of-service application-traffic-control statistics rule logical-system all
```
Logical System: root-logical-system
pic: 0/0

Logical System: L SYS 0
pic: 0/0

Logical System: L SYS 1
pic: 0/0

Logical System: L SYS 2
pic: 0/0

show class-of-service application-traffic-control statistics rule tenant T SYS 1
user@host> show class-of-service application-traffic-control statistics rule tenant T SYS 1

Tenant System: T SYS 1
pic: 0/0

show class-of-service application-traffic-control statistics rule tenant all
user@host> show class-of-service application-traffic-control statistics rule tenant all

Tenant System: root-logical-system
pic: 0/0
Tenant System: T SYS 0
pic: 0/0
Tenant System: T SYS 1
pic: 0/0
Tenant System: T SYS 2
pic: 0/0
show security advance-policy-based-routing detail

Syntax

```
show security advance-policy-based-routing detail
```

Release Information
Command introduced in Junos OS Release 15.1X49-D60. The option scheduler is added in Junos OS Release 18.4R1.

Description
Display a summary of all APBR policies configured on the device.

You can use this command to understand the details of an APBR policy such as:

- Name, status, zone-context of the APBR policy.
- The number of times traffic matches the APBR policy and the APBR profile is applied for a session.

Options
- **count**—Display the number of configured APBR policies.
  - Range: 1 to 65535
- **detail**—Display a detailed view of all of the APBR policies configured on the device.
- **from-zone**—Display specific zone details applicable to the APBR policy.
- **logical-system**—Display the logical system name.
- **root-logical-system**—Display information about the default root-logical-system.
- **start**—Display the policy from the given position.
  - Range: 1 to 65535

Required Privilege Level
- view

RELATED DOCUMENTATION
- Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management
  Solution | 222

Output Fields
Table 55 on page 723 lists the output fields for the **show security advance-policy-based-routing detail** command. Output fields are listed in the approximate order in which they appear.

**Table 55: show security advance-policy-based-routing statistics**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Name of the APBR policy</td>
</tr>
<tr>
<td>Enabled</td>
<td>Status of the policy (enabled or disabled)</td>
</tr>
<tr>
<td>Policy type</td>
<td>Type of the policy.</td>
</tr>
<tr>
<td>Index</td>
<td>An internal number associated with the policy.</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Number of the policy within a given context. For example, three policies that are applicable in a from-zone A-to-zone B context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zone C-to-zone D context, four policies might have sequence numbers 1, 2, 3, and 4.</td>
</tr>
<tr>
<td>From zone</td>
<td>The zone on which APBR profile is applied to.</td>
</tr>
<tr>
<td>Source addresses</td>
<td>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.</td>
</tr>
<tr>
<td>Destination addresses</td>
<td>The names and corresponding IP addresses of the destination addresses (or address sets) for a policy as entered in the destination zone's address book. A packet's destination address must match one of these addresses for the policy to apply to it.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of a preconfigured or custom application, or any if no application is specified.</td>
</tr>
<tr>
<td>ALG</td>
<td>If an ALG is associated with the session, the name of the ALG. Otherwise, 0.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol name or numeric value of the traffic.</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Elapsed time without activity after which the application is terminated.</td>
</tr>
<tr>
<td>Source port range</td>
<td>Range of matching source ports defined in the policy.</td>
</tr>
<tr>
<td>Destination port range</td>
<td>Range of matching destination ports defined in the policy.</td>
</tr>
<tr>
<td>APBR-Profile</td>
<td>Name of the APBR profile</td>
</tr>
<tr>
<td>Source identities</td>
<td>User details specified in the source-identity field of the named policy.</td>
</tr>
</tbody>
</table>
Table 55: show security advance-policy-based-routing statistics (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler name</td>
<td>Name of the scheduler associated with APBR policy.</td>
</tr>
</tbody>
</table>

Sample Output

show security advance-policy-based-routing statistics
user@host> show security advance-policy-based-routing detail

Policy: SLA1, State: enabled, Index: 5
Policy Type: Configured
Sequence number: 1
From 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]
APBR-Profile: profile1
Scheduler name: scheduler-1

Sample Output

show security advanced-policy-based-routing detail (Junos OS Release 19.1R1)
user@host> show security advanced-policy-based-routing detail

Policy: p1, State: enabled, Index: 4
  Sequence number: 1
  From 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]
APBR Profile: apbr-prl

Source identities:
  dev_user
show security advanced-policy-based-routing policy-name

Syntax

```
show security advanced-policy-based-routing policy-name policy-name
<count | detail | from-zone |logical-system |root-logical-system | start>
```

Release Information

Command introduced in Junos OS Release 18.2R1.

Description

Display a summary of all APBR policies configured on the device.

You can use this command to understand the details of an APBR policy such as:

- Name, status, zone-context of the APBR policy.
- The number of times the traffic matches the APBR policy and APBR profile applied for the session.

Options

- count— Display the number of configured APBR policies.
  - **Range:** 1 to 65535
- detail—Display a detailed view of all of the APBR policies configured on the device.
- from-zone—Display specific zone details applicable to the APBR policy.
- logical-system—Display the logical system name.
- root-logical-system—Display information about the default root-logical-system.
- start—Display the policy from the given position.
  - **Range:** 1 to 65535

Required Privilege Level

View

RELATED DOCUMENTATION

Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management
Solution | 222
Output Fields

Table 56 on page 727 lists the output fields for the `show security advanced-policy-based-routing policy-name` command. Output fields are listed in the approximate order in which they appear.

Table 56: show security advanced-policy-based-routing policy-name

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Name of the APBR policy.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the policy. The policy is in one of the following state:</td>
</tr>
<tr>
<td></td>
<td>• enabled: The policy can be used in the policy lookup process, which determines</td>
</tr>
<tr>
<td></td>
<td>access rights for a packet and the action taken in regard to it.</td>
</tr>
<tr>
<td></td>
<td>• disabled: The policy cannot be used in the policy lookup process, and therefore</td>
</tr>
<tr>
<td></td>
<td>it is not available for access control.</td>
</tr>
<tr>
<td>Index</td>
<td>Internal number associated with the policy.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>Number of the policy within a given context. For example, three policies that are</td>
</tr>
<tr>
<td></td>
<td>applicable in a from-zone A-to-zone B context might be ordered with sequence</td>
</tr>
<tr>
<td></td>
<td>numbers 1, 2, 3. Also, in a from-zone C-to-zone D context, four policies might</td>
</tr>
<tr>
<td></td>
<td>have sequence numbers 1, 2, 3, 4.</td>
</tr>
<tr>
<td>From zone</td>
<td>Name of the source zone.</td>
</tr>
<tr>
<td>Source addresses</td>
<td>The names of the source addresses for a policy. Address sets are resolved to their</td>
</tr>
<tr>
<td></td>
<td>individual names.</td>
</tr>
<tr>
<td>Destination addresses</td>
<td>Name of the destination address (or address set) as it was entered in the destination zone's address book</td>
</tr>
<tr>
<td>Applications</td>
<td>Name of a preconfigured or custom application whose type the packet matches,</td>
</tr>
<tr>
<td></td>
<td>as specified at configuration time.</td>
</tr>
<tr>
<td>APBR Profile</td>
<td>Name of the applicable ABPR profile.</td>
</tr>
</tbody>
</table>

Table 57 on page 727 lists the output fields for the `show security advanced-policy-based-routing detail` command. Output fields are listed in the approximate order in which they appear.

Table 57: show security advanced-policy-based-routing detail

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APBR Policy</td>
<td>Name of the APBR policy.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>Status of the policy. The policy is in one of the following state:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• disabled: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.</td>
</tr>
<tr>
<td>Index</td>
<td>Internal number associated with the policy.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>Number of the policy within a given context. For example, three policies that are applicable in a from-zone A-to-zone B context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zone C-to-zone D context, four policies might have sequence numbers 1, 2, 3, 4.</td>
</tr>
<tr>
<td>From zone</td>
<td>Name of the source zone.</td>
</tr>
<tr>
<td>Source addresses</td>
<td>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.</td>
</tr>
<tr>
<td>Destination addresses</td>
<td>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.</td>
</tr>
<tr>
<td>Applications</td>
<td>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</td>
</tr>
<tr>
<td></td>
<td>• IP protocol: The Internet protocol used by the application—for example, TCP, UDP, ICMP.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Inactivity timeout: Elapsed time without activity after which the application is terminated.</td>
</tr>
<tr>
<td></td>
<td>• Source port range: The low-high source port range for the session application.</td>
</tr>
<tr>
<td></td>
<td>• Destination port range: The low-high destination port range for the session application.</td>
</tr>
<tr>
<td>APBR Profile</td>
<td>Name of the applicable ABPR profile.</td>
</tr>
</tbody>
</table>
Table 58 on page 729 lists the output fields for the `show security advanced-policy-based-routing from-zone` command. Output fields are listed in the approximate order in which they appear.

Table 58: show security advanced-policy-based-routing from-zone

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From zone</td>
<td>Name of the source zone.</td>
</tr>
<tr>
<td>Policy count</td>
<td>Number of APBR policies configured for the zone.</td>
</tr>
</tbody>
</table>

Table 59 on page 729 lists the output fields for the `show security advanced-policy-based-routing hit-count` command. Output fields are listed in the approximate order in which they appear.

Table 59: show security advanced-policy-based-routing hit-count

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical system</td>
<td>Name of the associated logical system.</td>
</tr>
<tr>
<td>Index</td>
<td>Internal number associated with the policy.</td>
</tr>
<tr>
<td>From zone</td>
<td>Name of the source zone.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the APBR policy.</td>
</tr>
<tr>
<td>Policy count</td>
<td>Number of hits for each security policy.</td>
</tr>
<tr>
<td>Number of policy</td>
<td>Number of security policies for which hit counts are displayed.</td>
</tr>
</tbody>
</table>

Sample Output

`show security advanced-policy-based-routing detail`

```
user@host> show security advanced-policy-based-routing detail

Policy: p1, State: enabled, Index: 4
  Sequence number: 1
  From 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]
APBR Profile: apbr-pr1

show security advanced-policy-based-routing from-zone

user@host> show security advanced-policy-based-routing from-zone trust

From zone: trust
   Policy: p1, State: enabled, Index: 4, Sequence number: 1
      Source addresses: any
      Destination addresses: any
      Applications: any
      APBR Profile: apbr-pr1

1

show security advanced-policy-based-routing hit-count

user@host> show security advanced-policy-based-routing hit-count

Logical system: root-logical-system

<table>
<thead>
<tr>
<th>Index</th>
<th>From zone</th>
<th>Name</th>
<th>Hit count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>trust</td>
<td>p1</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of policy: 1

show security advanced-policy-based-routing policy-name

user@host> show security advanced-policy-based-routing policy-name sla_policy1

From zone: trust
   APBR Policy: sla_policy1, State: enabled, Index: 7, Sequence number: 1
      Source addresses: any
      Destination addresses: any
      Applications: any
      APBR profile: apbr-pr-default
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 | 222

Output Fields

Table 60 on page 731 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 60: show security advance-policy-based-routing profile

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pic</td>
<td>PIC number of the accumulated statistics.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340,</td>
</tr>
<tr>
<td></td>
<td>SRX345, SRX550M, and SRX1500 devices.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the advanced policy-based (APBR) routing profile.</td>
</tr>
<tr>
<td>Zone</td>
<td>The zone on which APBR profile is applied to.</td>
</tr>
</tbody>
</table>
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 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
Displays the statistics counter for the 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 is consulted to identify application traffic.

Required Privilege Level
view

RELATED DOCUMENTATION

Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution | 222

Output Fields
Table 56 on page 727 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 61: show security advance-policy-based-routing statistics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Processed</td>
<td>The number of sessions processed for the application-based routing.</td>
</tr>
<tr>
<td>ASC Success</td>
<td>The number of times the presence of an entry in the application system cache (ASC) is found.</td>
</tr>
<tr>
<td>Rule match success</td>
<td>The number of times the application traffic matches the APBR profile.</td>
</tr>
</tbody>
</table>
Table 61: show security advance-policy-based-routing statistics (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route modified</td>
<td>The number of times the APBR is applied for the session.</td>
</tr>
<tr>
<td>AppID Requested</td>
<td>The number of times AppID is consulted to identify application traffic.</td>
</tr>
</tbody>
</table>

Table 62 on page 734 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 62: show security advance-policy-based-routing statistics (Advanced Policy-Based Routing Midstream Support)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Processed</td>
<td>The number of sessions processed for the application-based routing.</td>
</tr>
<tr>
<td>AppID cache hits</td>
<td>The number of times the presence of an entry in the application system cache (ASC) is found.</td>
</tr>
<tr>
<td>AppID Requested</td>
<td>The number of times AppID was consulted to identify application traffic.</td>
</tr>
<tr>
<td>Rule matches</td>
<td>The number of times the application traffic matches the APBR profile.</td>
</tr>
<tr>
<td>Route changed on cache hits</td>
<td>The number of times the APBR is applied for the session.</td>
</tr>
<tr>
<td>Route changed midstream</td>
<td>Number of times a route is changed for a session.</td>
</tr>
<tr>
<td>Zone mismatch</td>
<td>No of times a zone for an interface is changed in the middle of a session.</td>
</tr>
<tr>
<td>Drop on zone mismatch</td>
<td>Number of times a session is terminated because of change of zone in the middle of the session.</td>
</tr>
</tbody>
</table>

Table 63 on page 734 lists the output fields for the **show security advance-policy-based-routing statistics** command starting in Junos OS Release 19.3R1 and later releases. Output fields are listed in the approximate order in which they appear.

Table 63: show security advance-policy-based-routing statistics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Processed</td>
<td>The number of sessions processed for the application-based routing.</td>
</tr>
<tr>
<td>App rule hit on cache hit</td>
<td>The number of times a rule with a matching entry in the application system cache (ASC) is found.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>App rule hit on HTTP Proxy/ALG</strong></td>
<td>The number of times a rule matching with the application obtained from ALG or secure Web (HTTP) proxy is found.</td>
</tr>
<tr>
<td><strong>Midstream disabled rule hit on cache hit</strong></td>
<td>The number of times a rule with a disabled midstream has matching entry in the ASC.</td>
</tr>
<tr>
<td><strong>URL cat rule hit on cache hit</strong></td>
<td>The number of times a rule with defined URL categories in ASC is found.</td>
</tr>
<tr>
<td><strong>DSCP rule hit on first packet</strong></td>
<td>The number of times the rule with defined DSCP value is matched for the first session.</td>
</tr>
<tr>
<td><strong>App and DSCP hit on first packet</strong></td>
<td>The number of times the rule with defined DSCP value and application is matched for the first session.</td>
</tr>
<tr>
<td><strong>App rule hit midstream</strong></td>
<td>The number of times a route is changed in the middle of a session because of the rule with defined application is matched.</td>
</tr>
<tr>
<td><strong>URL cat rule hit midstream</strong></td>
<td>The number of times a route is changed in the middle of a session because of the rule with defined URL categories is matched.</td>
</tr>
<tr>
<td><strong>App and DSCP rule hit midstream</strong></td>
<td>The number of times the rule with DSCP value and application is matched for the midstream session.</td>
</tr>
<tr>
<td><strong>Midstream disabled rule hit midstream</strong></td>
<td>The number of times a route remains unchanged in the middle of a session after rule with defined application is matched.</td>
</tr>
<tr>
<td><strong>DSCP rule hit midstream</strong></td>
<td>The number of times the rule with DSCP value is matched for the midstream session.</td>
</tr>
<tr>
<td><strong>Route changed on cache hits</strong></td>
<td>Number of times a route is changed for a session because of the APBR applied for the session.</td>
</tr>
<tr>
<td><strong>Route changed on HTTP Proxy/ALG</strong></td>
<td>Number of times a route is changed because of the rule match for secure Web (HTTP) proxy or ALG applied for the session.</td>
</tr>
<tr>
<td><strong>Route changed midstream</strong></td>
<td>Number of times a route is changed in the middle of a session because of the APBR applied for the session.</td>
</tr>
<tr>
<td><strong>Zone mismatch</strong></td>
<td>No of times a zone for an interface is changed in the middle of a session.</td>
</tr>
</tbody>
</table>
Table 63: show security advance-policy-based-routing statistics (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop on zone mismatch</td>
<td>Number of times a session is terminated because of change of zone in the middle of the session.</td>
</tr>
<tr>
<td>Next hop not found</td>
<td>Number of times a session is terminated because next-hop IP address was not reachable.</td>
</tr>
<tr>
<td>Application Services Bypass</td>
<td>The number of times the application services are bypassed for the session.</td>
</tr>
</tbody>
</table>

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 statistics (Changed Options from Junos OS Release 18.4R1)

user@host> show security advance-policy-based-routing statistics
### Advance Profile Based Routing statistics:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions Processed</td>
<td>2</td>
</tr>
<tr>
<td>App rule hit on cache hit</td>
<td>1</td>
</tr>
<tr>
<td>URL cat rule hit on cache hit</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit midstream</td>
<td>1</td>
</tr>
<tr>
<td>URL cat rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>Route changed on cache hits</td>
<td>1</td>
</tr>
<tr>
<td>Route changed midstream</td>
<td>1</td>
</tr>
<tr>
<td>Zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Drop on zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Next hop not found</td>
<td>0</td>
</tr>
</tbody>
</table>

### show security advance-policy-based-routing statistics (Changed Options from Junos OS Release 19.1R1)

```
user@host> show security advance-policy-based-routing statistics
```

### Advance Profile Based Routing statistics:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions Processed</td>
<td>110</td>
</tr>
<tr>
<td>AppID cache hits</td>
<td>110</td>
</tr>
<tr>
<td>AppID requested</td>
<td>0</td>
</tr>
<tr>
<td>Rule matches</td>
<td>2</td>
</tr>
<tr>
<td>Route changed on cache hits</td>
<td>1</td>
</tr>
<tr>
<td>Route changed midstream</td>
<td>1</td>
</tr>
<tr>
<td>Zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Drop on zone mismatch</td>
<td>0</td>
</tr>
<tr>
<td>Next hop not found</td>
<td>0</td>
</tr>
<tr>
<td>Application Services Bypass</td>
<td>1</td>
</tr>
</tbody>
</table>

### show security advance-policy-based-routing statistics (Changed Options from Junos OS Release 19.3R1)

```
user@host> show security advance-policy-based-routing statistics
```

### Advance Profile Based Routing statistics:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions Processed</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit on cache hit</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit on HTTP Proxy/ALG</td>
<td>0</td>
</tr>
<tr>
<td>URL cat rule hit on cache hit</td>
<td>0</td>
</tr>
<tr>
<td>DSCP rule hit on first packet</td>
<td>0</td>
</tr>
<tr>
<td>App and DSCP hit on first packet</td>
<td>0</td>
</tr>
<tr>
<td>App rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>URL cat rule hit midstream</td>
<td>0</td>
</tr>
<tr>
<td>App and DSCP rule hit midstream</td>
<td>0</td>
</tr>
</tbody>
</table>
show security advance-policy-based-routing statistics (Changed Options from Junos OS Release 19.4R1)

user@host> show security advance-policy-based-routing statistics

Advance Profile Based Routing statistics:
  Sessions Processed 9
  App rule hit on cache hit 0
  App rule hit on HTTP Proxy/ALG 0
  Midstream disabled rule hit on cache hit 2
  URL cat rule hit on cache hit 0
  DSCP rule hit on first packet 2
  App and DSCP hit on first packet 0
  App rule hit midstream 1
  Default rule match 0
  Midstream disabled rule hit midstream 1
  URL cat rule hit midstream 0
  App and DSCP rule hit midstream 0
  DSCP rule hit midstream 0
  Route changed on cache hits 2
  Route changed on HTTP Proxy/ALG 0
  Route changed midstream 0
  Default rule applied 0
  Zone mismatch 0
  Drop on zone mismatch 0
  Next hop not found 0
  Application services bypass 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 | 222

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 sla active-probe-statistics

Syntax

```
show security advance-policy-based-routing sla active-probe-statistics active-probe-params-name probe-name
```

Release Information

Command introduced in Junos OS Release 18.2R1.

Description

Displays the details of active probe parameters. Active probe parameters are used by AppQoE to evaluate the SLA of the link. In active probing, custom packets are sent between a spoke device and a hub device on multiple routes to measure RTT, jitter, and packet loss between two SRX Series devices.

Required Privilege Level

view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Application Quality of Experience</th>
<th>283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Policy-Based Routing</td>
<td>213</td>
</tr>
</tbody>
</table>

Output Fields

Table 64 on page 740 lists the output fields for the `show` command. Output fields are listed in the approximate order in which they appear.

Table 64: show security advance-policy-based-routing sla active-probe-statistics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src-IP</td>
<td>Probe IP addresses used as probes’ start point.</td>
</tr>
<tr>
<td>Dst-IP</td>
<td>Probe IP addresses used as probes’ end point.</td>
</tr>
<tr>
<td>PKT-LOSS</td>
<td>Percentage of number of packets lost.</td>
</tr>
<tr>
<td>RTT(us)</td>
<td>Round-trip time (in microseconds)</td>
</tr>
<tr>
<td>2way-Jit</td>
<td>Two-way jitter (in microseconds).</td>
</tr>
</tbody>
</table>
Table 64: show security advance-policy-based-routing sla active-probe-statistics (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing-Jit</td>
<td>Ingress jitter (in microseconds).</td>
</tr>
<tr>
<td>Egr-Jit</td>
<td>Egress jitter (in microseconds).</td>
</tr>
</tbody>
</table>

Sample Output

user@host> show security advance-policy-based-routing sla active-probe-statistics

<table>
<thead>
<tr>
<th>Active Probe Statistics:</th>
<th>Src-IP</th>
<th>Dst-IP</th>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ing-Jit (us)</td>
<td>Egr-Jit (us)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>42.1.1.2</td>
<td>42.1.1.1</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>41.1.1.2</td>
<td>41.1.1.1</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>40.1.1.2</td>
<td>40.1.1.1</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show security advance-policy-based-routing sla profile (Application Name)

Syntax

```
show security advance-policy-based-routing sla profile profile-name application application-name
```

Release Information

Command is modified in Junos OS Release 20.2R1.

Description

Displays the details of the best path among all the links to send all the instances of the application to the specified destination.

Required Privilege Level

view

RELATED DOCUMENTATION

- Application Quality of Experience | 283

Output Fields

Table 56 on page 727 lists the output fields for the show command. Output fields are listed in the approximate order in which they appear.

Table 65: show security advance-policy-based-routing sla profile profile-name application application-name

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best-Path Local IP Address</td>
<td>The best link selected among all the links in the selected destination path group to send the application traffic.</td>
</tr>
<tr>
<td>Destination-group name</td>
<td>The destination path group name from which the link is selected.</td>
</tr>
<tr>
<td>Next-Hop ID</td>
<td>Next hop by ID number. It is the address of the next station to which the packet is sent on the way to its final destination. The range of values is 1 through 65,535.</td>
</tr>
<tr>
<td>Server IP</td>
<td>IP address of the server. Displayed as N/A.</td>
</tr>
</tbody>
</table>
Sample Output

```bash
user@host> show security advance-policy-based-routing sla profile profile-1 application JUNOS:ssh
```

<table>
<thead>
<tr>
<th>Best-Path Local IP Address</th>
<th>172.16.4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination-group name</td>
<td>DPG-1</td>
</tr>
<tr>
<td>Next-Hop ID</td>
<td>262142</td>
</tr>
<tr>
<td>Server IP</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best-Path Local IP Address</th>
<th>182.17.5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination-group name</td>
<td>DPG-2</td>
</tr>
<tr>
<td>Next-Hop ID</td>
<td>263132</td>
</tr>
<tr>
<td>Server IP</td>
<td>N/A</td>
</tr>
</tbody>
</table>
show security advance-policy-based-routing sla profile (Application Name)

Syntax

```
show security advance-policy-based-routing sla profile profile-name application application-name
```

Release Information

Command is modified in Junos OS Release 20.2R1.

Description

Displays the details of the best path among all the links to send all the instances of the application to the specified destination.

Required Privilege Level

view

RELATED DOCUMENTATION

Application Quality of Experience | 283

Output Fields

Table 56 on page 727 lists the output fields for the `show` command. Output fields are listed in the approximate order in which they appear.

Table 66: show security advance-policy-based-routing sla profile profile-name application application-name

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best-Path Local IP Address</td>
<td>The best link selected among all the links in the selected destination path group to send the application traffic.</td>
</tr>
<tr>
<td>Destination-group name</td>
<td>The destination path group name from which the link is selected.</td>
</tr>
<tr>
<td>Next-Hop ID</td>
<td>Next hop by ID number. It is the address of the next station to which the packet is sent on the way to its final destination. The range of values is 1 through 65,535.</td>
</tr>
<tr>
<td>Server IP</td>
<td>IP address of the server. Displayed as N/A.</td>
</tr>
</tbody>
</table>
Sample Output

user@host> show security advance-policy-based-routing sla profile profile-1 application JUNOS:ssh

<table>
<thead>
<tr>
<th>Best-Path Local IP Address</th>
<th>172.16.4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination-group name</td>
<td>DPG-1</td>
</tr>
<tr>
<td>Next-Hop ID</td>
<td>262142</td>
</tr>
<tr>
<td>Server IP</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best-Path Local IP Address</th>
<th>182.17.5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination-group name</td>
<td>DPG-2</td>
</tr>
<tr>
<td>Next-Hop ID</td>
<td>263132</td>
</tr>
<tr>
<td>Server IP</td>
<td>N/A</td>
</tr>
</tbody>
</table>
show security advance-policy-based-routing sla profile (Next-Hop)

Syntax

show security advance-policy-based-routing sla profile profile-name application application-name next-hop next-hop-number

Syntax

Syntax for Junos OS Releases prior 20.2R1

show security advance-policy-based-routing sla profile sla-profile-name application application-name destination-group-name destination-group-name

Release Information

Command introduced in Junos OS Release 18.2R1. Command is modified in 20.2R1 to include the next-hop next-hop-number in the syntax.

Description

Displays the number of times SLA violations occurred, application traffic switched route path, and monitored sessions.

Required Privilege Level

view

RELATED DOCUMENTATION

Application Quality of Experience | 283
Advanced Policy-Based Routing | 213

Output Fields

Table 56 on page 727 lists the output fields for the show command. Output fields are listed in the approximate order in which they appear.

Table 67: show security advance-policy-based-routing sla profile

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Name of the application.</td>
</tr>
</tbody>
</table>
### Table 67: show security advance-policy-based-routing sla profile (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>ID of the application</td>
</tr>
<tr>
<td>DSCP</td>
<td>DSCP value. This value corresponds to decimal values 0-63. This field is introduced in Junos OS Release 19.4R1.</td>
</tr>
<tr>
<td>APBR Profile Name</td>
<td>Name of the advanced policy-based (APBR) routing profile.</td>
</tr>
<tr>
<td>APBR Rule Name</td>
<td>Name of the APBR rule.</td>
</tr>
<tr>
<td>Application State</td>
<td>State of the application traffic.</td>
</tr>
<tr>
<td>Path Switch Idle State</td>
<td>Path switch idle state where no subsequent switching of application traffic path occurred.</td>
</tr>
<tr>
<td>Routing Instance Name</td>
<td>Name of the routing instance applied.</td>
</tr>
<tr>
<td>SLA Rule Name</td>
<td>Name of the SLA rule applied.</td>
</tr>
<tr>
<td>Active Probe Name</td>
<td>Name of the active probe parameter configured.</td>
</tr>
<tr>
<td>Selected Tunnel Destination</td>
<td>Selected tunnel destination where active probes are sent.</td>
</tr>
<tr>
<td>SLA Metrics</td>
<td>SLA metrics parameters, that are used by AppQoE to evaluate the SLA of the link. The SLA metric includes following parameters such as packet loss, RTT, jitter, and jitter type. Starting in Junos OS Release 19.2, With application-level summarization feature, each application’s maximum, minimum, and average values of all the SLA metrics are displayed.</td>
</tr>
</tbody>
</table>

### Sample Output

```
user@host> show security advance-policy-based-routing sla profile apbr1 application junos:ssh next-hop
262142

Application Details:
  Application Name     junos:SSH
```
<table>
<thead>
<tr>
<th>Application ID</th>
<th>198</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>N/A</td>
</tr>
<tr>
<td>APBR Profile Name</td>
<td>apbr1</td>
</tr>
<tr>
<td>APBR Rule Name</td>
<td>rule1</td>
</tr>
<tr>
<td>Application State</td>
<td>SLA MET</td>
</tr>
<tr>
<td>Path Switch Idle State</td>
<td>0</td>
</tr>
<tr>
<td>Routing Instance Name</td>
<td>TC1_VPN</td>
</tr>
<tr>
<td>SLA Rule Name</td>
<td>sl1</td>
</tr>
<tr>
<td>Active Probe Name</td>
<td>probe1</td>
</tr>
<tr>
<td>Best-Path Local IP Address</td>
<td>40.1.1.2</td>
</tr>
</tbody>
</table>

Average SLA Metrics:

<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1979</td>
<td>3038</td>
<td>3091</td>
<td>52</td>
</tr>
</tbody>
</table>

Min SLA Metrics:

<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1167</td>
<td>23</td>
<td>17</td>
<td>16</td>
</tr>
</tbody>
</table>

Max SLA Metrics:

<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>36921</td>
<td>32053</td>
<td>26460</td>
<td>5593</td>
</tr>
</tbody>
</table>

---

**Sample Output**

```
user@host> show security advance-policy-based-routing sla profile p2 destination-group-name site3 dscp 15 (Junos OS Release 19.4 and Later)
```

**Application Details:**

<table>
<thead>
<tr>
<th>Application Name</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>N/A</td>
</tr>
<tr>
<td>DSCP</td>
<td>15</td>
</tr>
<tr>
<td>APBR Profile Name</td>
<td>p2</td>
</tr>
<tr>
<td>APBR Rule Name</td>
<td>def</td>
</tr>
<tr>
<td>Application State</td>
<td>SLA MET</td>
</tr>
<tr>
<td>Path Switch Idle State</td>
<td>0</td>
</tr>
<tr>
<td>Routing Instance Name</td>
<td>TC1_VPN</td>
</tr>
<tr>
<td>SLA Rule Name</td>
<td>sl1</td>
</tr>
<tr>
<td>Active Probe Name</td>
<td>probe1</td>
</tr>
<tr>
<td>Selected Tunnel Destination</td>
<td>111.111.114.1</td>
</tr>
</tbody>
</table>

**Average SLA Metrics:**

<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4645</td>
<td>1190</td>
<td>1318</td>
<td>722</td>
</tr>
</tbody>
</table>
Min SLA Metrics:
<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3589</td>
<td>104</td>
<td>4</td>
<td>195</td>
</tr>
</tbody>
</table>

Max SLA Metrics:
<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7329</td>
<td>3000</td>
<td>4452</td>
<td>1884</td>
</tr>
</tbody>
</table>

user@host> show security advanced-policy-based-routing sla profile apbrProf1 application junos:CNN destination-group-name p1 (Junos OS Release 19.2 and Later)

Application Details:
- Application Name: junos:CNN
- Application ID: 988
- APBR Profile Name: apbrProf1
- APBR Rule Name: rule1
- Application State: SLA MET
- Path Switch Idle State: 0
- Routing Instance Name: ri3
- SLA Rule Name: SLA1
- Active Probe Name: PP1
- Selected Tunnel Destination: 5.1.1.1

SLA Metrics:
Average:
<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1118</td>
<td>34</td>
<td>70</td>
<td></td>
</tr>
</tbody>
</table>

Minimum:
<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1000</td>
<td>34</td>
<td>70</td>
<td></td>
</tr>
</tbody>
</table>

Maximum:
<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1236</td>
<td>34</td>
<td>70</td>
<td></td>
</tr>
</tbody>
</table>

user@host> show security advance-policy-based-routing sla profile apbr-1 application junos:HTTP destination-group-name d1 (Junos OS Release Prior 19.2R1)

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:**

<table>
<thead>
<tr>
<th>PKT-LOSS(%)</th>
<th>RTT(us)</th>
<th>2way-Jit(us)</th>
<th>Ing-Jit(us)</th>
<th>Egr-Jit(us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

750
show security advance-policy-based-routing sla profile (Status)

Syntax

show security advance-policy-based-routing sla profile <sla-profile-name> application <application-name> status
dscp dscp-value.
next-hop next-hop-id.

Syntax

Syntax prior to Junos OS Release 20.2R1

show security advance-policy-based-routing sla profile sla-profile-name application application-name
   destination-group-name destination-group-name

Release Information

Command introduced in Junos OS Release 18.2R1. The syntax is changed to include the next-hop option in Junos OS Release 20.2R1.

Description

Displays the number of times SLA violations occurred, application traffic switched route path, and monitored sessions.

Required Privilege Level

view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Application Quality of Experience</th>
<th>283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Policy-Based Routing</td>
<td>213</td>
</tr>
</tbody>
</table>

Output Fields

Table 56 on page 727 lists the output fields for the show command. Output fields are listed in the approximate order in which they appear.

Table 68: show security advance-policy-based-routing sla profile

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num of SLA Violations</td>
<td>Number of times SLA violations occurred.</td>
</tr>
</tbody>
</table>
Table 68: show security advance-policy-based-routing sla profile (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num of Path Switches</td>
<td>Number of times application traffic switched route path.</td>
</tr>
<tr>
<td>Num of monitored sessions</td>
<td>Number of monitored sessions by passive probes.</td>
</tr>
<tr>
<td>Num of sessions</td>
<td>Number of sessions.</td>
</tr>
<tr>
<td>Num of Violated Probes</td>
<td>Number of violations collected through probes.</td>
</tr>
</tbody>
</table>

Sample Output

```bash
user@host> show security advance-policy-based-routing sla profile apbr1 application junos:ssh next-hop 262142 status (Junos OS Release 20.2R1)

Application status:
Num of SLA Violations 0
Num of Path Switches 0
Num of monitored sessions 1
Num of sessions 1
Num of Violated Probes 0

user@host> show security advanced-policy-based-routing sla profile apbr1 application junos:ssh destination-group-name p1 status (Prior to Junos OS Release 20.2R1)

Application status:
Num of SLA Violations 2
Num of Path Switches 0
Num of monitored sessions 0
Num of sessions 0
Num of Violated Probes 6
```
show security advance-policy-based-routing sla statistics

Syntax

```
show security advance-policy-based-routing sla statistics
```

Release Information
Command introduced in Junos OS Release 18.2R1.

Description
Display the SLA statistics.

Required Privilege Level
view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Application Quality of Experience</th>
<th>283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Policy-Based Routing</td>
<td>213</td>
</tr>
</tbody>
</table>

Output Fields

Table 69 on page 753 lists the output fields for the show security advance-policy-based-routing sla statistics command. Output fields are listed in the approximate order in which they appear.

Table 69: show security advance-policy-based-routing sla statistics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Probe Session Processed</td>
<td>Number of sessions on which passive probes are sent.</td>
</tr>
<tr>
<td>Possible Passive Probe Sessions</td>
<td>Number of sessions considered for passive probes.</td>
</tr>
<tr>
<td>Passive Probe Sessions Sampled</td>
<td>Number of sessions, from which, data is subjected to sampling.</td>
</tr>
<tr>
<td>Passive Probe Ongoing Sessions</td>
<td>Number of sessions on which passive probes are active.</td>
</tr>
<tr>
<td>SLA violations</td>
<td>Number of SLA violations detected.</td>
</tr>
<tr>
<td>Active Probe Paths</td>
<td>Number of links identified for active probe.</td>
</tr>
</tbody>
</table>
Table 69: show security advance-policy-based-routing sla statistics (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Probe Session</strong></td>
<td>Number of sessions on which active probes are sent.</td>
</tr>
<tr>
<td><strong>Active Probes Sent</strong></td>
<td>Number of active probes sent.</td>
</tr>
<tr>
<td><strong>Active Probe Paths down</strong></td>
<td>Number of links on which active probes are sent, are not active.</td>
</tr>
</tbody>
</table>

Sample Output

```
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 Probes Sent 18360
Active Probe Paths down 3
show security advance-policy-based-routing sla status

Syntax

show security advance-policy-based-routing sla status

Release Information

Command introduced in Junos OS Release 18.2R1.

Description

Display the status of enabling switching of application path to an alternate route.

When local route switching is enabled, switching of application traffic to other route is enabled and also SLA monitoring and reporting functionality is available. By enabling local switch routing, the best possible link is selected for the application traffic to meet performance requirements as specified in SLA (service-level agreement).

Required Privilege Level

view

RELATED DOCUMENTATION

Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution | 222

Sample Output

show security advance-policy-based-routing sla status

user@host> show security advance-policy-based-routing sla status

Local Switching is enabled.
show security advance-policy-based-routing sla version

Syntax

show security advance-policy-based-routing sla version

Release Information
Command introduced in Junos OS Release 18.2R1.

Description
Displays AppQoE version details. This information helps verify that the SLA version on both hub device and spoke device is same.

Required Privilege Level
view

RELATED DOCUMENTATION

Application Quality of Experience | 283
Advanced Policy-Based Routing | 213

show security advance-policy-based-routing sla version

user@host> show security advance-policy-based-routing sla version

SLA version: APPQOE.VERS.1.0.0.0
show security application-firewall rule-set

Syntax

show security application-firewall rule-set (<rule-set-name> | all)
show security application-firewall rule-set (rule-set-name | all) | (logical-system logical-system-name | all) | all-logical-systems-tenants | root-logical-system | tenant (tenant-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. The tenant and all-logical-systems-tenants options are introduced in Junos OS Release 18.4R1.

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— Display the name of the rule set.

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.

logical-system-name— Display application firewall rule set information for a specific logical system.

root-logical-system— Display application firewall rule set information for the root logical system (master administrator only).

all-logical-systems-tenants— Display application firewall rule set information for all the logical systems and tenants.

tenant— Display application firewall rule set information for the tenant systems.

Required Privilege Level

view

RELATED DOCUMENTATION
List of Sample Output

show security application-firewall rule-set my.ruleset1 on page 759
show security application-firewall rule-set all on page 759
show security application-firewall rule-set ruleset1 tenant all on page 760

Output Fields

Table 70 on page 758 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 70: show security application-firewall rule-set Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule-set</td>
<td>Name of the rule set.</td>
</tr>
<tr>
<td>Logical system</td>
<td>Name of the logical system of the rule set.</td>
</tr>
<tr>
<td>Tenant</td>
<td>Name of the tenant system of the rule set.</td>
</tr>
<tr>
<td>Profile</td>
<td>The redirect profile to be used for rules requiring redirection for reject or deny actions.</td>
</tr>
<tr>
<td>Rule</td>
<td>Name of the rule</td>
</tr>
</tbody>
</table>

- **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.
Table 70: show security application-firewall rule-set Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default rule</strong></td>
<td>The default rule applied when the identified application is not specified in any</td>
</tr>
<tr>
<td></td>
<td>rules of the rule set.</td>
</tr>
<tr>
<td></td>
<td>• Number of sessions matched—Number of sessions matched with the application</td>
</tr>
<tr>
<td></td>
<td>firewall default rule.</td>
</tr>
<tr>
<td></td>
<td>• Number of sessions redirected—Number of sessions redirected by the application</td>
</tr>
<tr>
<td></td>
<td>firewall rule.</td>
</tr>
<tr>
<td><strong>Number of sessions with appid pending</strong></td>
<td>Number of sessions that are pending application identification processing</td>
</tr>
</tbody>
</table>
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

Sample Output

show security application-firewall rule-set ruleset1 tenant all

user@host> show security application-firewall rule-set ruleset1 tenant all

Rule-set: ruleset1
  Logical system: root-logical-system
  Tenant: TSYS1
  Rule: rule1
Dynamic Applications: junos:HTTP, 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 | 677

List of Sample Output
show security application-firewall rule-set logical-system all on page 764
show security application-firewall rule-set all on page 764

Output Fields
Table 71 on page 763 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 71: show security application-firewall rule-set logical-system Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule-set</td>
<td>Name of the rule set.</td>
</tr>
<tr>
<td>Logical system</td>
<td>Name of the logical system.</td>
</tr>
<tr>
<td>Rule</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Dynamic applications</td>
<td>Name of the applications.</td>
</tr>
<tr>
<td>Dynamic application groups</td>
<td>Name of the application groups.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:</td>
</tr>
<tr>
<td></td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td>deny</td>
</tr>
<tr>
<td>Number of sessions matched</td>
<td>Number of sessions matched with the application firewall rule.</td>
</tr>
<tr>
<td>Default rule</td>
<td>The default rule applied when the identified application is not specified in any rules of the rule set.</td>
</tr>
<tr>
<td>Number of sessions matched</td>
<td>Number of sessions matched with the application firewall default rule.</td>
</tr>
<tr>
<td>Number of sessions with appid pending</td>
<td>Number of sessions that are pending with the application ID processing.</td>
</tr>
</tbody>
</table>
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 Application Tracking  |  168
Example: Configuring Application Tracking  |  177

Output Fields
Table 72 on page 766 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 72: show security application-tracking counters

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session create messages</td>
<td>The number of log messages generated when a session was created.</td>
</tr>
<tr>
<td>Session close messages</td>
<td>The number of log messages generated when a session was closed.</td>
</tr>
<tr>
<td>Session volume updates</td>
<td>The number of log messages generated when an update interval was exceeded.</td>
</tr>
<tr>
<td>Session route updates</td>
<td>The number of log messages generated when an egress interface was selected based on application carried in the session by APBR.</td>
</tr>
<tr>
<td>Failed messages</td>
<td>The number of messages that were not generated due to memory or session constraints.</td>
</tr>
</tbody>
</table>
### Sample Output

```
show security application-tracking counters

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

<table>
<thead>
<tr>
<th>AppTrack counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session create messages</td>
<td>1</td>
</tr>
<tr>
<td>Session close messages</td>
<td>1</td>
</tr>
<tr>
<td>Session volume updates</td>
<td>0</td>
</tr>
<tr>
<td>Session route updates</td>
<td>1</td>
</tr>
<tr>
<td>Failed messages</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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.
The tenant option introduced in Junos OS Release 18.3R1.

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 (SRX5K-MPC), IOC3 (SRX5K-MPC3-100G10G and SRX5K-MPC3-40G10G), and IOC4 (SRX5K-IOC4-MRAT and SRX5K-IOC4-10G) 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.

- **all-logical-systems-tenants**—All multitenancy systems.

- **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.
tenant—Displays the security flow session information for a tenant system.

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

Understanding Traffic Processing on Security Devices

clear security flow session all

List of Sample Output

show security flow session on page 773
show security flow session (with default policy) on page 773
show security flow session brief on page 774
show security flow session extensive on page 774
show security flow session extensive on page 775
show security flow session summary on page 776

Output Fields

Table 73 on page 770 lists the output fields for the show security flow session command. Output fields are listed in the approximate order in which they appear.

Table 73: show security flow session Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| Session ID   | Number that identifies the session. Use this ID to get more information about the session. | brief
              |                                                                                   | extensive
              |                                                                                   | none |
| If           | Interface name.                                                                    | brief
<pre><code>          |                                                                                   | none |
</code></pre>
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Status of security flow session.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Conn Tag</td>
<td>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.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>CP Session ID</td>
<td>Number that identifies the central point session. Use this ID to get more information about the central point session.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Policy name</td>
<td>Name and ID of the policy that the first packet of the session matched.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Timeout</td>
<td>Idle timeout after which the session expires.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>In</td>
<td>Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Bytes</td>
<td>Number of received and transmitted bytes.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>
Table 73: show security flow session Output Fields  *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkts</td>
<td>Number of received and transmitted packets.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Total sessions</td>
<td>Total number of sessions.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Out</td>
<td>Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Status</td>
<td>Session status.</td>
<td>extensive</td>
</tr>
<tr>
<td>Flag</td>
<td>Internal flag depicting the state of the session, used for debugging purposes.</td>
<td>extensive</td>
</tr>
<tr>
<td>Source NAT pool</td>
<td>The name of the source pool where NAT is used.</td>
<td>extensive</td>
</tr>
<tr>
<td>Dynamic application</td>
<td>Name of the application.</td>
<td>extensive</td>
</tr>
<tr>
<td>Application traffic</td>
<td>AppQoS rule set for this session.</td>
<td>extensive</td>
</tr>
<tr>
<td>control rule-set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule</td>
<td>AppQoS rule for this session.</td>
<td>extensive</td>
</tr>
<tr>
<td>Maximum timeout</td>
<td>Maximum session timeout.</td>
<td>extensive</td>
</tr>
<tr>
<td>Current timeout</td>
<td>Remaining time for the session unless traffic exists in the session.</td>
<td>extensive</td>
</tr>
<tr>
<td>Session State</td>
<td>Session state.</td>
<td>extensive</td>
</tr>
<tr>
<td>Start time</td>
<td>Time when the session was created, offset from the system start time.</td>
<td>extensive</td>
</tr>
<tr>
<td>Unicast-sessions</td>
<td>Number of unicast sessions.</td>
<td>Summary</td>
</tr>
</tbody>
</table>
Table 73: show security flow session Output Fields  *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast-sessions</td>
<td>Number of multicast sessions.</td>
<td>Summary</td>
</tr>
<tr>
<td>Services-offload-sessions</td>
<td>Number of services-offload sessions.</td>
<td>Summary</td>
</tr>
<tr>
<td>Failed-sessions</td>
<td>Number of failed sessions.</td>
<td>Summary</td>
</tr>
<tr>
<td>Sessions-in-use</td>
<td>Number of sessions in use.</td>
<td>Summary</td>
</tr>
<tr>
<td></td>
<td>• Valid sessions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pending sessions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalidated sessions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sessions in other states</td>
<td></td>
</tr>
<tr>
<td>Maximum-sessions</td>
<td>Maximum number of sessions permitted.</td>
<td>Summary</td>
</tr>
</tbody>
</table>

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 --> 10.10.1/179;tcp, Conn Tag: 0x0, If: ge-0/0/2.0, Pkts: 1, Bytes: 64,
```
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,
show security flow session extensive
oot> show security flow session extensive

Flow Sessions on FPC0 PIC0:

Session ID: 10000059, Status: Normal
Flags: 0x10000/0x0/0x10/0x1
Policy name: N/A
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 642, Duration: 369
  In: 3.0.0.2/64387 --> 2.0.0.1/8940;esp,
    Conn Tag: 0x0, Interface: xe-2/0/2.0,
    Session token: 0x7, Flag: 0x80100621
    Route: 0xc0010, Gateway: 2.0.0.2, Tunnel: 0
    ESP/AH frag Rx: 0, Generated: 0
    Inner IPv4 frag Rx: 0, Tx: 0, Generated: 0
    Inner IPv6 frag Rx: 0, Tx: 0, Generated: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 25, Bytes: 3760
    CP Session ID: 0

Session ID: 10000060, Status: Normal
Flags: 0x10000/0x0/0x10/0x1
Policy name: N/A
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 642, Duration: 369
  In: 3.0.0.2/0 --> 2.0.0.1/0; esp,
  Conn Tag: 0x0, Interface: xe-2/0/2.0,
  Session token: 0x7, Flag: 0x621
  Route: 0xc0010, Gateway: 2.0.0.2, Tunnel: 0
  ESP/AH frag Rx: 0, Generated: 0
  Inner IPv4 frag Rx: 0, Tx: 0, Generated: 0,
  Inner IPv6 frag Rx: 0, Tx: 0, Generated: 0
  Port sequence: 0, FIN sequence: 0,
  FIN state: 0,
  Pkts: 0, Bytes: 0
  CP Session ID: 0
  Total sessions: 2

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 ssl

Syntax

```
show security flow session ssl [brief | extensive]
```

Release Information
Command introduced in Junos OS Release 19.3R1.

Description
Display information about the active SSL sessions on the device.

Options
brief | extensive —Display the specified level of output.

Required Privilege Level
view

RELATED DOCUMENTATION

-  Operational Commands to Troubleshoot SSL Sessions | 439
-  show security flow session | 768

List of Sample Output
show security flow session ssl brief on page 780
show security flow session ssl extensive on page 780

Output Fields

Table 74 on page 778 lists the output fields for the show security flow session ssl command. Output fields are listed in the approximate order in which they appear.

Table 74: show security flow session ssl Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Displayed with Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Number that identifies the session. You can use this ID to get additional information about the session.</td>
<td>brief, extensive</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the session.</td>
<td>brief, extensive</td>
</tr>
</tbody>
</table>
Table 74: show security flow session ssl Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Displayed with Option</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy name</strong></td>
<td>Policy that permitted the traffic. Name and ID of the policy that the first packet of the session matched.</td>
<td>brief, extensive</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Idle timeout after which the session expires.</td>
<td>brief, extensive</td>
</tr>
<tr>
<td><strong>In</strong></td>
<td>Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
<td>brief, extensive</td>
</tr>
<tr>
<td><strong>Out</strong></td>
<td>Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
<td>brief, extensive</td>
</tr>
<tr>
<td><strong>Flag</strong></td>
<td>Internal flag depicting the state of the session, used for debugging purposes.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Source NAT pool</strong></td>
<td>The name of the source pool where NAT is used.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>dynamic-application</strong></td>
<td>Name of the application.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>encryption</strong></td>
<td>Encryption applied.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Application traffic control rule-set: INVALID, Rule: INVALID</strong></td>
<td>Name of the application quality of service rule.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Maximum timeout</strong></td>
<td>Maximum session timeout.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Current timeout</strong></td>
<td>Remaining time for the session unless traffic exists in the session.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Session State</strong></td>
<td>Status of security ssl session.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Start time</strong></td>
<td>Time when the session was created, offset from the system start time.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>duration</strong></td>
<td>Duration of the session</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 74: show security flow session ssl Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Displayed with Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
<td>extensive</td>
</tr>
<tr>
<td>Out</td>
<td>Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
<td>extensive</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>Total number of sessions.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

show security flow session ssl brief

user@host> show security flow session ssl brief

Output:

Session ID: 1, Policy name: default-permit/5, Timeout: 1746, Valid
In: 4.0.0.1/37369 --> 5.0.0.1/4433;tcp, Conn Tag: 0x0, If: xe-0/0/0.0, Pkts: 6, Bytes: 671,
Out: 5.0.0.1/4433 --> 4.0.0.1/37369;tcp, Conn Tag: 0x0, If: xe-0/0/1.0, Pkts: 7, Bytes: 1635,

show security flow session ssl extensive

user@host> show security flow session ssl extensive

Output:
Session ID: 1, Status: Normal
Flags: 0x42/0x20000000/0x2/0x10103
Policy name: 1/5
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID

Maximum timeout: 1800, Current timeout: 1636

Session State: Valid
Start time: 587131, Duration: 163
In: 4.0.0.1/37369 --> 5.0.0.1/4433;tcp,
Conn Tag: 0x0, Interface: xe-0/0/0.0,
Session token: 0x7, Flag: 0x2621
Route: 0xa0010, Gateway: 4.0.0.1, Tunnel: 0
Port sequence: 0, FIN sequence: 0,
FIN state: 0,
Pkts: 6, Bytes: 671

Out: 5.0.0.1/4433 --> 4.0.0.1/37369;tcp,
Conn Tag: 0x0, Interface: xe-0/0/1.0,
Session token: 0x8, Flag: 0x2620
Route: 0xb0010, Gateway: 5.0.0.1, Tunnel: 0
Port sequence: 0, FIN sequence: 0,
FIN state: 0,
Pkts: 7, Bytes: 1635
Total sessions: 1
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 Application Firewall with Application Groups | 158
List of Sample Output

- show security flow session application-firewall extensive on page 784
- show security flow session application-firewall dynamic-application junos:FTP extensive on page 785
- show security flow session application-firewall dynamic-application junos:UNKNOWN extensive on page 786
- show security flow session application-firewall dynamic-application-group junos:WEB extensive on page 787
- show security flow session application-firewall application-firewall-rule-set rule-set1 extensive on page 788

Output Fields

Table 75 on page 783 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 75: show security flow session application-firewall extensive Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Number that identifies the session. Use this ID to display more information about a session.</td>
</tr>
<tr>
<td>Status</td>
<td>Session status.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the session: Active, Pending, Closed, Unknown.</td>
</tr>
<tr>
<td>Flag</td>
<td>Internal flag depicting the state of the session. It is used for debugging purposes.</td>
</tr>
<tr>
<td>Policy name</td>
<td>The name of the policy that permitted the traffic.</td>
</tr>
<tr>
<td>Source NAT pool</td>
<td>The name of the source pool where NAT is used.</td>
</tr>
<tr>
<td>Dynamic application</td>
<td>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.</td>
</tr>
<tr>
<td>Dynamic application group</td>
<td>Name of the dynamic application group of the session. If the dynamic application cannot be determined, the output indicates junos:UNASSIGNED.</td>
</tr>
<tr>
<td>Dynamic nested application</td>
<td>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.</td>
</tr>
<tr>
<td>Application firewall rule-set</td>
<td>Name of the rule set that the session matched.</td>
</tr>
</tbody>
</table>
Table 75: show security flow session application-firewall extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Maximum timeout</strong></td>
<td>Maximum amount of idle time allowed for the session.</td>
</tr>
<tr>
<td><strong>Current timeout</strong></td>
<td>Number of seconds that the current session has been idle.</td>
</tr>
<tr>
<td><strong>Session State</strong></td>
<td>Session state.</td>
</tr>
<tr>
<td><strong>Start time</strong></td>
<td>Time when the session was created. Start time is indicated as an offset from the system start time.</td>
</tr>
<tr>
<td><strong>In</strong></td>
<td>Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
</tr>
<tr>
<td><strong>Out</strong></td>
<td>Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).</td>
</tr>
<tr>
<td><strong>Total sessions</strong></td>
<td>Total number of sessions per PIC that fit the display criteria.</td>
</tr>
</tbody>
</table>

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: 0x21
  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: 0x30
  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: 0x21
    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,
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
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: 0xffffd0000, 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 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: 0xffff0000, 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 792
- show security pki ca-certificate detail on page 792

Output Fields

Table 76 on page 790 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 76: show security pki ca-certificate Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate identifier</td>
<td>Name of the digital certificate.</td>
<td>All levels</td>
</tr>
<tr>
<td>Certificate version</td>
<td>Revision number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique serial number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Issued by</td>
<td>Authority that issued the digital certificate.</td>
<td>none brief</td>
</tr>
</tbody>
</table>
Table 76: show security pki ca-certificate Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issued to</td>
<td>Device that was issued the digital certificate.</td>
<td>none brief</td>
</tr>
</tbody>
</table>
| 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           |
| 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       | Encryption algorithm used with the private key, such as rsaEncryption(1024 bits).    | All levels       |
| algorithm        |                                                                                     |                 |
| Signature        | Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption. | detail           |
| algorithm        |                                                                                     |                 |
| 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: example
   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 after: 2008 Oct 19th, 00:25:59 GMT
   Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier: afe
   Issued to: First Officer, Issued by: example
   Validity:
      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)
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
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 after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
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 after: 2008 Oct 19th, 00:25:59 GMT

Public key algorithm: rsaEncryption(1024 bits)

Signature algorithm: sha1WithRSAEncryption

Fingerprint:

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


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 797
- show security pki local-certificate certificate-id hello detail on page 798
- show security pki local-certificate system-generated on page 799
- show security pki local-certificate system-generated detail on page 799
- show security pki local-certificate certificate-id mycert - (local certificate enrolled online using SCEP) on page 800
show security pki local-certificate certificate-id mycert detail - (local certificate enrolled online using SCEP) on page 800
show security pki local-certificate detail on page 801

Output Fields
Table 77 on page 796 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 77: show security pki local-certificate Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate identifier</td>
<td>Name of the digital certificate.</td>
</tr>
<tr>
<td>Certificate version</td>
<td>Revision number of the digital certificate.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique serial number of the digital certificate. Starting in Junos OS Release 20.1R1, PKI local certificate serial number is displayed with 0x as prefix to indicate that the PKI local certificate is in the hexadecimal format.</td>
</tr>
<tr>
<td>Issued to</td>
<td>Device that was issued the digital certificate.</td>
</tr>
<tr>
<td>Issued by</td>
<td>Authority that issued the digital certificate.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:</td>
</tr>
<tr>
<td></td>
<td>• Organization—Organization of origin.</td>
</tr>
<tr>
<td></td>
<td>• Organizational unit—Department within an organization.</td>
</tr>
<tr>
<td></td>
<td>• Country—Country of origin.</td>
</tr>
<tr>
<td></td>
<td>• Locality—Locality of origin.</td>
</tr>
<tr>
<td></td>
<td>• Common name—Name of the authority.</td>
</tr>
<tr>
<td>LSYS</td>
<td>Name of the logical systems.</td>
</tr>
<tr>
<td>Subject</td>
<td>Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:</td>
</tr>
<tr>
<td></td>
<td>• Organization—Organization of origin.</td>
</tr>
<tr>
<td></td>
<td>• Organizational unit—Department within an organization.</td>
</tr>
<tr>
<td></td>
<td>• Country—Country of origin.</td>
</tr>
<tr>
<td></td>
<td>• Locality—Locality of origin.</td>
</tr>
<tr>
<td></td>
<td>• Common name—Name of the authority.</td>
</tr>
<tr>
<td></td>
<td>• Serial number—Serial number of the device.</td>
</tr>
<tr>
<td></td>
<td>If the certificate contains multiple subfield entries, all entries are displayed.</td>
</tr>
</tbody>
</table>
### Table 77: show security pki local-certificate Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject string</td>
<td>Subject field as it appears in the certificate.</td>
</tr>
<tr>
<td>Alternate subject</td>
<td>Domain name or IP address of the device related to the digital certificate.</td>
</tr>
<tr>
<td>Validity</td>
<td>Time period when the digital certificate is valid. Values are:</td>
</tr>
<tr>
<td></td>
<td>• Not before—Start time when the digital certificate becomes valid.</td>
</tr>
<tr>
<td></td>
<td>• Not after—End time when the digital certificate becomes invalid.</td>
</tr>
<tr>
<td>Public key algorithm</td>
<td>Encryption algorithm used with the private key, such as rsaEncryption(1024 bits).</td>
</tr>
<tr>
<td>Public key verification status</td>
<td>Public key verification status: Failed or Passed. The detail output also provides the verification hash.</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.</td>
</tr>
<tr>
<td>Distribution CRL</td>
<td>Distinguished name information and URL for the certificate revocation list (CRL) server.</td>
</tr>
<tr>
<td>Use for key</td>
<td>Use of the public key, such as Certificate signing, CRL signing, Digital signature, or Data encipherment.</td>
</tr>
</tbody>
</table>

### Sample Output

```shell
show security pki local-certificate certificate-id hello
user@host> show security pki local-certificate certificate-id hello

LSYS: root-logical-system
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)
```
show security pki local-certificate certificate-id hello detail

Certificate identifier: hello
Certificate version: 3
Serial number: 61ba9da0000000000d72e
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)
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:
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: e90d42ebd14ef954b3e48c2e6ed5b30fb
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)
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
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

LSYS: root-logical-system
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)
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

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:

Auto-re-enrollment:
Status: Disabled
Next trigger time: Timer not started

---

Sample Output

show security pki local-certificate detail

user@host>show security pki local-certificate detail

Certificate identifier: Root-CA
Certificate version: 3
Serial number: 0x64fd90f39e513fb3435946f893f19360

Issuer:
    Common name: vpnqa-msca

Subject:
    Common name: vpnqa-msca

Subject string:
    CN=vpnqa-msca

Validity:
    Not before: 11-26-2019 02:37 UTC
    Not after: 11-26-2024 02:47 UTC

Public key algorithm: rsaEncryption(2048 bits)

    5d:ae:55:cc:2b:bd:02:03:01:00:01

Signature algorithm: sha256WithRSAEncryption

Use for key: CRL signing, Certificate signing, Digital signature

Fingerprint:
show security policies

Syntax

```
show security policies
<all-logical-systems-tenants>
<checksum>
<count>
<detail>
<from-zone zone-name>
<global>
<hit-count>
<information>
<logical-system logical-system-name>
<policy-name policy-name>
<root-logical-system>
<service-set>
<start>
<tenant tenant-name>
<to-zone zone-name>
<unknown-source-identity>
<zone-context>
```

Release Information

Command modified in Junos OS Release 9.2.
Support for IPv6 addresses is added in Junos OS Release 10.2.
Support for wildcard addresses is added in Junos OS Release 11.1.
Support for global policy and services offloading is added in Junos OS Release 11.4.
Support for source-identities and the Description output field is 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 are 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 is added in Junos OS Release 12.3X48-D20.
Output field and description for source-end-user-profile option is added in Junos OS Release 15.1x49-D70.
Output field and description for dynamic-applications option is added in Junos OS Release 15.1x49-D100.
Output field and description for dynapp-redir-profile option is added in Junos OS Release 18.2R1.
The tenant option is introduced in Junos OS Release 18.3R1.
The <all-logical-systems-tenants> option is introduced in Junos OS Release 18.4R1.
The information option is introduced in Junos OS Release 18.4R1.
The checksum option is introduced in Junos OS Release 18.4R1.

Description
Displays a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy. The existing show commands for displaying the policies configured with multiple tenant support are enhanced. A security policy controls the traffic flow from one zone to another zone. The security policies allow you to deny, permit, reject (deny and send a TCP RST or ICMP port unreachable message to the source host), encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another.

**Options**
- **all-logical-systems-tenants**—Displays all multitenancy systems.
- **checksum**—Displays the policy information checksum.
- **count**—Displays the number of policies to show. Range is 1 through 65,535.
- **detail**—(Optional) Displays a detailed view of all of the policies configured on the device.
- **from-zone**—Displays the policy information matching the given source zone.
- **global**—(Optional) Displays the policy information about global policies.
- **hit-count**—Displays the policies hit count.
- **information**—Displays the policy information.
- **logical-system**—Displays the logical system name.
- **policy-name**—(Optional) Displays the policy information matching the given policy name.
- **root-logical-system**—Displays root logical system as default.
- **service-set**—Displays the name of the service set.
- **start**—Displays the policies from a given position. Range is 1 through 65,535.
- **tenant**—Displays the name of the tenant system.
- **to-zone**—Displays the policy information matching the given destination zone.
- **unknown-source-identity**—Displays the unknown-source-identity of a policy.
- **zone-context**—Displays the count of policies in each context (from-zone and to-zone).

**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 809
show security policies (Dynamic Applications) on page 809
show security policies policy-name p2 on page 810
show security policies policy-name detail on page 811
show security policies (Services-Offload) on page 813
show security policies (Device Identity) on page 813
show security policies detail on page 813
show security policies detail (TCP Options) on page 816
show security policies policy-name (Negated Address) on page 817
show security policies policy-name detail (Negated Address) on page 817
show security policies global on page 818
show security policies detail tenant on page 818

Output Fields

Table 78 on page 805 lists the output fields for the show security policies command. Output fields are listed in the approximate order in which they appear.

Table 78: show security policies Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From zone</td>
<td>Name of the source zone.</td>
</tr>
<tr>
<td>To zone</td>
<td>Name of the destination zone.</td>
</tr>
<tr>
<td>Policy-name</td>
<td>Name of the applicable policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the applicable policy.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the policy:</td>
</tr>
<tr>
<td></td>
<td>• enabled: The policy can be used in the policy lookup process, which determines</td>
</tr>
<tr>
<td></td>
<td>access rights for a packet and the action taken in regard to it.</td>
</tr>
<tr>
<td></td>
<td>• disabled: The policy cannot be used in the policy lookup process, and therefore</td>
</tr>
<tr>
<td></td>
<td>it is not available for access control.</td>
</tr>
<tr>
<td>Index</td>
<td>Internal number associated with the policy.</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Number of the policy within a given context. For example, three policies that are</td>
</tr>
<tr>
<td></td>
<td>applicable in a from-zoneA-to-zoneB context might be ordered with sequence</td>
</tr>
<tr>
<td></td>
<td>numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have</td>
</tr>
<tr>
<td></td>
<td>sequence numbers 1, 2, 3, 4.</td>
</tr>
</tbody>
</table>
Table 78: show security policies Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source addresses</td>
<td>For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Destination addresses</td>
<td>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.</td>
</tr>
<tr>
<td>source-end-user-profile</td>
<td>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.</td>
</tr>
<tr>
<td>Source addresses (excluded)</td>
<td>Name of the source address excluded from the policy.</td>
</tr>
<tr>
<td>Destination addresses (excluded)</td>
<td>Name of the destination address excluded from the policy.</td>
</tr>
<tr>
<td>Source identities</td>
<td>One or more user roles specified for a policy.</td>
</tr>
<tr>
<td>Applications</td>
<td>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</td>
</tr>
<tr>
<td></td>
<td>• IP protocol: The Internet protocol used by the application—for example, TCP, UDP, ICMP.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Inactivity timeout: Elapsed time without activity after which the application is terminated.</td>
</tr>
<tr>
<td></td>
<td>• Source port range: The low-high source port range for the session application.</td>
</tr>
<tr>
<td>Dynamic Applications</td>
<td>Application identification-based Layer 7 dynamic applications.</td>
</tr>
</tbody>
</table>
Table 78: show security policies Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination Address Translation</strong></td>
<td>Status of the destination address translation traffic:</td>
</tr>
<tr>
<td></td>
<td>• drop translated—Drop the packets with translated destination addresses.</td>
</tr>
<tr>
<td></td>
<td>• drop untranslated—Drop the packets without translated destination addresses.</td>
</tr>
<tr>
<td><strong>Application Firewall</strong></td>
<td>An application firewall includes the following:</td>
</tr>
<tr>
<td></td>
<td>• Rule-set—Name of the rule set.</td>
</tr>
<tr>
<td></td>
<td>• Rule—Name of the rule.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic applications—Name of the applications.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic application groups—Name of the application groups.</td>
</tr>
<tr>
<td></td>
<td>• Action—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:</td>
</tr>
<tr>
<td></td>
<td>• permit</td>
</tr>
<tr>
<td></td>
<td>• deny</td>
</tr>
<tr>
<td></td>
<td>• Default rule—The default rule applied when the identified application is not specified in any rules of the rule set.</td>
</tr>
<tr>
<td><strong>Action or Action-type</strong></td>
<td>• The action taken for a packet that matches the policy’s tuples. Actions include the following:</td>
</tr>
<tr>
<td></td>
<td>• permit</td>
</tr>
<tr>
<td></td>
<td>• feed</td>
</tr>
<tr>
<td></td>
<td>• firewall-authentication</td>
</tr>
<tr>
<td></td>
<td>• tunnel ipsec-vpn vpn-name</td>
</tr>
<tr>
<td></td>
<td>• pair-policy pair-policy-name</td>
</tr>
<tr>
<td></td>
<td>• source-nat pool pool-name</td>
</tr>
<tr>
<td></td>
<td>• pool-set pool-set-name</td>
</tr>
<tr>
<td></td>
<td>• interface</td>
</tr>
<tr>
<td></td>
<td>• destination-nat name</td>
</tr>
<tr>
<td></td>
<td>• deny</td>
</tr>
<tr>
<td></td>
<td>• reject</td>
</tr>
<tr>
<td></td>
<td>• services-offload</td>
</tr>
<tr>
<td><strong>Session log</strong></td>
<td>Session log entry that indicates whether the at-create and at-close flags were set at configuration time to log session information.</td>
</tr>
<tr>
<td><strong>Scheduler name</strong></td>
<td>Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.</td>
</tr>
</tbody>
</table>
Table 78: show security policies Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy statistics</td>
<td>- <strong>Input bytes</strong>—The total number of bytes presented for processing by the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initial direction</strong>—The number of bytes presented for processing by the device from the initial direction.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reply direction</strong>—The number of bytes presented for processing by the device from the reply direction.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Output bytes</strong>—The total number of bytes actually processed by the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initial direction</strong>—The number of bytes from the initial direction actually processed by the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reply direction</strong>—The number of bytes from the reply direction actually processed by the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Input packets</strong>—The total number of packets presented for processing by the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initial direction</strong>—The number of packets presented for processing by the device from the initial direction.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reply direction</strong>—The number of packets presented for processing by the device from the reply direction.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Output packets</strong>—The total number of packets actually processed by the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initial direction</strong>—The number of packets actually processed by the device from the initial direction.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reply direction</strong>—The number of packets actually processed by the device from the reply direction.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Session rate</strong>—The total number of active and deleted sessions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Active sessions</strong>—The number of sessions currently present because of access control lookups that used this policy.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Session deletions</strong>—The number of sessions deleted since system startup.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Policy lookups</strong>—The number of times the policy was accessed to check for a match.</td>
</tr>
<tr>
<td>dynapp-redir-profile</td>
<td>Displays unified policy redirect profile. See profile(dynamic-application).</td>
</tr>
<tr>
<td>Per policy TCP Options</td>
<td>Configured syn and sequence checks, and the configured TCP MSS value for the initial direction, the reverse direction or, both.</td>
</tr>
</tbody>
</table>
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::8/32
  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  
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 p2

user@host> show security policies policy-name p2

Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1  
From zones: any  
To zones: any  
Source vrf group: any  
Destination vrf group: any  
Source addresses: any  
Destination addresses: any
Applications: any
Dynamic Applications: any
Action: permit, application services, feed

show security policies policy-name detail

user@host> show security policies policy-name p2 detail

Policy: p2, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured, global
Sequence number: 1
From zones:
   any
To zones:
   any
Source vrf group:
   any
Destination vrf group:
   any
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 ports: [0-0]
Dynamic Application:
   any: 0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Intrusion Detection and Prevention: disabled
Unified Access Control: disabled
Feed: add-source-ip-to-feed

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
show security policies (Services-Offload)

user@host> show security policies

Policy: pl, 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
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):
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 security policies detail tenant

user@host> show security policies detail tenant TN1

Default policy: deny-all
Pre ID default policy: permit-all
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: any
Destination addresses: any
Application: junos-ping
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input bytes : 0 0 bps
Initial direction: 0 0 bps
Reply direction : 0 0 bps
Output bytes : 0 0 bps
Initial direction: 0 0 bps
Reply direction : 0 0 bps
Input packets : 0 0 pps
Initial direction: 0 0 bps
Reply direction : 0 0 bps
Output packets : 0 0 pps
Initial direction: 0 0 bps
Reply direction : 0 0 bps
Session rate : 0 0 sps
Active sessions : 0
Session deletions: 0
Policy lookups : 0
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

List of Sample Output
show services application-identification application summary on page 823
show services application-identification application detail on page 824
show services application-identification application detail (Custom Applications) on page 825
show services application-identification application detail (Unified Policies) on page 825
show services application-identification application detail (Junos OS Release 20.2R1) on page 827

Output Fields
Table 79 on page 821 lists shows the output details for the show services application-identification application detail command.
### Table 79: show services application-identification application summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application(s)</td>
<td>The number of applications present.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the custom application.</td>
</tr>
<tr>
<td>Disabled</td>
<td>The status of the application and whether the mapping method is currently used to identify this application.</td>
</tr>
<tr>
<td>ID</td>
<td>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.</td>
</tr>
<tr>
<td>Order</td>
<td>Number used to specify priority when multiple applications match the traffic. The lowest order number takes the highest priority.</td>
</tr>
</tbody>
</table>

Table 80 on page 821 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 80: show services application-identification application Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Application Type</td>
<td>The basic application type, such as HTTP.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the application.</td>
</tr>
<tr>
<td>Application ID</td>
<td>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.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority over other signature applications.</td>
</tr>
<tr>
<td>Order</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>The status of the application and whether the mapping method is currently used to identify this application.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Cacheable</strong></td>
<td>The status whether the application identification results caching is enabled or not for the application.</td>
</tr>
<tr>
<td></td>
<td>When this option is enabled, you can cache the application detection result in an ASC table.</td>
</tr>
<tr>
<td><strong>Activation Date</strong></td>
<td>Date when the application was activated for the first time.</td>
</tr>
<tr>
<td><strong>Last Modified</strong></td>
<td>Date when the application was last updated.</td>
</tr>
<tr>
<td><strong>Number of Parent Group(s)</strong></td>
<td>Total number of parent groups in this application signature group or cluster.</td>
</tr>
</tbody>
</table>
| **Underlying consolidated Protocols/ports application is dependent on** | List of default protocols and ports for dependent applications of the specified application.  
   - **Protocols**—List of default protocols.  
   - **TCP ports**—List of default TCP ports.                                                                                                                                                                                                                                                                                                           |
| **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.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| **Signature:**                      | Signature mapping criteria for application identification                                                                                                                                                                                                                                                                                                                                                      |
| **Protocol**                        | Application protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| **Port range**                      | Port range. This option is applicable for TCP or UDP-based applications only.                                                                                                                                                                                                                                                                                                                                      |
| **Member(s)**                       | Member name for a custom application signature.  
   - **Depth**—Maximum number of bytes to check for context match. Byte limit for ApplID to identify custom application pattern for applications running over TCP or UDP or Layer 7 applications.  
   - **Context**—Service-specific context, such as http-header-content-type.  
   - **Pattern**—Deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature.  
   - **Direction**—Connection direction of the packets to match pattern (example: CTS [client-to-server]) |
### Sample Output

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

Application(s): 3616

<table>
<thead>
<tr>
<th>Application</th>
<th>Disabled</th>
<th>ID</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>junos:SLACKER</td>
<td>No</td>
<td>1179</td>
<td>1</td>
</tr>
<tr>
<td>junos:GOOGLE-TRUSTED-STORE</td>
<td>No</td>
<td>2819</td>
<td>5</td>
</tr>
<tr>
<td>junos:AMJILT</td>
<td>No</td>
<td>2272</td>
<td>4</td>
</tr>
<tr>
<td>junos:DSI</td>
<td>No</td>
<td>2644</td>
<td>3</td>
</tr>
<tr>
<td>junos:HLN</td>
<td>No</td>
<td>2096</td>
<td>2</td>
</tr>
<tr>
<td>junos:ETSI-LI</td>
<td>No</td>
<td>537</td>
<td>1</td>
</tr>
<tr>
<td>junos:CRAZYSALOON</td>
<td>No</td>
<td>1720</td>
<td>5</td>
</tr>
<tr>
<td>junos:EKSISOZLUK</td>
<td>No</td>
<td>2436</td>
<td>4</td>
</tr>
<tr>
<td>junos:SABAH</td>
<td>No</td>
<td>2574</td>
<td>3</td>
</tr>
<tr>
<td>junos:AFREECA</td>
<td>No</td>
<td>2373</td>
<td>2</td>
</tr>
<tr>
<td>junos:SENEWEB</td>
<td>No</td>
<td>2068</td>
<td>1</td>
</tr>
<tr>
<td>junos:DIINO</td>
<td>No</td>
<td>776</td>
<td>5</td>
</tr>
<tr>
<td>junos:CARE2</td>
<td>No</td>
<td>376</td>
<td>4</td>
</tr>
<tr>
<td>junos:MOBAGE</td>
<td>No</td>
<td>1456</td>
<td>3</td>
</tr>
<tr>
<td>junos:CARTOONNETWORK</td>
<td>No</td>
<td>982</td>
<td>2</td>
</tr>
<tr>
<td>junos:AVATARS-UNITED</td>
<td>No</td>
<td>363</td>
<td>1</td>
</tr>
<tr>
<td>junos:CONVIVA</td>
<td>No</td>
<td>2015</td>
<td>5</td>
</tr>
<tr>
<td>junos:DREAMORA</td>
<td>No</td>
<td>1725</td>
<td>4</td>
</tr>
<tr>
<td>junos:ELWATANNEWS</td>
<td>No</td>
<td>2381</td>
<td>3</td>
</tr>
</tbody>
</table>
```
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
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 detail (Junos OS Release 20.2R1)

user@host> show services application-identification application detail

Application Name: test
Application type: TEST
Description: N/A
Application ID: 16777221
Priority: high
Order: 65500
Disabled: No
Cacheable: No
Activation Date: N/A
Last Modified: N/A

Underlying consolidated Protocols/ports application is dependent on:

Protocols:
  Protocol: junos:HTTP / 67
  Protocol: junos:UDP / 216
  Protocol: junos:TCP / 205
  Protocol: junos:NET-PROXY / 2629
  Protocol: junos:SPDY / 1469
  Protocol: junos:SSL / 199
  Protocol: junos:LIBJINGLE-PSEUDOTCP / 3237
  Protocol: junos:STUN / 201
  Protocol: junos:HTTPS / 68
Protocol: junos:HTTP / 67
Protocol: junos:HTTP2 / 2553
Protocol: junos:HTTP-TUNNEL / 750
Protocol: junos:HTTP-PROXY / 2956
Protocol: junos:HAPROXY / 3331
Protocol: junos:COTP / 22

TCP Ports:
Port: 80
Port: 3128
Port: 8000
Port: 8080

Layer-7 Immediate Protocol(s):
Protocol: HTTP / 67
Signature: fgnm
Port range: N/A
Member(s): 1
Member m01
  Depth: 4
  Context: http-get-url-parsed-param-parsed
  Pattern: ads
  Direction: CTS
show services application-identification application-system-cache (View)

Syntax

```
show services application-identification application-system-cache
<logical-system (logical-system-name | all | root-logical-system)>
<tenant (tenant-name | all)>
```

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.

logical-system option introduced in Junos OS Release 18.3R1.
tenant option introduced in Junos OS Release 19.4R1.

Description

Displays application ID from default port/protocol binding or from the application system cache.

Options

none—Displays application system cache for the root logical system, all logical systems, and all tenant systems.

logical-system logical-system-name—(Optional) Displays application system cache for the specified logical system.

logical-system all—(Optional) Displays application system cache for all the logical systems.

root-logical-system—(Optional) Displays application system cache for the root logical system.

tenant tenant-name—(Optional) Displays application system cache for the specified tenant system.

tenant all—(Optional) Displays application system cache for all the tenant systems.

Required Privilege Level

view

RELATED DOCUMENTATION

| clear services application-identification application-system-cache (Junos OS) | 682 |
List of Sample Output

show services application-identification application-system-cache on page 831
show services application-identification application-system-cache (Application System Cache Changes with Unified Policy Support) on page 831
show services application-identification application-system-cache on page 832
show services application-identification application-system-cache tenant TSYS1 on page 832
show services application-identification application-system-cache tenant all on page 832

Output Fields

Table 81 on page 830 and Table 82 on page 830 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 81: show services application-identification application-system-cache Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application-cache</td>
<td>On or Off status of the application cache.</td>
</tr>
<tr>
<td>nested-application-cache</td>
<td>On or Off status of the nested application cache.</td>
</tr>
<tr>
<td>cache-unknown-result</td>
<td>On or Off status for caching unknown results.</td>
</tr>
<tr>
<td>cache-entry-timeout</td>
<td>The number of seconds the mapping information is saved.</td>
</tr>
<tr>
<td>pic</td>
<td>PIC number of the accumulated statistics.</td>
</tr>
<tr>
<td>Logical system name</td>
<td>Name of a specific logical system.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Type of protocol.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Yes or No to identify the traffic as encrypted or not.</td>
</tr>
</tbody>
</table>

Table 82: show services application-identification application-system-cache Output Fields (For Unified Policies)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application-cache</td>
<td>On or Off status of the application cache.</td>
</tr>
</tbody>
</table>

Table 82: show services application-identification application-system-cache Output Fields (For Unified Policies) (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache lookup for security-services</td>
<td>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.</td>
</tr>
<tr>
<td>Cache lookup for miscellaneous-services</td>
<td>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.</td>
</tr>
<tr>
<td>cache-entry-timeout</td>
<td>The number of seconds the mapping information is saved.</td>
</tr>
</tbody>
</table>

Sample Output

```
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

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:
```
show services application-identification application-system-cache

user@host:TSYS1> 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
pic: 0/0
Logical system name: TSYS1
IP address: 4.0.0.1  Port: 22  Protocol: TCP
Application: SSH  Encrypted: No
Classification Path: IP:TCP:SSH

show services application-identification application-system-cache tenant TSYS1

user@host> show services application-identification application-system-cache tenant TSYS1

Application System Cache Configurations:
  application-cache: on
  Cache lookup for security-services: off
  Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: TSYS1
IP address: 192.0.2.0  Port: 22  Protocol: TCP
Application: SSH  Encrypted: No
Classification Path: IP:TCP:SSH

show services application-identification application-system-cache tenant all

user@host> show services application-identification application-system-cache tenant all

Application System Cache Configurations:
  application-cache: on
  Cache lookup for security-services: off
Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: TSYS1
IP address: 192.0.2.0 Port: 22 Protocol: TCP
Application: SSH Encrypted: No
Classification Path: IP:TCP:SSH

pic: 0/0
Logical system name: TSYS2
IP address: 203.0.113.0 Port: 22 Protocol: TCP
Application: SSH Encrypted: No
Classification Path: IP:TCP:SSH
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 | 696

List of Sample Output
show services application-identification commit-status on page 834
show services application-identification commit-status on page 834
show services application-identification commit-status on page 835

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>
<logical-system (logical-system-name | all | root-logical-system)>
<tenant (tenant-name | all)>
```

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.  
logical-system option introduced in Junos OS Release 18.3R1.  
tenant option introduced in Junos OS Release 19.4R1.

Description
Display the status of all Junos OS application identification counter values per SPU.

Options

none—Displays the application identification counter for the root logical system, all logical systems, and all tenant systems.

ssl-encrypted-sessions—(Optional) Displays counters for SSL encrypted sessions.

logical-system logical-system-name—(Optional) Displays the application identification counter for the specified logical system.

logical-system all—(Optional) Displays the application identification counter for all the logical systems.

root-logical-system—(Optional) Displays the application identification counter for the root logical system.

tenant tenant-name—(Optional) Displays the application identification counter for the specified tenant system.

tenant all—(Optional) Displays the application identification counter for all the tenant systems.

Required Privilege Level
view

RELATED DOCUMENTATION
clear services application-identification counter (Values) | 684

List of Sample Output

- show services application-identification counter ssl-encrypted-sessions on page 839
- show services application-identification counter on page 840
- show services application-identification counter logical-system all on page 841
- show services application-identification counter on page 841
- show services application-identification counter tenant all on page 842

Output Fields

Table 83 on page 837 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 83: show services application-identification counter Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC</td>
<td>PIC number of the accumulated statistics.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, and SRX345 devices.</td>
</tr>
<tr>
<td>Unknown applications</td>
<td>Number of unknown applications.</td>
</tr>
<tr>
<td>Encrypted unknown applications</td>
<td>Number of encrypted unknown applications.</td>
</tr>
<tr>
<td>Cache hits</td>
<td>Number of sessions that matched the application in the AI cache.</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>Number of packet plugin hits in a session.</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>Number of stream plugin hits in a session.</td>
</tr>
<tr>
<td>Cache misses</td>
<td>Number of sessions that did not find the application in the AI cache.</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>Number of packet plugin miss in a session.</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>Number of stream plugin miss in a session</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>Number of client-to-server packets processed.</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>Number of server-to-client packets processed.</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>Number of client-to-server payload bytes processed.</td>
</tr>
</tbody>
</table>
Table 83: show services application-identification counter Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server-to-client layer bytes processed</td>
<td>Number of server-to-client payload bytes processed.</td>
</tr>
<tr>
<td>Client-to-server encrypted packets processed</td>
<td>Number of client-to-server encrypted packets processed.</td>
</tr>
<tr>
<td>Server-to-client encrypted packets processed</td>
<td>Number of server-to-client encrypted packets processed.</td>
</tr>
<tr>
<td>Client-to-server encrypted bytes processed</td>
<td>Number of client-to-server encrypted payload bytes processed.</td>
</tr>
<tr>
<td>Server-to-client encrypted bytes processed</td>
<td>Number of server-to-client encrypted payload bytes processed.</td>
</tr>
<tr>
<td>Sessions bypassed due to resource allocation failure</td>
<td>Number of sessions bypassed due to resource allocation failure.</td>
</tr>
<tr>
<td>Segment case 1 - New segment to left</td>
<td>Number of TCP segments contained before the previous segment.</td>
</tr>
<tr>
<td>Segment case 2 - New segment overlap right</td>
<td>Number of TCP segments that start before the previous segment and are contained in it</td>
</tr>
<tr>
<td>Segment case 3 - Old segment overlapped</td>
<td>Number of TCP segments that start before the previous segment and extend beyond it.</td>
</tr>
<tr>
<td>Segment case 4 - New segment overlapped</td>
<td>Number of TCP segments that start and end within the previous segment.</td>
</tr>
<tr>
<td>Segment case 5 - New segment overlap left</td>
<td>Number of TCP segments that start within the previous segments and extend beyond it.</td>
</tr>
<tr>
<td>Segment case 6 - New segment to right</td>
<td>Number of TCP segments that start after the previous segment. This is the normal case.</td>
</tr>
</tbody>
</table>
### Sample Output

```
show services application-identification counter ssl-encrypted-sessions
user@host> show services application-identification counter ssl-encrypted-sessions
```

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI cache hits</td>
<td>0</td>
</tr>
<tr>
<td>AI cache hits by nested application</td>
<td>0</td>
</tr>
<tr>
<td>AI cache misses</td>
<td>0</td>
</tr>
<tr>
<td>AI matches</td>
<td>0</td>
</tr>
<tr>
<td>AI uni-matches</td>
<td>0</td>
</tr>
<tr>
<td>AI no-matches</td>
<td>0</td>
</tr>
<tr>
<td>AI partial matches</td>
<td>0</td>
</tr>
<tr>
<td>AI no-partial matches</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that triggered Appid create session API</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that do not incur signature match or decoding</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that incur signature match or decoding</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server layer-7 bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client layer-7 bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Terminal first data packets on both direction</td>
<td>0</td>
</tr>
</tbody>
</table>

```
pic: 1/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI cache hits</td>
<td>0</td>
</tr>
<tr>
<td>AI cache hits by nested application</td>
<td>0</td>
</tr>
<tr>
<td>AI cache misses</td>
<td>0</td>
</tr>
<tr>
<td>AI matches</td>
<td>0</td>
</tr>
<tr>
<td>AI uni-matches</td>
<td>0</td>
</tr>
<tr>
<td>AI no-matches</td>
<td>0</td>
</tr>
<tr>
<td>AI partial matches</td>
<td>0</td>
</tr>
<tr>
<td>AI no-partial matches</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that triggered Appid create session API</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that do not incur signature match or decoding</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that incur signature match or decoding</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server layer-7 bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client layer-7 bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Terminal first data packets on both direction</td>
<td>0</td>
</tr>
</tbody>
</table>
```

```
pic: 1/1

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI cache hits</td>
<td>0</td>
</tr>
<tr>
<td>AI cache hits by nested application</td>
<td>0</td>
</tr>
<tr>
<td>AI cache misses</td>
<td>0</td>
</tr>
<tr>
<td>AI matches</td>
<td>0</td>
</tr>
<tr>
<td>AI uni-matches</td>
<td>0</td>
</tr>
<tr>
<td>AI no-matches</td>
<td>0</td>
</tr>
<tr>
<td>AI partial matches</td>
<td>0</td>
</tr>
<tr>
<td>AI no-partial matches</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that triggered Appid create session API</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that do not incur signature match or decoding</td>
<td>0</td>
</tr>
<tr>
<td>Sessions that incur signature match or decoding</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server layer-7 bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client layer-7 bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Terminal first data packets on both direction</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show services application-identification counter

user@host> show services application-identification counter

Logical System: root-logical-system

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Encrypted unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions bypassed due to resource allocation failure</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 1 - New segment to left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 2 - New segment overlap right</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 3 - Old segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 4 - New segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 5 - New segment overlap left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 6 - New segment to right</td>
<td>0</td>
</tr>
</tbody>
</table>

Tenant: TSYS1

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Encrypted unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>983</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>82572</td>
</tr>
<tr>
<td>Server-to-client bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted packets processed</td>
<td>0</td>
</tr>
</tbody>
</table>
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

show services application-identification counter logical-system all

user@host> show services application-identification counter logical-system all

Logical System: root-logical-system\pic: 0/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Encrpted unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions bypassed due to resource allocation failure</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 1 - New segment to left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 2 - New segment overlap right</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 3 - Old segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 4 - New segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 5 - New segment overlap left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 6 - New segment to right</td>
<td>0</td>
</tr>
</tbody>
</table>

show services application-identification counter

user@host:TSYS1> show services application-identification counter
Tenant: TSYS1

pic: 0/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Encrypted unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>5</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>1</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>1169</td>
</tr>
<tr>
<td>Server-to-client bytes processed</td>
<td>73</td>
</tr>
<tr>
<td>Client-to-server encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions bypassed due to resource allocation failure</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 1 - New segment to left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 2 - New segment overlap right</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 3 - Old segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 4 - New segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 5 - New segment overlap left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 6 - New segment to right</td>
<td>0</td>
</tr>
</tbody>
</table>

show services application-identification counter tenant all

user@host> show services application-identification counter tenant all

Tenant: TSYS1

pic: 0/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Encrypted unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>1006</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>84504</td>
</tr>
<tr>
<td>Server-to-client bytes processed</td>
<td>0</td>
</tr>
</tbody>
</table>
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

Tenant: TSYS2

pic: 0/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Encrypted unknown applications</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache hits stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses pkt-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Cache misses stream-plugin</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server packets processed</td>
<td>1006</td>
</tr>
<tr>
<td>Server-to-client packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server bytes processed</td>
<td>84504</td>
</tr>
<tr>
<td>Server-to-client bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted packets processed</td>
<td>0</td>
</tr>
<tr>
<td>Client-to-server encrypted bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Server-to-client encrypted bytes processed</td>
<td>0</td>
</tr>
<tr>
<td>Sessions bypassed due to resource allocation failure</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 1 - New segment to left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 2 - New segment overlap right</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 3 - Old segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 4 - New segment overlapped</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 5 - New segment overlap left</td>
<td>0</td>
</tr>
<tr>
<td>Segment case 6 - New segment to right</td>
<td>0</td>
</tr>
</tbody>
</table>
show services application-identification entries

Syntax

```
show services application-identification entries (detail | filter)
```

Release Information

Command introduced in Junos OS Release 18.4R1.
The `category-list` and `subcategory-list` options are introduced in the Junos OS Release 19.1R1.

Description

Displays detailed information or filtered information about a specified application signature or group signature, detailed information about all application signatures or application group signatures. Used to Support and improve the J-Web search mechanism and to search the applications easily.

Options

detail — Displays detailed information for all application signatures or application group signatures.

filter — Displays filtered information about a specified application signatures or application group signatures. Apply filter details like the `show services application-identification entries filter type application limit 1 offset 5` command. Similarly, any combination from allowed filters can be used.

category-list — Displays the list of categories of available application signatures or application group signatures.

subcategory-list — Displays the list of subcategories of available application signatures or application group signatures.

Required Privilege Level

view

RELATED DOCUMENTATION

| request services application-identification application | 696 |

List of Sample Output

- `show services application-identification entries detail on page 845`
- `show services application-identification entries filter on page 845`

Output Fields

The below table lists the output fields for the `show services application-identification entries` command.
Table 84: show services application-identification entries Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry-name</td>
<td>Entry by name of the application or the group.</td>
</tr>
<tr>
<td>Entry Type</td>
<td>Type the application name or the group name to filter by application or group entry.</td>
</tr>
<tr>
<td>Entry Category</td>
<td>Entry by entry category name.</td>
</tr>
<tr>
<td>Entry Subcategory</td>
<td>Entry by subcategory name of the application.</td>
</tr>
<tr>
<td>Entry Risk</td>
<td>Entry risk. ID numbers 1 to 5. The default value is -1 when the risk is not configured.</td>
</tr>
<tr>
<td>Entry Characteristic</td>
<td>Entry by entry characteristic name.</td>
</tr>
<tr>
<td>Entry Status</td>
<td>Entry status enabled or disabled.</td>
</tr>
<tr>
<td>Entry Predefined</td>
<td>Entry by predefined or custom entry.</td>
</tr>
<tr>
<td>Total Entries</td>
<td>Number of entries in the application or group.</td>
</tr>
</tbody>
</table>

Sample Output

`show services application-identification entries detail`

`user@host> show services application-identification entries detail`

```
Entry Name: c1
Entry Type: application
Entry Category: (null)
Entry Subcategory: (null)
Entry Risk: -1
Entry Characteristic: (null)
Entry Status: enabled
Entry Predefined: custom
Total Entries: 1
```

`show services application-identification entries filter`

`user@host> show services application-identification entries filter type application limit 1 offset 5`
Entry Name: junos:104COM
Entry Type: application
Entry Category: Web
Entry Subcategory: miscellaneous
Entry Risk: 2
Entry Status: enabled
Entry Predefined: predefined
Total Entries: 1
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 | 702 |

List of Sample Output

show services application-identification group summary on page 848
show services application-identification group detail on page 848

Output Fields

Table 85 on page 847 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 85: show services application-identification group Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the specified application in the detailed display.</td>
</tr>
</tbody>
</table>
Table 85: show services application-identification group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group ID or ID</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Disabled</strong></td>
<td>The status of the application signature group and whether the signature method is currently used to identify this application. The default is No.</td>
</tr>
<tr>
<td><strong>Application Group(s)</strong></td>
<td>The application signature groups present.</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td>The application signatures associated with this application signature group.</td>
</tr>
</tbody>
</table>

**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 packet-capture counters

Syntax

```
show services application-identification packet-capture counters
```

Release Information

Command introduced in Junos OS Release 20.2R1.

Description

Display the packet capture counter details for unknown application traffic.

Required Privilege Level

```
view
```

RELATED DOCUMENTATION

- Configure Packet Capture of Unknown Application Traffic | 49
- packet-capture | 583
- request services application-identification clear packet-capture all | 698
- clear services application-identification packet-capture counters | 686

Output Fields

Table 72 on page 766 lists the output fields for the `show services application-identification packet-capture counters` command. Output fields are listed in the approximate order in which they appear.

Table 86: show services application-identification packet-capture counters

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total sessions captured</td>
<td>Total number of sessions captured in the packet capture file</td>
</tr>
<tr>
<td>Total packets captured</td>
<td>Total number of packets captured in the packet capture file</td>
</tr>
<tr>
<td>Active sessions being captured</td>
<td>Number of active sessions currently being captured in the packet capture file</td>
</tr>
<tr>
<td>Sessions ignored because of memory allocation failures</td>
<td>Number of sessions not captured in the packet capture file because of memory allocation failure</td>
</tr>
</tbody>
</table>
Table 86: show services application-identification packet-capture counters (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets ignored because of memory allocation failures</td>
<td>Number of packets not captured in the packet capture file because of memory allocation failure</td>
</tr>
<tr>
<td>Ipc messages ignored because of storage limit</td>
<td>Number of interprocess communication (IPC) messages ignored because the storage limit is reached</td>
</tr>
<tr>
<td>Sessions ignored because of buffer-packets limit</td>
<td>Number of sessions not captured in the packet capture file because the buffer packet limit is reached</td>
</tr>
<tr>
<td>Packets ignored because of buffer-packets limit</td>
<td>Number of packets not captured in packet capture file because buffer packet limit has reached</td>
</tr>
<tr>
<td>Inconclusive sessions captured</td>
<td>Number of inconclusive sessions captured in the packet capture file</td>
</tr>
<tr>
<td>Inconclusive sessions ignored</td>
<td>Number of inconclusive sessions not captured in the packet capture file</td>
</tr>
<tr>
<td>Cache entries timed out</td>
<td>Number of times the cache entries timeout value is reached</td>
</tr>
</tbody>
</table>

Sample Output

```
show services application-identification packet-capture counters

user@host> show services application-identification packet-capture counters

pic: 0/0

<table>
<thead>
<tr>
<th>Counter type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total sessions captured</td>
<td>1</td>
</tr>
<tr>
<td>Total packets captured</td>
<td>6</td>
</tr>
<tr>
<td>Active sessions being captured</td>
<td>0</td>
</tr>
<tr>
<td>Sessions ignored because of memory allocation failures</td>
<td>0</td>
</tr>
<tr>
<td>Packets ignored because of memory allocation failures</td>
<td>0</td>
</tr>
<tr>
<td>Ipc messages ignored because of storage limit</td>
<td>0</td>
</tr>
<tr>
<td>Sessions ignored because of buffer-packets limit</td>
<td>0</td>
</tr>
<tr>
<td>Packets ignored because of buffer-packets limit</td>
<td>0</td>
</tr>
<tr>
<td>Inconclusive sessions captured</td>
<td>0</td>
</tr>
<tr>
<td>Inconclusive sessions ignored</td>
<td>0</td>
</tr>
<tr>
<td>Cache entries timed out</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show services application-identification statistics applications

Syntax

```
show services application-identification statistics applications
    interval
        <logical-system (logical-system-name | all | root-logical-system)>
        <tenant (tenant-name | all)>
```

Release Information

Command introduced in Junos OS Release 11.4.
Command updated in Junos OS Release 12.1.

**logical-system** option introduced in Junos OS Release 18.3R1.
Command is updated to include micro-applications in Junos OS Release 19.2R1.

**tenant** option introduced in Junos OS Release 19.4R1.

Description

Displays application usage statistics.

Options

**none**—Displays the application identification statistics for the root logical system, all logical systems, and all tenant systems.

**interval**—(Optional) Displays interval statistics per application. Interval statistics are displayed in Top-N format, such that the first application displayed has the largest byte count. The default interval is 1, if no parameter is specified. The current interval is 1.

**logical-system logical-system-name**—(Optional) Displays the application identification statistics for the specified logical system.

**logical-system all**—(Optional) Displays the application identification statistics for all the logical systems.

**root-logical-system**—(Optional) Displays the application identification statistics for the root logical system.

**tenant tenant-name**—(Optional) Displays the application identification statistics for the specified tenant system.

**tenant all**—(Optional) Displays the application identification statistics for all the tenant systems.

Required Privilege Level

view
RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>statistics (Services)</th>
<th>635</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear services application-identification application-statistics</td>
<td>679</td>
</tr>
</tbody>
</table>

List of Sample Output

show services application-identification statistics applications on page 854
show services application-identification statistics applications interval 1 on page 854
show services application-identification statistics applications logical-system all on page 854
show services application-identification statistics applications on page 854
show services application-identification statistics applications on page 854
show services application-identification statistics applications tenant TSYS1 on page 855
show services application-identification statistics applications tenant all on page 855
show services application-identification statistics applications interval 1 on page 855

Output Fields

Table 87 on page 853 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 87: show services application-identification statistics applications Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Name of the application or micro-application.</td>
</tr>
<tr>
<td>Sessions</td>
<td>Number of sessions for the application.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Size of the application in bytes.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When an SRX Series device is operating in chassis cluster mode (Active/Active mode - Z mode), the <code>show services application-identification statistics applications</code> 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.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Yes or No identifying the traffic as encrypted or not.</td>
</tr>
<tr>
<td>Last Reset</td>
<td>Displays date, time, and how long ago the statistics for the sessions were cleared. The format None specified is <code>year-month-day hour:minute:second timezone</code>. If you did not clear the statistics previously at any point, <strong>Never</strong> is displayed.</td>
</tr>
</tbody>
</table>
Sample Output

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSLOG</td>
<td>2</td>
<td>18610</td>
<td></td>
</tr>
</tbody>
</table>

show services application-identification statistics applications interval 1
user@host> show services application-identification statistics applications interval 1

Logical System: root-logical-system
Interval Start: 2018-07-16 16:11:27 PDT
Elapsed time: 04:47:50

show services application-identification statistics applications logical-system all
user@host> show services application-identification statistics applications logical-system all

Logical System: root-logical-system
Last Reset: 2018-06-21 16:11:21 PDT

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>1</td>
<td>6022</td>
<td>No</td>
</tr>
<tr>
<td>ICMP-ECHO</td>
<td>12</td>
<td>1764</td>
<td>No</td>
</tr>
</tbody>
</table>

show services application-identification statistics applications
user@host:TSYS1> show services application-identification statistics applications
Tenant: TSYS1  
Last Reset: 2019-05-13 03:02:56 PDT  

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP-ECHO</td>
<td>10</td>
<td>1680</td>
<td>No</td>
</tr>
</tbody>
</table>

```
show services application-identification statistics applications tenant TSYS1
user@host> show services application-identification statistics applications tenant TSYS1
```

Tenant: TSYS1  
Last Reset: 2019-05-12 23:47:58 PDT  

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP-ECHO</td>
<td>3</td>
<td>504</td>
<td>No</td>
</tr>
<tr>
<td>SSH</td>
<td>1</td>
<td>10890</td>
<td>No</td>
</tr>
</tbody>
</table>

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

Tenant: TSYS1  
Last Reset: 2019-05-12 23:47:58 PDT  

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP-ECHO</td>
<td>3</td>
<td>504</td>
<td>No</td>
</tr>
<tr>
<td>SSH</td>
<td>1</td>
<td>10890</td>
<td>No</td>
</tr>
</tbody>
</table>

Tenant: TSYS2  
Last Reset: 2019-05-12 23:47:58 PDT  

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP-ECHO</td>
<td>3</td>
<td>504</td>
<td>No</td>
</tr>
<tr>
<td>SSH</td>
<td>1</td>
<td>10890</td>
<td>No</td>
</tr>
</tbody>
</table>

```
show services application-identification statistics applications interval 1
user@host:TSYS1> show services application-identification statistics applications interval 1
```

Tenant: TSYS1  
Interval Start: 2019-05-13 03:04:16 PDT  
Elapsed time: 00:00:04  

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Bytes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP-ECHO</td>
<td>4</td>
<td>672</td>
<td>No</td>
</tr>
</tbody>
</table>
show services application-identification statistics application-groups

Syntax

```
show services application-identification statistics applications
<interval>
<logical-system (logical-system-name | all | root-logical-system)>
<tenant (tenant-name | all)>
```

Release Information

Command introduced in Junos OS Release 11.4.
logical-system option introduced in Junos OS Release 18.3R1.
tenant option introduced in Junos OS Release 19.4R1.

Description

Displays application group usage statistics.

Options

none—Displays application group usage statistics for the root logical system, all logical systems, and all tenant systems.

interval—(Optional) Displays 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. The default interval is 1, if no parameter is specified. The current interval is 1.

logical-system logical-system-name—(Optional) Displays application group usage statistics for the specified logical system.

logical-system all—(Optional) Displays application group usage statistics for all the logical systems.

root-logical-system—(Optional) Displays application group usage statistics for the root logical system.

tenant tenant-name—(Optional) Displays application group usage statistics for the specified tenant system.

tenant all—(Optional) Displays application group usage statistics for all the tenant systems.

Required Privilege Level

view

RELATED DOCUMENTATION

| statistics (Services) | 635 |
List of Sample Output
show services application-identification statistics application-groups on page 857
show services application-identification statistics application-groups interval 1 on page 858
show services application-identification statistics application-groups logical-system all on page 858
show services application-identification statistics application-groups on page 858
show services application-identification statistics application-groups tenant TSYS1 on page 858
show services application-identification statistics application-groups tenant all on page 859

Output Fields
Table 88 on page 857 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 88: show services application-identification statistics application-groups Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Reset</td>
<td>Displays date, time, and how long ago the statistics for the sessions were cleared. The format None specified is <code>in-year-month-day hour:minute:second timezone</code>. If you did not clear the statistics previously at any point, <strong>Never</strong> is displayed.</td>
</tr>
<tr>
<td>Application Group</td>
<td>Displays the name of the application group.</td>
</tr>
<tr>
<td>Sessions</td>
<td>Displays the number of sessions for the application group.</td>
</tr>
<tr>
<td>Kilo Bytes</td>
<td>Displays the size of the application group in kilobytes.</td>
</tr>
</tbody>
</table>

**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
```
### show services application-identification statistics application-groups interval 1

```
user@host>  show services application-identification statistics application-groups interval 1

Logical System: root-logical-system
Interval Start: 2018-07-16 16:11:27 PDT
Elapsed time: 04:56:01
```

### show services application-identification statistics application-groups logical-system all

```
user@host>  show services application-identification statistics application-groups logical-system all

Logical System: root-logical-system
Last Reset: 2018-06-21 16:11:21 PDT
```

### show services application-identification statistics application-groups

```
user@host:TSYS1>  show services application-identification statistics application-groups

Tenant: TSYS1
Last Reset: 2019-05-12 23:47:58 PDT

<table>
<thead>
<tr>
<th>Application Group</th>
<th>Sessions</th>
<th>Kilo Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>junos:infrastructure</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>junos:infrastructure:networking</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>junos:infrastructure:networking:icmp</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>junos:remote-access</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>junos:remote-access:command</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>junos:remote-access:tunneling</td>
<td>1</td>
<td>10</td>
</tr>
</tbody>
</table>
```

### show services application-identification statistics application-groups tenant TSYS1

```
user@host>  show services application-identification statistics application-groups tenant TSYS1

Tenant: TSYS1
Last Reset: 2019-05-12 23:47:58 PDT

<table>
<thead>
<tr>
<th>Application Group</th>
<th>Sessions</th>
<th>Kilo Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>junos:infrastructure</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>junos:encryption</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>junos:infrastructure:monitoring</td>
<td>2</td>
<td>18</td>
</tr>
</tbody>
</table>
```
show services application-identification statistics application-groups tenant all

user@host> show services application-identification statistics application-groups tenant all

<table>
<thead>
<tr>
<th>Tenant: TSYS1</th>
<th>Last Reset: 2019-05-12 23:47:58 PDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Group</td>
<td>Sessions</td>
</tr>
<tr>
<td>junos:infrastructure</td>
<td>3</td>
</tr>
<tr>
<td>junos:infrastructure:networking</td>
<td>3</td>
</tr>
<tr>
<td>junos:infrastructure:networking:icmp</td>
<td>3</td>
</tr>
<tr>
<td>junos:remote-access</td>
<td>1</td>
</tr>
<tr>
<td>junos:remote-access:command</td>
<td>1</td>
</tr>
<tr>
<td>junos:remote-access:tunneling</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Group</td>
<td>Sessions</td>
</tr>
<tr>
<td>junos:infrastructure</td>
<td>3</td>
</tr>
<tr>
<td>junos:infrastructure:networking</td>
<td>3</td>
</tr>
<tr>
<td>junos:infrastructure:networking:icmp</td>
<td>3</td>
</tr>
<tr>
<td>junos:remote-access</td>
<td>1</td>
</tr>
<tr>
<td>junos:remote-access:command</td>
<td>1</td>
</tr>
<tr>
<td>junos:remote-access:tunneling</td>
<td>1</td>
</tr>
</tbody>
</table>
show services application-identification status

Syntax

```
show services application-identification status
```

Release Information
Command introduced in Junos OS Release 12.1X47-D10.
Command introduced in Junos OS Release 18.3R1 for logical systems.

Description
Displays detailed information about application identification status.

Required Privilege Level
view

RELATED DOCUMENTATION
request services application-identification application | 696

List of Sample Output
show services application-identification status on page 862
show services application-identification status (Junos OS Release 19.2R1 and Later) on page 863
show services application-identification status (DPI Performance Mode Enabled) on page 864
show services application-identification status (Logical Systems) on page 866
show services application-identification status (Micro-Applications) on page 867

Output Fields
Table 89 on page 860 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 89: show services application-identification status Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status of application identification: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Sessions under app detection</td>
<td>Sessions undergoing application identification detection.</td>
</tr>
<tr>
<td>Engine Version</td>
<td>Application identification detector engine version. This field displays <strong>0</strong> when there is no JDPI-Decoder engine installed or uninstalled, and displays the JDPI-Decoder engine version when it is installed.</td>
</tr>
</tbody>
</table>
Table 89: show services application-identification status Output Fields  *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max TCP session packet memory</td>
<td>Maximum number of TCP sessions that application identification maintains.</td>
</tr>
<tr>
<td>Force packet plugin</td>
<td>Force packet plugin status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Force stream plugin</td>
<td>Force stream plugin status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>DPI Performance mode</td>
<td>DPI performance mode status. This field is displayed only if the DPI performance mode is enabled.</td>
</tr>
<tr>
<td>Statistics collection interval</td>
<td>Frequency (in minutes) for collecting statistics.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of application system cache: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Negative cache status</td>
<td>Status on the number of sessions that reach the Unknown cache entry: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Max Number of entries in cache</td>
<td>Maximum number of cache entries.</td>
</tr>
<tr>
<td>Cache timeout</td>
<td>Idle timeout after which the cache entries expires.</td>
</tr>
<tr>
<td>Download Server CGI</td>
<td>Name of the server from where protocol bundle was downloaded.</td>
</tr>
<tr>
<td>Auto Update</td>
<td>Status of auto update to receive protocol bundle updates from the server: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of protocol bundle: <strong>Active</strong> or <strong>Free</strong>.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of protocol bundle.</td>
</tr>
<tr>
<td>Or PB Version</td>
<td>NOTE: Starting from Junos OS Release 17.4R1, the field <strong>PB Version</strong> is used for displaying version of the protocol bundle.</td>
</tr>
<tr>
<td>Proxy Profile</td>
<td>Display the proxy profile name.</td>
</tr>
<tr>
<td></td>
<td>If you have disabled proxy server for downloading application signature package, the <strong>Proxy Profile</strong> displays <strong>Not Configured</strong>.</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>Display the IP address and the port number of the proxy server.</td>
</tr>
<tr>
<td>Session</td>
<td>The number of active sessions.</td>
</tr>
</tbody>
</table>
Table 89: show services application-identification status Output Fields  *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro apps version</td>
<td>The version of micro-applications.</td>
</tr>
<tr>
<td>Session</td>
<td>The number of active sessions.</td>
</tr>
</tbody>
</table>

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.

Starting in Junos OS Release 12.3X48-D80, on SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 Series devices, the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) engine is separated from Junos OS and allows you to download the JDPI-Decoder engine along with the protobundle. This implementation allows you to upgrade the JDPI-Decoder engine separately without upgrading Junos OS.

However, if you require latest versions of the protocol bundle, you must download and install the application signature package separately.

Starting in Junos OS Release 19.2R1, Junos OS Release 15.1X49-D200, and Junos OS Release 12.3X48-D95, the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) engine comes with a default application signature package version 999 that includes the protobundle version 1.380.0-64.005 and the JDPI-Decoder engine version 5.3.0-56. You can upgrade the application signature package when a new signature package version is available.

---

**Sample Output**

```shell
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
```
show services application-identification status (Junos OS Release 19.2R1 and Later)

user@host>  show services application-identification status

Application Identification
Status: Enabled
Sessions under app detection: 0
Max TCP session packet memory: 0
Force packet plugin: Disabled
Force stream plugin: Disabled
DPI Performance mode: Enabled
Statistics collection interval: 1440 (in minutes)

Application System Cache
Status: Enabled
Cache lookup security-services: Enabled
Cache lookup miscellaneous-services: Enabled
Max Number of entries in cache: 0
Cache timeout: 3600 (in seconds)

Protocol Bundle
Download Server: https://devdb.secteam.juniper.net/cgi-bin/index.cgi
AutoUpdate: Disabled
Proxy Details
Proxy Profile                     Not Configured
Slot 1:
  Application package version       50041
  Status                            Active
  PB Version                        1.380.0-64.005 (build date May 6 2019)
  Engine version                    5.3.0-56 (build date Mar 6 2019)
  Micro-App Version                 0
  Sessions                          0

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
### show services application-identification status (Application Identification Detector Engine Version)

<table>
<thead>
<tr>
<th>Application Identification</th>
<th>Status</th>
<th>Sessions under app detection</th>
<th>Max TCP session packet memory</th>
<th>Force packet plugin</th>
<th>Force stream plugin</th>
<th>Statistics collection interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Enabled</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1 (in minutes)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application System Cache</th>
<th>Status</th>
<th>Max Number of entries in cache</th>
<th>Cache timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Enabled</td>
<td>131072</td>
<td>3600 (in seconds)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Bundle</th>
<th>Download Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>antigen</td>
<td>Download Server</td>
</tr>
</tbody>
</table>

| user@host> show services application-identification status |
show services application-identification status (Logical Systems)
user@host> show services application-identification status

Application Identification
Status: Enabled
Sessions under app detection: 0
Max TCP session packet memory: 0
Force packet plugin: Disabled
Force stream plugin: Disabled
DPI Performance mode: Enabled
Statistics collection interval: 1440 (in minutes)

Application System Cache
Status: Enabled
Cache lookup security-services: Enabled
Cache lookup miscellaneous-services: Enabled
Max Number of entries in cache: 131072
Cache timeout: 3600 (in seconds)

Protocol Bundle
Download Server: https://signatures.juniper.net/cgi-bin/index.cgi

AutoUpdate: Disabled

Proxy Details
Proxy Profile: pl
Proxy Address: http://5.0.0.1:3128

Slot 1:
Application package version: 3058
Status: Active
PB Version: 1.340.0-57.005 (build date Apr 19 2018)
Engine version: 4.20.0-91 (build date Feb 27 2018)
Sessions: 0
### Application System Cache

<table>
<thead>
<tr>
<th>Status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache lookup security-services</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cache lookup miscellaneous-services</td>
<td>Enabled</td>
</tr>
<tr>
<td>Max Number of entries in cache</td>
<td>131072</td>
</tr>
<tr>
<td>Cache timeout</td>
<td>3600 (in seconds)</td>
</tr>
</tbody>
</table>

### Protocol Bundle

<table>
<thead>
<tr>
<th>Download Server</th>
<th><a href="https://services.netscreen.com/cgi-bin/index.cgi">https://services.netscreen.com/cgi-bin/index.cgi</a></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>AutoUpdate</th>
<th>Disabled</th>
</tr>
</thead>
</table>

### Proxy Details

<table>
<thead>
<tr>
<th>Proxy Profile</th>
<th>Not Configured</th>
</tr>
</thead>
</table>

### Slot 1:

<table>
<thead>
<tr>
<th>Application package version</th>
<th>534</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Active</td>
</tr>
<tr>
<td>PB Version</td>
<td>1.270.0-48.005 (build date May 22 2017)</td>
</tr>
<tr>
<td>Engine version</td>
<td>4.20.0-49.005 (build date May 22 2017)</td>
</tr>
<tr>
<td>Sessions</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**show services application-identification status (Micro-Applications)**

**user@host> show services application-identification status**

### Application Identification

<table>
<thead>
<tr>
<th>Status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions under app detection</td>
<td>0</td>
</tr>
<tr>
<td>Max TCP session packet memory</td>
<td>0</td>
</tr>
<tr>
<td>Force packet plugin</td>
<td>Disabled</td>
</tr>
<tr>
<td>Force stream plugin</td>
<td>Disabled</td>
</tr>
<tr>
<td>Statistics collection interval</td>
<td>1440 (in minutes)</td>
</tr>
</tbody>
</table>

### Application System Cache

<table>
<thead>
<tr>
<th>Status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache lookup security-services</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cache lookup miscellaneous-services</td>
<td>Disabled</td>
</tr>
<tr>
<td>Max Number of entries in cache</td>
<td>0</td>
</tr>
<tr>
<td>Cache timeout</td>
<td>3600 (in seconds)</td>
</tr>
</tbody>
</table>

### Protocol Bundle

<table>
<thead>
<tr>
<th>Download Server</th>
<th><a href="https://signatures.juniper.net/cgi-bin/index.cgi">https://signatures.juniper.net/cgi-bin/index.cgi</a></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>AutoUpdate</th>
<th>Disabled</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Proxy Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Profile</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Slot 1:</td>
<td></td>
</tr>
<tr>
<td>Application package version</td>
<td>3172</td>
</tr>
<tr>
<td>Status</td>
<td>Active</td>
</tr>
<tr>
<td>PB Version</td>
<td>1.380.0-64.005 (build date May 13 2019)</td>
</tr>
<tr>
<td>Engine version</td>
<td>5.3.0-56 (build date May 13 2019)</td>
</tr>
<tr>
<td>Micro-App Version</td>
<td>1.0.0-0</td>
</tr>
<tr>
<td>Sessions</td>
<td>0</td>
</tr>
</tbody>
</table>
show services application-identification version

Syntax

show services application-identification version

Release Information
Command introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 18.3R1 for logical systems.

Description
Displays the Junos OS application package version.

Required Privilege Level
view

RELATED DOCUMENTATION

| request services application-identification download | 699 |

List of Sample Output
show services application-identification version on page 869
show services application-identification version (Logical Systems) on page 869

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 application-identification version (Logical Systems)
The following output shows that the application package version is 534.

user@host> show services application-identification version
Application package version: 534
show services icap-redirect server status

Syntax

show services icap-redirect server status

Release Information

Command introduced in Junos OS Release 18.1R1.
The logical system option is introduced in Junos OS Release 18.3R1.

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 icap-redirect server status logical-system

user@host> show services icap-redirect server status logical-system LSYS1

ICAP Status :
   spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status:
   spu-2 Profile: icap-pfl Server: icap-svr1 : UP
ICAP Status:
   spu-3 Profile: icap-pfl Server: icap-svr1 : UP
show services icap-redirect statistic

Syntax

```
show services icap-redirect statistic
<all-logical-systems-tenants>
<root-logical-system>
<logical-system (logical-system-name | all)>
<tenant (tenant-name | all)>
```

Release Information

Command introduced in Junos OS Release 18.3R1.
tenant option introduced in Junos OS Release 20.1R1.

Description

Displays the ICAP services redirects statistic. ICAP services redirect redirects the HTTP or HTTPS traffic to any third-party server. The security device acts as an SSL proxy server and decrypts the pass-through traffic with the proper SSL profile under a security policy.

Options

- **all-logical-systems-tenants**—(Optional) Displays the ICAP services redirects statistic for the root logical system, all logical systems, and all tenant systems.
- **logical-system logical-system-name**—(Optional) Displays the ICAP services redirects statistic for the specified logical system.
- **logical-system all**—(Optional) Displays the ICAP services redirects statistic for all the logical systems.
- **root-logical-system**—(Optional) Displays the ICAP services redirects statistic for the root logical system.
- **tenant tenant-name**—(Optional) Displays the ICAP services redirects statistic for the specified tenant system.
- **tenant all**—(Optional) Displays the ICAP services redirects statistic for all the tenant systems.

Required Privilege Level

view

RELATED DOCUMENTATION

- ICAP Service Redirect | 416

List of Sample Output

show services icap-redirect statistic root-logical-system on page 874
show services icap-redirection statistic all-logical-systems-tenants on page 874
show services icap-redirection statistic logical-system LSYS1 on page 875
show services icap-redirection statistic tenant TSYS1 on page 876
show services icap-redirection statistic on page 876

Output Fields

Table 90 on page 874 lists the output fields for the `show services icap-redirection statistic` command. Output fields are listed in an approximate order in which they appear.

Table 90: show services icap-redirection statistic

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Redirected</td>
<td>Number of messages redirected.</td>
</tr>
<tr>
<td>Message Received</td>
<td>Number of messages received.</td>
</tr>
</tbody>
</table>

Sample Output

show services icap-redirection statistic root-logical-system

user@host> show services icap-redirection statistic root-logical-system

ICAP Redirect statistic:
Message Redirected : 0
Message REQMOD Redirected : 0
Message RESPMOD Redirected : 0
Message Received : 38
Message REQMOD Received : 0
Message RESPMOD Received : 0

Fallback: permit log-permit reject
Timeout : 0 : 0 : 0
Connectivity : 0 : 0 : 0
Default : 0 : 0 : 0

show services icap-redirection statistic all-logical-systems-tenants

user@host> show services icap-redirection statistic all-logical-systems-tenants

Logical system: root-logical-system
ICAP Redirect statistic:
Message Redirected : 0
<table>
<thead>
<tr>
<th>Message</th>
<th>Redirected</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message REQMOD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message Received</td>
<td>38</td>
<td>0</td>
</tr>
<tr>
<td>Message REQMOD Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Received</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fallback</th>
<th>permit</th>
<th>log-permit</th>
<th>reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connectivity</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical system: LSYS1

ICAP Redirect statistic:

<table>
<thead>
<tr>
<th>Message</th>
<th>Redirected</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message REQMOD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message REQMOD Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Received</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fallback</th>
<th>permit</th>
<th>log-permit</th>
<th>reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connectivity</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Tenants: TSYS1

ICAP Redirect statistic:

<table>
<thead>
<tr>
<th>Message</th>
<th>Redirected</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message REQMOD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message REQMOD Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Received</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fallback</th>
<th>permit</th>
<th>log-permit</th>
<th>reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connectivity</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show services icap-redirect statistic logical-system LSYS1

user@host> show services icap-redirect statistic logical-system LSYS1

ICAP Redirect statistic:

<table>
<thead>
<tr>
<th>Message</th>
<th>Redirected</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message REQMOD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Redirected</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message REQMOD Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Message RESPROMD Received</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fallback</th>
<th>permit</th>
<th>log-permit</th>
<th>reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connectivity</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show services icap-redirect statistic tenant TSYS1

user@host> show services icap-redirect statistic tenant TSYS1

ICAP Redirect statistic:
Message Redirected : 0
  Message REQMOD Redirected : 0
  Message RESPMOD Redirected : 0
Message Received : 0
  Message REQMOD Received : 0
  Message RESPMOD Received : 0

Fallback: permit log-permit reject
Timeout 0 0 0
Connectivity 0 0 0
Default 0 0 0

show services icap-redirect statistic

user@host:TSYS1> show services icap-redirect statistic

ICAP Redirect statistic:
Message Redirected : 0
  Message REQMOD Redirected : 0
  Message RESPMOD Redirected : 0
Message Received : 0
  Message REQMOD Received : 0
  Message RESPMOD Received : 0

Fallback: permit log-permit reject
Timeout 0 0 0
Connectivity 0 0 0
Default 0 0 0
show services icap-redirect status

Syntax

```bash
show services icap-redirect status
<all-logical-systems-tenants>
<root-logical-system>
<logical-system (logical-system-name | all)>
<tenant (tenant-name | all)>
```

Release Information

Command introduced in Junos OS Release 18.3R1.

`tenant` option introduced in Junos OS Release 20.1R1.

Description

Displays the status of ICAP services redirects. ICAP services redirect redirects the HTTP or HTTPS traffic to any third-party server. The security device acts as an SSL proxy server and decrypts the pass-through traffic with the proper SSL profile under a security policy.

Options

- **all-logical-systems-tenants**—(Optional) Displays the status of ICAP services redirects for the root logical system, all logical systems, and all tenant systems.

- **logical-system logical-system-name**—(Optional) Displays the status of ICAP services redirects for the specified logical system.

- **logical-system all**—(Optional) Displays the status of ICAP services redirects for all the logical systems.

- **root-logical-system**—(Optional) Displays the status of ICAP services redirects for the root logical system.

- **tenant tenant-name**—(Optional) Displays the status of ICAP services redirects for the specified tenant system.

- **tenant all**—(Optional) Displays the status of ICAP services redirects for all the tenant systems.

Required Privilege Level

`view`

RELATED DOCUMENTATION

- ICAP Service Redirect | 416

List of Sample Output

`show services icap-redirect status root-logical-system` on page 878
Output Fields

Table 91 on page 878 lists the output fields for the `show services icap-redirect status` command. Output fields are listed in an approximate order in which they appear.

Table 91: show services icap-redirect status

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICAP Status</td>
<td>Status of the ICAP services redirect.</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of the security profile assigned to the tenant systems or logical systems.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the server associated with the tenant systems or logical systems.</td>
</tr>
</tbody>
</table>

Sample Output

`show services icap-redirect status root-logical-system`

```
user@host> show services icap-redirect status root-logical-system

ICAP Status:
    Profile: p1 Server: s1 : UP
ICAP Status:
    Profile: p1 Server: s1 : UP
ICAP Status:
    Profile: p2 Server: s2 : UP
ICAP Status:
    Profile: p2 Server: s2 : UP
```

`show services icap-redirect status all-logical-systems-tenants`

```
user@host> show services icap-redirect status all-logical-systems-tenants

LSYS1
ICAP Status:
    Spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status:
```
show services icap-redirect status logical-system LSYS1

user@host> show services icap-redirect status logical-system LSYS1

ICAP Status :
Spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
Spu-1 Profile: icap-pf1 Server: icap-svr2 : UP

show services icap-redirect status tenant TSYS1

user@host> show services icap-redirect status tenant TSYS1

ICAP Status :
Spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
Spu-1 Profile: icap-pf1 Server: icap-svr2 : UP

show services icap-redirect status

user@host:TSYS1> show services icap-redirect status

ICAP Status :
Spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
Spu-1 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.
logical-system option is introduced in Junos OS Release 18.3R1.

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

Sample Output

show services icap-redirect statistic logical-system

user@host> show services icap-redirect statistic logical-system LSYS1
ICAP Redirect statistic:

<table>
<thead>
<tr>
<th>Message/Received</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Redirected</td>
<td>12</td>
</tr>
<tr>
<td>Message REQMOD Redirected</td>
<td>6</td>
</tr>
<tr>
<td>Message RESPMOD Redirected</td>
<td>6</td>
</tr>
<tr>
<td>Message Received</td>
<td>12</td>
</tr>
<tr>
<td>Message REQMOD Received</td>
<td>6</td>
</tr>
<tr>
<td>Message RESPMOD Received</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fallback:</th>
<th>permit</th>
<th>log-permit</th>
<th>reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Connectivity</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show services ssl droplogs

Syntax

show services ssl droplogs
cpic-info fpc-slot slot number pic-slot slot-number

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display the denied or dropped session details. The messages log file records the details about the dropped packets.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options
pic-info fpc0.pic0 fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.

Required Privilege Level
view

RELATED DOCUMENTATION
Operational Commands to Troubleshoot SSL Sessions | 439
show services ssl session | 926

Sample Output

user@host > show services ssl droplogs

Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0]------
log mesg is File:
../../../../../../../src/junos/jsf/plugin/ssl/jssl_common.c Function:
jssl_X509_verify_cert Line: 3767 Message: unable to get local issuer certificate
show services ssl initiation counters

Syntax

```
show services ssl initiation counters [all | error | handshake]
pic-info fpc-slot slot number pic-slot slot-number
```

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display statistical counters for the SSL initiation sessions.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options
```
pic-info fpc0.pic0 fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.
all—Display all the counters generated during SSL initiation.
error—Display all the counters related to errors occurred during SSL initiation.
handshake—Display all the counters related to handshake during SSL initiation.
```

Required Privilege Level
view

RELATED DOCUMENTATION

| Operational Commands to Troubleshoot SSL Sessions | 439 |
| show services ssl initiation profile | 889 |

List of Sample Output
show services ssl initiation counters all on page 886
show services ssl initiation counters error on page 887
show services ssl initiation counters handshake on page 887

Output Fields
Table 92 on page 885 lists the output fields for the `show services ssl initiation counters` command. Output fields are listed in the approximate order in which they appear.

### Table 92: show services ssl initiation counters Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Display Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory errors</td>
<td>Errors related to memory allocation.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Handshake errors</td>
<td>Number of errors occurred during handshake.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Cert Cache errors</td>
<td>Number of certificate cache errors.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Server Protection errors</td>
<td>Errors occurred during SSL reverse proxy.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Proxy errors</td>
<td>Errors occurred in SSL proxy sessions.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Crypto errors</td>
<td>Number of crypto errors.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Certificate errors</td>
<td>Errors related to digital certificate</td>
<td>all, errors</td>
</tr>
<tr>
<td>One-Crypto errors</td>
<td>Number of one-crypto errors</td>
<td>all, errors</td>
</tr>
<tr>
<td>Async-Crypto errors</td>
<td>Number of async-crypto errors</td>
<td>all, errors</td>
</tr>
<tr>
<td>Mirror errors</td>
<td>SSL decryption mirrors</td>
<td>all, errors</td>
</tr>
<tr>
<td>handshakes started</td>
<td>Number of SSL handshakes started.</td>
<td>all, errors</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>Number of SSL handshakes completed successfully.</td>
<td>all, errors</td>
</tr>
<tr>
<td>active sessions</td>
<td>Number of active SSL sessions</td>
<td>all, errors</td>
</tr>
<tr>
<td>Interdicted cert generated</td>
<td>Number of interdicted certificates generated</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: sessions created</td>
<td>Number of proxy sessions created</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: sessions active</td>
<td>Number of active proxy sessions</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: sessions ignored</td>
<td>Number of proxy sessions ignored.</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: renegotiation ignored</td>
<td>Number of renegotiation requests ignored.</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: session resumption</td>
<td>Number of session resumption requests</td>
<td>all, errors</td>
</tr>
</tbody>
</table>
Table 92: show services ssl initiation counters Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Display Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy: secure renegotiation</td>
<td>Number of SSL sessions with secure renegotiation</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: insecure renegotation</td>
<td>Number of SSL sessions with insecure renegotiation</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: multiple renegotation</td>
<td>Number of SSL sessions with multiple renegotiation</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: reneg after resumption</td>
<td>Number of SSL sessions undergo renegotiation after resumption</td>
<td>all, errors</td>
</tr>
<tr>
<td>init: passthrough requests</td>
<td>Passthrough requests during initiation</td>
<td>all, errors</td>
</tr>
<tr>
<td>init: start requests</td>
<td>Start requests during initiation</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: ECDSA based srvr auth</td>
<td>Sessions completed ECDSA-based server authentication</td>
<td>all, errors</td>
</tr>
<tr>
<td>proxy: RSA based srvr auth</td>
<td>Sessions completed RSA-based server authentication</td>
<td>all, errors</td>
</tr>
</tbody>
</table>

Sample Output

show services ssl initiation counters all
user@host > show services ssl initiation counters all

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

Memory errors 0
Handshake errors 0
Cert Cache errors 0
Server Protection errors 0
Proxy errors 0
Crypto errors 0
Certificate errors 0
One-Crypto errors 0
Async-Crypto errors 0
Mirror errors 0
handshakes started 0
handshakes completed 0
active sessions 0
show services ssl initiation counters error

user@host > show services ssl initiation counters error

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

Memory errors 0
Handshake errors 0
Cert Cache errors 0
Server Protection errors 0
Proxy errors 0
Crypto errors 0
Certificate errors 0
One-Crypto errors 0
Async-Crypto errors 0
Mirror errors 0

show services ssl initiation counters handshake

user@host > show services ssl initiation counters handshake

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

handshakes started 0
handshakes completed 0
active sessions 0
Interdicted cert generated 0
proxy: sessions created 0
proxy: sessions active 0
proxy: sessions ignored 0
proxy: renegotiation ignored 0
proxy: session resumption 0
proxy: secure renegotiation 0
proxy: insecure renegotiation 0
proxy: multiple renegotiation 0
proxy: reneg after resumption 0
init: passthrough requests 0
init: start requests 0
proxy: ECDSA based srvr auth 0
proxy: RSA based srvr auth 0
show services ssl initiation profile

Syntax

```
show services ssl initiation profile [all | brief | detail]
pic-info fpc-slot slot number pic-slot slot-number
```

Release Information

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description

Display the SSL initiation profiles details.

**NOTE:** When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options

- `pic-info fpc-slot slot number pic-slot slot-number`—Display the information for the FPC in the specified slot.
- `all`—Display all SSL initiation profiles configured on the device.
- `brief`—Display brief information about SSL initiation profiles.
- `detail`—Display detail information about SSL initiation profiles.

Required Privilege Level

view

RELATED DOCUMENTATION

- Operational Commands to Troubleshoot SSL Sessions | 439
- show services ssl initiation counters | 884

Output Fields

Table 93 on page 890 lists the output fields for the `show services ssl initiation profile` command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>SSL initiation profile name</td>
<td>brief, detail</td>
</tr>
<tr>
<td>allow non-ssl session</td>
<td>Allow or not allow (bypass) non-SSL sessions.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>preferred-ciphers</td>
<td>SSL cipher that can be used with acceptable key strength. Possible values are strong, medium, weak, and custom.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>Num of url categories configured</td>
<td>URL categories exempted from SSL proxy.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>Protocol-version</td>
<td>SSL protocol version. Possible values are all, TLS version 1.0, TLS version 1.1, and TLS version 1.2.</td>
<td>detail</td>
</tr>
<tr>
<td>Client authentication</td>
<td>Status of client certificate verification process.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Authentication</td>
<td>Status of server certificate verification process.</td>
<td>detail</td>
</tr>
<tr>
<td>Crypto-mode</td>
<td>Crypto mode used. Options are synchronous-hardware or software or asynchronous-hardware.</td>
<td>detail</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>SSL session resumption status.</td>
<td>detail</td>
</tr>
<tr>
<td>CRL check</td>
<td>Status of the CRL checking of certificate validity.</td>
<td>detail</td>
</tr>
<tr>
<td>Certificate</td>
<td>Digital certificate used.</td>
<td>detail</td>
</tr>
<tr>
<td>Renegotiation</td>
<td>Renegotiation option. Possible values are allow, allow secure, and drop.</td>
<td>detail</td>
</tr>
<tr>
<td>Custom ciphers</td>
<td>Custom ciphers configured.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Cert</td>
<td>Server certificate configured.</td>
<td>detail</td>
</tr>
<tr>
<td>Decrypt Mirror</td>
<td>Status of decrypt mirroring functionality.</td>
<td>detail</td>
</tr>
<tr>
<td>Trusted CA:</td>
<td>Trusted CA configured for a profile</td>
<td>detail</td>
</tr>
<tr>
<td>handshakes started</td>
<td>Number of SSL handshakes started.</td>
<td>detail</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>Number of SSL handshakes completed successfully.</td>
<td>detail</td>
</tr>
<tr>
<td>active sessions</td>
<td>Number of active SSL sessions</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 93: show services ssl initiation profile Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>total handshake errors</td>
<td>Number of errors occurred during handshake process.</td>
<td>detail</td>
</tr>
<tr>
<td>data errors</td>
<td>Cumulative errors in a single counter</td>
<td></td>
</tr>
<tr>
<td>session resumption</td>
<td>Number of SSL session resumption count.</td>
<td>detail</td>
</tr>
<tr>
<td>secure renegotiation</td>
<td>Secure sessions allowed after renegotiation.</td>
<td>detail</td>
</tr>
<tr>
<td>insecure renegotiation</td>
<td>All sessions allowed after renegotiation.</td>
<td>detail</td>
</tr>
<tr>
<td>multiple renegotiation</td>
<td>Sessions with multiple renegotiation.</td>
<td>detail</td>
</tr>
<tr>
<td>reneg after resumption</td>
<td>Sessions undergoing renegotiation after resumption.</td>
<td>detail</td>
</tr>
<tr>
<td>no_reneg alert by peer</td>
<td>Number of times no renegotiation alerts received from peer.</td>
<td>detail</td>
</tr>
<tr>
<td>drop on reneg</td>
<td>Sessions dropped after renegotiation.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

user@host > show services ssl initiation profile all

```
Lsys Name : root-logical-system

PIC: fpc0  fpc[0]  pic[0]  -------
ID          Name
65536  SSLPROFILE_65536_proxy_i
```

user@host > show services ssl initiation profile brief profile-name

```
Lsys Name : root-logical-system

PIC: fpc0  fpc[0]  pic[0]  -------
Profile                          : SSLPROFILE_65536_proxy_i
```
allow non-ssl session : true
preferred-ciphers : medium
Num of url categories configured : 0

user@host > show services ssl initiation profile detail profile-name

Lsys Name : root-logical-system

PIC: fpc0 fpc[0] pic[0] -----------

Profile : SSL_PROFILE_65536_proxy_i
allow non-ssl session : true
preferred-ciphers : medium
Num of url categories configured : 0
Protocol version : all
Client Authentication : notset
Server Authentication : Ignore Failure
Crypto Mode : sw
Session Resumption : Enabled
CRL check : Enabled
Certificate RSA : ssl-inspect-ca
Renegotiation : only secure allowed
Custom ciphers : 0
Server cert : 0
Decrypt Mirror : Disabled
Trusted CA : 0
  handshakes started : 0
  handshakes completed : 0
  active sessions : 0
  total handshake errors : 0
  Data Errors : 0
  session resumption : 0
  secure renegotiation : 0
  insecure renegotiation : 0
  multiple renegotiation : 0
  reneg after resumption : 0
  no_reneg alert by peer : 0
  drop on reneg : 0
show services ssl proxy certificate-cache entries

Syntax

    show services ssl proxy certificate-cache entries [detail | summary]
    <pic-info fpc-slot slot number pic-slot slot-number>

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display information about the entries stored in the SSL proxy certificate cache.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options
pic-info fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.
detail—Display the detail information about the SSL proxy certificate cache entries.
summary—Display the summary of the SSL proxy certificate cache entries.

Required Privilege Level
view

RELATED DOCUMENTATION

| Operational Commands to Troubleshoot SSL Sessions | 439 |
| show services ssl proxy certificate-cache statistics | 896 |

Output Fields
Table 94 on page 893 lists the output fields for the show services ssl proxy certificate-cache command. Output fields are listed in the approximate order in which they appear.

Table 94: show services ssl proxy certificate-cache Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Entries</td>
<td>Index number of the entry.</td>
<td>summary, detail</td>
</tr>
</tbody>
</table>
Table 94: show services ssl proxy certificate-cache Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial number</td>
<td>Serial number of the server certificate.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>SSL-I Profile Id</td>
<td>SSL initiation profile identification number.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Num of CRL updates</td>
<td>Number of times the CRL updates done till the interdicted certificate is added to the certificate-cache.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the cache entry. That is—whether the cache entry has expired or not, because the cache entries are valid only for short interval.</td>
<td>detail</td>
</tr>
<tr>
<td>Interdicted cert type</td>
<td>Interdicted certificate details such as type and authentication status.</td>
<td>detail</td>
</tr>
<tr>
<td>Server cert verification result</td>
<td>Server certificate validation results.</td>
<td>detail</td>
</tr>
<tr>
<td>Cert reference count</td>
<td>Certificate reference count.</td>
<td>detail</td>
</tr>
<tr>
<td>Issuer</td>
<td>Authority that issued the digital certificate, including details of the authority organized using the distinguished name format.</td>
<td>detail</td>
</tr>
<tr>
<td>Subject</td>
<td>Details of the digital certificate holder organized using the distinguished name format.</td>
<td>detail</td>
</tr>
</tbody>
</table>

---

### Sample Output

**user@host > show services ssl proxy certificate-cache entries summary**

```
Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------
Cache Entries : 1
Serial number : 0x12345678
SSL-I Profile Id: 1
Num of CRL updates: 0
```

**user@host > show services ssl proxy certificate-cache entries detail**
Lsys Name: root-logical-system
PIC: fwdd0 fpc[0] pic[0] ------
Cache entry: 1
Serial number: 0x12345678
SSL-I Profile ID: 1
Num of CRL updates: 0
Status: Active: Time to expire 570 seconds

Cert Info:
-------------
Interdicted cert type [0x0]: CA issued, Authentication failed
Server cert verification result: unable to get local issuer certificate [0x14]
Cert reference count: 2
Subject: /C=IN/ST=KA/O=XYZ Inc/CN=XYZ Root CA/emailAddress=host@xyz.com
Issuer: /CN=SSL-PROXY:DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE
show services ssl proxy certificate-cache statistics

Syntax

```
show services ssl proxy certificate-cache statistics
<pic-info fpc-slot slot number pic-slot slot-number>
```

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display SSL proxy certificate cache statistics.

Options

```
pic-info fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.
```

Required Privilege Level
view

RELATED DOCUMENTATION

| Operational Commands to Troubleshoot SSL Sessions | 439 |
| show services ssl proxy certificate-cache entries | 893 |

Output Fields

Table 95 on page 896 lists the output fields for the `show services ssl proxy certificate-cache statistics` command. Output fields are listed in the approximate order in which they appear.

Table 95: show services ssl proxy certificate-cache statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cert cache hit</td>
<td>Number times the certificate matched the entry in the certificate cache</td>
</tr>
<tr>
<td>cert cache miss</td>
<td>Number times the certificate did not find the match in the certificate cache</td>
</tr>
<tr>
<td>cert cache full</td>
<td>Number of times the certificate cache limit is reached.</td>
</tr>
</tbody>
</table>
Sample Output

```
user@host > show services ssl proxy certificate-cache statistics

Lsys Name : root-logical-system

PIC: fpc0 fpc[0] pic[0]-----------

cert cache hit 0
cert cache miss 0
cert cache full
```
show services ssl proxy counters

Syntax

show services ssl proxy counters [all | errors | info]
<pic-info fpc-slot slot number pic-slot slot-number>

Release Information

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description

Display statistical counters for the SSL proxy sessions.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options

all—Display information about counter values for all SSL proxy sessions
errors—Display information about counter values for all SSL proxy sessions errors.
info—Display some informational counters which are subset of all the counters
pic-info fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.

Required Privilege Level
view

RELATED DOCUMENTATION

| Operational Commands to Troubleshoot SSL Sessions | 439 |
| show services ssl proxy status | 909 |
| show services ssl proxy session-cache entries | 911 |
| show services ssl proxy session-cache statistics | 916 |

List of Sample Output

show services ssl proxy counters info on page 900
show services ssl proxy counters errors on page 901
show services ssl proxy counters all on page 901
Output Fields

Table 96 on page 899 lists the output fields for the `show services ssl certificate` command. Output fields are listed in the approximate order in which they appear.

Table 96: show services ssl proxy counters Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session create failed</td>
<td>The number of failed proxy sessions</td>
<td>errors, all</td>
</tr>
<tr>
<td>non SSL sessions received</td>
<td>The number of non-SSL sessions received</td>
<td>errors, all</td>
</tr>
<tr>
<td>memory failures</td>
<td>The number of errors related to memory. Example, memory errors such as the device is on “low memory” is indicated by this counter.</td>
<td>errors, all</td>
</tr>
<tr>
<td>session dropped</td>
<td>The number of dropped proxy sessions.</td>
<td>errors, all</td>
</tr>
<tr>
<td>sessions matched</td>
<td>The number of matched proxy sessions.</td>
<td>info, all</td>
</tr>
<tr>
<td>sessions created</td>
<td>The number of newly created proxy sessions.</td>
<td>info, all</td>
</tr>
<tr>
<td>sessions destroyed</td>
<td>The number of dropped or destroyed proxy sessions.</td>
<td>info, all</td>
</tr>
<tr>
<td>sessions ignored</td>
<td>The number of proxy sessions that are ignored.</td>
<td>info, all</td>
</tr>
<tr>
<td>sessions ignored : backup only</td>
<td>The number of sessions ignored on the backup node in a chassis cluster setup.</td>
<td>info, all</td>
</tr>
<tr>
<td></td>
<td>In chassis cluster or high-availability mode, the SSL session is processed only on the active node and on the backup node session is ignored. This counter indicates the session ignored on the backup node.</td>
<td></td>
</tr>
<tr>
<td>sessions whitelisted : IP based</td>
<td>The number of all sessions that are whitelisted based on IP addresses.</td>
<td>info, all</td>
</tr>
<tr>
<td>sessions whitelisted : url based</td>
<td>The number of all sessions that are whitelisted based on the URL categories.</td>
<td>info, all</td>
</tr>
<tr>
<td>crl : data added</td>
<td>The number of times CRL data is added.</td>
<td>info, all</td>
</tr>
<tr>
<td>crl : certificate revoked</td>
<td>The number of sessions dropped because of checking for revoked certificates from servers.</td>
<td>info, all</td>
</tr>
<tr>
<td>crl : no crl info present</td>
<td>The number of sessions dropped because no CRL information was present.</td>
<td>info, all</td>
</tr>
<tr>
<td>crl : no CA certificate</td>
<td>The number of sessions dropped because no CA certificate was present.</td>
<td>info, all</td>
</tr>
<tr>
<td>SSL sessions</td>
<td>Number of SSL sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
<td>Level of Output</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SMTP over STARTTLS</td>
<td>Number of SMTP over STARTTLS sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>IMAP over STARTTLS</td>
<td>Number of IMAP over STARTTLS sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>POP3 over STARTTLS</td>
<td>Number of POP3 over STARTTLS sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>SMTP sessions</td>
<td>Number of SMTP sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>IMAP sessions</td>
<td>Number of IMAP sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>POP3 sessions</td>
<td>Number of POP3 sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>Server not supporting STARTTLS</td>
<td>Number of times server not supported STARTTLS sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>Client not supporting STARTTLS</td>
<td>Number of times client not supported STARTTLS sessions</td>
<td>info, all</td>
</tr>
<tr>
<td>Unified policy : default profile hit</td>
<td>The number of times sessions matched default SSL proxy profile.</td>
<td>info, all</td>
</tr>
<tr>
<td>Unified policy : no default profile</td>
<td>The number of times sessions are dropped because no default SSL proxy profile available.</td>
<td>info, all</td>
</tr>
</tbody>
</table>

---

**Sample Output**

```
show services ssl proxy counters info
user@host > show services ssl proxy counters info

Lsys Name : root-logical-system
PIC:fpc0 ------

sessions matched 0
sessions created 0
sessions destroyed 0
sessions ignored 0
sessions ignored : backup only 0
sessions whitelisted : IP based 0
sessions whitelisted : url based 0
crl : data added 1
```
crl : certificate revoked 0
crl : no crl info present 0
crl : no CA certificate 0
SSL sessions 0
SMTP over STARTTLS 0
IMAP over STARTTLS 0
POP3 over STARTTLS 0
SMTP sessions 0
IMAP sessions 0
POP3 sessions 0
Server not supporting STARTTLS 0
Client not supporting STARTTLS 0
Unified policy : default profile hit 0
Unified policy : no default profile 0

show services ssl proxy counters errors
user@host > show services ssl proxy counters errors

Lsys Name : root-logical-system
PIC:fpc0 -------

Session create failed 0
non SSL sessions received 0
memory failures 0
session dropped 7

show services ssl proxy counters all
user@host > show services ssl proxy counters all

Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0] -------

session create failed 0
non SSL sessions received 0
Memory failures 0
session dropped 0
sessions matched 0
sessions created 0
sessions destroyed 0
sessions ignored 0
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessions ignored : backup only</td>
<td>0</td>
</tr>
<tr>
<td>sessions whitelisted : IP based</td>
<td>0</td>
</tr>
<tr>
<td>sessions whitelisted : url based</td>
<td>0</td>
</tr>
<tr>
<td>crl : data added</td>
<td>0</td>
</tr>
<tr>
<td>crl : certificate revoked</td>
<td>0</td>
</tr>
<tr>
<td>crl : no crl info present</td>
<td>0</td>
</tr>
<tr>
<td>crl : no CA certificate</td>
<td>0</td>
</tr>
<tr>
<td>SSL sessions</td>
<td>0</td>
</tr>
<tr>
<td>SMTP over STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>IMAP over STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>POP3 over STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>SMTP sessions</td>
<td>0</td>
</tr>
<tr>
<td>IMAP sessions</td>
<td>0</td>
</tr>
<tr>
<td>POP3 sessions</td>
<td>0</td>
</tr>
<tr>
<td>Server not supporting STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>Client not supporting STARTTLS</td>
<td>0</td>
</tr>
<tr>
<td>Unified policy : default profile hit</td>
<td>0</td>
</tr>
<tr>
<td>Unified policy : no default profile</td>
<td>0</td>
</tr>
</tbody>
</table>
show services ssl proxy profile

Syntax

    show services ssl proxy profile [all | profile-name]
    <pic-info fpc-slot slot number pic-slot slot-number>

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display information about the SSL proxy profile details.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options
all—Display all SSL proxy profiles configured on the device.
profile-name—Display information about SSL proxy profile.
pic-info fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.

Required Privilege Level
view

RELATED DOCUMENTATION

| Operational Commands to Troubleshoot SSL Sessions | 439 |
| show services ssl proxy counters | 898 |
| show services ssl proxy status | 909 |

List of Sample Output
show services ssl proxy profile on page 904
show services ssl proxy all on page 904

Output Fields
Table 97 on page 904 lists the output fields for the show services ssl proxy profile command. Output fields are listed in the approximate order in which they appear.
Table 97: show services ssl proxy profile Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>SSL proxy profile name.</td>
</tr>
<tr>
<td>enable-tracing</td>
<td>Enable flow tracing option is set or not set for the profile.</td>
</tr>
<tr>
<td>root-ca expired</td>
<td>Enable or disable ignoring server authentication when root CA is expired.</td>
</tr>
<tr>
<td>allow non-ssl session</td>
<td>Allow or not allow (bypass) non-SSL sessions.</td>
</tr>
<tr>
<td>ssl-termination-id</td>
<td>SSL termination profile ID.</td>
</tr>
<tr>
<td>ssl-initiation-id</td>
<td>SSL initiation profile ID.</td>
</tr>
<tr>
<td>Number of whitelist entries</td>
<td>The number of whitelisted domains (both IP-based and DNS-based) that are configured for this particular SSL proxy profile.</td>
</tr>
</tbody>
</table>

Sample Output

show services ssl proxy profile

user@host > show services ssl proxy profile profile-name

Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------
Profile: ssl-proxy
enable-tracing: false
root-ca expired: false
allow non-ssl session: true
ssl-termination-id: 65537
ssl-initiation-id: 65537
Number of whitelist entries: 0

Sample Output

show services ssl proxy all

user@host > show services ssl proxy all
Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] ------

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>p1</td>
</tr>
<tr>
<td>11</td>
<td>p2</td>
</tr>
</tbody>
</table>
show services ssl proxy statistics

Syntax

show services ssl proxy statistics

Release Information

Command introduced in Junos OS Release 12.1.
The **logical system** option is added in Junos OS Release 19.1R1.

Description

Display information about the SSL proxy statistics. An SSL proxy profile defines SSL behavior for the SRX Series device.

**NOTE:** When devices are operating in chassis cluster mode, the SSL proxy statistics increment only on the active node of the chassis cluster setup.

Options

**logical-system**—Displays summary information about SSL proxy.

Required Privilege Level

view

RELATED DOCUMENTATION

| clear services ssl proxy statistics | 689 |

List of Sample Output

show services ssl proxy statistics on page 907
show services ssl proxy statistics logical-system on page 908

Output Fields

Table 98 on page 906 describes the output fields for the **show services ssl proxy statistics** command. Output fields are listed in the approximate order in which they appear.

**Table 98: show services ssl proxy statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions matched</td>
<td>The number of proxy sessions that are matched.</td>
</tr>
</tbody>
</table>
### Table 98: show services ssl proxy statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions bypassed: non SSL</td>
<td>The number of proxy sessions that are bypassed because the non SSL sessions limit was exceeded</td>
</tr>
<tr>
<td>Sessions bypassed: memory overflow</td>
<td>The number of proxy sessions that are bypassed because the memory usage limit per session was reached.</td>
</tr>
<tr>
<td>sessions bypassed: low memory</td>
<td>The number of proxy sessions that are bypassed because of low memory on Packet Forwarding Engine.</td>
</tr>
<tr>
<td>Sessions created</td>
<td>The number of proxy sessions that are newly created.</td>
</tr>
<tr>
<td>Sessions ignored</td>
<td>The number of proxy sessions that are ignored.</td>
</tr>
<tr>
<td>Sessions active</td>
<td>The number of proxy sessions that are active.</td>
</tr>
<tr>
<td>Sessions dropped</td>
<td>The number of proxy sessions that are dropped.</td>
</tr>
<tr>
<td>Sessions whitelisted</td>
<td>The number of sessions that are whitelisted. Whitelists comprise addresses or domain names that you want to exempt from the SSL proxy processing.</td>
</tr>
<tr>
<td>whitelisted url category match</td>
<td>Whitelists comprise url hostnames that you want to exempt from the SSL proxy processing.</td>
</tr>
<tr>
<td>default profile hit</td>
<td>The number of default profiles that are matched when the sessions are whitelisted.</td>
</tr>
<tr>
<td>session dropped no default profile</td>
<td>The number of sessions dropped when no default profiles are matched.</td>
</tr>
<tr>
<td>policy hit no profile configured</td>
<td>The number of policies matched when no profile is configured.</td>
</tr>
</tbody>
</table>

### Sample Output

```plaintext
show services ssl proxy statistics
user@host>  show services ssl proxy statistics

PIC:fwdd0 fpc[0] pic[0] ------
sessions matched                  30647
```
sessions bypassed:non-ssl                      0
sessions bypassed:mem overflow                0
sessions bypassed:low memory                 0
sessions created                               25665
sessions ignored                              6
sessions active                                0
sessions dropped                               0
sessions whitelisted                           0
whitelisted url category match                 0

show services ssl proxy statistics logical-system

user@host> show services ssl proxy statistics logical-system LSYS1

  sessions matched                       1
  sessions bypassed:non-ssl              0
  sessions bypassed:mem overflow         0
  sessions bypassed:low memory           0
  sessions created                       1
  sessions ignored                       0
  sessions active                        1
  sessions dropped                       0
  sessions whitelisted                   0
  whitelisted url category match         0
  default profile hit                    0
  session dropped no default profile     0
  policy hit no profile configured       0
**show services ssl proxy status**

**Syntax**

```
show services ssl proxy status
```

**Release Information**

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

**Description**

Display information about the SSL proxy status.

**Options**

- `pic-info fpc-slot slot number pic-slot slot-number`—Display the information for the FPC in the specified slot.

**Required Privilege Level**

`view`

**RELATED DOCUMENTATION**

- Operational Commands to Troubleshoot SSL Sessions | 439
- `show services ssl proxy counters` | 898
- `show services ssl proxy profile` | 903

**Output Fields**

Table 99 on page 909 list the output fields for the `show services ssl proxy status` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-Crypto</td>
<td>One-crypto status: enabled or disabled.</td>
</tr>
<tr>
<td>Async Crypto</td>
<td>Async Crypto status: enabled or disabled.</td>
</tr>
<tr>
<td>Proxy activation</td>
<td>Status of proxy activation.</td>
</tr>
<tr>
<td>Local logging</td>
<td>Status of local logging.</td>
</tr>
<tr>
<td>SSLFP &lt;-&gt; PKID Link Status</td>
<td>SSL forward proxy to PKID link status.</td>
</tr>
</tbody>
</table>
Table 99: show services ssl proxy status Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate cache activated</td>
<td>Status of the certificate cache</td>
</tr>
<tr>
<td>Max cert cache nodes</td>
<td>Maximum number of certificates in cache nodes</td>
</tr>
<tr>
<td>Invalidate certificate cache on CRL update : Disabled</td>
<td>Status of invalidation of the existing certificate cache</td>
</tr>
<tr>
<td>Cert cache node in use</td>
<td>Number of cached certificates in in use</td>
</tr>
<tr>
<td>Session cache activated</td>
<td>Status of the session cache</td>
</tr>
<tr>
<td>Max session cache node</td>
<td>Maximum number of sessions in cache nodes</td>
</tr>
<tr>
<td>Session cache node in use</td>
<td>Number of cached sessions in use.</td>
</tr>
</tbody>
</table>

Sample Output

user@host > show services ssl proxy status

PIC:fwdd0 fpc[0] pic[0] ------
    One-Crypto : Enable
    Async Crypto : disable
    Proxy-activation : Only if interested svcs configured
    Local Logging : disable
    SSLFP-PKID Link : Down
    Certificate cache : -
    Certificate Cache activated : no
    Invalidate certificate cache on CRL update : Disabled
    Max cert cache nodes : 4000
    Cert cache node in use : 0
    Session cache : -
    Session cache activated : Deactivated
    Max session cache node : 0
    Session cache node in use : 0
show services ssl proxy session-cache entries

Syntax

    show services ssl proxy session-cache entries [detail | summary]
    <pic-info fpc-slot slot number pic-slot slot-number>

Release Information

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description

Display information about the entries stored in the SSL proxy session cache.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options

pic-info fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.

detail—Display the detail information about the SSL proxy session cache entries.

summary—Display the summary of the SSL proxy session cache entries.

Required Privilege Level

view

RELATED DOCUMENTATION

| show services ssl proxy session-cache statistics | 916 |
| Operational Commands to Troubleshoot SSL Sessions | 439 |

List of Sample Output

show services ssl proxy session-cache entries summary on page 913
show services ssl proxy session-cache entries detail on page 913

Output Fields

Table 100 on page 912 lists the output fields for the show services ssl proxy session-cache entries command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Display Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Entry</td>
<td>Index number of the entry.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the cache entry—active or expired. The cache entries are valid only for short interval.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Session Id Length</td>
<td>Length of the session ID. 32-bit field that identifies an SSL session.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Session Id</td>
<td>SSL session identifier.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Destination IP address.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Destination port number.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>SSL-T Profile Id</td>
<td>SSL termination profile identification number.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>SSL-I Profile Id</td>
<td>SSL initiation profile identification number.</td>
<td>summary, detail</td>
</tr>
<tr>
<td>Interdicted cert type [0x0]:</td>
<td>Interdicted server certificate</td>
<td>detail</td>
</tr>
<tr>
<td>Server cert verification result:</td>
<td>Server certificate validation results.</td>
<td>detail</td>
</tr>
<tr>
<td>Server name extn len</td>
<td>Extension length in the TLS server name extension.</td>
<td>detail</td>
</tr>
<tr>
<td>name</td>
<td>Server name in the TLS server name extension</td>
<td>detail</td>
</tr>
<tr>
<td>Server cert chain hash</td>
<td>The hash value of the server certificate chain.</td>
<td>detail</td>
</tr>
<tr>
<td>SSL-TERM session:</td>
<td>SSL termination session details. It includes the following fields.</td>
<td>detail</td>
</tr>
<tr>
<td>• SSL ver—SSL/TLS protocol version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Compression Method—Agreed-upon compression method used to compress data and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cipher Id—Identification number for the cipher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Master Key Length—Length of the master secret key</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 100: show services ssl proxy session-cache entries Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Display Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL-INIT session:</td>
<td>SSL initiation session details. It includes the following fields.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• SSL ver—SSL/TLS protocol version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Compression Method—Agreed-upon compression method used to compress data and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cipher Id—Identification number for the cipher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Master Key Length—Length of the master secret key.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show services ssl proxy session-cache entries summary

user@host > show services ssl proxy session-cache entries summary

Lsys Name : root-logical-system
PIC: fpc0 fpc[0] pic[0]
Hash Entry: 1
Status: ACTIVE, Time to expire 294 seconds
Session Id Length: 32
Session Id: 1b 2a 9f 5f d8 6e d2 cd 6b b8 89 e8 88 07 75 80 32 c2 54 5a c7 9b 12 a2 e6 5c f0 6d 85 c5 40 4b
Dst IP: 5.0.0.1, Dst Port: 20753
SSL-T Profile Id: 2, SSL-I Profile Id: 2

show services ssl proxy session-cache entries detail

user@host > show services ssl proxy session-cache entries detail

Lsys Name : root-logical-system
PIC: fpc0 fpc[0] pic[0]
Hash Entry: 1
Status: ACTIVE, Time to expire 294 seconds
Session Id Length: 32
Session Id: c1 6e 88 65 43 9f 57 2f 0f 06 f7 4b 03 c5 38 58 74 b4 4f 43 66 9a 6f c7 a6 2a ae 22 ab f8 b4 ce
Dst IP: 5.0.0.1, Dst Port: 4433
SSL-T Profile Id: 2, SSL-I Profile Id: 2
Session Info:
Interdicted cert type [0x0]: CA issued, Authentication failed
Server cert verification result: unable to get local issuer certificate [0x14]
Server name extn len: 0, name: None
Server cert chain hash: b5 3d cd cb ca 35 81 5a db 6f 83 ab 5e a0 19 73

SSL-TERM session:
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

SSL-INIT session:
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

Hash Entry:2
Status: EXPIRED
Session Id Length: 32
Session Id: 1b 2a 9f 5f d8 6e d2 cd 6b b8 89 e8 88 07 75 80 32 c2 54 5a c7 9b 12
a2 e6 5c f0 6d 85 c5 40 4b
Dst IP: 5.0.0.1, Dst Port: 4433,
SSL-T Profile Id: 2, SSL-I Profile Id: 2
Session Info:
-------------
Interdicted cert type [0x0]: CA issued, Authentication failed
Server cert verification result: unable to get local issuer certificate [0x14]
Server name extn len: 0, name: None
Server cert chain hash: b5 3d cd cb ca 35 81 5a db 6f 83 ab 5e a0 19 73

SSL-TERM session:
----------------
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

SSL-INIT session:
----------------
SSL ver: 0x303
Compression Method: 0
Cipher Id: 0x3000004
Master Key Length: 48

Stale entry in cache: 1
show services ssl proxy session-cache statistics

Syntax

```
show services ssl proxy session-cache statistics
<pic-info fpc-slot slot number pic-slot slot-number>
```

Release Information

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Description

Display the data for the SSL proxy session cache.

Options

**pic-info fpc-slot slot number pic-slot slot-number**—Display the information for the FPC in the specified slot.

Required Privilege Level

view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Operational Commands to Troubleshoot SSL Sessions</th>
<th>439</th>
</tr>
</thead>
<tbody>
<tr>
<td>show services ssl proxy session-cache entries</td>
<td>911</td>
</tr>
</tbody>
</table>

List of Sample Output

show services ssl proxy session-cache statistics on page 917

Output Fields

Table 101 on page 916 lists the output fields for the `show services ssl proxy session-cache statistics` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session cache hit</td>
<td>Number times the session matched the entry in the SSL proxy session cache.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Session cache miss</td>
<td>Number times the session did not find the match in the SSL proxy session cache.</td>
</tr>
<tr>
<td>Session cache full</td>
<td>Number of times the session cache limit is reached.</td>
</tr>
</tbody>
</table>

**Sample Output**

```text
show services ssl proxy session-cache statistics
user@host > show services ssl proxy session-cache statistics

Lsys Name : root-logical-system
PIC: fpc0 fpc[0] pic[0]------------

Session cache hit : 0
Session cache miss : 0
Session cache full : 0
```
show services ssl proxy statistics

Syntax

```
show services ssl proxy statistics
```

Release Information

Command introduced in Junos OS Release 12.1.
The *logical system* option is added in Junos OS Release 19.1R1.

Description

Display information about the SSL proxy statistics. An SSL proxy profile defines SSL behavior for the SRX Series device.

NOTE: When devices are operating in chassis cluster mode, the SSL proxy statistics increment only on the active node of the chassis cluster setup.

Options

*logical-system*—Displays summary information about SSL proxy.

Required Privilege Level

view

RELATED DOCUMENTATION

| clear services ssl proxy statistics | 689 |

List of Sample Output

- show services ssl proxy statistics on page 919
- show services ssl proxy statistics logical-system on page 920

Output Fields

Table 98 on page 906 describes the output fields for the `show services ssl proxy statistics` command. Output fields are listed in the approximate order in which they appear.

Table 102: show services ssl proxy statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions matched</td>
<td>The number of proxy sessions that are matched.</td>
</tr>
</tbody>
</table>
Table 102: show services ssl proxy statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sessions bypassed:</strong> non SSL</td>
<td>The number of proxy sessions that are bypassed because the non SSL sessions limit was exceeded</td>
</tr>
<tr>
<td><strong>Sessions bypassed:</strong> memory overflow</td>
<td>The number of proxy sessions that are bypassed because the memory usage limit per session was reached.</td>
</tr>
<tr>
<td><strong>sessions bypassed:</strong> low memory</td>
<td>The number of proxy sessions that are bypassed because of low memory on Packet Forwarding Engine.</td>
</tr>
<tr>
<td><strong>Sessions created</strong></td>
<td>The number of proxy sessions that are newly created.</td>
</tr>
<tr>
<td><strong>Sessions ignored</strong></td>
<td>The number of proxy sessions that are ignored.</td>
</tr>
<tr>
<td><strong>Sessions active</strong></td>
<td>The number of proxy sessions that are active.</td>
</tr>
<tr>
<td><strong>Sessions dropped</strong></td>
<td>The number of proxy sessions that are dropped.</td>
</tr>
<tr>
<td><strong>Sessions whitelisted</strong></td>
<td>The number of sessions that are whitelisted. Whitelists comprise addresses or domain names that you want to exempt from the SSL proxy processing.</td>
</tr>
<tr>
<td><strong>whitelisted url category match</strong></td>
<td>Whitelists comprise url hostnames that you want to exempt from the SSL proxy processing.</td>
</tr>
<tr>
<td><strong>default profile hit</strong></td>
<td>The number of default profiles that are matched when the sessions are whitelisted.</td>
</tr>
<tr>
<td><strong>session dropped no default profile</strong></td>
<td>The number of sessions dropped when no default profiles are matched.</td>
</tr>
<tr>
<td><strong>policy hit no profile configured</strong></td>
<td>The number of policies matched when no profile is configured.</td>
</tr>
</tbody>
</table>

Sample Output

```
show services ssl proxy statistics
user@host> show services ssl proxy statistics

PIC:fwdd0 fpc[0] pic[0] ------
    sessions matched                    30647
```
sessions bypassed:non-ssl       0
sessions bypassed:mem overflow  0
sessions bypassed:low memory    0
sessions created                25665
sessions ignored                6
sessions active                 0
sessions dropped                0
sessions whitelisted            0
whitelisted url category match  0

show services ssl proxy statistics logical-system
user@host> show services ssl proxy statistics logical-system LSYS1

sessions matched              1
sessions bypassed:non-ssl     0
sessions bypassed:mem overflow 0
sessions bypassed:low memory   0
sessions created               1
sessions ignored               0
sessions active                1
sessions dropped               0
sessions whitelisted           0
whitelisted url category match 0
default profile hit            0
session dropped no default profile 0
policy hit no profile configured 0
show services ssl certificate

Syntax

```bash
show services ssl certificate [all | brief | detail]
<pic-info fpc-slot slot number pic-slot slot-number>
```

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display information about the SSL certificates available on the device.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options

- **all**—Display information about all SSL certificates.
- **brief**—Display brief information about SSL certificate.
- **detail**—Display detail information about SSL certificates.
- **pic-info fpc-slot slot number pic-slot slot-number**—Display the information for the FPC in the specified slot.

Required Privilege Level

view

RELATED DOCUMENTATION

- Operational Commands to Troubleshoot SSL Sessions | 439
- List of Sample Output
  - `show services ssl certificate all on page 923`
  - `show services ssl certificate detail (Local Certificate) on page 924`
  - `show services ssl certificate detail (CA Certificate) on page 925`

Output Fields

Table 94 on page 893 lists the output fields for the `show services ssl certificate` command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertID</td>
<td>Name of the local digital certificate.</td>
<td>all, brief, detail</td>
</tr>
<tr>
<td>Certificate Type</td>
<td>Type of certificate. That is—Signing certificate (LOCAL-CERT) which is used to sign other certificates or it is CA-CERT used to verify other certificates in context of SSL-proxy.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>cert modify time</td>
<td>Indicates the time when the certificate data was last modified.</td>
<td>detail</td>
</tr>
<tr>
<td>key modify time</td>
<td>Indicates the time when the certificate key was last modified (displayed in local certificate only).</td>
<td>detail</td>
</tr>
<tr>
<td>certificate version</td>
<td>Version of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique serial number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Issuer</td>
<td>Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:</td>
<td>brief, detail</td>
</tr>
<tr>
<td></td>
<td>• C—Country of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ST—State or province name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L—Locality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• O—Organization of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OU—Organizational unit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CN—Common name of the authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• emailAddress—Common name of the authority.</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:</td>
<td>brief, detail</td>
</tr>
<tr>
<td></td>
<td>• C—Country of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ST—State or province name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L—Locality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• O—Organization of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OU—Organizational unit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CN—Common name of the authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• emailAddress—Common name of the authority.</td>
<td></td>
</tr>
<tr>
<td>validity</td>
<td>Validity of the certificate (displayed in local certificate only). It includes:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• not before—Start time when the digital certificate becomes valid.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• not after—End time when the digital certificate becomes invalid.</td>
<td></td>
</tr>
</tbody>
</table>
Table 103: show services ssl certificate Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| Public Key algorithm | Encryption algorithm used with the private key, such as `rsaEncryption (1024 bits)`.
| Signature algorithm | Encryption algorithm that the CA used to sign the digital certificate, such as `sha1WithRSAEncryption`.
| CRL              | Certificate revocation list related information (displayed for CA certificates only). It includes:
|                  | • present—list of digital certificates that have been revoked before their expiration date are present or not.
|                  | • check—CRL check status: enabled or disabled.
|                  | • download-failed—Indicates the download status of the certificate revocation list.
|                  | • check-on-download-fail—Indicates checking of the certificates against the local CRL file is enabled when the CRL download fails.

---

**Sample Outputs**

```plaintext
show services ssl certificate all
user@host > show services ssl certificate all

Lsys Name : root-logical-system
PIC:fwdd0 fpc[0] pic[0] -------
CertID
-----------------------------
ssl-inspect-ca
ssl-cert-4k

user@host > show services ssl certificate brief certificate-id

Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0] -------
CertID : trusted-ca
Certificate Type : CA-CERT
```
Issuer : /C=IN/ST=KA/L=BNG/O=XYZ/OU=ABC/CN=5.0.0.1/emailAddress=newca@test.com
Subject : /C=IN/ST=KA/L=BNG/O=XYZ/OU=ABC/CN=5.0.0.1/emailAddress=newca@test.com
Public Key algorithm : rsaEncryption

user@host> show services ssl certificate brief certificate-id ssl-inspect-ca

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] -------

CertID : ssl-inspect-ca
Certificate Type : LOCAL-CERT
Issuer : /DC=dc/CN=xyz.com/OU=IT/O=abc/L=bng/ST=KA/C=IN
Subject : /DC=dc/CN=xyz.com/OU=IT/O=abc/L=bng/ST=KA/C=IN
Validity :
   Not before : Mon 02/18/2019 07:30:37 AM
   Not after : Sat 02/17/2024 07:30:37 AM
Public Key algorithm : rsaEncryption

show services ssl certificate detail (Local Certificate)
user@host > show services ssl certificate detail

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] -------

CertID : ssl-inspect-ca
Certificate Type : LOCAL-CERT
cert modify time : Mon 02/18/2019 07:30:37 AM
key modify time : Mon 02/18/2019 07:30:23 AM
certificate version : 3
serial number : 72 a4 a8 12 0e a0 da 5f ee 27 47 d8 19 7c 76 b5
Issuer : /DC=dc/CN=XYZ.com/OU=IT/O=jnpr/L=bng/ST=KA/C=IN
Subject : /DC=dc/CN=XYZ.com/OU=IT/O=jnpr/L=bng/ST=KA/C=IN
Validity :
   Not before : Mon 02/18/2019 07:30:37 AM
   Not after : Sat 02/17/2024 07:30:37 AM
Public Key algorithm : rsaEncryption
Signature Algorithm : sha256WithRSAEncryption
show services ssl certificate detail (CA Certificate)

user@host > show services ssl certificate detail

Lsys Name : root-logical-system

PIC:fpc0 fpc[0] pic[0] ------

CertID : test
Certificate Type : CA-CERT
cert modify time : Mon 09/02/2019 09:47:48 PM
certificate version : 1
serial number : 21 a8 d6 00 eb 24 1f 78 9a e5 0e ec 6a 39 ce 65 66 42 8c 0a
Issuer :
/C=IN/ST=KA/L=BLR/O=XYZ.com/OU=IT/CN=5.0.0.1/emailAddress=newca@test.com
Subject :
/C=IN/ST=KA/L=BLR/O=XYZ.con/OU=IT/CN=5.0.0.1/emailAddress=newca@test.com
Public Key algorithm : rsaEncryption
Signature Algorithm : sha256WithRSAEncryption
CRL :
   present : no
   check : enabled
download-failed : true
   check-on-download-fail : enabled
show services ssl session

Syntax

```
show services ssl session flow-session-id
pic-info fpc-slot slot number pic-slot slot-number
```

Release Information

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description

Display information about the Secure Sockets Layer (SSL) session.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options

```
pic-info fpc-slot slot number pic-slot slot-number
```

— Display the information for the FPC in the specified slot.

Required Privilege Level

view

RELATED DOCUMENTATION

Operational Commands to Troubleshoot SSL Sessions | 439

show security flow session ssl | 778

List of Sample Output

show services ssl session on page 927

Output Fields

Table 104 on page 926 lists the output fields for the `show services ssl session` command. Output fields are listed in the approximate order in which they appear.

Table 104: show services ssl session Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Session identifier.</td>
</tr>
</tbody>
</table>
Table 104: show services ssl session Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>SSL connection type.</td>
</tr>
<tr>
<td>SSL Profile:</td>
<td>SSL profile applied - proxy or termination or initiation.</td>
</tr>
<tr>
<td>Resumed Session</td>
<td>Session resumption applied.</td>
</tr>
<tr>
<td>One-Crypto</td>
<td>One-crypto status for this particular session: Enabled or Disabled.</td>
</tr>
<tr>
<td>Async-crypto</td>
<td>Async-crypto status for this particular session: Enabled or Disabled.</td>
</tr>
<tr>
<td>Renegotiation Count</td>
<td>Number of times the session renegotiation was done.</td>
</tr>
<tr>
<td>Server Certificate Subject Name</td>
<td>Full subject name of the certificate.</td>
</tr>
<tr>
<td>Server Cert verification status</td>
<td>Status of the server certificate validation.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the certificate.</td>
</tr>
<tr>
<td>CRL check</td>
<td>Status of cRL validation is enabled or disabled.</td>
</tr>
<tr>
<td>Action</td>
<td>Actions related to certification revocations checks.</td>
</tr>
<tr>
<td>SSL_T Details:</td>
<td>SSL termination details:</td>
</tr>
<tr>
<td></td>
<td>• Key Size—Server certificates key size</td>
</tr>
<tr>
<td></td>
<td>• Cipher—SSL Cipher.</td>
</tr>
<tr>
<td></td>
<td>• TLS version—Protocol version used.</td>
</tr>
<tr>
<td>SSL_I Details</td>
<td>SSL initiation details:</td>
</tr>
<tr>
<td></td>
<td>• Key Size—Server certificates key size</td>
</tr>
<tr>
<td></td>
<td>• Cipher—SSL Cipher.</td>
</tr>
<tr>
<td></td>
<td>• TLS version—Protocol version used.</td>
</tr>
</tbody>
</table>

Sample Output

```bash
show services ssl session
user@host > show services ssl session flow-session-id
```
Lsys Name : root-logical-system

PIC: fpc0 fpc[0] pic[0] ------

Session ID : 56
Connection Type : PROXY
SSL Profile : SSL_PROFILE
Resumed Session : No
One-crypto : Disabled
Async-crypto : Enabled
Renegotiation count : 0
Server Certificate Subject Name : /C=IN/ST=KAR/L=BNG/O=JN/OU=JNPR/CN=server/emailAddress=ser
Server Cert verification status : OK
CRL check : Enabled
Action : Allow
SSL_T Details :
  Key size : 2048
  cipher : ECDHE-RSA-AES256-GCM-SHA384
  TLS version : 1.2
SSL_I Details :
  Key size : 2048
  Cipher : ECDHE-RSA-AES256-GCM-SHA384
  TLS version : 1.2
show services ssl termination counters

Syntax

```
show services ssl termination counters [all | errors | handshake]
pic-info fpc-slot slot number pic-slot slot-number
```

Release Information

Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description

Display statistical counters for the SSL termination session.

**NOTE:** When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options

```
pic-info fpc0.pic0 fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.
all—Display all the counters generated during SSL termination.
error—Display all the counters related to errors occurred during SSL termination.
handshake—Display all the counters related to handshake during SSL termination.
```

Required Privilege Level

view

**RELATED DOCUMENTATION**

- Operational Commands to Troubleshoot SSL Sessions | 439
- show services ssl termination profile | 934

**List of Sample Output**

- show services ssl termination counters all on page 931
- show services ssl termination counters error on page 932

**Output Fields**
Table 105 on page 930 lists the output fields for the `show services ssl termination counters` command. Output fields are listed in the approximate order in which they appear.

Table 105: show services ssl termination counters Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Display Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory errors</td>
<td>Errors related to memory allocation.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Handshake errors</td>
<td>Number of errors occurred during handshake.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Cert Cache errors</td>
<td>Number of certificate cache errors.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Server Protection errors</td>
<td>Errors occurred during SSL reverse proxy.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Proxy errors</td>
<td>Errors occurred in SSL proxy sessions.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Crypto errors</td>
<td>Errors related to Cryptographic modules.</td>
<td>all, errors</td>
</tr>
<tr>
<td>Certificate errors</td>
<td>Errors related to digital certificates</td>
<td>all, errors</td>
</tr>
<tr>
<td>One-Crypto errors</td>
<td>Number of one-crypto errors</td>
<td>all, errors</td>
</tr>
<tr>
<td>Async-Crypto errors</td>
<td>Number of Async-crypto errors</td>
<td>all, errors</td>
</tr>
<tr>
<td>Mirror errors</td>
<td>Errors in SSL decryption mirroring</td>
<td>all, errors</td>
</tr>
<tr>
<td>handshakes started</td>
<td>Number of SSL handshakes started.</td>
<td>all, handshake</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>Number of SSL handshakes completed successfully.</td>
<td>all, handshake</td>
</tr>
<tr>
<td>active sessions</td>
<td>Number of active SSL sessions</td>
<td>all, handshake</td>
</tr>
<tr>
<td>Interdicted cert generated</td>
<td>Number of interdicted certificates generated</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: sessions created</td>
<td>Number of proxy sessions created</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: sessions active</td>
<td>Number of active proxy sessions</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: sessions ignored</td>
<td>Number of proxy sessions ignored.</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: renegotation ignored</td>
<td>Number of renegotiation requests ignored.</td>
<td>all, handshake</td>
</tr>
</tbody>
</table>
Table 105: show services ssl termination counters Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Display Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy: session resumption</td>
<td>Number of session resumption requests</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: secure renegotiation</td>
<td>Number of SSL sessions with secure renegotiation</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: insecure renegotiation</td>
<td>Number of SSL sessions with insecure renegotiation</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: multiple renegotiation</td>
<td>Number of SSL sessions with multiple renegotiation</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: reneg after resumption</td>
<td>Number of SSL sessions undergo renegotiation after resumption</td>
<td>all, handshake</td>
</tr>
<tr>
<td>init: passthrough requests</td>
<td>Passthrough requests during initiation</td>
<td>all, handshake</td>
</tr>
<tr>
<td>init: start requests</td>
<td>Start requests during initiation</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: ECDSA based srvr auth</td>
<td>Sessions completed ECDSA-based server authentication</td>
<td>all, handshake</td>
</tr>
<tr>
<td>proxy: RSA based srvr auth</td>
<td>Sessions completed RSA-based server authentication</td>
<td>all, handshake</td>
</tr>
</tbody>
</table>

Sample Output

show services ssl termination counters all
user@host > show services ssl termination counters all

Lsys Name : root-logical-system
PIC:fpc0 fpc[0] pic[0] -----

Memory errors 0
Handshake errors 0
Cert Cache errors 0
Server Protection errors 0
Proxy errors 0
show services ssl termination counters error
user@host > show services ssl termination counters errors

Lsys Name : root-logical-system
PIC:fpc0 -----
Memory errors 0
Handshake errors 0
Cert Cache errors 0
Server Protection errors 0
Proxy errors 0
Crypto errors 0
Certificate errors 0
One-Crypto errors 0
Async-Crypto errors 0
Mirror errors 0

user@host > show services ssl termination counters handshake
Lsys Name : root-logical-system
PIC: fpc0 fpc[0] pic[0] ------

handshakes started 0
handshakes completed 0
active sessions 0
Interdicted cert generated 0
proxy: sessions created 0
proxy: sessions active 0
proxy: sessions ignored 0
proxy: renegotiation ignored 0
proxy: session resumption 0
proxy: secure renegotiation 0
proxy: insecure renegotiation 0
proxy: multiple renegotiation 0
proxy: reneg after resumption 0
init: passthrough requests 0
init: start requests 0
proxy: ECDSA based srvr auth 0
proxy: RSA based srvr auth 0
show services ssl termination profile

Syntax

show services ssl termination profile [all | brief | detail]
<pic-info fpc-slot slot number pic-slot slot-number>

Release Information
Command introduced in Junos OS Release 19.3R1 for SRX Series devices.

Description
Display the SSL termination profile details.

NOTE: When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Options
pic-info fpc-slot slot number pic-slot slot-number—Display the information for the FPC in the specified slot.

all—Display all SSL termination profiles configured on the device.

brief—Display brief information about SSL termination profile.

detail—Display detail information about SSL termination profiles.

Required Privilege Level
view

RELATED DOCUMENTATION

Operational Commands to Troubleshoot SSL Sessions | 439
show services ssl termination counters | 929

List of Sample Output
show services ssl termination profile all on page 936
show services ssl termination profile brief profile-name on page 937
show services ssl termination profile detail profile-name on page 937

Output Fields
Table 106 on page 935 lists the output fields for the `show services ssl termination profile` command. Output fields are listed in the approximate order in which they appear.

### Table 106: `show show services ssl termination profile` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>SSL termination profile name.</td>
<td>detail</td>
</tr>
<tr>
<td>allow non-ssl session</td>
<td>Allow or not allow (bypass) non-SSL sessions.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>preferred-ciphers</td>
<td>SSL cipher that can be used with acceptable key strength. Possible values are strong, medium, weak, and custom.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>Num of url categories configured</td>
<td>URL categories exempted from SSL proxy.</td>
<td>brief, detail</td>
</tr>
<tr>
<td>Number of whitelist entries</td>
<td>Whitelisted sessions bypassing SSL proxy processing.</td>
<td>brief</td>
</tr>
<tr>
<td>Protocol-version</td>
<td>SSL protocol version. Possible values are all, TLS version 1.0, TLS version 1.1, and TLS version 1.2.</td>
<td>detail</td>
</tr>
<tr>
<td>Client authentication</td>
<td>Status of client certificate verification process.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Authentication</td>
<td>Status of server certificate verification process.</td>
<td>detail</td>
</tr>
<tr>
<td>Crypto-mode</td>
<td>Crypto mode used. Options are synchronous-hardware or software or asynchronous-hardware.</td>
<td>detail</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>SSL session resumption status.</td>
<td>detail</td>
</tr>
<tr>
<td>CRL check</td>
<td>Status of the CRL checking of certificate validity.</td>
<td>detail</td>
</tr>
<tr>
<td>Certificate</td>
<td>Types of certificates used.</td>
<td>detail</td>
</tr>
<tr>
<td>Renegotiation</td>
<td>Renegotiation option. Possible values are allow, allow secure, and drop.</td>
<td>detail</td>
</tr>
<tr>
<td>Custom ciphers</td>
<td>Custom ciphers configured.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Cert</td>
<td>Server certificate configured.</td>
<td>detail</td>
</tr>
<tr>
<td>Custom ciphers</td>
<td>Custom ciphers configured.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Cert</td>
<td>Server certificate configured.</td>
<td>detail</td>
</tr>
<tr>
<td>Decrypt Mirror</td>
<td>Status of decrypt mirroring functionality.</td>
<td>detail</td>
</tr>
</tbody>
</table>
### Table 106: show show services ssl termination profile Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted CA:</td>
<td>Trusted CA configured for a profile</td>
<td>detail</td>
</tr>
<tr>
<td>Counters</td>
<td>Details of the counters generated in the session</td>
<td>detail</td>
</tr>
<tr>
<td>handshakes started</td>
<td>Number of SSL handshakes started.</td>
<td>detail</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>Number of SSL handshakes completed successfully.</td>
<td>detail</td>
</tr>
<tr>
<td>active sessions</td>
<td>Number of active SSL sessions</td>
<td>detail</td>
</tr>
<tr>
<td>total handshake errors</td>
<td>Number of errors occurred during handshake process.</td>
<td>detail</td>
</tr>
<tr>
<td>Data Errors</td>
<td>Cumulative errors in a single counter. Any errors related to data such as read or write errors.</td>
<td>detail</td>
</tr>
<tr>
<td>session resumption</td>
<td>Number of SSL session resumption count.</td>
<td>detail</td>
</tr>
<tr>
<td>secure renegotiation</td>
<td>Secure sessions allowed after renegotiation.</td>
<td>detail</td>
</tr>
<tr>
<td>insecure renegotation</td>
<td>All sessions allowed after renegotiation.</td>
<td>detail</td>
</tr>
<tr>
<td>multiple renegotation</td>
<td>Sessions with multiple renegotiation.</td>
<td>detail</td>
</tr>
<tr>
<td>reneg after resumption</td>
<td>Sessions undergoing renegotiation after resumption.</td>
<td>detail</td>
</tr>
<tr>
<td>no_reneg alert by peer</td>
<td>Number of times no renegotiation alerts received from peer.</td>
<td>detail</td>
</tr>
<tr>
<td>drop on reneg</td>
<td>Sessions dropped after renegotiation.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

```bash
show services ssl termination profile all
user@host > show services ssl termination profile

Lsys Name : root-logical-system

PIC: fwdd0 fpc[0] pic[0] ---------
```
show services ssl termination profile brief profile-name
user@host > show services ssl termination profile brief profile-name

Lsys Name : root-logical-system

PIC: fwdd0 fpc[0] pic[0] ----------

Profile: ssl-termination
allow non-ssl session: true
preferred-ciphers: medium
Num of url categories configured: NIL
Number of whitelist entries: 0

show services ssl termination profile detail profile-name
user@host > show services ssl termination profile detail profile-name

Lsys Name : root-logical-system

PIC: fwdd0 fpc[0] pic[0] ----------

Profile: root_profile_65536_proxy_t
allow non-ssl session: true
preferred-ciphers: medium
Num of url categories configured: 0
Protocol version: all
Client Authentication: notset
Server Authentication: Required
Crypto Mode: hw-sync
Session Resumption: Enabled
CRL check: Enabled
Certificate RSA: p_5
Renegotiation: disabled
Custom ciphers: 0
Server cert: 0
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypt Mirror</td>
<td>Disabled</td>
</tr>
<tr>
<td>Trusted CA</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>handshakes started</td>
<td>0</td>
</tr>
<tr>
<td>handshakes completed</td>
<td>0</td>
</tr>
<tr>
<td>active sessions</td>
<td>0</td>
</tr>
<tr>
<td>total handshake errors</td>
<td>0</td>
</tr>
<tr>
<td>Data Errors</td>
<td>0</td>
</tr>
<tr>
<td>session resumption</td>
<td>0</td>
</tr>
<tr>
<td>secure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>insecure renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>multiple renegotiation</td>
<td>0</td>
</tr>
<tr>
<td>reneg after resumption</td>
<td>0</td>
</tr>
<tr>
<td>no_reneg alert by peer</td>
<td>0</td>
</tr>
<tr>
<td>drop on reneg</td>
<td>0</td>
</tr>
</tbody>
</table>
show services web-proxy dns forwarding-cache

Syntax

```
show services web-proxy dns forwarding-cache
```

Release Information
Command introduced in Junos OS Release 19.2R1.

Description
Display DNS cache information available at the packet forwarding engine for a secure Web proxy session.

Required Privilege Level
view

RELATED DOCUMENTATION

- show services web-proxy session
- show services web-proxy session statistics

List of Sample Output

- show services web-proxy dns forwarding-cache statistics on page 940
- show services web-proxy dns forwarding-cache on page 940

Output Fields

Table 107 on page 939 and Table 108 on page 940 describe the output fields for the `show services web-proxy dns forwarding-cache` command. Output fields are listed in the approximate order in which they appear.

Table 107: show services web-proxy dns forwarding-cache statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DNS Cache Entries</td>
<td>Number of active DNS cache entries.</td>
</tr>
<tr>
<td>Total DNS Cache Entries</td>
<td>Total number of DNS cache entries.</td>
</tr>
<tr>
<td>DNS Cache hits</td>
<td>DNS requests finding the match in the cache.</td>
</tr>
<tr>
<td>DNS Cache miss</td>
<td>DNS requests missing in the cache.</td>
</tr>
<tr>
<td>DNS Cache add failed</td>
<td>DNS requests failed to add in the DNS cache memory.</td>
</tr>
</tbody>
</table>
Table 108: show services web-proxy dns forwarding-cache Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name</td>
<td>Name of the Domain Name System (DNS).</td>
</tr>
<tr>
<td>Address Family</td>
<td>IPv4 or IPv6 address family.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address for the DNS name.</td>
</tr>
</tbody>
</table>

**Sample Output**

show services web-proxy dns forwarding-cache statistics

```
user@host> show services web-proxy dns forwarding-cache statistics

DNS status                                      Active
Active DNS Cache entries                        4294967270
Total DNS Cache Entries                         1
DNS Cache hits                                  61
DNS Cache miss                                  191
DNS Cache add failed                            0
```

show services web-proxy dns forwarding-cache

```
user@host> show services web-proxy dns forwarding-cache

DNS Name: settings-win.data.microsoft.com
  Address Family: IPv4
  IP Address: 40.90.221.9
```
show services web-proxy dns global-cache statistics

Syntax

```
show services web-proxy dns global-cache statistics
```

Release Information

Command introduced in Junos OS Release 19.2R1.

Description

Display DNS cache information available at the routing engine for a secure Web proxy session.

Required Privilege Level

view

RELATED DOCUMENTATION

- `show services web-proxy session`
- `show services web-proxy session statistics`

List of Sample Output

`show services web-proxy dns global-cache statistics on page 942`
`show services web-proxy dns global-cache on page 942`

Output Fields

`Table 109 on page 941` and `Table 110 on page 942` describe the output fields for the `show services web-proxy dns global-cache` commands. Output fields are listed in the approximate order in which they appear.

Table 109: show services web-proxy statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DNS Cache Entries</td>
<td>Number of active DNS cache entries.</td>
</tr>
<tr>
<td>Total DNS Cache Entries</td>
<td>Total number of DNS cache entries.</td>
</tr>
<tr>
<td>DNS Cache hits</td>
<td>Number of DNS requests finding the match in the cache.</td>
</tr>
<tr>
<td>DNS Cache miss</td>
<td>Number of DNS requests missing the match in the cache.</td>
</tr>
<tr>
<td>DNS resolve request send failed</td>
<td>Number of failed DNS resolve requests.</td>
</tr>
<tr>
<td>DNS resolve request Timeout</td>
<td>Number of DNS resolve requests timed out.</td>
</tr>
</tbody>
</table>
Table 110: show services web-proxy dns global-cache Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name</td>
<td>Name of the Domain Name System (DNS).</td>
</tr>
<tr>
<td>Address Family</td>
<td>IPv4 or IPv6 address family.</td>
</tr>
<tr>
<td>TTL</td>
<td>Time-to-live value.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address for the DNS name.</td>
</tr>
</tbody>
</table>

Sample Output

show services web-proxy dns global-cache statistics

user@host>  show services web-proxy dns global-cache statistics

<table>
<thead>
<tr>
<th>DNS Status</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DNS Cache entries</td>
<td>1</td>
</tr>
<tr>
<td>Total DNS Cache Entries</td>
<td>1</td>
</tr>
<tr>
<td>DNS Cache hits</td>
<td>0</td>
</tr>
<tr>
<td>DNS Cache miss</td>
<td>191</td>
</tr>
<tr>
<td>DNS resolve request send failed</td>
<td>0</td>
</tr>
<tr>
<td>DNS resolve request Timeout</td>
<td>6</td>
</tr>
</tbody>
</table>

show services web-proxy dns global-cache

user@host>  show services web-proxy dns global-cache

DNS Name: settings-win.data.microsoft.com
Address Family: IPv4, TTL: 0
IP Address: 40.90.221.9
show services web-proxy session

Syntax

```
show services web-proxy session
```

Release Information
Command introduced in Junos OS Release 19.2R1.

Description
Display information about the secure Web proxy session.

Options
- detail—Shows the web proxy session detail.
- summary—Shows the web proxy session summary.

Required Privilege Level
view

RELATED DOCUMENTATION

- Secure Web Proxy | 122

List of Sample Output
- show services web-proxy session summary on page 944
- show services web-proxy session detail on page 944

Output Fields
Table 111 on page 943 describes the output fields for the `show services web-proxy session` command. Output fields are listed in the approximate order in which they appear.

Table 111: show services web-proxy session Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Session</td>
<td>Session originating from the client to proxy server.</td>
</tr>
<tr>
<td>Proxy Session</td>
<td>Session originating from the proxy server to the client.</td>
</tr>
<tr>
<td>Client Session ID</td>
<td>Number that identifies the client session. Use this ID to get more information about the session.</td>
</tr>
</tbody>
</table>
Table 111: show services web-proxy session Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Session ID</td>
<td>Number that identifies the proxy session. Use this ID to get more information about the session.</td>
</tr>
<tr>
<td>Proxy Request</td>
<td>Connect request details.</td>
</tr>
<tr>
<td>Dynamic Web App</td>
<td>Dynamic Web application details.</td>
</tr>
</tbody>
</table>

Sample Output

show services web-proxy session summary

```
user@host> show services web-proxy session summary

Web Proxy sessions:
Client Session                   Proxy Session
[34] 6.0.0.1/62746 ---> 5.0.0.1/8080          [35] 6.0.0.1/62746 ---> 208.80.154.224/443
208.80.154.224/443
[37] 6.0.0.1/62747 ---> 5.0.0.1/8080          [38] 6.0.0.1/62747 ---> 208.80.154.224/443
208.80.154.224/443
```

Sample Output

show services web-proxy session detail

```
user@host> show services web-proxy session detail

Web Proxy sessions:
Client Session ID: 36994, Proxy Session ID: 36995
Client: 6.0.0.1/61324 ---> 5.0.0.1/8080
Proxy: 6.0.0.1/61324 ---> 74.125.195.188/443
Proxy Request: CONNECT:mtalk.google.com:443
Dynamic Web App: junos:GOOGLE-MAPS

Client Session ID: 38037, Proxy Session ID: 38038
```
Client: 6.0.0.1/57342 ---> 5.0.0.1/8080
Proxy : 6.0.0.1/57342 ---> 216.58.194.202/443
Proxy Request: CONNECT:safebrowsing.googleapis.com:443
Dynamic Web App: junos:GOOGLE-GEN