



Junos[®] OS

AppSecure Services Feature Guide for Security Devices



Modified: 2017-07-18

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.

Junos® OS AppSecure Services Feature Guide for Security Devices
Copyright © 2017 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 <http://www.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	xv
	Documentation and Release Notes	xv
	Supported Platforms	xv
	Using the Examples in This Manual	xv
	Merging a Full Example	xvi
	Merging a Snippet	xvi
	Documentation Conventions	xvii
	Documentation Feedback	xix
	Requesting Technical Support	xix
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xx
Chapter 1	Overview	21
	Understanding AppSecure Services	21
Chapter 2	Understanding Application Identification	23
	Understanding Application Identification Techniques	23
	Junos OS Next-Generation Application Identification	23
	Application Signature Mapping	24
	Application Identification Match Sequence	24
	Understanding the Junos OS Application Identification Database	26
Chapter 3	Installing Application Signature Package	27
	Understanding the Junos OS Application Package Installation	27
	Upgrading to Next-Generation Application Identification	29
	Installing and Verifying Licenses for an Application Signature Package	30
	Downloading and Installing the Junos OS Application Signature Package Manually	32
	Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package	35
	Example: Scheduling the Application Signature Package Updates	38
	Scheduling the Application Signature Package Updates As Part of the IDP Security Package	40
	Example: Downloading and Installing the Application Identification Package in Chassis Cluster Mode	42
	Verifying the Junos OS Application Identification Extracted Application Package	46
	Uninstalling the Junos OS Application Identification Application Package	47
	Disabling and Reenabling Junos OS Application Identification	48

Chapter 4	Custom Application Signatures	49
	Understanding Junos OS Application Identification Custom Application	
	Signatures	49
	ICMP-Based Mapping	50
	Address-Based Mapping	50
	IP Protocol-Based Mapping	51
	Layer 7-Based Signatures	51
	Example: Configuring Junos OS Application Identification Custom Application	
	Signatures	52
Chapter 5	Configuring Application Groups	59
	Customizing Application Groups for Junos OS Application Identification	59
	Enabling or Disabling Application Groups in Junos OS Application	
	Identification	60
	Example: Configuring a Custom Application Group for Junos OS Application	
	Identification for Simplified Management	60
Chapter 6	Configuring Application System Cache	65
	Understanding the Application System Cache	65
	Deactivating Application System Cache Information for Application Identification	
	(CLI Procedure)	66
	Verifying Application System Cache Statistics	66
Chapter 7	Controlling Application Identification Performance	69
	Onbox Application Identification Statistics	69
	Understanding Jumbo Frames Support for Junos OS Application Identification	
	Services	70
	Improving the Application Traffic Throughput	70
Chapter 8	Configuring SSL Proxy	73
	SSL Proxy Overview	73
	Perfect Forward Secrecy	75
	Supported Ciphers in Proxy Mode	76
	Server Authentication	77
	Trusted CA List	78
	Root CA	79
	Client Authentication	79
	Whitelists	79
	Dynamic Resolution of Domain Names	79
	Session Resumption	79
	Session Renegotiation	80
	SSL Proxy Logs	80
	Leveraging Dynamic Application Identification	81
	Logical Systems Support	82
	Limitations	82
	Configuring SSL Proxy	83
	SSL Proxy Configuration Overview	84
	Configuring a Root CA Certificate	85
	Configuring a CA Profile Group	87
	Configuring a Trusted CA Profile	88

	Importing a Root CA Certificate into a Browser	89
	Applying an SSL Proxy Profile to a Security Policy	90
	Creating a Whitelist of Exempted Destinations	91
	Configuring SSL Proxy Logging	93
	Configuring Ciphers	94
	Exporting Certificates to a Specified Location	94
	Ignoring Server Authentication	94
	Configuring SSL Forward Proxy Certificate Chain	95
	Understanding SSL Certificate Chain	95
	SSL Proxy Overview	95
	SSL Certificate Chain Overview	96
	Advantage of Certificate Chains	97
	Understanding Certificate Chain Processing	97
	Configuring the SSL Certificate Chain	98
	Application Firewall, IDP, and Application Tracking with SSL Proxy Overview . .	102
	Working with the Certificate Revocation Lists for SSL Proxy	103
	Disabling CRL Verification	103
	Allowing Sessions When CRL Information Is Not Available	104
	Allowing Sessions When CRL Status Is Unknown	104
	Enabling Debugging and Tracing for SSL Proxy	105
Chapter 9	Configuring Application Firewall	107
	Application Firewall Overview	107
	Understanding Application Firewall Rule Sets	108
	Configuring an Application Firewall Within a Security Policy	109
	Application Group Support for Application Firewall	109
	Redirecting Users	110
	Session Logging for Application Firewalls	111
	Application Firewall Support in Chassis Cluster	111
	Example: Configuring Application Firewall Rule Sets Within a Security Policy . .	112
	Example: Configuring an Application Group for Application Firewall	116
	Example: Configuring Application Firewall When SSL Proxy Is Enabled	120
Chapter 10	Configuring Application Tracking	125
	Understanding AppTrack	125
	Example: Configuring AppTrack	127
	Example: Configuring AppTrack When SSL Proxy Is Enabled	132
	Disabling AppTrack	134
Chapter 11	Configuring Application QoS	135
	Understanding Application QoS (AppQoS)	135
	Unique Forwarding Classes and Queue Assignments	136
	Application-Aware DSCP Code-Point and Loss Priority Settings	137
	Rate Limiters and Profiles	138
	Rate-Limiter Assignment	139
	Rate-Limiter Action	141
	AppQoS Security Policy Configuration	141
	Example: Configuring AppQoS	141

Chapter 12	Advanced Policy-Based Routing	149
	Understanding Advanced Policy-Based Routing	149
	Application Identification	149
	Filter-Based Forwarding or Policy-Based Routing (PBR)	150
	Advanced Policy-Based Routing	150
	Understanding How APBR Works	151
	Use Case	152
	Limitations	152
	Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution	152
Chapter 13	Configuration Statements	161
	actions (Services SSL Proxy)	164
	actions (Services SSL Initiation)	166
	address-mapping (Application Identification)	167
	advance-policy-based-routing	168
	advance-policy-based-routing (Security Zones)	169
	appfw-profile (System)	170
	appfw-rule	171
	appfw-rule-set	172
	application-firewall	173
	application (Application Identification)	175
	application-firewall (Application Services)	177
	application-identification	178
	application-group (Services)	180
	application-services (Security Policies)	181
	application-system-cache	182
	application-system-cache-timeout (Services)	183
	application-tracking	184
	application-tracking (Security Zones)	185
	application-traffic-control	186
	application-traffic-control (Application Services)	187
	block-message (Application Firewall)	188
	context (Application Identification)	190
	custom-ciphers	192
	default-rule	193
	direction (Application Identification)	194
	disable (Application Tracking)	195
	download (Services)	196
	dynamic-application	197
	dynamic-application-group	197
	enable-flow-tracing (Services)	198
	enable-performance-mode	199
	enable-session-cache	200
	file (Services)	201
	files (Services)	202
	file (System Logging)	203
	first-update	205
	first-update-interval	206

flag (Services)	207
format (Security Log)	208
forwarding-classes (CoS)	209
global-config (Services)	210
icmp-mapping (Application Identification)	211
ip (Application Identification)	212
ip-protocol-mapping (Application Identification)	212
initiation (Services)	213
level (Services)	214
log (Security)	215
log (Services)	219
match (Services)	220
no-application-identification (Services)	220
no-application-system-cache (Services)	221
no-remote-trace (Services)	221
over (Application Identification)	222
policies	224
policy (Security Policies)	229
port-range (Application Identification)	231
preferred-ciphers	232
profile (Application Firewall)	233
profile (Rule Sets)	234
profile (Services)	235
profile (SSL Initiation)	236
profile (SSL Termination)	237
protocol-version	238
proxy (Services)	239
rate-limiters	241
renegotiation (Services)	242
root-ca (Services)	242
routing-instance (Advanced Policy-Based Routing)	243
rule (Advanced Policy-Based Routing)	244
rule-sets (CoS AppQoS)	245
rule-sets (Security Application Firewall)	247
security-zone	248
server-certificate (Services)	249
session-update-interval	250
size (Services)	251
ssl (Services)	252
ssl-encryption	254
ssl-proxy (Application Services)	255
statistics (Services)	256
stream (Security Log)	257
termination (Services)	258
then (Security Application Firewall)	259
trusted-ca (Services)	260
traceoptions (advanced policy-based routing)	261
traceoptions (Security Application Firewall)	263
traceoptions (Services Application Identification)	265

Chapter 14

traceoptions (Services SSL)	267
transport (Security Log)	269
whitelist (Services)	270
whitelist-url-categories	271
zones	272
Operational Commands	275
clear security application-firewall rule-set statistics	277
clear security application-firewall rule-set statistics logical-system	278
clear services application-identification application-statistics	279
clear services application-identification application-statistics cumulative ...	280
clear services application-identification application-statistics interval	281
clear services application-identification application-system-cache (Junos OS)	282
clear services application-identification counter (Values)	283
clear services ssl proxy statistics	284
request security pki ca-certificate ca-profile-group load	285
request security pki local-certificate export	287
request security pki local-certificate generate-self-signed	288
request security pki local-certificate load	290
request services application-identification application	291
request services application-identification download	292
request services application-identification download status	293
request services application-identification group	294
request services application-identification install	296
request services application-identification install status	297
request services application-identification proto-bundle-status	298
request services application-identification uninstall	299
request services application-identification uninstall status	300
show class-of-service application-traffic-control counter	301
show class-of-service application-traffic-control statistics rate-limiter	303
show class-of-service application-traffic-control statistics rule	305
show security advance-policy-based-routing statistics	307
show security advance-policy-based-routing status	308
show security advance-policy-based-routing profile	309
show security application-firewall rule-set	310
show security application-firewall rule-set logical-system	313
show security application-tracking counters	316
show security flow session	318
show security flow session application-firewall	325
show security pki ca-certificate	331
show security pki local-certificate (View)	335
show security policies	340
show services application-identification application	349
show services application-identification application-system-cache (View) ...	353
show services application-identification commit-status	355
show services application-identification counter (AppSecure)	356
show services application-identification group	360
show services application-identification statistics applications	362

show services application-identification statistics application-groups	364
show services application-identification status	366
show services application-identification version	369
show services ssl proxy statistics	370

List of Figures

Chapter 2	Understanding Application Identification	23
	Figure 1: Mapping Sequence	25
Chapter 8	Configuring SSL Proxy	73
	Figure 2: SSL Inspection on an Existing SRX Series IDP Module	74
	Figure 3: SSL Proxy on an Encrypted Payload	75
	Figure 4: SSL Proxy Configuration Overview	85
	Figure 5: Applying an SSL Proxy Profile to a Security Policy	91
	Figure 6: Certificate Chaining	97
	Figure 7: Certification Path from the Certificate Owner to the Root CA	98
Chapter 12	Advanced Policy-Based Routing	149
	Figure 8: APBR Flow Diagram	151

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xvii
	Table 2: Text and Syntax Conventions	xviii
Chapter 8	Configuring SSL Proxy	73
	Table 3: Supported SSL Cipher List	76
	Table 4: SSL Proxy Logs	80
	Table 5: SSL Proxy Log Prefixes	81
	Table 6: Trace Levels	105
	Table 7: Supported Flags in Trace	105
Chapter 9	Configuring Application Firewall	107
	Table 8: Application Firewall Actions	112
Chapter 11	Configuring Application QoS	135
	Table 9: Standard CoS Aliases and Bit Values	137
Chapter 12	Advanced Policy-Based Routing	149
	Table 10: APBR Configuration Parameters	153
Chapter 13	Configuration Statements	161
	Table 11: Supported Context-Direction Combination for Custom Application Signatures	191
Chapter 14	Operational Commands	275
	Table 12: show class-of-service application-traffic-control counter Output Fields	301
	Table 13: show class-of-service application-traffic-control statistics rate-limiter Output Fields	303
	Table 14: show class-of-service application-traffic-control statistics rule Output Fields	305
	Table 15: show security advance-policy-based-routing statistics	307
	Table 16: show security advance-policy-based-routing profile	309
	Table 17: show security application-firewall rule-set Output Fields	310
	Table 18: show security application-firewall rule-set logical-system Output Fields	314
	Table 19: show security application-tracking counters	316
	Table 20: show security flow session Output Fields	320
	Table 21: show security flow session application-firewall extensive Output Fields	326
	Table 22: show security pki ca-certificate Output Fields	331
	Table 23: show security pki local-certificate Output Fields	336
	Table 24: show security policies Output Fields	341

Table 25: show services application-identification application summary Output Fields	349
Table 26: show services application-identification application Output Fields . .	350
Table 27: show services application-identification application-system-cache Output Fields	353
Table 28: show services application-identification counter Output Fields	356
Table 29: show services application-identification group Output Fields	360
Table 30: show services application-identification statistics applications Output Fields	362
Table 31: show services application-identification statistics application-groups Output Fields	364
Table 32: show services application-identification status Output Fields	366
Table 33: show services ssl proxy statistics Output Fields	370

About the Documentation

- Documentation and Release Notes on page xv
- Supported Platforms on page xv
- Using the Examples in This Manual on page xv
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xix

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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- vSRX
- SRX Series

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.xml;
    }
  }
}
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.xml; }
```

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 xvii defines notice icons used in this guide.

Table 1: Notice Icons




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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Overview

- [Understanding AppSecure Services on page 21](#)

Understanding AppSecure Services

Supported Platforms [SRX Series, vSRX](#)

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. Junos OS application identification 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.

- AppTrack—Tracks and reports applications passing through the device.
- AppFW—Implements an application firewall using application-based rules.
- AppQoS—Provides quality-of-service prioritization based on application awareness.
- Advanced policy-based routing—Classifies session based on applications and applies the configured rules to reroute the traffic.
- 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.

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)

CHAPTER 2

Understanding Application Identification

- [Understanding Application Identification Techniques on page 23](#)
- [Understanding the Junos OS Application Identification Database on page 26](#)

Understanding Application Identification Techniques

Supported Platforms [SRX Series, vSRX](#)

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.

- [Junos OS Next-Generation Application Identification on page 23](#)
- [Application Signature Mapping on page 24](#)
- [Application Identification Match Sequence on page 24](#)

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

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.

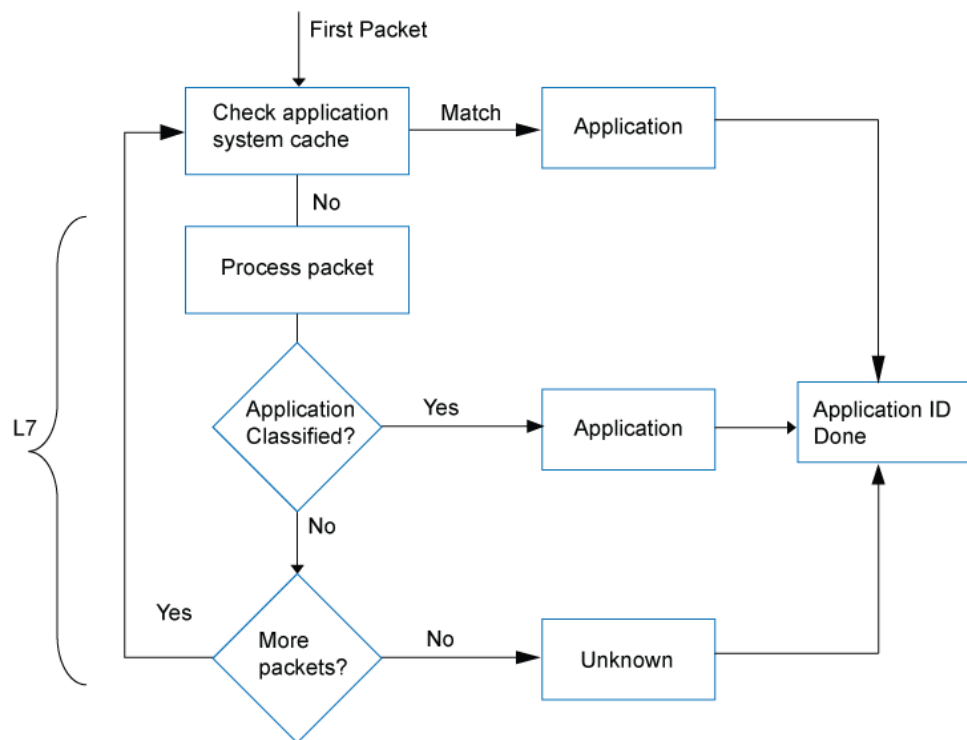
Applications are identified by using a downloadable protocol bundle. Application signatures and parsing information of the first few packets are compared to the content of the database. If the payload contains the same information as an entry in the database, the application of the traffic is identified 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 25](#) shows the sequence in which mapping techniques are applied and how the application is determined.

Figure 1: Mapping Sequence



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

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

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

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

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

- Related Documentation**
- [Understanding AppTrack on page 125](#)
 - [Application Firewall Overview on page 107](#)
 - [IDP Policies Overview](#)
 - [Understanding Application QoS \(AppQoS\) on page 135](#)

Understanding the Junos OS Application Identification Database

Supported Platforms [SRX Series, vSRX](#)

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.

- Related Documentation**
- [Understanding the Junos OS Application Package Installation on page 27](#)
 - [Understanding IDP Application Identification](#)

CHAPTER 3

Installing Application Signature Package

- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Installing and Verifying Licenses for an Application Signature Package on page 30](#)
- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)
- [Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package on page 35](#)
- [Example: Scheduling the Application Signature Package Updates on page 38](#)
- [Scheduling the Application Signature Package Updates As Part of the IDP Security Package on page 40](#)
- [Example: Downloading and Installing the Application Identification Package in Chassis Cluster Mode on page 42](#)
- [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)
- [Uninstalling the Junos OS Application Identification Application Package on page 47](#)
- [Disabling and Reenabling Junos OS Application Identification on page 48](#)

Understanding the Junos OS Application Package Installation

Supported Platforms [SRX Series, vSRX](#)

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 35.](#)



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 32](#) or [“Example: Scheduling the Application Signature Package Updates” on page 38.](#)



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 reenabling AppFW and AppQoS rules once the upgrade or downgrade procedure is complete.



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

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.

SRX Series 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.

Release History Table

Release	Description
12.1X47-D10	Starting from Junos OS Release 12.1X47-D10, next-generation application identification is supported.

Related Documentation

- [Understanding the Junos OS Application Identification Database on page 26](#)
- [Understanding the IDP Signature Database](#)
- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)
- [Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package on page 35](#)
- [Example: Scheduling the Application Signature Package Updates on page 38](#)

Installing and Verifying Licenses for an Application Signature Package

Supported Platforms SRX Series, vSRX

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 <http://kb.juniper.net/InfoCenter/index?page=home>.



NOTE: Starting from 15.1X49-D30 and Junos OS Release 17.3R1, on SRX1500 devices, AppSecure is part of Juniper Networks Secure Edge software (a default shipping software package on the SRX1500). A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.



NOTE: Starting from 15.1X49-D30 and Junos OS Release 17.3R1, on SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license. A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

You can install the license on the 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
```

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

Paste the license key and press Enter to continue.

- Verify the license is installed on your device.

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

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
logical-system	4	1	3	permanent

License identifier: JUN0SXXXXXX

License version: 2

Valid for device: AA4XXXX005

Features:

appid-sig - APPID Signature
date-based, 2014-02-17 08:00:00 GMT-8 - 2015-02-11 08:00:00 GMT-8

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

Release History Table

Release	Description
15.1X49-D40	Starting from 15.1X49-D30 and Junos OS Release 17.3R1, on SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license.
15.1X49-D30	Starting from 15.1X49-D30 and Junos OS Release 17.3R1, on SRX1500 devices, AppSecure is part of Juniper Networks Secure Edge software (a default shipping software package on the SRX1500).

Related Documentation

- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)

- [Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package on page 35](#)

Downloading and Installing the Junos OS Application Signature Package Manually

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 32](#)
- [Overview on page 32](#)
- [Configuration on page 32](#)
- [Verification on page 34](#)

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. See [“Installing and Verifying Licenses for an Application Signature Package” on page 30](#).

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.

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

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

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

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

- To download a specific version of the application package:

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

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

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



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

2. Check the download status.

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

Application package 2345 is downloaded successfully



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

3. Install the application package.

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

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

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

4. Check the installation status of the application package.

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

- To view the installation status:

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

```
Install application package 2345 succeed
```

- To view the protocol bundle status:

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

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



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

Verification

Confirm that the configuration is working properly.

Verifying the Application Identification Status

Purpose Verify that the application identification configuration is working properly.

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

pic: 1/0

Application Identification

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

Application System Cache

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

Protocol Bundle

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

AutoUpdate	Enabled
------------	---------

Slot 1:

Status	Active
Version	1.30.4-22.005 (build date Jan 17 2014)
Sessions	0

Slot 2

Status	Free
--------	------

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

Related Documentation

- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Installing and Verifying Licenses for an Application Signature Package on page 30](#)
- [Example: Scheduling the Application Signature Package Updates on page 38](#)
- [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)
- [Uninstalling the Junos OS Application Identification Application Package on page 47](#)

Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package

Supported Platforms [SRX Series, vSRX](#)

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 on page 36](#)
- [Overview on page 36](#)
- [Configuration on page 36](#)
- [Verification on page 38](#)

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. See [“Installing and Verifying Licenses for an Application Signature Package” on page 30](#).

This example uses the following hardware and software components:

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

Overview

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

Configuration

Downloading and Installing the Signature Database

CLI Quick Configuration

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

Step-by-Step Procedure

To download and install application signatures:

1. Download the signature database.

[edit]

user@host# **run request security idp security-package download**

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



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

2. Check the security package download status.

[edit]

user@host# run request security idp security-package download status

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

3. Install the attack database.

[edit]

user@host# run request security idp security-package install

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



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

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

[edit]

user@host# run request security idp security-package install status

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

5. Confirm your IDP security package version.

[edit]

user@host# run show security idp security-package-version

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

6. Confirm your application identification package version.

[edit]

user@host# run show services application-identification version

```
Application package version: 1884
```

Verification

Confirm that the application signature package is being updated properly.

Verifying application signature package

Purpose Verify the services application identification version.

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

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

```
Application package version: 1884
```

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

- Related Documentation**
- [Understanding the Junos OS Application Package Installation on page 27](#)
 - [Installing and Verifying Licenses for an Application Signature Package on page 30](#)
 - [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)
 - [Uninstalling the Junos OS Application Identification Application Package on page 47](#)

Example: Scheduling the Application Signature Package Updates

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 38](#)
- [Overview on page 39](#)
- [Configuration on page 39](#)
- [Verification on page 40](#)

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. See [“Installing and Verifying Licenses for an Application Signature Package” on page 30.](#)

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 MM-DD.hh:mm format, and click **OK**.
 - Start Time: **12-10.23:59**
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 11:59 pm on December 10:

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

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

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

Verification

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

Related Documentation

- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Installing and Verifying Licenses for an Application Signature Package on page 30](#)
- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)
- [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)

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

Supported Platforms [SRX Series, vSRX](#)

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 on page 40](#)
- [Overview on page 41](#)
- [Configuration on page 41](#)
- [Verification on page 42](#)

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. See [“Installing and Verifying Licenses for an Application Signature Package” on page 30.](#)

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.

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

```
Application package version: 1884
```

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

Related Documentation

- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Installing and Verifying Licenses for an Application Signature Package on page 30](#)
- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)
- [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)

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

Supported Platforms [SRX Series](#), [vSRX](#)

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

- [Requirements on page 43](#)
- [Overview on page 43](#)
- [Downloading and Installing the Application Identification Package on page 44](#)

Requirements

Before you begin:

- Set the chassis cluster node ID and cluster ID. See *Example: Setting the Chassis Cluster Node ID and Cluster ID for SRX Series Devices*.
- 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 application identification feature license. See [“Installing and Verifying Licenses for an Application Signature Package” on page 30](#).

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 27](#).

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 be 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
```

```
node0:
```

```
-----
Uninstall application package 2345 succeed
```

```
node1:
```

```
-----
Uninstall application package 2345 succeed
```

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
```

Related Documentation

- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Installing and Verifying Licenses for an Application Signature Package on page 30](#)
- [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)

Verifying the Junos OS Application Identification Extracted Application Package

Supported Platforms [SRX Series, vSRX](#)

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

```

Related Documentation

- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)

Uninstalling the Junos OS Application Identification Application Package

Supported Platforms [SRX Series, vSRX](#)

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.

- Related Documentation**
- [Downloading and Installing the Junos OS Application Signature Package Manually on page 32](#)
 - [Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package on page 35](#)
 - [Verifying the Junos OS Application Identification Extracted Application Package on page 46](#)

Disabling and Reenabling Junos OS Application Identification

Supported Platforms [SRX Series](#)

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 reenabling 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.

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Understanding the Junos OS Application Identification Database on page 26](#)

CHAPTER 4

Custom Application Signatures

- [Understanding Junos OS Application Identification Custom Application Signatures on page 49](#)
- [Example: Configuring Junos OS Application Identification Custom Application Signatures on page 52](#)

Understanding Junos OS Application Identification Custom Application Signatures

Supported Platforms [SRX Series, vSRX](#)

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

Custom application signatures are required:

- To control traffic particular to an environment
- To bring visibility for unknown or unclassified applications by developing custom applications.
- To identify applications over Layer 7 and transiting or temporary applications, and to achieve further granularity of known applications
- To perform QoS for your specific application

You can create custom application signatures using CLI by specifying a name, protocol, port where the application runs, and match criteria. For more details, see [“Example: Configuring Junos OS Application Identification Custom Application Signatures” on page 52](#).



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

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



NOTE: The following features are not supported:

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

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

SRX Series devices support the following types of custom signatures:

- [ICMP-Based Mapping on page 50](#)
- [Address-Based Mapping on page 50](#)
- [IP Protocol-Based Mapping on page 51](#)
- [Layer 7-Based Signatures on page 51](#)

ICMP-Based Mapping

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



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



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

Address-Based Mapping

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

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

Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port. When both IP address and port are

configured, both should match destination tuples (IP address and port range) of the packet.

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



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

IP Protocol-Based Mapping

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



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

Layer 7-Based Signatures

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

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

Related Documentation

- [Understanding Application Identification Techniques on page 23](#)
- [Understanding the Junos OS Application Package Installation on page 27](#)
- [Understanding the Junos OS Application Identification Database on page 26](#)

Example: Configuring Junos OS Application Identification Custom Application Signatures

Supported Platforms [SRX Series, vSRX](#)

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



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

- [Requirements on page 52](#)
- [Overview on page 52](#)
- [Configuration on page 52](#)
- [Verification on page 56](#)

Requirements

Before you begin:

- Ensure that the SRX Series device with application signature package installed. See [“Downloading and Installing the Junos OS Application Signature Package Manually” on page 32](#) or [“Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package” on page 35](#).
- The SRX Series device must be running Junos OS Release 15.1X49-D40 or later.

Overview

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

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

Configuration

CLI Quick Configuration

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

HTTP Context-Based Custom Signatures

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

SSL Context-Based Custom Signatures	<pre> set services application-identification application mycustom-ssl over SSL signature s1 member m01 context ssl-server-name set services application-identification application mycustom-ssl over SSL signature s1 member m01 pattern "example\.com" set services application-identification application mycustom-ssl over SSL signature s1 member m01 direction any </pre>
TCP Stream-Based Custom Signatures	<pre> set services application-identification application mycustom-tcp over TCP signature s1 member m01 context stream set services application-identification application mycustom-tcp over TCP signature s1 member m01 pattern "123456789012345678901234567890" set services application-identification application mycustom-tcp over TCP signature s1 member m01 direction client-to-server </pre>
ICMP-Based	<pre> set services application-identification application MY-ICMP icmp-mapping type 100 set services application-identification application MY-ICMP icmp-mapping code 1 </pre>
Layer 3/Layer 4 Address-Based	<pre> set services application-identification application My-ADDRESS address-mapping ADDR-SAMPLE filter ip 192.0.2.1/24 set services application-identification application My-ADDRESS address-mapping ADDR-SAMPLE filter port-range udp 5000-6000 </pre>
IP Protocol-Based	<pre> set services application-identification application MY-IGMP ip-protocol-mapping protocol 2 </pre>
Step-by-Step Procedure	<p>The following examples require you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see <i>CLI User Guide</i>.</p> <p>To configure HTTP context-based custom signatures:</p> <ol style="list-style-type: none"> 1. Configure an application based on HTTP context. Define an application signature to match the pattern, a unique application signature identifier, application signature member identifier, and set the context to be matched. <pre> [edit services application-identification] user@host# set application mycustom-http over HTTP signature s1 member m01 context http-header-host </pre> 2. Configure a pattern to match the context. <pre> [edit services application-identification] user@host# set application mycustom-http over HTTP signature s1 member m01 pattern .*agent1.* </pre> 3. Configure the connection direction of the packets to apply pattern matching. <pre> [edit services application-identification] user@host# set application mycustom-http over HTTP signature s1 member m01 direction any </pre>

- Step-by-Step Procedure** To configure SSL context-based custom signatures:
1. Configure an application based on SSL. Define an application signature to match the pattern, a unique application signature identifier, application signature member identifier, and set the context to be matched.

```
[edit services application-identification]  
user@host# set application mycustom-ssl over SSL signature s1 member m01  
context ssl-server-name
```
 2. Configure a pattern to match the context.

```
[edit services application-identification]  
user@host# set application mycustom-ssl over SSL signature s1 member m01  
pattern "example\.com"
```
 3. Configure the connection direction of the packets to apply pattern matching.

```
[edit services application-identification]  
user@host# set application mycustom-ssl over SSL signature s1 member m01  
direction any
```
- Step-by-Step Procedure** To configure TCP stream-based custom signatures:
1. Configure an application based on TCP. Define an application signature to match the pattern, a unique application signature identifier, application signature member identifier, and set the context to be matched.

```
[edit services application-identification]  
user@host# set application mycustom-tcp over TCP signature s1 member m01  
context stream
```
 2. Configure a pattern to match the context.

```
[edit services application-identification]  
user@host# set application mycustom-tcp over TCP signature s1 member m01  
pattern ""123456789012345678901234567890"
```
 3. Configure the connection direction of the packets to apply pattern matching.

```
[edit services application-identification]  
user@host# set application mycustom-tcp over TCP signature s1 member m01  
direction client-to-server
```
- Step-by-Step Procedure** To configure ICMP-based custom applications signatures:
1. Define the type of ICMP mapping. The type field identifies the ICMP message.

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

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

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

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

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

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

2. Configure the port range for TCP or UDP.

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



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

Step-by-Step Procedure To configure IP protocol mapping-based custom application signatures:

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

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

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

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

download {
  url https://services.netscreen.com/cgi-bin/index.cgi;
}
application MY-ICMP {
  icmp-mapping {
    type 100;
    code 1;
  }
}
application MY-IGMP {
  ip-protocol-mapping {
    protocol 2;
  }
}
```

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

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

Verification

Verifying the Custom Application Definitions

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

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

See [show services application-identification application](#)

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Understanding Junos OS Application Identification Custom Application Signatures on page 49](#)
 - [Understanding the Junos OS Application Package Installation on page 27](#)
 - [Understanding the Junos OS Application Identification Database on page 26](#)

CHAPTER 5

Configuring Application Groups

- [Customizing Application Groups for Junos OS Application Identification on page 59](#)
- [Enabling or Disabling Application Groups in Junos OS Application Identification on page 60](#)
- [Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management on page 60](#)

Customizing Application Groups for Junos OS Application Identification

Supported Platforms [SRX Series, vSRX](#)

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

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

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

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

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

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

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Enabling or Disabling Application Groups in Junos OS Application Identification on page 60](#)
 - [Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management on page 60](#)

Enabling or Disabling Application Groups in Junos OS Application Identification

Supported Platforms [SRX Series, vSRX](#)

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

- For predefined application groups, you can disable and reenabling 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 reenabling a disabled predefined application group:

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

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Customizing Application Groups for Junos OS Application Identification on page 59](#)
 - [Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management on page 60](#)

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

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 61](#)
- [Overview on page 61](#)
- [Configuration on page 61](#)

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 32](#) or [“Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package” on page 35](#).

Overview

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

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



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

Configuration

- [Configuring Junos OS Application Identification User-Defined Application Groups on page 61](#)
- [Deleting an Application from a User-Defined Application Group on page 63](#)
- [Creating Child Application Groups for an Application Group on page 63](#)

Configuring Junos OS Application Identification User-Defined Application Groups

CLI Quick Configuration

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

```
set services application-identification application-group my_web
set services application-identification application-group my_web applications junos:HTTP
```

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

**Step-by-Step
Procedure**

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

To configure a custom application group for application identification:

1. Set the name of your custom application group.

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

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

```
[edit services application-identification]
user@host# set application-group my_web applications junos:HTTP
user@host# set application-group my_web applications junos:FTP
user@host# set application-group my_web applications junos:GOPHER
user@host# set application-group my_web applications junos:AMAZON
```

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

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

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

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

Results

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

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

```

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

```

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

Deleting an Application from a User-Defined Application Group

CLI Quick Configuration

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

```

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

```

Step-by-Step Procedure

To delete an application from a custom application group:

- Delete an application from a custom application group.

```

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

```

Results

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

```

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

```

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

Creating Child Application Groups for an Application Group

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your

network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

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

**Step-by-Step
Procedure**

To configure child application groups for a custom application group:

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

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

2. Add the child application groups.

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

Results

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

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

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

**Related
Documentation**

- [Understanding Application Identification Techniques on page 23](#)
- [Customizing Application Groups for Junos OS Application Identification on page 59](#)
- [Enabling or Disabling Application Groups in Junos OS Application Identification on page 60](#)

CHAPTER 6

Configuring Application System Cache

- [Understanding the Application System Cache on page 65](#)
- [Deactivating Application System Cache Information for Application Identification \(CLI Procedure\) on page 66](#)
- [Verifying Application System Cache Statistics on page 66](#)

Understanding the Application System Cache

Supported Platforms [SRX Series, vSRX](#)

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 one matching entry is required for 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.

To minimize the impact on performance, application system cache is refreshed only when Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) traffic triggers a cache lookup. Without a cache lookup, the entries in the ASC remain unchanged even after cache timeout.



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.

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Understanding the Junos OS Application Identification Database on page 26](#)
 - [Verifying Application System Cache Statistics on page 66](#)

Deactivating Application System Cache Information for Application Identification (CLI Procedure)

Supported Platforms [SRX Series, vSRX](#)

Application caching is turned on by default. You can manually turn this caching off using the CLI.

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

When you use the **show** command in the CLI operation mode for the application system cache (ASC), application cache is listed as **off**. Note that if the cache contains data from the prior implementation, the cached data is also displayed.

```
user@host> show services application-identification application-system-cache
```

```
application-cache: off
nested-application-cache: on
cache-unknown-result: on
cache-entry-timeout: 3600 seconds
```

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Verifying Application System Cache Statistics on page 66](#)
 - [Understanding the Junos OS Application Identification Database on page 26](#)

Verifying Application System Cache Statistics

Supported Platforms [SRX Series, vSRX](#)

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.

- Related Documentation**
- [Understanding Application Identification Techniques on page 23](#)
 - [Deactivating Application System Cache Information for Application Identification \(CLI Procedure\) on page 66](#)

CHAPTER 7

Controlling Application Identification Performance

- [Onbox Application Identification Statistics on page 69](#)
- [Understanding Jumbo Frames Support for Junos OS Application Identification Services on page 70](#)
- [Improving the Application Traffic Throughput on page 70](#)

Onbox Application Identification Statistics

Supported Platforms [SRX Series, vSRX](#)

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. SRX Series 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.

**Related
Documentation**

- [Understanding Application Identification Techniques on page 23](#)

Understanding Jumbo Frames Support for Junos OS Application Identification Services

Supported Platforms [SRX Series, vSRX](#)

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.

**Related
Documentation**

- [Understanding Application Identification Techniques on page 23](#)
- [Understanding the Junos OS Application Identification Database on page 26](#)
- [Example: Setting Memory Limits for IDP Application Identification Services](#)

Improving the Application Traffic Throughput

Supported Platforms [SRX Series, vSRX](#)

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 SRX Series devices.

To improve the application traffic throughput:

1. Enable the DPI performance mode.

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

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

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

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

3. Commit the configuration.

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

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

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

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

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

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

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

Related Documentation

- [enable-performance-mode on page 199](#)

CHAPTER 8

Configuring SSL Proxy

- [SSL Proxy Overview on page 73](#)
- [Configuring SSL Proxy on page 83](#)
- [Configuring SSL Forward Proxy Certificate Chain on page 95](#)
- [Application Firewall, IDP, and Application Tracking with SSL Proxy Overview on page 102](#)
- [Working with the Certificate Revocation Lists for SSL Proxy on page 103](#)
- [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

SSL Proxy Overview

Supported Platforms [SRX Series, vSRX](#)

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 is supported on the SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and the SRX5800 devices.

Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a webserver. Confidentiality mechanisms ensure that communications are private. SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

SSL proxy is transparent; that is, it performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. Existing features like SSL offload and SSL inspection require the servers to share their secret keys to be able to decrypt the SSL traffic. However, sharing server keys is sometimes not feasible or might not be available in certain circumstances, in which case the SSL traffic cannot be decrypted.

SSL proxy addresses this problem by ensuring that it has the keys to encrypt and decrypt the payload:

- For the server, SSL proxy acts as a client—Because SSL proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.

- For the client, SSL proxy acts as a server—SSL proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then 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). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

Figure 2 on page 74 depicts how SSL inspection (on an existing SRX Series IDP module) is typically used to protect servers. SSL inspection requires access to the private keys used by the servers so that the SRX Series device can decrypt the encrypted traffic.

Figure 2: SSL Inspection on an Existing SRX Series IDP Module

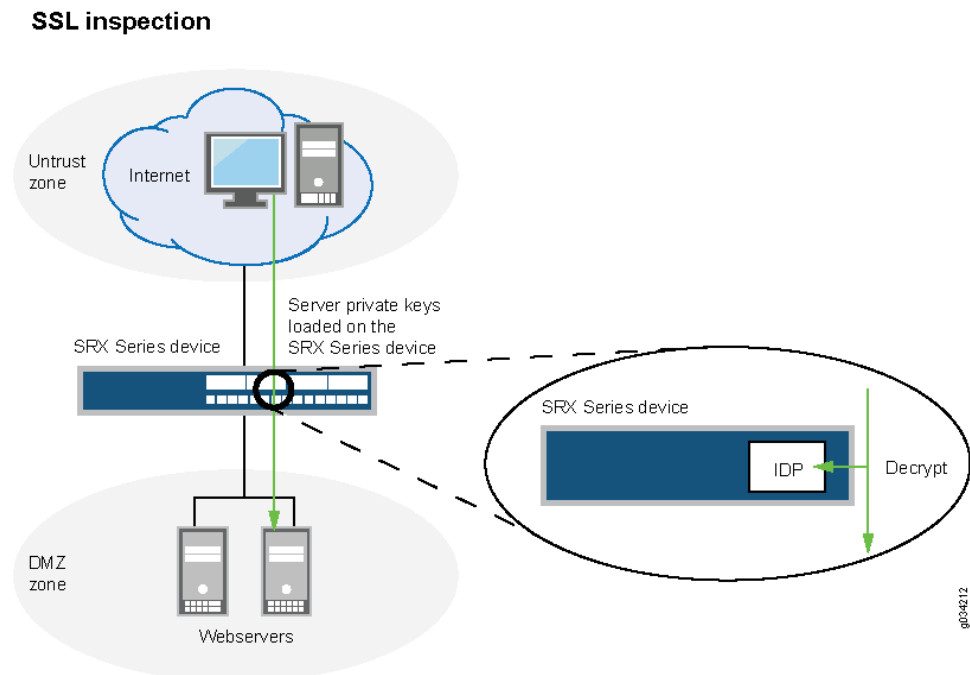


Figure 3 on page 75 shows how SSL proxy works on an encrypted payload. When application firewall (AppFW), Intrusion Detection and Prevention (IDP), or application tracking (AppTrack) is configured, the SSL proxy acts as an SSL server by terminating the SSL session from the client and establishing a new SSL session to the server, the SRX Series device decrypts and then reencrypts all SSL proxy traffic. SSL proxy uses the following:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.
- Configured AppFW, IDP, or AppTrack services use the decrypted SSL sessions.



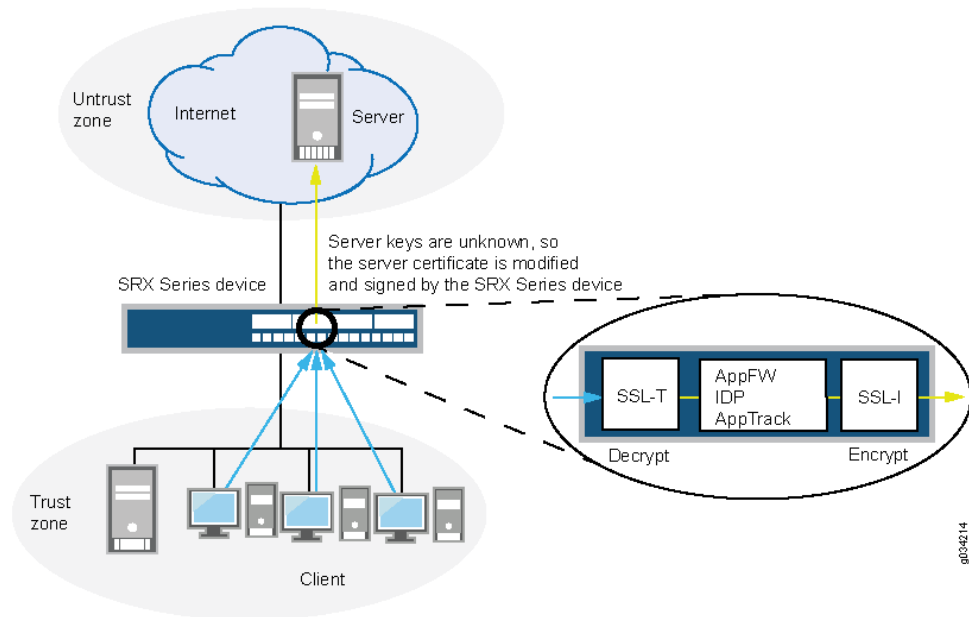
NOTE: If none of the services (AppFW, IDP, or AppTrack) are configured, then SSL proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy.



NOTE: The IDP module will not perform its SSL inspection on a session if 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.

Figure 3: SSL Proxy on an Encrypted Payload

SSL forward proxy



Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) is a feature of specific key agreement protocols that provides assurances your session keys will not be compromised even if the private key of the server is compromised. By generating a unique session key for every session flow a user initiates, the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key. For PFS to function, the key used to protect transmission of data must not be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material must not be used to derive any further keys.

The ECDHE (Elliptic Curve DHE) cipher suits are used to enable the PFS on SSL proxy. ECDHE cipher suits are based on elliptic curve cryptography, which provides the same level of security as the RSA with smaller keys. SSL proxy is targeted to support only ECDHE ciphers suites as they are less expensive computationally than DHE ciphers.

Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. [Table 3 on page 76](#) displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported on SRX Series devices:

- TLS version 1.0—Provides secure communication over networks by providing privacy and data integrity 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.

Table 3: Supported SSL Cipher List

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE/RSA key exchange	256-bit AES/GCM	SHA384 hash
ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE/RSA key exchange	256-bit AES/CBC	SHA384 hash
ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE/RSA key exchange	256-bit AES/CBC	SHA hash
ECDHE_RSA_WITH_DES_CBC3_SHA	ECDHE/RSA key exchange	DES CBC	SHA hash
ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE/RSA key exchange	128-bit AES/GCM	SHA256 hash
ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE/RSA key exchange	128-bit AES/CBC	SHA256 hash
ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE/RSA key exchange	128-bit AES/CBC	SHA hash
RSA_WITH_AES_256_GCM_SHA384	ECDHE/RSA key exchange	256-bit AES/GCM	SHA384 hash
RSA_WITH_AES_256_CBC_SHA256	ECDHE/RSA key exchange	256-bit AES/CBC	SHA256 hash
RSA_WITH_AES_128_GCM_SHA256	ECDHE/RSA key exchange	128-bit AES/GCM	SHA256 hash
RSA_WITH_AES_128_CBC_SHA256	ECDHE/RSA key exchange	128-bit AES/CBC	SHA256 hash
RSA_WITH_RC4_128_MD5	RSA key exchange	128-bit RC4	Message Digest 5 (MD5) hash

Table 3: Supported SSL Cipher List (*continued*)

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_SHA	RSA key exchange	128-bit RC4	Secure Hash Algorithm (SHA) hash
RSA_WITH_DES_CBC_SHA	RSA key exchange	DES CBC	SHA hash
RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange	3DES EDE/CBC	SHA hash
RSA_WITH_AES_128_CBC_SHA	RSA key exchange	128-bit AES/CBC	SHA hash
RSA_WITH_AES_256_CBC_SHA	RSA key exchange	256-bit AES/CBC	SHA hash
RSA_EXPORT_WITH_RC4_40_MD5	RSA-export	40-bit RC4	MD5 hash
RSA_EXPORT_WITH_DES40_CBC_SHA	RSA-export	40-bit DES/CBC	SHA hash
RSA_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



NOTE: 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.



NOTE: Supported SSL ciphers for HTTPS firewall authentication are RSA_WITH_3DES_EDE_CBC_SHA, RSA_WITH_AES_128_CBC_SHA, and RSA_WITH_AES_256_CBC_SHA.

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.

- By default, the **ignore-server-auth-failure** option is not defined as an action in the SSL proxy profile, and the following occurs:

- 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.
- If the **ignore-server-auth-failure** option is defined as an action in the SSL proxy profile, the following occurs:
 - If the certificate is self-signed, a new certificate is generated by replacing the keys only. 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 SRVR AUTH FAILURE`. This ensures that the client browser displays a warning that the certificate is not valid.

Trusted CA List

SSL proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL proxy checks CA certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

Junos OS provides the following options for trusted CA certificates:

- Loading the default trusted CA list—Junos OS provides a default list of certificates that contains well-known trusted CA certificates similar to the default certificates used by most common browsers. Without these default certificates, browsers would not be able to validate the identity of most websites and would mark them as untrusted sites.

The Junos OS package contains the default CA certificates as a PEM file (for example, `trusted_CA.pem`). After you download the package and reboot your device, you can easily load the default certificates on your system using a CLI command.

We recommend you load the default trusted CA list if you want to trust the same CA certificates as common browsers and avoid importing CA certificates manually.

- Importing the trusted CA list manually—You can 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.
- Ignoring server authentication—You can use the **ignore-server-auth-failure** option to ignore server authentication completely. In this case, SSL proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

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 105](#).

Root CA

In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.

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.

Whitelists

Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions. Such sessions mostly include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under whitelists.

Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, the whitelisting feature is extended to include URL categories supported by UTM in the whitelist configuration of SSL forward proxy. In this implementation, the Server Name Indication (SNI) field is extracted by the UTM module from client hello messages to determine the URL category. Each URL category has a unique ID. The list of URL categories under whitelist is parsed and the corresponding category IDs are pushed to the Packet Forwarding Engine for each SSL forward proxy profile. The SSL forward proxy then determines through APIs whether to accept, and proxy, or to ignore the session.

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).

Session Resumption

An SSL session refers to the set of parameters and encryption keys created by performing a full handshake. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of master keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer.

To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached 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.

Session Renegotiation

After a session is created and SSL tunnel transport has been 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.

A change in an SSL proxy profile that modifies a certificate, cipher strength, or trusted CA list flushes cache entries when the modified policy is committed. When a session is resumed, the SSL parameters associated with its session ID are retrieved from the cache. If the SSL proxy profile is not altered, cache entries corresponding to that profile are not flushed and the session continues. If the cache has been flushed, however, a full handshake must be performed to establish the new SSL parameters. (There is no impact to non-SSL sessions.)

SSL Proxy Logs

When logging is enabled in an SSL proxy profile, SSL proxy can generate the messages shown in [Table 4 on page 80](#).

Table 4: SSL Proxy Logs

Syslog Type	Description
SSL_PROXY_SSL_SESSION_DROP	Logs generated when a session is dropped by SSL proxy.
SSL_PROXY_SSL_SESSION_ALLOW	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
SSL_PROXY_SESSION_IGNORE	Logs generated if non-SSL sessions are initially mistaken as SSL sessions.
SSL_PROXY_SESSION_WHITELIST	Logs generated when a session is whitelisted.
SSL_PROXY_ERROR	Logs used for reporting errors.
SSL_PROXY_WARNING	Logs used for reporting warnings.
SSL_PROXY_INFO	Logs used for reporting general information.

All logs contain similar information as shown in the following example (actual order of appearance):

```
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 5 on page 81](#) identifies the source of the message. Other fields are descriptively labeled.

Table 5: SSL Proxy Log Prefixes

Prefix	Description
system	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.
openssl error	Logs generated during the handshaking process if an error is detected by the openssl library.
certificate error	Logs generated during the handshaking process if an error is detected in the certificate (x509 related errors).

Sample logs:

```
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.

```
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:<
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:system: session whitelisted
```

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.

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



NOTE:

- Starting from Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, certificate revocation list (CRL) checks are supported.
- Starting from Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, server certificates that have key size greater than 4096 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.



NOTE: 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, and application tracking. If none of the above listed features are active on a session, the SSL proxy bypasses the session and logs are not generated in this scenario.



NOTE: 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.

Release History Table

Release	Description
15.1X49-D80	Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, the whitelisting feature is extended to include URL categories supported by UTM in the whitelist configuration of SSL forward proxy. In this implementation, the Server Name Indication (SNI) field is extracted by the UTM module from client hello messages to determine the URL category. Each URL category has a unique ID. The list of URL categories under whitelist is parsed and the corresponding category IDs are pushed to the Packet Forwarding Engine for each SSL forward proxy profile. The SSL forward proxy then determines through APIs whether to accept, and proxy, or to ignore the session.
15.1X49-D30	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.
15.1X49-D30	Starting from Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, certificate revocation list (CRL) checks are supported.
15.1X49-D30	Starting from Junos OS Release 15.1X49-D30 and Junos OS Release 17.3R1, server certificates that have key size greater than 4096 are supported.
15.1X49-D20	Starting with Junos OS Release 15.1X49-D20 and Junos OS Release 17.3R1, the SSL protocol 3.0 (SSLv3) support is deprecated.

Related Documentation

- [Understanding Address Books](#)
- [Understanding Global Address Books](#)
- [Understanding Self-Signed Certificates](#)
- [Configuring SSL Proxy on page 83](#)

Configuring SSL Proxy

Supported Platforms [SRX Series, vSRX](#)

SSL proxy works transparently between the client and the server. All requests from a client first go to the proxy server; the proxy server evaluates the request, and if the request is valid, forwards the request to the outbound side. Similarly, inbound requests are also evaluated by the proxy server. Both client and server interpret that they are communicating with each other; however, it is the SSL proxy that functions between the two. SSL proxy is supported on SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 devices and vSRX instances. For release-specific support, see [Feature Explorer](#)

SSL proxies provide encryption and decryption by residing between the server and the client. Because SSL proxies are hidden from both the server and the client, secret keys are shared between the two to decrypt the SSL traffic. Proxies are known as *forward proxies* because proxy servers are used to hide any detailed information from the servers.

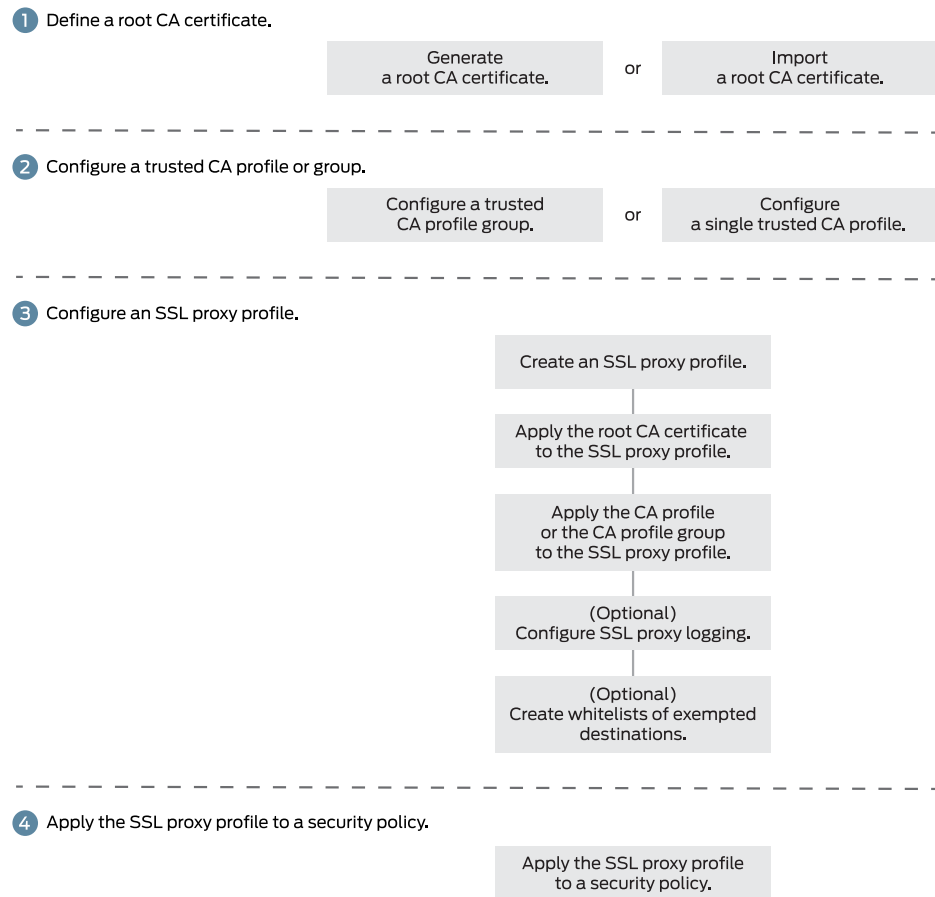
Integrity, confidentiality, and authenticity of traffic are validated through PKI, which includes digital certificates issued by the CA, certificate validity and expiration dates, details about the certificate owner and issuer, and security policies.

- [SSL Proxy Configuration Overview on page 84](#)
- [Configuring a Root CA Certificate on page 85](#)
- [Configuring a CA Profile Group on page 87](#)
- [Configuring a Trusted CA Profile on page 88](#)
- [Importing a Root CA Certificate into a Browser on page 89](#)
- [Applying an SSL Proxy Profile to a Security Policy on page 90](#)
- [Creating a Whitelist of Exempted Destinations on page 91](#)
- [Configuring SSL Proxy Logging on page 93](#)
- [Configuring Ciphers on page 94](#)
- [Exporting Certificates to a Specified Location on page 94](#)
- [Ignoring Server Authentication on page 94](#)

SSL Proxy Configuration Overview

[Figure 4 on page 85](#) displays an overview of how SSL proxy is configured. It includes some required steps, such as configuring the root CA certificate, loading a CA profile group, and applying an SSL proxy profile to a security policy, and some optional steps, such as creating whitelists and SSL proxy logging.

Figure 4: SSL Proxy Configuration Overview



8042395

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.

To generate a root CA certificate using the Junos OS CLI, follow these steps on an SRX Series device:

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
```

2. From operational mode, define a self-signed certificate. Specify certificate details such as the certificate identifier (generated in the previous step), a fully qualified domain name (FQDN) for the certificate, and an e-mail address of the entity owning the certificate. You can also specify other information such as the common name and the organization involved. By configuring the **add-ca-constraint** option, you make sure that the certificate can be used for signing other certificates.

```
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
```

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
```

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 89](#).

To generate a root CA certificate using OpenSSL, follow these steps on a UNIX device:

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. The following command 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.

```
% openssl genrsa -des3 -out keys/ssl-proxy-ca.key 2048
```

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.

```
% openssl req -new -x509 -days 1095 -key keys/ssl-proxy-ca.key -out
certs/ssl-inspect-ca.cer
```

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-inspect-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 89](#).

Configuring a CA Profile Group

The CA profile defines the certificate information to be used 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 following one of these methods:
 - Junos OS provides a default list of trusted CA certificates that you can load on your system using the **default** command option. 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 and reboot your device, 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
```

- 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):

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name
group-name filename /var/tmp/IE-all.pem
```

2. From configuration mode, attach the CA profile group to the SSL proxy profile. You can attach one or all CA profile groups at a time:

- To attach one CA profile group (the group name identifies the CA profile group):

```
[edit]
user@host# set services ssl proxy profile profile-name trusted-ca group-name
```

- To attach all CA profile groups:

```
[edit]
user@host# set services ssl proxy profile profile-name trusted-ca all
```

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
```

Configuring a Trusted CA Profile

Typically, you import a list of trusted CA certificates by creating a group of CA profiles. However, you can also configure a single CA profile (containing one or multiple certificates) and import it using PKI commands. This section shows you how to import a trusted CA certificate from your browser's certificate store into your SRX Series device. The certificate that is configured under the trusted CA is loaded using the PKI commands and is used for validating the server certificate chain.

1. From configuration mode, configure the CA profile used for loading the certificate.

```
[edit]
user@host# set security pki ca-profile profile-name ca-identity ca-identity
```

2. From operational mode, load the certificate using PKI commands.

```
user@host> request security pki ca-certificate load ca-profile profile-name filename
filename
```

3. From configuration mode, disable the revocation check.



NOTE: CRL checks are not supported; we recommend that you disable revocation checks.

```
[edit]
user@host# set security pki ca-profile profile-name ca-identity ca-identity
revocation-check disable
```

4. 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
```



NOTE: More than one trusted CA can be configured for a profile.

5. (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 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](#).

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, choose **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, choose **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, choose **Show Advanced Settings**.

b. From the Advanced menu, select the **Certificates** tab and click **View Certificate**.

c. Under HTTPS/SSL, click **Manage Certificates**.

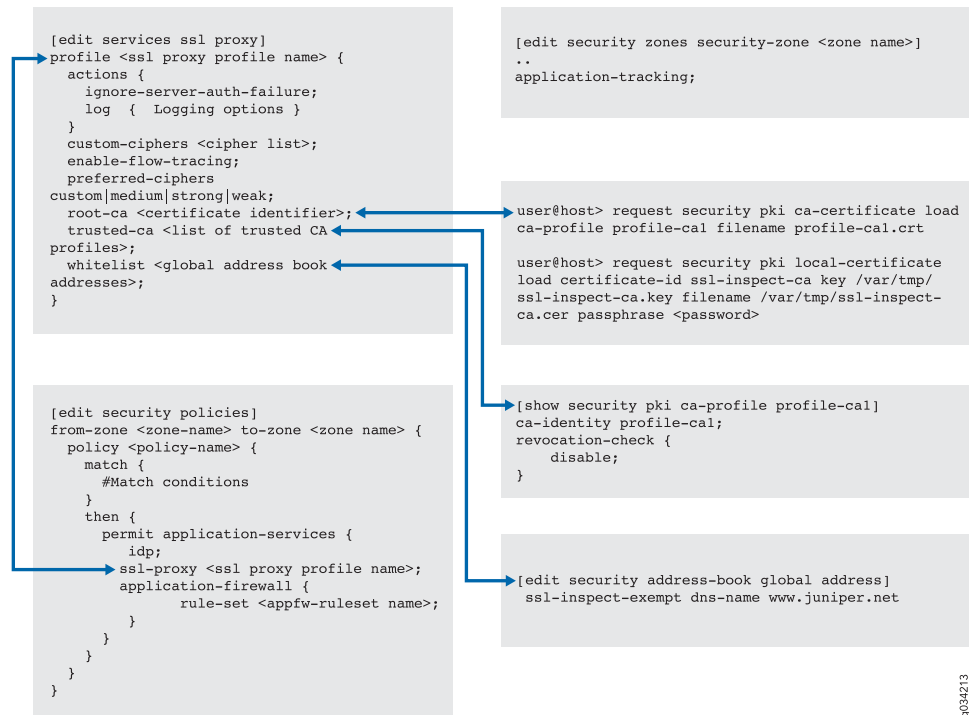
d. In the Certificate window, select **Trusted Root Certification Authorities** and click **Import**.

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 5 on page 91](#) displays a graphical view of SSL proxy profile and security policy configuration.

Figure 5: Applying an SSL Proxy Profile to a Security Policy



9034213

To enable SSL proxy in a security policy:

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.

```

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

```

2. Apply the SSL proxy profile to the security policy.

```

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

```

Creating a Whitelist of Exempted Destinations

SSL encryption and decryption are complicated and expensive procedures. You can selectively bypass SSL proxy processing for some sessions by configuring a whitelist. Typically, you would configure the whitelist to include trusted servers or domains with which you are very familiar. You might also include financial and banking sites that you are legally required to include.

Whitelists include addresses that you want to exempt from undergoing SSL proxy processing. For example, if you want to exempt all sessions to **www.mycompany.com**, then you would include it in the whitelist. To configure the whitelist, you specify the domain that you want to exempt in an 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 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-name whitelist address
```

Whitelist addresses and address sets are created under the global address book. The following type of addresses (from the global address book) are supported:

- IPv4 addresses (plain text). For example:

```
[edit]
user@host# set security address-book global address address-name ipv4-prefix
```

- IPv4 address range. For example:

```
[edit]
user@host# set security address-book global address address-name range-address
range-low to range-high
```

- IPv4 wildcard. For example:

```
[edit]
user@host# set security address-book global address address-name wildcard-address
addr/netmask
```

Noncontiguous netmasks are not supported. For example:

- 203.0.113.9/255.255.0.0 is supported.
- 203.0.113.9/255.255.0.255 is NOT supported.

- IPv6 address (plain text). For example:

```
[edit]
user@host# set security address-book global address address-name ipv6-prefix
```

- DNS name. For example:

```
[edit]
user@host# set security address-book global address address-name dns-name
domain-name
```

- 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 addresses.

For example, consider a destination NAT rule that translates destination IP address 192.0.2.10/24 to 198.51.100.8/24 using the following commands:

```
[edit]
user@host# set security nat destination pool d1 address 198.51.100.8/24
user@host# set security nat destination rule-set dst-nat rule r1 match
destination-address 192.0.2.10/24
user@host# set security nat destination rule-set dst-nat rule r1 then destination-nat
pool d1
```

In this scenario, to exempt a session from SSL proxy inspection, the following IP address should be added to the whitelist:

```
[edit]
user@host# set security address-book global address ssl-proxy-exempted-addr
192.0.2.10/24
user@host# set services ssl proxy profile ssl-inspect-profile whitelist
ssl-proxy-exempted-addr
```

Whitelist URL categories. the whitelisting feature is extended to include URL categories supported by UTM in the whitelist configuration of SSL forward proxy. In this implementation, the Server Name Indication (SNI) field is extracted by the UTM module from client hello messages to determine the URL category. Each URL category has a unique ID. The list of URL categories under whitelist is parsed and the corresponding category IDs are pushed to the Packet Forwarding Engine for each SSL forward proxy profile. The SSL forward proxy then determines through APIs whether to accept, and proxy, or to ignore the session.

In this example, Enhanced_Financial_Data_and_Services is one of the supported url categories:

```
[edit]
user@host# set services ssl proxy profilesslfp_url_whitelist
whitelist-url-categoriesEnhanced_Financial_Data_and_Services
```



NOTE: The predefined url categories depends on UTM. To enable url based whitelisting in SSL proxy, the following basic url configurations are required:

```
[edit]
user@host# set security utm feature-profile web-filtering type
juniper-enhanced
user@host# set security utm utm-policy utmpolicy web-filtering http-profile
junos-wf-enhanced-default
```

Configuring 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.

[edit]

```
user@host# set services ssl proxy profile profile-name actions log all
user@host# set services ssl proxy profile profile-name actions log sessions-whitelisted
user@host# set services ssl proxy profile profile-name actions log sessions-allowed
user@host# set services ssl proxy profile profile-name actions log errors
```

You can use **enable-flow-tracing** option to enable debug tracing.

Configuring Ciphers

You can configure the following ciphers for an SSL proxy profile:

- **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**—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.

The following example shows how to create a custom cipher. In this example, you set **preferred-cipher** to custom and add the cipher list (rsa-with-3des-ede-cbc-sha and rsa-with-aes-256-cbc-sha):

```
set services ssl proxy profile profile-name preferred-ciphers custom
set services ssl proxy profile profile-name custom-ciphers rsa-with-3des-ede-cbc-sha
set services ssl proxy profile profile-name custom-ciphers rsa-with-aes-256-cbc-sha
```

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
user@host> request security pki local-certificate export filename filename
user@host> request security pki local-certificate export 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
```

**Related
Documentation**

- [SSL Proxy Overview on page 73](#)
- [Enabling Debugging and Tracing for SSL Proxy on page 105](#)
- [Understanding Self-Signed Certificates](#)
- [show services ssl proxy statistics on page 370](#)
- [clear services ssl proxy statistics on page 284](#)

Configuring SSL Forward Proxy Certificate Chain

Supported Platforms [SRX Series](#)

- [Understanding SSL Certificate Chain on page 95](#)
- [Configuring the SSL Certificate Chain on page 98](#)

Understanding SSL Certificate Chain

This topic includes the following sections:

- [SSL Proxy Overview on page 95](#)
- [SSL Certificate Chain Overview on page 96](#)
- [Advantage of Certificate Chains on page 97](#)
- [Understanding Certificate Chain Processing on page 97](#)

SSL Proxy Overview

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.

An SSL certificate (digital certificate) is provided by trusted companies to authenticate the identity of website owners and ensure secure communication between those websites and their customers by ensuring legitimacy of the identification information. However, many certificate authorities (CAs) use a complex certificate chain that includes a number of intermediate certificates.

In order to validate (and trust) an SSL certificate, the CA that issued the certificate must be included in the trusted CA list of the device that is connecting.

For example, when a connection is initiated, the connecting device (such as a Web browser) checks whether the certificate is issued by a trusted CA. If not, the device checks whether the certificate of the issuing CA was issued by a trusted CA. This check continues until either a trusted CA is found (at which point a trusted, secure connection will be established), or no trusted CA can be found (at which point the device will usually display an error).

If the intermediate certificates are not included in the trusted CA list, then the Web browser of the clients might display a warning message stating that the certificate presented by the device they are accessing is not trusted.

You can resolve this issue by using an SSL certificate chain. The list of SSL certificates, from the root certificate to the end-user certificate, represents the SSL certificate chain.

SSL Certificate Chain Overview

Starting in Junos OS Release 15.1X49-D30, SSL forward proxy supports the certificate chain and sends it to facilitate the certification chain validation by the client (that is, the connecting device).

The certificate chain is a file that contains an ordered list of certificates, including an SSL certificate and a chain of intermediate CA certificates, in Privacy-Enhanced Mail (PEM) format. This enables the receiver to verify that the sender and all CAs are trustworthy.

A root CA certificate is a certificate issued by a trusted certificate authority. A certificate authority issues certificates in the form of a tree structure. A root certificate is the topmost certificate of the tree. All certificates below the root certificate inherit the trustworthiness of the root certificate; these certificates are called intermediate certificates.

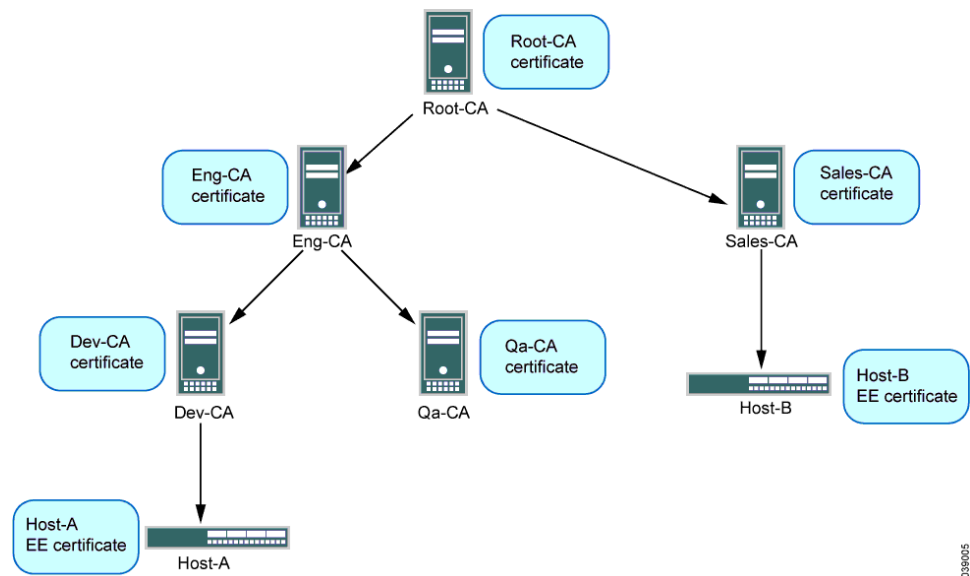
Any certificate placed between the root CA certificate and the SSL certificate (used by end-users) is considered an intermediate certificate. These must be installed to the webserver with the end-user certificate for your website to link your certificate to a trusted authority.

Any certificate signed by a trusted root CA certificate is also trusted. The root CA certificate is always signed by the CA itself. The root CA certificate is the signer/issuer of the intermediate certificate. In turn, the signed intermediate certificate can sign another intermediate certificate and it will also be trusted. The chain terminates at the end-user certificate.

SSL forward proxy sends the entire certificate chain, excluding or including the root CA certificate, to facilitate certificate validation at the client side.

[Figure 6 on page 97](#) illustrates certificate chaining.

Figure 6: Certificate Chaining



Root-CA is the common trusted CA for all devices in the network. Root-CA issues CA certificates to the engineering and sales CAs, which are identified as Eng-CA and Sales-CA, respectively. Eng-CA issues CA certificates to the development and quality assurance CAs, which are identified as Dev-CA and Qa-CA, respectively. Host-A receives its certificate from Dev-CA while Host-B receives its certificate from Sales-CA.

The end-user device needs to be loaded with the entire certificate chain. In this example, Host-A must have Root-CA, Eng-CA, and Dev-CA certificates; and Host-B must have Root-CA and Sales-CA certificates.

Advantage of Certificate Chains

SSL certificate chains eliminate the need to deploy all intermediate certificates separately on all clients.

Understanding Certificate Chain Processing

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.
- 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.

Configuring the SSL Certificate Chain

This example shows how to install the certificate chain to enable browsers to trust your certificate. It shows how to install the root CA certificate and enable the certificate chain in order to ensure secure communications over the Web when using the service.

- [Requirements on page 98](#)
- [Overview on page 98](#)
- [Configuration on page 99](#)

Requirements

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

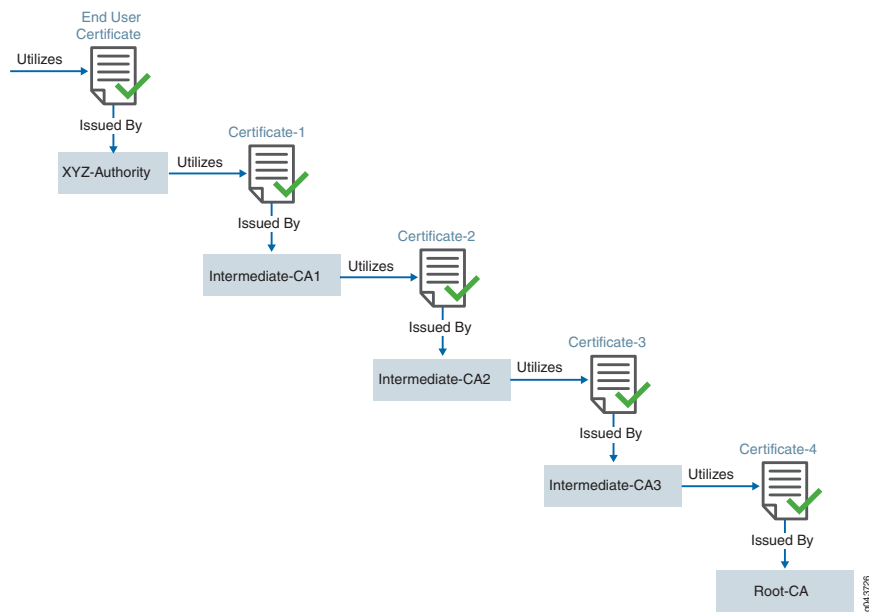
Overview

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.

In order to trust a server's certificate, the client must be configured to trust the CA that signed the server certificate. However, clients are configured to trust only the root CA certificate. Therefore the server must present the chain of intermediate CA certificates to ensure that the trust is properly established when clients connect to a server.

[Figure 7 on page 98](#) depicts a full certificate chain, from the root CA certificate to the end-user certificate. The chain terminates at the end-user certificate.

Figure 7: Certification Path from the Certificate Owner to the Root CA



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):

- End User Certificate is issued to example.domain-1; issued by XYZ-Authority.
- XYZ-Authority utilizes a certificate (Certificate-1) issued by Intermediate CA-1.
- Intermediate CA-1 utilizes a certificate (Certificate-2) issued by Intermediate CA-2.
- Intermediate CA-2 utilizes a certificate (Certificate-3) issued by Intermediate CA-3.
- Intermediate CA-3 utilizes a certificate (Certificate-4) issued by root-example-authority. The root-example-authority is a root CA.

Its certificate is directly embedded in your Web browser; therefore it can be explicitly trusted. 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.

Certificate-1 is your end-user certificate, the one you purchase from the CA. The certificates from 2 to 3 are called *intermediate certificates*. Certificate-4, at the end, is called the *root CA certificate*.

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. 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.
- All certificates must be added into one file; ensure that they are placed in the order in which they will appear.
- 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

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 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.
- 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.

To configure the SSL certificate chain, you must:

1. Load the signing certificate and the key on your device.
2. Create a trusted CA profile for the intermediate or root CA certificate.
3. Attach the signing certificate profile as created in Step 1 to the SSL proxy profile.
4. Attach the trusted CA profiles created in Step 2 to the SSL proxy profile.

This example assumes that you have already purchased an SSL certificate from a CA.

- [Loading the Signing Certificate on page 100](#)
- [Configuring Trusted CA Profiles for Intermediate or Root CA Certificates on page 100](#)
- [Configuring the SSL Proxy Profile on page 101](#)
- [Verifying the Certificate Chain on the Device on page 102](#)

Loading the Signing Certificate

Step-by-Step Procedure

To load the local certificate into the PKI memory:

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 ssl_proxy_ca.crt  
key sslserver.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.

Configuring Trusted CA Profiles for Intermediate or Root CA Certificates

Step-by-Step Procedure

The CA profile defines the certificate information to be used 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.

- Load the intermediate or root CA certificate in the PKI memory.

```
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.

```
Do you want to load this CA certificate? [yes,no] (no) yes
```

```
Loading 1 certificates for group 'ca-latest'.
ca-latest_1: Loading done.
ca-profile-group 'ca-latest' successfully loaded
Success[1] Skipped[0]
```

This certificate will be attached as a certificate chain.

Configuring the SSL Proxy Profile

Step-by-Step Procedure

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.

1. Attach the CA profile group to the SSL proxy profile. You can attach CA profiles one at a time or load of group of profiles in one action.

```
user@host# set services ssl proxy profile ssl-profile trusted-ca all
```

2. 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
```

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 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
```

4. Apply the SSL proxy profile to the security policy.

```
user@host# set security policies from-zone trust to-zone untrust policy 1 then permit
application-services ssl-proxy profile-name ssl-proxy
```

5. 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 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
```

6. Apply the SSL proxy profile to the security policy.

```
user@host# set security policies from-zone untrust to-zone trust policy 1 then permit
application-services ssl-proxy profile-name ssl-proxy
```

Verifying the Certificate Chain on the Device

Purpose Viewing the certificate chain on the SRX Series device.

Action You can view the certificate chain on the connecting Web browser (that is, the client).

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

Supported Platforms SRX1500, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX550M, SRX5600, SRX5800, vSRX

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), and application tracking (AppTrack) services can use the decrypted content from SSL proxy. 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.

Related Documentation

- [SSL Proxy Overview on page 73](#)
- [Configuring SSL Proxy on page 83](#)
- [Example: Configuring Application Firewall When SSL Proxy Is Enabled on page 120](#)

Working with the Certificate Revocation Lists for SSL Proxy

Supported Platforms SRX1500, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX550M, SRX5600, SRX5800, vSRX

A certificate issued by a certificate authority (CA) is supposed to be valid until the expiration of the validity period. In the normal course of business, a CA can revoke an issued certificate. A certificate is revoked if it is suspected that the certificate has been compromised. Some of the examples are:

- Unspecified (no particular reason is given).
- Private key associated with the certificate was compromised.
- Private key associated with the CA that issued the certificate was compromised.
- The owner of the certificate is no longer affiliated with the issuer of the certificate and does not have rights to access the certificate or does not require it any longer.
- 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.

Once the CA determines to revoke a certificate, it publishes the information by some means so that the enduser certificate can use the information to validate a certificate. The CA can publish this information using certificate revocation list (CRL).

The 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 proxy profile.

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.

- [Disabling CRL Verification on page 103](#)
- [Allowing Sessions When CRL Information Is Not Available on page 104](#)
- [Allowing Sessions When CRL Status Is Unknown on page 104](#)

Disabling CRL Verification

In order to enhance security, the certificate revocation checking feature has been enabled by default on SRX Series devices on any SSL proxy profile. You can enable or disable the CRL validation to meet your specific security requirements.

- To disable CRL verification:

[edit]

```
user@host# set services ssl proxy profile profile-name actions crl disable
```

You can reenable CRL validation by using the **delete services ssl proxy profile *profile-name* actions *crl* disable** command.

Allowing Sessions When CRL Information Is Not Available

Sometimes CRL information might not be available because of various reasons. For example:

- CRL download failed and the PKI daemon did not or could not fetch the CRL from the CA.
- The CRL path was not available from the configuration and it is not present in the root or intermediate certificate, or no URL was configured.

You can allow or drop the sessions when a CRL information is not available.

- To ensure that the sessions are not dropped for any reason when CRL information is not available:

```
[edit]
user@host# edit set services ssl proxy profile profile-name actions crl if-not-present
allow
```

- To drop the sessions when CRL information is not available:

```
[edit]
user@host# edit set services ssl proxy profile profile-name actions crl if-not-present
drop
```

Allowing Sessions When CRL Status Is Unknown

You can configure how an SRX Series device will respond when updated CRL information is not available, and the server certificate that is currently offered is not known to be revoked from a previous query. Certificates are presumed not to be revoked, by default, which means they are valid, and a temporary failure to obtain a CRL does not automatically result in an SSL handshake failure. By default, sessions are allowed if CRL status is unknown.

You can configure an SRX Series device to accept a certificate without a reliable confirmation available on the revocation status.

- To allow the sessions when a certificate is revoked and the revocation reason is on hold:

```
[edit]
user@host# edit set services ssl proxy profile profile-name actions crl
ignore-hold-instruction-code
```

Related Documentation

- [SSL Proxy Overview on page 73](#)
- [Configuring SSL Proxy on page 83](#)

Enabling Debugging and Tracing for SSL Proxy

Supported Platforms [SRX Series, vSRX](#)

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
```

SSL proxy is supported on SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 devices and vSRX instances. [Table 6 on page 105](#) shows the supported levels for trace options.

Table 6: Trace Levels

Cause Type	Description
Brief	Only error traces on both the Routing Engine and the Packet Forwarding Engine.
Detail	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
Extensive	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.
Verbose	All traces are available.

[Table 7 on page 105](#) shows the flags that are supported.

Table 7: Supported Flags in Trace

Cause Type	Description
cli-configuration	Configuration-related traces only.
initiation	Enable tracing on the SSL-I plug-in.
proxy	Enable tracing on the SSL-Proxy-Policy plug-in.
termination	Enable tracing on the SSL-T plug-in.
selected-profile	Enable tracing only for profiles that have enable-flow-tracing set.

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.

**Related
Documentation**

- [SSL Proxy Overview on page 73](#)
- [Configuring SSL Proxy on page 83](#)

CHAPTER 9

Configuring Application Firewall

- [Application Firewall Overview on page 107](#)
- [Example: Configuring Application Firewall Rule Sets Within a Security Policy on page 112](#)
- [Example: Configuring an Application Group for Application Firewall on page 116](#)
- [Example: Configuring Application Firewall When SSL Proxy Is Enabled on page 120](#)

Application Firewall Overview

Supported Platforms [SRX Series, vSRX](#)

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

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

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

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

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

This topic includes the following sections:

- [Understanding Application Firewall Rule Sets on page 108](#)
- [Configuring an Application Firewall Within a Security Policy on page 109](#)
- [Application Group Support for Application Firewall on page 109](#)
- [Redirecting Users on page 110](#)
- [Session Logging for Application Firewalls on page 111](#)
- [Application Firewall Support in Chassis Cluster on page 111](#)

Understanding Application Firewall Rule Sets

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

An application firewall rule set consists of:

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

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

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

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

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

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

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

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

Configuring an Application Firewall Within a Security Policy

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

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

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

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

Traffic is processed in the following sequence:

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



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

Application Group Support for Application Firewall

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



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

For information on creating or listing application groups, see [“Customizing Application Groups for Junos OS Application Identification” on page 59](#).



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

Redirecting Users

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

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

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

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

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

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

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

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

```
[edit security application-firewall rule-sets application-firewall-3]
```

```

set profile deny-profile-1
set rule redirect-on-deny
set match dynamic-application [junos:KAZAA junos:EDONKEY junos:YMSG]
set then deny block-message

```

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

Session Logging for Application Firewalls

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

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

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

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

Application Firewall Support in Chassis Cluster

When the application ID is not identified during failover sessions, the ID is considered an unknown application ID. During this session, the traffic is processed based on the action defined in a rule specified for unknown. If there is no rule defined for unknown, then the default rule is applied.



NOTE: When an SRX Series device is operating in chassis cluster mode and application identification is enabled, 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.

When the application ID is identified before sessions fail over, the same action taken before the failover is effective after the failover. The application firewall action taken before and after the failover depends on the application ID state, as shown in [Table 8 on page 112](#).

Table 8: Application Firewall Actions

Before Failover		After Failover	
Application ID State	Application Firewall Action	Application ID State	Application Firewall Action
Success	Deny	Success	Deny
Success	Permit	Success	Permit
Pending	—	UNKNOWN	Action based on the rule defined for unknown application



NOTE: 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.

Related Documentation

- [Example: Configuring an Application Group for Application Firewall on page 116](#)
- [Understanding Application Identification Techniques on page 23](#)
- *Security Basics Guide for Security Devices*

Example: Configuring Application Firewall Rule Sets Within a Security Policy

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 112](#)
- [Overview on page 112](#)
- [Configuration on page 113](#)
- [Verification on page 116](#)

Requirements

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

Overview

In Junos OS, the security policies provide firewall security functionality by enforcing rules for the traffic so that traffic passing through the device is permitted or denied based on

the action defined in the rules. The application firewall support in the policies provides additional security control for dynamic applications.

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

This configuration example shows how to:

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



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

Configuration

CLI Quick Configuration

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

```
set security policies from-zone untrust to-zone trust policy policy1 match source-address 198.51.100.1
set security policies from-zone untrust to-zone trust policy policy1 match destination-address 192.0.2.1
set security policies from-zone untrust to-zone trust policy policy1 match application junos-http
set security policies from-zone untrust to-zone trust policy policy1 then permit application-services application-firewall rule-set rs1
set security policies from-zone untrust to-zone trust policy policy2 match source-address 198.51.100.1
set security policies from-zone untrust to-zone trust policy policy2 match destination-address 192.0.2.1
set security policies from-zone untrust to-zone trust policy policy2 match application any
set security policies from-zone untrust to-zone trust policy policy2 then permit application-services application-firewall rule-set rs2
set security application-firewall rule-sets rs1 rule r1 match dynamic-application [junos:KAZAA junos:EDONKEY junos:YMSG]
set security application-firewall rule-sets rs1 rule r1 then deny
set security application-firewall rule-sets rs1 default-rule permit
set security application-firewall rule-sets rs2 rule r1 match dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLETALK junos:MEEBOME junos:UNKNOWN]
set security application-firewall rule-sets rs2 rule r1 then permit
set security application-firewall rule-sets rs2 default-rule deny
```

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

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

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

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

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

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

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

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

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

```
[edit security application-firewall rule-sets rs2]
user@host# set rule r1 match dynamic-application [junos:FACEBOOK-ACCESS
junos:GOOGLETALK junos:MEEBOME junos:UNKNOWN]
user@host# set rule r1 then permit
user@host# set default-rule deny
```

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

```
[edit]
user@host# show security policies
from-zone untrust to-zone trust {
  policy 1 {
    match {
      source-address 198.51.100.1;
```

```

        destination-address 192.0.2.1;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set rs1;
                }
            }
        }
    }
}
policy 2 {
    match {
        source-address 198.51.100.1;
        destination-address 192.0.2.1;
        application any;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set rs2;
                }
            }
        }
    }
}
}
user@host# show security application-firewall
rule-sets rs1 {
    rule r1 {
        match {
            dynamic-application [junos:KAZAA junos:EDONKEY junos:YMSG];
        }
        then {
            deny;
        }
    }
    default-rule {
        permit;
    }
}
rule-sets rs2 {
    rule r1 {
        match {
            dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLETALK
                                junos:MEEBOME junos:UNKNOWN];
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}

```

```
}  
}
```

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

Verification

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

- [Verifying Application Firewall Configuration on page 116](#)

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	<p>The output displays information about application firewall enabled policies configured on the system. Verify the following information.</p> <ul style="list-style-type: none">• Rule set• Rules• Match criteria
Related Documentation	<ul style="list-style-type: none">• Application Firewall Overview on page 107• Understanding Application Identification Techniques on page 23• <i>Security Basics Guide for Security Devices</i>

Example: Configuring an Application Group for Application Firewall

Supported Platforms [SRX Series, vSRX](#)

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



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

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

- [Requirements on page 117](#)
- [Overview on page 117](#)
- [Configuration on page 117](#)
- [Verification on page 119](#)

Requirements

Before you begin:

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

Overview

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

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

This configuration example shows how to:

- Configure dynamic application groups in an application firewall.

Configuration

CLI Quick Configuration

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

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

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

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

1. Create the rule-set social-network.

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

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

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

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

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

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

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

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

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

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

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

```
[edit]
user@host# show security application-firewall
...
```

```

rule-sets social-network {
  rule google-rule {
    match {
      dynamic-application junos:GOOGLETALK;
    }
  }
  then {
    permit ;
  }
  rule denied-sites {
    match {
      dynamic-application-groups junos:social-networking
      dynamic-application junos:UNKNOWN;
    }
    then {
      deny ;
    }
  }
  default-rule {
    permit;
  }
}
...

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

```

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

Verification

Verifying Application Firewall Configuration

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

- Action**
- To verify the application firewall policy configuration enabled with application grouping, from the operational mode, enter the **show security policies** and **show security policies detail** commands.
 - To verify all the application firewall rule sets configured on the device, from the operational mode, enter the **show security application-firewall rule-set all** command.
 - To verify the list of applications defined within the application group, from the operational mode, enter the **show services application-identification application-group application-group-name** command.
- Related Documentation**
- [Application Firewall Overview on page 107](#)
 - [Example: Configuring Application Firewall Rule Sets Within a Security Policy on page 112](#)
 - [Understanding Application Identification Techniques on page 23](#)
 - [Security Policies Overview](#)

Example: Configuring Application Firewall When SSL Proxy Is Enabled

Supported Platforms SRX1500, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX550M, SRX5600, SRX5800, vSRX



NOTE: If none of the services (AppFW, IDP, or AppTrack) are configured, then SSL proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy.

This example describes how AppFW supports this AppID functionality when SSL proxy is enabled.

- [Requirements on page 120](#)
- [Overview on page 121](#)
- [Configuration on page 121](#)

Requirements

Before you begin:

- Create zones. See *Example: Creating Security Zones*.
- Configure an address book with addresses for the policy. See *Example: Configuring Address Books and Address Sets*.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See *Example: Configuring Applications and Application Sets*.
- Create a SSL proxy profile that enables SSL proxy by means of a policy. See [“Configuring SSL Proxy” on page 83](#).

Overview

This example shows how to verify the functionality of AppFW when SSL proxy is enabled and a different action, deny or permit, is performed on plain text and encrypted 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 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]
user@host# set security application-firewall rule-sets appfw-rs-1 rule rule1 then permit
user@host# set security application-firewall rule-sets appfw-rs-1 default-rule deny
user@host# set security application-firewall rule-sets appfw-rs-2 rule rule1 match
  dynamic-application [junos:HULU]
user@host# set security application-firewall rule-sets appfw-rs-2 rule rule1 then deny
user@host# 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*.

In this example, you configure two security policies with AppFW rule sets that 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.
1. Configure a policy to process the traffic with AppFW rule set appfw-rs-1 and SSL proxy profile ssl-profile-1.

```
[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 policy with rule set appfw-rs-2.

```
[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 appfw-rs-1 to permit an encrypted version of Oracle 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 the AppFW rule set appfw-rs-2 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: For application **junos-https**, SSL proxy detects an SSL session based on the dynamic application identified for that session. If you know any webserver that is running nonstandard ports, you can use a custom Junos OS application to identify the application. However, if the webserver is not known, for example on the Internet, 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.

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.

- Related Documentation**
- [SSL Proxy Overview on page 73](#)
 - [Application Firewall, IDP, and Application Tracking with SSL Proxy Overview on page 102](#)
 - [Understanding Security Policy Elements](#)
 - [Security Policies Configuration Overview](#)
 - [Application Firewall Overview on page 107](#)
 - [Example: Configuring Application Firewall Rule Sets Within a Security Policy on page 112](#)

CHAPTER 10

Configuring Application Tracking

- [Understanding AppTrack on page 125](#)
- [Example: Configuring AppTrack on page 127](#)
- [Example: Configuring AppTrack When SSL Proxy Is Enabled on page 132](#)
- [Disabling AppTrack on page 134](#)

Understanding AppTrack

Supported Platforms [SRX Series, vSRX](#)

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. The Security Threat Response Manager (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.

Apptrack generates a log whenever a session is created, or during the session at predefined intervals, and at the session close. 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.

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.

Release History Table

Release	Description
15.1X49-D100	Starting from Junos OS Release 15.1X49-D100, AppTrack session create, session close, and volume update logs include a new field called destination interface.
15.1X49-D100	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.

Related Documentation

- [Example: Configuring AppTrack on page 127](#)
- [Disabling AppTrack on page 134](#)
- [Understanding Application Identification Techniques on page 23](#)

Example: Configuring AppTrack

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 127](#)
- [Overview on page 127](#)
- [Configuration on page 127](#)
- [Verification on page 130](#)

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 32](#) or [“Downloading and Installing the Junos OS Application Signature Package As Part of the IDP Security Package” on page 35](#). 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 Security Threat Response Manager (STRM) 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: On all SRX Series devices, 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
```

```
user@host# set security log stream app-track-logs host 192.0.2.2
```

2. Enable AppTrack for the security zone trust.

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

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

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

The default interval between messages is 5 minutes. If a session starts and ends within this update interval, AppTrack generates one message at session close. However, if the session is long-lived, an update message is sent every 5 minutes. The **session-update-interval** *minutes* is configurable as shown in this step.

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

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

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

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



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

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

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

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

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

```
...
application-tracking {
    first-update;
    session-update-interval 4;
}
log {
    mode stream;
    format sd-syslog;
    source-address 192.0.2.2;
    stream app-track-logs {
        host {
            192.0.2.1;
        }
    }
}
...

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

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

Verification

Use the STRM 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 SRX Series device:

- [Reviewing AppTrack Statistics on page 130](#)
- [Verifying AppTrack Counter Values on page 131](#)
- [Verifying Security Flow Session Statistics on page 131](#)
- [Verifying Application System Cache Statistics on page 132](#)
- [Verifying the Status of Application Identification Counter Values on page 132](#)

Reviewing AppTrack Statistics

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

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

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

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

Application	Sessions	Bytes	Encrypted
HTTP	1	2291	Yes

HTTP	1	942	No
SSL	1	2291	Yes
unknown	1	100	No
unknown	1	100	Yes



NOTE: For more information on the `show services application-identification statistics applications` command, see [show services application-identification statistics applications](#).

Verifying AppTrack Counter Values

Purpose View the AppTrack counters periodically to monitor logging activity.

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

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

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

Verifying Security Flow Session Statistics

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

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

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

```
Flow Sessions on FPC6 PIC0:
```

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

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

Byte and packet totals in the session statistics should approximate the counts logged by AppTrack but might not be exactly the same. AppTrack counts only incoming bytes

and packets. System-generated packets are not included in the total, and dropped packets are not deducted.

Verifying Application System Cache Statistics

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

Verifying the Status of Application Identification Counter Values

- Purpose** Compare session statistics for application identification counter values from the **show services application-identification counter** command output.
- Action** From operational mode, enter the **show services application-identification counter** command.

- Related Documentation**
- [Understanding AppTrack on page 125](#)
 - [Disabling AppTrack on page 134](#)
 - [Understanding Application Identification Techniques on page 23](#)

Example: Configuring AppTrack When SSL Proxy Is Enabled

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

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

- [Requirements on page 132](#)
- [Overview on page 133](#)
- [Configuration on page 133](#)

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 Proxy” on page 83](#).

Overview

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

Configuration

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

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

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

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

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

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

2. Configure SSL proxy profile.

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

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

```
from-zone Z_1 to-zone Z_2 {
  policy policy1 {
    match {
      source-address any;
      destination-address any;
    }
  }
}
```

```
then {
  permit {
    application-services {
      ssl-proxy {
        profile-name ssl-profile-1;
      }
    }
  }
}
```



NOTE: Verify that the configuration is working properly. Verification in AppTrack works similarly to verification in AppFW. See the verification section of “[Example: Configuring Application Firewall When SSL Proxy Is Enabled](#)” on page 120.

Related Documentation

- [SSL Proxy Overview on page 73](#)
- [Application Firewall, IDP, and Application Tracking with SSL Proxy Overview on page 102](#)
- [Understanding Security Policy Elements](#)
- [Security Policies Configuration Overview](#)
- [Example: Configuring AppTrack on page 127](#)

Disabling AppTrack

Supported Platforms [SRX Series, vSRX](#)

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 reenble it, delete the configuration statement that specifies disabling of application tracking:

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

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

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

Related Documentation

- [Understanding AppTrack on page 125](#)
- [Example: Configuring AppTrack on page 127](#)
- [Understanding Application Identification Techniques on page 23](#)

CHAPTER 11

Configuring Application QoS

- [Understanding Application QoS \(AppQoS\) on page 135](#)
- [Example: Configuring AppQoS on page 141](#)

Understanding Application QoS (AppQoS)

Supported Platforms [SRX Series, vSRX](#)

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 SRX Series devices:

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

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

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

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

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

- [Unique Forwarding Classes and Queue Assignments on page 136](#)
- [Application-Aware DSCP Code-Point and Loss Priority Settings on page 137](#)
- [Rate Limiters and Profiles on page 138](#)
- [Rate-Limiter Assignment on page 139](#)
- [Rate-Limiter Action on page 141](#)
- [AppQoS Security Policy Configuration on page 141](#)

Unique Forwarding Classes and Queue Assignments

The forwarding class provides three functions:

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

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

Each forwarding class is assigned to an egress queue that provides the appropriate degree of enhanced or standard processing. Many forwarding classes can be assigned to a single queue. Therefore, any queues defined for the device can be used by IDP, AppQoS, and firewall filter-based rewriters. It is the forwarding class name, not the queue, that distinguishes the transmission priority. (See the *Class of Service Feature Guide for Security Devices* for information about configuring queues and schedulers.)

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, SRX550M, SRX650, and SRX1500 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 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 9 on page 137](#) provides a list of Junos OS default DSCP alias names and bitmap values.

Table 9: Standard CoS Aliases and Bit Values

CoS Value Type	Alias	Bit Value
Expedited forwarding	ef	101110
Assured forwarding	af11	001010
Assured forwarding	af12	001100
Assured forwarding	af13	001110
Assured forwarding	af21	010010
Assured forwarding	af22	010100
Assured forwarding	af23	010110
Assured forwarding	af31	011010
Assured forwarding	af32	011100
Assured forwarding	af33	011110
Assured forwarding	af41	100010
Assured forwarding	af42	100100
Assured forwarding	af43	100110
Best effort	be	000000
	cs1	001000
	cs2	010000
	cs3	011000
	cs4	100000

Table 9: Standard CoS Aliases and Bit Values (*continued*)

CoS Value Type	Alias	Bit Value
	cs5	101000
Network control	nc1/cs6	110000
Network control	nc2/cs7	111000

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

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

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

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

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

Rate Limiters and Profiles

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

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

A rate-limiter profile defines the limitations. It is a unique combination of **bandwidth-limit** and **burst-size-limit** specifications. The **bandwidth-limit** defines the maximum number

of kilobits per second that can traverse the port. The **burst-size-limit** defines the maximum number of bytes that can traverse the port in a single burst. The **burst-size-limit** reduces starvation of lower priority traffic by ensuring a finite size for each burst.

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

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

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

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

Rate-Limiter Assignment

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

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

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

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

- client-to-server limiter-1
- server-to-client limiter-1

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

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

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

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

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



NOTE: If packets are dropped from a PIC, the SRX Series 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 SRX Series 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
```

- Related Documentation**
- [Example: Configuring AppQoS on page 141](#)
 - [Understanding Application Identification Techniques on page 23](#)

Example: Configuring AppQoS

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 142](#)
- [Overview on page 142](#)
- [Configuration on page 142](#)
- [Verification on page 145](#)

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: On all SRX Series devices, 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:

```
[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 SRX5400 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

```
[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.

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

```

    }
  }
  ...

```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Flow Session Configuration on page 145](#)
- [Verifying Session Statistics on page 146](#)
- [Verifying Rate-Limiter Statistics on page 146](#)
- [Verifying Rule Statistics on page 147](#)

Verifying Flow Session Configuration

Purpose Verify that AppQoS is enabled.

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

```

user@host> show security flow session application-traffic-control extensive
Session ID: 3729, Status: Normal, State: Active
Flag: 0x40
Policy name: p1
Source NAT pool: Null
Dynamic application: junos:FTP
Application traffic control rule-set: ftp-test1, Rule: rule0
Maximum timeout: 300, Current timeout: 276
Session State: Valid
Start time: 18292, Duration: 603536
  In: 192.0.2.1/1 --> 203.0.113.0/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
  Out: 203.0.113.0/1 --> 192.0.2.0/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xffffd0000, Gateway: 192.0.2.0, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

```

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

Verifying Session Statistics

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

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

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

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

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

Verifying Rate-Limiter Statistics

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

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

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

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

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

Verifying Rule Statistics

Purpose Verify that the rule matches the rule statistics.

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

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

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

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

Related Documentation

- [Understanding Application Identification Techniques on page 23](#)

CHAPTER 12

Advanced Policy-Based Routing

- [Understanding Advanced Policy-Based Routing on page 149](#)
- [Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152](#)

Understanding Advanced Policy-Based Routing

Supported Platforms [SRX Series, vSRX](#)

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 on page 149](#)
- [Filter-Based Forwarding or Policy-Based Routing \(PBR\) on page 150](#)
- [Advanced Policy-Based Routing on page 150](#)
- [Understanding How APBR Works on page 151](#)
- [Use Case on page 152](#)
- [Limitations on page 152](#)

Application Identification

SRX Series 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)

SRX Series 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.

APBR provides the following advantages:

- APBR allows you to define the routing behavior based on applications.

- APBR extends the scope of static routes by providing more flexible traffic-handling capabilities by offering granular control for forwarding packets based on application attributes.

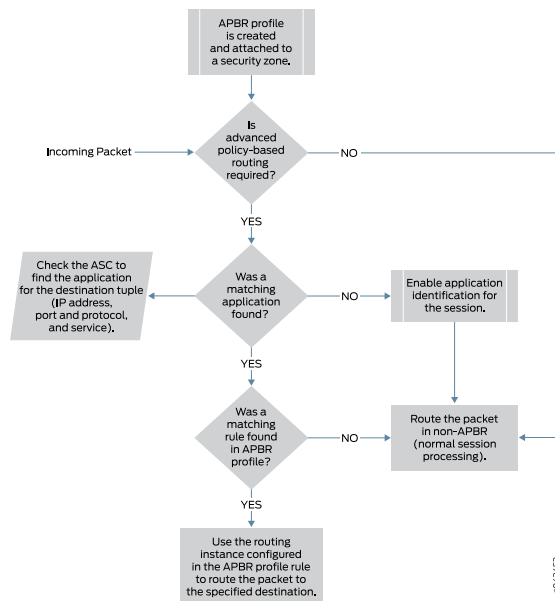
Understanding How APBR Works

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 8 on page 151 shows the sequence in which APBR techniques are applied.

Figure 8: 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-ABPR 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.

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.
- 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.

Related Documentation

- [Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152](#)

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

Supported Platforms [SRX Series, vSRX](#)

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

- [Requirements on page 153](#)
- [Overview on page 153](#)
- [Configuration on page 155](#)
- [Verification on page 159](#)

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.

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.

[Table 10 on page 153](#) provides the details of the parameters used in this example.

Table 10: APBR Configuration Parameters

Parameter	Name	Description
Routing Instance	<ul style="list-style-type: none"> • Instance name—R1 • Instance type— forwarding • Static route— 5.0.0.0/8 • Next-hop— 7.0.0.1 	Routing instance of type forwarding is used for forwarding the traffic.
	<ul style="list-style-type: none"> • Instance name—R2 • Instance type— forwarding • Static route— 5.0.0.0/8 • Next-hop— 8.0.0.1 	All the qualified traffic destined for the static route (example: 5.0.0.0/8) is forwarded to the next-hop device (example: with 7.0.0.1 address on its interface).
	<ul style="list-style-type: none"> • Instance name—R3 • Instance type— forwarding • Routing option— static • Static route— 5.0.0.0/8 • Next-hop— 9.0.0.1; 	

Table 10: APBR Configuration Parameters (*continued*)

Parameter	Name	Description
RIB Group	apbr_group	<p>Name of the routing information base (RIB) (also known as routing table) group.</p> <p>This RIB group is configured to import interface route entries from inet.0, R11.inet.0, R12.inet.0, and R13.inet.0.</p>
APBR Profile	profile-1	Name of the APBR profile. This profile matches applications and application groups and redirects the matching traffic to the specified routing instance (example: R1) for the route lookup. The profile includes multiple rules.
Rule	<ul style="list-style-type: none"> • Rule name—ruleApp1 • matching application—junos:HTTP • Associated routing instance—R1 <hr/> <ul style="list-style-type: none"> • rule name—ruleApp2 • matching application—junos:web:social-networking • Routing instance— R2 <hr/> <ul style="list-style-type: none"> • rule name— ruleApp3 • matching application— junos:YAHOO • Routing instance— R3 	<p>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.</p>
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 RGO failover due to limitations. We recommend not configure fxp0 local route in the routing table of non-default routing instance. Following sample depicts a sample configuration of policy options. Note that the reject action helps in eliminating the routes that are not required. You can use specific routes to reject the fxp0 routes.

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



NOTE: APBR is used for routing the packets in a forward path. For return traffic to arrive over the same path, we recommend to configure the remote 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 5.0.0.0/8 next-hop 7.0.0.1
```

```
set routing-instances R2 instance-type forwarding;
set routing-instances R2 routing-options static route 5.0.0.0/8 next-hop 8.0.0.1
set routing-instances R3 instance-type forwarding;
set routing-instances R3 routing-options static route 5.0.0.0/8 next-hop 9.0.0.1
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 R11.inet.0
set routing-options rib-groups apbr_group import-rib R12.inet.0
set routing-options rib-groups apbr_group import-rib R13.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 junos:junos:web:social-networking
set security advance-policy-based-routing profile profile1 rule rule-app2 then
routing-instance R2
set security advance-policy-based-routing profile profile1 rule rule-app3 match
dynamic-application junos:YAHOO
set security advance-policy-based-routing profile profile1 rule rule-app3 then
routing-instance R3
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-2/2/0.0
set security zones security-zone trust advance-policy-based-routing-profile profile1
```

Configuring Advanced Policy-Based Routing

Step-by-Step Procedure

To configure APBR:

1. Create routing instances.

```
[edit]
user@host# set routing-instances R1 instance-type forwarding
user@host# set routing-instances R1 routing-options static route 5.0.0.0/8 next-hop
7.0.0.1
user@host# set routing-instances R2 instance-type forwarding;
user@host# set routing-instances R2 routing-options static route 5.0.0.0/8 next-hop
8.0.0.1
user@host# set routing-instances R3 instance-type forwarding;
user@host# set routing-instances R3 routing-options static route 5.0.0.0/8 next-hop
9.0.0.1
```

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 R11.inet.0
set routing-options rib-groups apbr_group import-rib R12.inet.0
set routing-options rib-groups apbr_group import-rib R13.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 junos:junos:web:social-networking
user@host# set security advance-policy-based-routing profile profile1 rule rule-app2
then routing-instance R2
user@host# set security advance-policy-based-routing profile profile1 rule rule-app3
match dynamic-application junos:YAHOO
user@host# set security advance-policy-based-routing profile profile1 rule rule-app3
then routing-instance R3
```

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 xe-2/2/0.0
user@host# set security zones security-zone trust
advance-policy-based-routing-profile profile1
```

Results

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

```
[edit]
user@host# show routing-instances
R1 {
  instance-type forwarding;
  routing-options {
    static {
      route 5.0.0.0/8 next-hop 7.0.0.1;
    }
  }
}
R2 {
  instance-type forwarding;
  routing-options {
    static {
      route 5.0.0.0/8 next-hop [ 8.0.0.1 9.0.0.1 ];
    }
  }
}
R3 {
  instance-type forwarding;
  routing-options {
```

```
        static {
            route 5.0.0.0/8 next-hop 9.0.0.1;
        }
    }
}

[edit]
user@host# show routing-options
interface-routes {
    rib-group inet apbr_group;
}
rib inet6.0 {
    static {
        route 2001::/16 next-hop 2006::10;
    }
}
static {
    route 4.0.0.0/8 next-hop 11.0.0.254;
}
rib-groups {
    apbr_group {
        import-rib [ inet.0 RI1.inet.0 RI2.inet.0 RI3.inet.0 ];
    }
}

[edit]
user@host# show security advance-policy-based-routing
profile profile1 {
    rule rule-app1 {
        match {
            dynamic-application junos:HTTP;
        }
        then {
            routing-instance R1;
        }
    }
    rule rule-app2 {
        match {
            dynamic-application junos:junos:web:social-networking;
        }
        then {
            routing-instance R2;
        }
    }
    rule rule-app3 {
        match {
            dynamic-application junos:YAHOO;
        }
        then {
            routing-instance R3;
        }
    }
}

[edit]
user@host# show security zones
security-zone trust {
```

```

host-inbound-traffic {
  system-services {
    all;
  }
  protocols {
    all;
  }
}
interfaces {
  xe-2/2/0.0;
}
advance-policy-based-routing-profile {
  profile1;
}
}

```

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

Verification

Verifying Advanced Policy-Based Routing

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

Related Documentation

- [Understanding Advanced Policy-Based Routing on page 149](#)

CHAPTER 13

Configuration Statements

- [actions \(Services SSL Proxy\) on page 164](#)
- [actions \(Services SSL Initiation\) on page 166](#)
- [address-mapping \(Application Identification\) on page 167](#)
- [advance-policy-based-routing on page 168](#)
- [advance-policy-based-routing \(Security Zones\) on page 169](#)
- [appfw-profile \(System\) on page 170](#)
- [appfw-rule on page 171](#)
- [appfw-rule-set on page 172](#)
- [application-firewall on page 173](#)
- [application \(Application Identification\) on page 175](#)
- [application-firewall \(Application Services\) on page 177](#)
- [application-identification on page 178](#)
- [application-group \(Services\) on page 180](#)
- [application-services \(Security Policies\) on page 181](#)
- [application-system-cache on page 182](#)
- [application-system-cache-timeout \(Services\) on page 183](#)
- [application-tracking on page 184](#)
- [application-tracking \(Security Zones\) on page 185](#)
- [application-traffic-control on page 186](#)
- [application-traffic-control \(Application Services\) on page 187](#)
- [block-message \(Application Firewall\) on page 188](#)
- [context \(Application Identification\) on page 190](#)
- [custom-ciphers on page 192](#)
- [default-rule on page 193](#)
- [direction \(Application Identification\) on page 194](#)
- [disable \(Application Tracking\) on page 195](#)
- [download \(Services\) on page 196](#)
- [dynamic-application on page 197](#)

- [dynamic-application-group](#) on page 197
- [enable-flow-tracing \(Services\)](#) on page 198
- [enable-performance-mode](#) on page 199
- [enable-session-cache](#) on page 200
- [file \(Services\)](#) on page 201
- [files \(Services\)](#) on page 202
- [file \(System Logging\)](#) on page 203
- [first-update](#) on page 205
- [first-update-interval](#) on page 206
- [flag \(Services\)](#) on page 207
- [format \(Security Log\)](#) on page 208
- [forwarding-classes \(CoS\)](#) on page 209
- [global-config \(Services\)](#) on page 210
- [icmp-mapping \(Application Identification\)](#) on page 211
- [ip \(Application Identification\)](#) on page 212
- [ip-protocol-mapping \(Application Identification\)](#) on page 212
- [initiation \(Services\)](#) on page 213
- [level \(Services\)](#) on page 214
- [log \(Security\)](#) on page 215
- [log \(Services\)](#) on page 219
- [match \(Services\)](#) on page 220
- [no-application-identification \(Services\)](#) on page 220
- [no-application-system-cache \(Services\)](#) on page 221
- [no-remote-trace \(Services\)](#) on page 221
- [over \(Application Identification\)](#) on page 222
- [policies](#) on page 224
- [policy \(Security Policies\)](#) on page 229
- [port-range \(Application Identification\)](#) on page 231
- [preferred-ciphers](#) on page 232
- [profile \(Application Firewall\)](#) on page 233
- [profile \(Rule Sets\)](#) on page 234
- [profile \(Services\)](#) on page 235
- [profile \(SSL Initiation\)](#) on page 236
- [profile \(SSL Termination\)](#) on page 237
- [protocol-version](#) on page 238
- [proxy \(Services\)](#) on page 239
- [rate-limiters](#) on page 241

- renegotiation (Services) on page 242
- root-ca (Services) on page 242
- routing-instance (Advanced Policy-Based Routing) on page 243
- rule (Advanced Policy-Based Routing) on page 244
- rule-sets (CoS AppQoS) on page 245
- rule-sets (Security Application Firewall) on page 247
- security-zone on page 248
- server-certificate (Services) on page 249
- session-update-interval on page 250
- size (Services) on page 251
- ssl (Services) on page 252
- ssl-encryption on page 254
- ssl-proxy (Application Services) on page 255
- statistics (Services) on page 256
- stream (Security Log) on page 257
- termination (Services) on page 258
- then (Security Application Firewall) on page 259
- trusted-ca (Services) on page 260
- traceoptions (advanced policy-based routing) on page 261
- traceoptions (Security Application Firewall) on page 263
- traceoptions (Services Application Identification) on page 265
- traceoptions (Services SSL) on page 267
- transport (Security Log) on page 269
- whitelist (Services) on page 270
- whitelist-url-categories on page 271
- zones on page 272

actions (Services SSL Proxy)

Supported Platforms SRX Series, vSRX

Syntax

```
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);
  }
}
```

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 15.1X49-D30.

Description Specify the logging and traffic related actions.

- 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.
 - **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 on page 73](#)
- [Configuring SSL Proxy on page 83](#)
- [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

actions (Services SSL Initiation)

Supported Platforms	SRX1500, SRX5400, SRX5600, SRX5800, vSRX
Syntax	<pre>actions { ignore-server-auth-failure; }</pre>
Hierarchy Level	[edit services ssl initiation profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify the logging and traffic related actions.
Options	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• SSL Proxy Overview on page 73• Configuring SSL Proxy on page 83• Enabling Debugging and Tracing for SSL Proxy on page 105

address-mapping (Application Identification)

Supported Platforms [SRX Series](#)

Syntax

```
address-mapping address-name {
  filter {
    ip ip-address-and-prefix-length;
    port-range {
      tcp [port];
      udp [port];
    }
  }
}
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Defines an application by the IP address and the port range of the traffic.

Options filter—Specify the application matching criteria by the IP address of the application or the port range to match TCP or UDP destination port.

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 on page 49](#)

advance-policy-based-routing

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
advance-policy-based-routing {
  profile profile-name {
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-group [system-application-group];
      }
      then {
        routing-instance name ;
      }
    }
  }
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 15.1X49-D60.

Description 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 context established in the first packet of a session must match the context contained in all subsequent packets if a session is to remain active.

The APBR profile is associated 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.

Options **profile *profile-name***—Name of the profile. Must be a unique name with a maximum length of 63 characters.

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	<ul style="list-style-type: none"> • Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152 • Understanding Advanced Policy-Based Routing on page 149

advance-policy-based-routing (Security Zones)

Supported Platforms	SRX Series , vSRX
Syntax	advance-policy-based-routing;
Hierarchy Level	[edit security zones security-zone <i>zone-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1X49-D60.
Description	<p>Enable or apply the advanced policy-based (APBR) routing profile (application profile) on the specified security zone.</p> <p>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.</p> <p>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.</p>
Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152 • Understanding Advanced Policy-Based Routing on page 149

appfw-profile (System)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
appfw-profile {  
    maximum amount;  
    reserved amount;  
}
```

Hierarchy Level [edit system security-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the application firewall profile quota of a logical system.

- Options**
- **maximum *amount***—Specify the maximum allowed quota value.
Range: 0 through 1024
 - **reserved *amount***—Specify a reserved quota value that guarantees that the resource amount specified is always available to the logical system.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Application Firewall Overview on page 107](#)

appfw-rule

Supported Platforms SRX5400, SRX5600, SRX5800, vSRX

Syntax appfw-rule {
 maximum *amount*;
 reserved *amount*;
}

Hierarchy Level [edit system security-profile *security-profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the number of application firewall rule configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.

The master administrator:

- Uses security profiles to provision logical systems with resources
- Binds security profiles to the master logical system and the user logical systems
- Can configure more than one security profile, allocating different numbers of resources in various profiles

Only the master administrator can create security profiles and bind them to logical systems.

- Options**
- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can use resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
 - **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Application Firewall Overview on page 107](#)

appfw-rule-set

Supported Platforms	SRX1500, SRX5400, SRX5600, SRX5800, vSRX
Syntax	<pre>appfw-rule-set { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	<p>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.</p> <p>The master administrator:</p> <ul style="list-style-type: none">• 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 <p>Only the master administrator can create security profiles and bind them to logical systems.</p>
Options	<ul style="list-style-type: none">• maximum <i>amount</i>—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 <i>amount</i>—A reserved quota that guarantees that the resource amount specified is always available to the logical system.
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Application Firewall Overview on page 107

application-firewall

Supported Platforms [SRX Series, vSRX](#)

Syntax

```

application-firewall {
  profile profile-name {
    block-message type {
      custom-text content custom-html-text;
      custom-redirect-url content custom-redirect-url;
    }
  }
  rule-sets rule-set-name {
    default-rule {
      (deny [block-message] | permit | reject [block-message]);
    }
    profile profile-name;
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-groups [system-application-group];
        ssl-encryption (any | yes | no);
      }
      then {
        (deny [block-message] | permit | reject [block-message]);
      }
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (world-readable | no-world-readable);
      size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
  }
}

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 11.1. Updated with the **ssl-encryption** and **reject** options in Junos OS Release 12.1X44-D10. Updated with the **block-message** option in Junos OS Release 12.1X45-D10.

Description Specify the profile options, rule set and rule specifications, and trace options to be used for application firewall implementations.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related • [Application Firewall Overview on page 107](#)
Documentation

application (Application Identification)

Supported Platforms [SRX Series](#)

```
Syntax  application application-name {
        address-mapping address-name {
            filter {
                ip ip-address-and-prefix-length;
                port-range {
                    tcp [port];
                    udp [port];
                }
            }
        }
        cacheable;
        description;
        icmp-mapping {
            code number;
            type number;
        }
        ip-protocol-mapping {
            protocol number;
        }
        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];
            }
        }
    }
```

Hierarchy Level [\[edit services application-identification\]](#)

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Configure a custom application definition for the desired application name that will be used by the system to identify the application as it passes through the device. Custom application definitions can be used for applications that are not part of the Juniper Networks predefined application database.

Options **application *application-name***—Name of the custom application signature. Must be a unique name with a maximum length of 63 characters.



NOTE: Application names are case insensitive.

cacheable—Enable caching of application identification results. By enabling this option, you can cache the application detection result in an ASC table. If there is an entry in the ASC table, based on the destination IP address, protocol, and the port, we can identify AppID without again sending packet to engine. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.

description—Description of the application.

order *number*—Specify the order for the custom application. Lower order has higher priority. This option is used when multiple custom applications of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications.

priority [high | low]—Specify the priority over other signature applications.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring Junos OS Application Identification Custom Application Signatures on page 52](#)

application-firewall (Application Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
application-firewall {  
    rule-set rule-set-name;  
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure application firewall rule sets with rules defining match criteria and the action to be performed.

Options **rule-set *rule-set-name***—Name of the rule set that contains application firewall specification rules.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Application Firewall Overview on page 107](#)

application-identification

Supported Platforms [SRX Series, vSRX](#)

```
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;
        }
        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];
                }
            }
        }
        application-group group-name {
            application-groups application-group-name;
            applications application-name;
        }
    }
}
```

```

application-system-cache-timeout value;
download {
    automatic {
        interval hours;
        start-time MM-DD.hh:mm;
    }
    url url;
}
enable-performance-mode max-packet-threshold number;
no-application-identification;
no-application-system-cache;
statistics {
    interval minutes;
}
traceoptions {
    file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level [all | error | info | notice | verbose | warning]
    no-remote-trace;
}
}

```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 10.2. Custom application definition option introduced in Junos OS Release 15.1X49-D40.

Description Configure application identification options to identify the TCP or UDP application session running on nonstandard ports to match the application properties of transiting network traffic.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Understanding Application Identification Techniques on page 23](#)

application-group (Services)

Supported Platforms [SRX Series, vSRX](#)

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 Specify any number of associated predefined applications, user-defined applications, and other groups for ease of use in configuring application-based policies.

An application group is hierarchical: a tree structure of groups with applications as the leaf nodes.

Options *group-name*—Name of the group. This name is used in policy configuration statements in place of multiple predefined applications, user-defined applications, or other groups.

application-groups application-group-name— Name of an application group to be assigned to this group. There is no maximum number of groups that can be assigned to a group. Use multiple commands to assign multiple groups.

applications application-name—Name of an application to be assigned to this group. An application can remain unassigned or be assigned to a group, but it cannot be assigned to more than one group. There is no maximum number of applications that can be assigned to a group. Use multiple commands to assign multiple groups.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring a Custom Application Group for Junos OS Application Identification for Simplified Management on page 60](#)

application-services (Security Policies)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```

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;
}

```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information Statement modified in Junos OS Release 11.1.

Description Enable application services within a security policy.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Application Firewall Overview on page 107](#)

application-system-cache

Supported Platforms [SRX Series, vSRX](#)

Syntax application-system-cache;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 9.2.

Description When a session is created, specify an application ID to match the application properties of transiting network traffic. The application port mappings are saved in the application system cache.

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 on page 65](#)

application-system-cache-timeout (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax `application-system-cache-timeout value;`

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 9.2. Support for application identification in the services hierarchy added in Junos OS Release 10.2.

Description Specify the timeout value in seconds for the application system cache entries. Note that the cache is not cleared when the IDP policy is loaded. Users need to manually clear or wait for the cache entries to expire.



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.

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 on page 65](#)

application-tracking

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
application-tracking {  
  disable;  
  (first-update | first-update-interval first-update-interval);  
  session-update-interval session-update-interval;  
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 10.2. Support for **disable** added in Junos OS Release 11.4.

Description AppTrack, an application tracking tool, is a form of statistical profiling. Enabling this feature for a zone logs flow statistics (the byte count, packet count, and start and end times for a session) at session end. You can modify the logging time and log frequency with command options. Periodically, a network management tool, such as STRM, collects the logged statistics sent by each network device for bandwidth usage analysis of the network.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppTrack on page 127](#)

application-tracking (Security Zones)

Supported Platforms [SRX Series, vSRX](#)

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 security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation • [Example: Configuring AppTrack on page 127](#)

application-traffic-control

Supported Platforms [SRX Series, vSRX](#)

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-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]

Release Information Statement introduced in Junos OS Release 11.4.

Description Mark DSCP values for outgoing packets or apply rate limits based on the specified Layer 7 application types.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation • [Example: Configuring AppTrack on page 127](#)

application-traffic-control (Application Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax `application-traffic-control {
 rule-set rule-set-name;
}`

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information Statement introduced in Junos OS Release 11.4.

Description Enables AppQoS, application-aware quality of service, as specified in the rules of the specified rule set.

Options • **rule-set *rule-set-name***—Name of the rule set that contains application-aware traffic control specification rules.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation • [Example: Configuring AppQoS on page 141](#)
• [Security Policies Overview](#)

block-message (Application Firewall)

Supported Platforms SRX Series, vSRX

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. 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.

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.

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	<ul style="list-style-type: none"> • Example: Configuring AppQoS on page 141
------------------------------	---

context (Application Identification)

Supported Platforms [SRX Series](#)

Syntax

```
context {  
    http-get-url-parsed-param-parsed;  
    http-header-content-type;  
    http-header-cookie;  
    http-header-host;  
    http-header-user-agent;  
    http-post-url-parsed-param-parsed;  
    http-post-variable-parsed ;  
    http-url-parsed;  
    http-url-parsed-param-parsed;  
    ssl-server-name;  
    stream;  
}
```

Hierarchy Level [edit services application-identification application *application-name* over *protocol-type* signature *name* member *name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify context for matching application running over TCP, UDP, or Layer 7.

Options

http-get-url-parsed-param-parsed—The decoded, normalized GET URL in an HTTP request along with the decoded CGI parameters (if any).

http-header-content-type —The content-type header in an HTTP transaction.

http-header-cookie—The cookie header in an HTTP transaction.

http-header-host —The host header in an HTTP transaction.

http-header-user-agent—The user-agent header in an HTTP transaction.

http-post-url-parsed-param-parsed —The decoded, normalized POST URL in an HTTP request along with the decoded CGI parameters (if any).

http-post-variable-parsed—The decoded POST URL or form data variables.

http-url-parsed—The decoded, normalized URL in an HTTP request.

http-url-parsed-param-parsed—The decoded, normalized URL in an HTTP request along with the decoded CGI parameters (if any).

ssl-server-name —Server name in the TLS server name extension or the SSL server certificate. This is also known as Server Name Indication (SNI).

stream —TCP or UDP stream data.

Starting from Junos OS release 15.1X49-D60 and Junos OS Release 17.3R1, when configuring custom application signatures, the context-direction combinations as mentioned in [Table 11 on page 191](#) is supported. Any other combination other than this is not supported.

Table 11: Supported Context-Direction Combination for Custom Application Signatures

Context	Direction
http-get-url-parsed-param-parsed	client-to-server
http-header-host	client-to-server
http-header-user-agent	client-to-server
http-post-url-parsed-param-parsed	client-to-server
http-post-variable-parsed	client-to-server
http-url-parsed	client-to-server
http-url-parsed-param-parsed	client-to-server
ssl-server-name	client-to-server
stream	any/client-to-server/server-to-client
http-header-content-type	any/client-to-server/server-to-client
http-header-cookie	any/client-to-server/server-to-client



NOTE: If you are planning to upgrade the device to Junos OS release 15.1X49-D60 from the previous versions of the Junos OS, you must change the configuration to the valid combination of context-direction as mentioned in [Table 11 on page 191](#) 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 on page 49](#)

custom-ciphers

Supported Platforms [SRX Series, vSRX](#)

Syntax custom-ciphers [ecdhe-rsa-with-3des-edc-cbc-sha | ecdhe-rsa-with-aes-128-cbc-sha | ecdhe-rsa-with-aes-128-cbc-sha256 | ecdhe-rsa-with-aes-128-gcm-sha256 | ecdhe-rsa-with-aes-256-cbc-sha | ecdhe-rsa-with-aes-256-cbc-sha384 | ecdhe-rsa-with-aes-256-gcm-sha384 | rsa-with-aes-128-cbc-sha256 RSA | rsa-with-aes-128-gcm-sha256 RSA | rsa-with-aes-256-cbc-sha256 RSA | rsa-with-aes-256-gcm-sha384 RSA | rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha RSA | 128bit rc4 | sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash rsa-with-3des-edc-cbc-sha RSA | 3des edc/cbc | sha hash rsa-with-aes-128-cbc-sha RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc | sha hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no symmetric cipher | sha hash];

Hierarchy Level [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]
[edit services ssl initiation profile *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Display the custom cipher list. This statement is supported in the SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances.

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 on page 73](#)
- [Configuring SSL Proxy on page 83](#)
- [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

default-rule

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
default-rule {
    (deny [block-message] | permit | reject [block-message]);
}
```

Hierarchy Level [edit security application-firewall rule-sets *rule-set-name*]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 with the **reject** option. The **block-message** option added in Junos OS Release 12.1X45-D10.

Description Configure the default rule that defines the actions to be performed on a packet that does not match any defined rule.

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.

- Options**
- **deny**—Block the traffic at the firewall. The device drops the packet. No message is returned to the sender.
 - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for denied HTTP or HTTPS traffic. All other traffic is dropped silently.
 - **permit**—Permit traffic at the firewall.
 - **reject**—Block the traffic at the firewall. For TCP traffic, by default the device drops the packet and returns a TCP reset (RST) message to the source host and to the server in some cases. For UDP and other protocol traffic, by default the device drops the packet and returns an ICMP “destination unreachable, port unreachable” message to both the client and the server.
 - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for rejected HTTP or HTTPS traffic. All other traffic is dropped as specified in the default action for the **reject** option.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

- Related Documentation**
- [Example: Configuring Application Firewall Rule Sets Within a Security Policy on page 112](#)

direction (Application Identification)

Supported Platforms [SRX Series](#)

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.

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 are from client-side to server-side.

server-to-client—The direction of packets are 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 on page 49](#)

disable (Application Tracking)

Supported Platforms [SRX Series, vSRX](#)

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.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppTrack on page 127](#)

download (Services)

Supported Platforms [SRX Series, vSRX](#)

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 on page 38](#)

dynamic-application

Supported Platforms	SRX Series, vSRX
Syntax	dynamic-application [<i>system-application</i>];
Hierarchy Level	[edit security application-firewall rule-sets <i>rule-set-name</i> rule <i>rule-name</i> match]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Specify the dynamic application names for match criteria.
Options	<i>system-application</i> —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	<ul style="list-style-type: none"> • Application Firewall Overview on page 107

dynamic-application-group

Supported Platforms	SRX Series, vSRX
Syntax	dynamic-application-group [<i>system-application-group</i>];
Hierarchy Level	[edit security application-firewall rule-sets <i>rule-set-name</i> rule <i>rule-name</i> match]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the dynamic application group to match.
Options	<i>system-application-group</i> —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	<ul style="list-style-type: none"> • Application Firewall Overview on page 107

enable-flow-tracing (Services)

Supported Platforms [SRX Series, vSRX](#)

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.

Description Enable flow tracing for the profile. This statement is supported on the SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

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 on page 73](#)
- [Configuring SSL Proxy on page 83](#)
- [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

enable-performance-mode

Supported Platforms [SRX Series, vSRX](#)

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 with default packet inspection limit as two packets, including both client-to-server and server-to-client directions.

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 on page 70](#)
- [show services application-identification status on page 366](#)

enable-session-cache

Supported Platforms	SRX Series, vSRX
Syntax	enable-session-cache;
Hierarchy Level	[edit services ssl termination profile <i>profile-name</i>] [edit services ssl initiation profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10. This statement is supp
Description	Enable SSL session cache. This statement is supported on the SRX550M, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.
Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• SSL Proxy Overview on page 73• Configuring SSL Proxy on page 83• Enabling Debugging and Tracing for SSL Proxy on page 105

file (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax `file file-name; {
files;
match;
no-world-readable size;
world-readable;
}`

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 trace file information. This statement is supported on the SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX.

- Options**
- **files**—Specify the maximum number of trace files. Range: 2 through 1000.
 - **match**—Specify the regular expression for lines to be logged.
 - **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.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- [Configuring SSL Proxy on page 83](#)

files (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax `files files;`

Hierarchy Level `[edit services ssl traceoptions file file-name]`

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the maximum number of trace files.

Options `files`—Specify the maximum number of trace files.

Range: 2 through 1000

Required Privilege Level `services`—To view this statement in the configuration.
`services-control`—To add this statement to the configuration.

Related Documentation

- [Configuring SSL Proxy on page 83](#)

file (System Logging)

Supported Platforms M Series, MX Series, SRX Series, T Series

Syntax

```
file filename {
    allow-duplicates;
    any (alert | any | critical | emergency | error | info | none | notice | warning);
    archive {
        archive-sites {
            url password;
        }
        (binary-data | no-binary-data);
        files number;
        size size;
        start-time start-time;
        transfer-interval transfer-interval;
        (world-readable | no-world-readable);
    }
    authorization (alert | any | critical | emergency | error | info | none | notice | warning);
    change-log (alert | any | critical | emergency | error | info | none | notice | warning);
    conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);
    daemon (alert | any | critical | emergency | error | info | none | notice | warning);
    dfc (alert | any | critical | emergency | error | info | none | notice | warning);
    explicit-priority;
    external (alert | any | critical | emergency | error | info | none | notice | warning);
    firewall (alert | any | critical | emergency | error | info | none | notice | warning);
    ftp (alert | any | critical | emergency | error | info | none | notice | warning);
    interactive-commands (alert | any | critical | emergency | error | info | none | notice | warning);
    kernel (alert | any | critical | emergency | error | info | none | notice | warning);
    match "regular-expression";
    ntp (alert | any | critical | emergency | error | info | none | notice | warning);
    pfe (alert | any | critical | emergency | error | info | none | notice | warning);
    security (alert | any | critical | emergency | error | info | none | notice | warning);
    structured-data {
        brief;
    }
    user (alert | any | critical | emergency | error | info | none | notice | warning);
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description Specify the file in which to log data.

- Options**
- *filename*—Specify the name of the file in which to log data.
 - *allow-duplicates*—Do not suppress the repeated messages.
 - *any*—Specify all facilities information.
 - *alert*—Specify the conditions that should be corrected immediately.

- *critical*—Specify the critical conditions.
- *emergency*—Specify the conditions that cause security functions to stop.
- *error*—Specify the general error conditions.
- *info*—Specify the information about normal security operations.
- *none*—Do not specify any messages.
- *notice*—Specify the conditions that should be handled specifically.
- *warning*—Specify the general warning conditions.
- *archive*—Specify the archive file information.
 - *archive-sites*—Specify a list of destination URLs for the archived log files.
 - *url*—Specify the primary and failover URLs to receive archive files.
 - *binary-data*—Mark file such that it contains binary data.
 - *no-binary-data*—Do not mark the file such that it contains binary data.
 - *files*—Specify the number of files to be archived. Range: 1 through 1000 files.
 - *size*—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
 - *world-readable*—Allow any user to read the log file.
 - *no-world-readable*—Do not allow any user to read the log file.
 - *start-time*—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
 - *transfer-interval*—Specify the frequency at which to transfer the files to archive sites.
- *authorization*—Specify the authorization system.
- *change-log*—Specify the configuration change log.
- *conflict-log*—Specify the configuration conflict log.
- *daemon*—Specify the various system processes.
- *dfc*—Specify the dynamic flow capture.
- *explicit-priority*—Include the priority and facility in messages.
- *external*—Specify the local external applications.
- *firewall*—Specify the firewall filtering system.
- *ftp*—Specify the FTP process.
- *interactive-commands*—Specify the commands executed by the UI.
- *kernel*—Specify the kernel information.
- *match*—Specify the regular expression for lines to be logged.
- *ntp*—Specify the NTP process.

- *pfe*—Specify the Packet Forwarding Engine.
- *security*—Specify the security-related information.
- *structured-data*—Log the messages in structured log format.
 - *brief*—Omit English language text from the end of the logged message.
- *user*—Specify the user processes.
 - *info*—Specify the informational messages.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

first-update

Supported Platforms [SRX Series, vSRX](#)

Syntax first-update;

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Junos OS Release 10.2.

Description Generate an AppTrack start message when a new session begins. (A final message is produced at session end with any option.) This option overrides the **first-update-interval** option if both are specified.

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppTrack on page 127](#)

first-update-interval

Supported Platforms [SRX Series, vSRX](#)

Syntax `first-update-interval first-update-interval;`

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Junos OS Release 10.2.

Description For long-lived sessions being monitored by AppTrack, configure this value to issue the first update message after a specified number of minutes.



NOTE: The `first-update-interval` setting is disregarded if the `first-update` option is set to log the first message at session start.

Options *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

Required Privilege Level `security`—To view this statement in the configuration.
`security-control`—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppTrack on page 127](#)

flag (Services)

Supported Platforms [SRX Series, vSRX](#)

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 Proxy on page 83](#)

format (Security Log)

Supported Platforms [SRX Series, vSRX](#)

Syntax format (binary | sd-syslog | syslog)

Hierarchy Level [edit security log]

Release Information Statement introduced prior to Junos OS Release 10.0. Statement updated in Junos OS Release 12.1.

Description Set the default log format for event mode security logging on the device.

- Options**
- **binary**—Binary encoded text to conserve resources.
 - **sd-syslog**—Structured system log file.
 - **syslog**—Traditional system log file.

Default: syslog.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [log \(Security\) on page 215](#)

forwarding-classes (CoS)

Supported Platforms SRX Series, vSRX

Syntax

```
forwarding-classes {
  class class-name {
    priority (high | low);
    queue-num number;
    spu-priority (high | low | medium-high | medium-low);
  }
  queue queue-number {
    class-name {
      priority (high | low);
    }
  }
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Junos OS Release 8.5. Statement updated in Junos OS Release 11.4. The **spu-priority** option introduced in Junos OS Release 11.4R2.

Description Configure forwarding classes and assign queue numbers.

Options

- **class *class-name***—Display the forwarding class name assigned to the internal queue number.



NOTE: This option is supported only on SRX1500, SRX5400, SRX5600, and SRX5800.



NOTE: AppQoS forwarding classes must be different from those defined for interface-based rewriters.

- **priority**—Fabric priority value:
 - **high**—Forwarding class' fabric queuing has high priority.
 - **low**—Forwarding class' fabric queuing has low priority.

The default **priority** is **low**.

- **queue *queue-number***—Specify the internal queue number to which a forwarding class is assigned.
- **spu-priority**—Services Processing Unit (SPU) priority queue, **high**, **medium-high**, **medium-low**, or **low**. The default **spu-priority** is **low**.



NOTE: The `spu-priority` option is only supported on SRX1500 devices and SRX5000 line devices.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppQoS on page 141](#)

global-config (Services)

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800, vSRX](#)

Syntax

```
global-config {  
    session-cache-timeout seconds;  
}
```

Hierarchy Level [edit services ssl proxy]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the global proxy configuration.

Options *session-cache-timeout*—Specify the session cache timeout.

Range: 300 to 3600 seconds

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- [SSL Proxy Overview on page 73](#)
- [Configuring SSL Proxy on page 83](#)
- [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

icmp-mapping (Application Identification)

Supported Platforms [SRX Series](#)

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. 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.

- Options**
- **code *number***—Numeric value of an ICMP code. The code field provides further information about the associated type field.
 - **type *number***—Numeric value of an ICMP type. The type field identifies the ICMP message.

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 on page 49](#)

ip (Application Identification)

Supported Platforms	SRX Series
Syntax	<code>ip <i>ip-address-and-prefix-length</i>;</code>
Hierarchy Level	[edit services application-identification application <i>application-name</i> address-mapping <i>address-name</i> filter]
Release Information	Statement introduced in Junos OS Release 15.1X49-D40.
Description	Specify the IP address and the prefix length of the application for address mapping.
Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Junos OS Application Identification Custom Application Signatures on page 49

ip-protocol-mapping (Application Identification)

Supported Platforms	SRX Series
Syntax	<code>ip-protocol-mapping { protocol <i>number</i>; }</code>
Hierarchy Level	[edit services application-identification application <i>application-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1X49-D40.
Description	Specify the IP protocol value for an application to match. Standard IP protocol numbers can map an application to IP traffic. As with address mapping, to ensure adequate security, use IP protocol mapping only in your private network for trusted servers.
Options	protocol <i>number</i> —Numeric value of an IP protocol
Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Junos OS Application Identification Custom Application Signatures on page 49

initiation (Services)

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
initiation {
  profile profile-name {
    actions {
      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] );
  }
}
```

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.

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 Proxy on page 83](#)
- [Firewall User Authentication Overview](#)

level (Services)

Supported Platforms [SRX Series](#), [vSRX](#)

Syntax `level [brief | detail | extensive | verbose];`

Hierarchy Level `[edit services ssl traceoptions]`

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the level of debugging the output. This statement is supported on the SRX550M, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

- Options**
- *brief*—Specify brief debugging output.
 - *detail*—Specify detailed debugging output.
 - *extensive*—Specify extensive debugging output.
 - *verbose*—Specify verbose debugging output.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- [Configuring SSL Proxy on page 83](#)

log (Security)

Supported Platforms [SRX Series, vSRX](#)

```
Syntax log {
    cache {
        exclude exclude-name {
            destination-address destination-address;
            destination-port destination-port;
            event-id event-id;
            failure;
            interface-name interface-name;
            policy-name policy-name;
            process process-name;
            protocol protocol;
            source-address source-address;
            source-port source-port;
            success;
            user-name user-name;
        }
        limit value;
    }
    disable;
    event-rate rate;
    facility-override (authorization | daemon | ftp | kernel | local | user);
    file {
        files max-file-number;
        name file-name;
        path binary-log-file-path;
        size maximum-file-size;
    }
    format (binary | sd-syslog | syslog);
    max-database-record <max-database-record>;
    mode (event | stream);
    rate-cap <rate-cap-value>;
    report;
    (source-address source-address | source-interface interface-name);
    stream stream-name {
        category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp
            | rtlog | pst-ds-lite | appqos | secintel);
        file {
            name file-name;
            size file-size;
            rotation max-rotation-number;
        }
        filter {
            threat-attack;
        }
        format (binary | sd-syslog | syslog | welf);
        host {
            ip-address;
            port port-number;
        }
        rate-limit {
```

```
        log-rate;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag (all | configuration | hpl | report | source);
    no-remote-trace;
}
transport {
    protocol (udp | tcp | tls);
    tcp-connections tcp-connections;
    tls-profile tls-profile-name;
}
utc-timestamp;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

Options **cache**—Cache security log events in the audit log buffer.

disable—Disable the security logging for the device.

event-rate **rate**—Limit the rate at which logs are streamed per second.

Range: 0 through 1500

Default: 1500

facility-override—Alternate facility for logging to remote host.

file—Specify the security log file options for logs in binary format.

Values:

- **max-file-number**—Maximum number of binary log files.
 - The range is 2 through 10 and the default value is 10.
- **file-name**—Name of binary log file.
- **binary-log-file-path**—Path to binary log files.
- **maximum-file-size**—Maximum size of binary log file in megabytes.
 - The range is 1 through 10 and the default value is 10.

format—Set the security log format for the device.

max-database-record—The following are the disk usage range limits for the database:

Range:

- SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
- vSRX: 0 through 1,000,000

Default:

- SRX1500, SRX4100, and SRX4200: 15,000,000
- vSRX: 1,000,000



NOTE: Be sure there is enough free space in `/var/log/hostlogs/`, otherwise logs might be dropped when written into the database.

mode—Control how security logs are processed and exported.

rate-cap **rate-cap-value**—Work with event mode only. This option limits the rate at which data plane logs are generated per second.

Range: 0 through 5000 logs per second

Default: 5000 logs per second

source-address **source-address**—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface *interface-name*—Specify a source interface name, which is mandatory to configure *stream host*.



NOTE: The **source-address** and **source-interface** are alternate values. Using one of the options is mandatory.

stream—Every stream can configure file or host.

- **category**— Type of events that might be logged.
- **file name**—Specify the filename.
- **file size**—Specify the file size.
 - SRX1500, SRX4100, and SRX4200—The default value is 25 MB and the range is 10 MB through 50 MB.
 - vSRX - The default value is 2 MB and the range is 1 MB through 3 MB.
- **rotation**—Configure the maximum file number for rotation.
 - The default value is 10 and the range is 2 through 19.
- **rate-limit**—Rate-limit for security logs.
 - The range is 1 through 65,535 logs per second and the default value is 65,535 .
- **filter**—Selects the filter to filter the logs to be logged.
- **format**—Specify the log stream format.
- **host**—Destination to send security logs.
- **severity**—Severity threshold for security logs.

traceoptions—Specify security log daemon trace options.

transport—Set security log transport settings.

utc-timestamp—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level	security—To view this statement in the configuration.
	security-control—To add this statement to the configuration.

log (Services)

Supported Platforms [SRX Series, vSRX](#)

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.

- 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 Proxy on page 83](#)

match (Services)

Supported Platforms	SRX Series , vSRX
Syntax	<code>match <i>match</i>;</code>
Hierarchy Level	[edit services ssl traceoptions file <i>file-name</i>]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	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.
Options	match —Specify the regular expression for lines to be logged.
Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SSL Proxy on page 83

no-application-identification (Services)

Supported Platforms	SRX Series , vSRX
Syntax	<code>no-application-identification;</code>
Hierarchy Level	[edit services application-identification]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Disable the TCP/UDP application identification of applications running on nonstandard ports.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Disabling and Reenabling Junos OS Application Identification on page 48

no-application-system-cache (Services)

Supported Platforms [SRX Series, vSRX](#)

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.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Deactivating Application System Cache Information for Application Identification \(CLI Procedure\)](#) on page 66

no-remote-trace (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax no-remote-trace;

Hierarchy Level [edit services ssl traceoptions]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Disable remote tracing.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- [Configuring SSL Proxy](#) on page 83

over (Application Identification)

Supported Platforms [SRX Series](#)

Syntax

```
over protocol-type {
    signature name {
        member name {
            context {
                http-get-url-parsed-param-parsed;
                http-header-content-type;
                http-header-cookie;
                http-header-host;
                http-header-user-agent;
                http-post-url-parsed-param-parsed;
                http-post-variable-parsed ;
                http-url-parsed;
                http-url-parsed-param-parsed;
                ssl-server-name;
                stream;
            }
            direction {
                any;
                client-to-server;
                server-to-client;
            }
            pattern pattern;
        }
    }
    port-range value;
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Junos OS Release 15.1X49-D40.

Description Specify application running over TCP, UDP, or Layer 7.

Options

signature *name* —Name of the custom application signature. Must be a unique name with a maximum length of 63 characters.

member *name* —Member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01 through m15.)

context—Service-specific context, such as http-header-content-type.

direction—Connection direction of the packets to match pattern

patterns—(Optional) Deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature. Maximum length is 128.

port-range—Port range. This option is applicable for TCP or UDP-based applications only.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Understanding Junos OS Application Identification Custom Application Signatures on page 49
------------------------------	--

policies

Supported Platforms [SRX Series, vSRX](#)

```
Syntax policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-identity {
          [role-name];
          any;
          authenticated-user;
          unauthenticated-user;
          unknown-user;
        }
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
          application-firewall {
            rule-set rule-set-name;
          }
          application-traffic-control {
            rule-set rule-set-name;
          }
        }
      }
    }
  }
}
```

```

    }
    gprs-gtp-profile profile-name;
    gprs-sctp-profile profile-name;
    idp;
    redirect-wx | reverse-redirect-wx;
    ssl-proxy {
        profile-name profile-name;
    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    user-firewall {
        access-profile profile-name;
        domain domain-name;
        ssl-termination-profile profile-name;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    sequence-check-required;
    syn-check-required;
}
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
}
reject;
}
}
global {
    policy policy-name {
        description description;
        match {
            application {
                [application];
                any;
            }
        }
    }
}

```

```
}
destination-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
from-zone {
    [zone-name];
    any;
}
source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
source-identity {
    [role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
}
to-zone {
    [zone-name];
    any;
}
}
scheduler-name scheduler-name;
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
            profile-name profile-name;
        }
    }
}
```

```

    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    initial-tcp-mss mss-value;
    reverse-tcp-mss mss-value;
    sequence-check-required;
    syn-check-required;
}
}
reject;
}
}
}
policy-rematch;
policy-stats {
    system-wide (disable | enable) ;
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
}

```

Hierarchy Level [edit security]

Release Information	<p>Statement introduced in Junos OS Release 8.5.</p> <p>Support for the services-offload option added in Junos OS Release 11.4.</p> <p>Support for the source-identity option added in Junos OS Release 12.1.</p> <p>Support for the description option added in Junos OS Release 12.1.</p> <p>Support for the ssl-termination-profile and web-redirect-to-https options added on SRX5400, SRX5600, and SRX5800 devices starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40.</p> <p>Support for the user-firewall option added in Junos OS Release 12.1X45-D10.</p> <p>Support for the domain option, and for the from-zone and to-zone global policy match options, added in Junos OS Release 12.1X47-D10.</p> <p>Support for the initial-tcp-mss and reverse-tcp-mss options added in Junos OS Release 12.3X48-D20. Support for the extensive option for policy-rematch added in Junos OS Release 15.1X49-D20.</p>
Description	Configure network security policies.
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Security Policies Overview</i>

policy (Security Policies)

Supported Platforms [SRX Series, vSRX](#)

Syntax `policy policy-name {
 description description;
 match {
 application {
 [application];
 any;
 }
 destination-address {
 [address];
 any;
 any-ipv4;
 any-ipv6;
 }
 source-address {
 [address];
 any;
 any-ipv4;
 any-ipv6;
 }
 source-identity {
 [role-name];
 any;
 authenticated-user;
 unauthenticated-user;
 unknown-user;
 }
 }
 scheduler-name scheduler-name;
 then {
 count {
 alarm {
 per-minute-threshold number;
 per-second-threshold number;
 }
 }
 deny;
 log {
 session-close;
 session-init;
 }
 permit {
 application-services {
 application-firewall {
 rule-set rule-set-name;
 }
 application-traffic-control {
 rule-set rule-set-name;
 }
 gprs-gtp-profile profile-name;
 gprs-sctp-profile profile-name;
 }
 }
}`

```

idp;
redirect-wx | reverse-redirect-wx;
ssl-proxy {
    profile-name profile-name;
}
uac-policy {
    captive-portal captive-portal;
}
utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        web-redirect;
    }
    user-firewall {
        access-profile profile-name;
        domain domain-name;
        ssl-termination-profile profile-name;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    initial-tcp-mss mss-value;
    reverse-tcp-mss mss-value;
    sequence-check-required;
    syn-check-required;
}
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
}
reject;
}
}

```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 8.5. The **services-offload** option added in Junos OS Release 11.4. Statement updated with the **source-identity** option and the **description** option added in Junos OS Release 12.1. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.

Description	Define a security policy.
Options	<p><i>policy-name</i>—Name of the security policy.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring SSL Proxy on page 83 • Security Policies Overview

port-range (Application Identification)

Supported Platforms	SRX Series
Syntax	<pre>port-range { tcp [port]; udp [port]; }</pre>
Hierarchy Level	[edit services application-identification application <i>application-name</i> address-mapping <i>address-name</i> filter]
Release Information	Statement introduced in Junos OS Release 15.1X49-D40.
Description	Specify a port to match a TCP or UDP destination port.
Options	<ul style="list-style-type: none"> • tcp [port]—Define the TCP port range for the application. • udp [port]—Define the UDP port range for the application.
Required Privilege Level	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Junos OS Application Identification Custom Application Signatures on page 49

preferred-ciphers

Supported Platforms [SRX Series, vSRX](#)

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 the preferred ciphers.

- 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 on page 73](#)

profile (Application Firewall)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
profile profile-name {
  block-message type {
    custom-text content custom-html-text;
    custom-redirect-url content custom-redirect-url;
  }
}
```

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. You can display a default or custom message, or redirect traffic to a URL where an explanation or further action is provided.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- [Application Firewall Overview on page 107](#)

profile (Rule Sets)

Supported Platforms [SRX Series, vSRX](#)

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.

Options *profile-name*—Name of the block-message profile to be used for this rule set.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Application Firewall Overview on page 107](#)

profile (Services)

Supported Platforms SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
profile profile-name {
  actions {
    crt {
      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 proxy]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The `crt` statement is supported from 15.1X49-D30.

Description Specify the SSL server profile.

Options *profile-name*—Specify the profile identifier.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

- Related Documentation**
- [SSL Proxy Overview on page 73](#)
 - [Configuring SSL Proxy on page 83](#)
 - [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

profile (SSL Initiation)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
profile profile-name {  
    actions {  
        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] );  
}
```

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.

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 Proxy on page 83](#)
 - [Firewall User Authentication Overview](#)

profile (SSL Termination)

Supported Platforms [SRX Series, vSRX](#)

Syntax `profile profile-name {
 custom-ciphers [cipher];
 enable-flow-tracing;
 enable-session-cache;
 preferred-ciphers (custom | medium | strong | weak);
 protocol-version (all | tls1 | tls11 | tls12);
 server-certificate certificate-identifier;
 }`

Hierarchy Level [edit services ssl 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.

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 Proxy on page 83](#)
- [Firewall User Authentication Overview](#)

protocol-version

Supported Platforms [SRX Series, vSRX](#)

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.

- 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 on page 73](#)

proxy (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```

proxy {
  global-config {
    session-cache-timeout seconds;
  }
  profile profile-name {
    actions {
      crt {
        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 **crt** 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 services—To view this statement in the configuration.
Level services-control—To add this statement to the configuration.

Related • [SSL Proxy Overview on page 73](#)
Documentation • [Configuring SSL Proxy on page 83](#)
• [Enabling Debugging and Tracing for SSL Proxy on page 105](#)

rate-limiters

Syntax

```
rate-limiters {
    rate-limiter-name {
        bandwidth-limit value-in-kbps;
        burst-size-limit value-in-bytes;
    }
}
```

Hierarchy Level [edit class-of-service application-traffic-control]

Release Information Statement introduced in Junos OS Release 11.4.

Description Share the available bandwidth and burst size of a device's PICs by defining rate limiter profiles and applying them in AppQoS rules.

Options

- **rate-limiter-name**—Name of the rate limiter. It is applied in AppQoS rules to share device resources based on quality-of-service requirements.

The combination of rate limiting parameters, namely bandwidth-limit and burst-size-limit rate limit, make up the rate limiter profile. A maximum of 16 profiles are allowed per device. The same profile can be used by multiple rate limiters. For example, a profile with a bandwidth-limit of 200 Kbps and a burst-limit of 130,000 bytes, could be used in several rate limiters.

A maximum of 1000 rate limiters can be created. Rate limiters are defined for the device, and are assigned in rules in a rule set. A single rate limiter can be used multiple times within the same rule set. However, the rate limiter cannot be used in another rule set.

- **bandwidth-limit value-in-Kbps**—Maximum number of kilobits to be transmitted per second for this rate limiter. Up to 2 GB of bandwidth can be provisioned among multiple rate limiters to share the resource proportionally.
- **burst-size-limit value-in-bytes**—Maximum number of bytes to be transferred in a single burst or time-slice. This limit ensures that a high-priority transmission does not keep a lower priority transmission from transmitting.



NOTE: The number of bandwidth-limit and burst-size-limit combinations cannot exceed 16.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppQoS on page 141](#)

renegotiation (Services)

Supported Platforms	SRX1500, SRX5400, SRX5600, SRX5800, vSRX
Syntax	renegotiation (allow allow-secure drop);
Hierarchy Level	[edit services ssl proxy profile <i>profile-name</i> actions]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify the renegotiation options.
Options	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Configuring SSL Proxy on page 83

root-ca (Services)

Supported Platforms	SRX Series, vSRX
Syntax	root-ca <i>root-certificate</i> ;
Hierarchy Level	[edit services ssl proxy profile <i>profile-name</i>] [edit services ssl termination profile <i>profile-name</i>]
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	<i>root-ca-name</i> —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	<ul style="list-style-type: none">• Configuring SSL Proxy on page 83• Firewall User Authentication Overview

routing-instance (Advanced Policy-Based Routing)

Supported Platforms [SRX Series, vSRX](#)

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 on page 152](#)
- [Understanding Advanced Policy-Based Routing on page 149](#)

rule (Advanced Policy-Based Routing)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
rule rule-name {  
    match {  
        dynamic-application [system-application];  
        dynamic-application-group [system-application-group];  
    }  
    then {  
        routing-instance name ;  
    }  
}
```

Hierarchy Level [edit security advance-policy-based-routing profile *profile-name*]

Description Configure rules for the advanced policy-based routing (APBR) profile (application profile). Associate the rule with one or more than one applications (example: for HTTP) or application groups.

The deep packet inspection and pattern matching capabilities of AppID to identify application traffic and application system cache (ASC) is consulted to get application type for matching the rule condition.

If the application matches any of the application or application groups of a rule in a profile, the application profile rule is considered as a match and the traffic will be redirected to the defined routing instance for the route lookup.

Options **match**—Define an APBR term as dynamic application or dynamic application group for match criteria.

then—Define the action for matching condition by specifying the name of the routing instance for redirecting traffic.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152](#)
- [Understanding Advanced Policy-Based Routing on page 149](#)

rule-sets (CoS AppQoS)

```
Syntax  rule-sets {
        rule-set-name {
            rule rule-name {
                match {
                    application application-name;
                    application-any;
                    application-group application-group-name;
                    application-known;
                    application-unknown;
                }
                then {
                    dscp-code-point dscp-value ;
                    forwarding-class forwarding-class-name;
                    log;
                    loss-priority [ high | medium-high | medium-low | low ];
                    rate-limit {
                        loss-priority-high;
                        client-to-server rate-limiter-name;
                        server-to-client rate-limiter-name;
                    }
                }
            }
        }
    }
```

Hierarchy Level [edit class-of-service application-traffic-control]

Release Information Statement introduced in Junos OS Release 11.4.

Description Defines AppQoS rule sets and the rules that establish priorities based on quality-of-service requirements for the associated applications. AppQoS rules can be included in policy statements to implement application-aware quality of service control.

- Options**
- **rule-set-name**—Name used to refer to a collection of AppQoS rules.
 - **rule rule-name**—Name applied to the match criteria and resulting actions that control the quality-of-service provided to any matching applications.
 - **application application-name**—Name of the application to be used as match criteria for the rule.
 - **application-any**—Any application encountering this rule. Note that when you use this specification, all application matching ends. Any application rule following this one will never be encountered.
 - **application-group application-group-name**—Group of applications to be used as match criteria for the rule. Both applications and application groups can be match criteria for a single rule.

- **application-known**—Match criteria specifying any session that is identified, but its corresponding application is not specified.
- **application-unknown**—Match criteria specifying any session that is not identified.
- **forwarding-class *forwarding-class-name***—The AppQoS class with which matching applications will be marked. This field identifies the rewriter that has marked the DSCP value. Therefore, the AppQoS forwarding class must be different from those used by IDP or firewall filters. With this class specified, firewall filter class will not overwrite the existing DSCP value.
- **dscp-code-point**—DSCP alias or bit map with which matching applications will be marked to establish the output queue. This value can be marked by rewriters from IDP, AppQoS, or a firewall filter. The forwarding-class value identifies which rewriter has re-marked the packet with the current DSCP value. If a packet triggers all three rewriters, IDP takes precedence over AppQoS, which takes precedence over a firewall filter.
- **loss-priority**—Loss priority with which matching applications will be marked. This value is used to determine the likelihood that a packet would be dropped when encountering congestion. A high loss priority means that there is an 80% chance of packet loss in congestion. Possible values are high, medium-high, medium-low and low.
- **rate-limit**—Rate limiters to be associated with client-to-server and with server-to-client traffic for this application. The rate limiter profile defines maximum speed and volume limits for matching applications.
- **log**—AppQoS event logging.

Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	• Example: Configuring AppQoS on page 141
------------------------------	---

rule-sets (Security Application Firewall)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
rule-sets rule-set-name {
  default-rule {
    (deny [block-message] | permit | reject [block-message]);
  }
  profile profile-name;
  rule rule-name {
    match {
      dynamic-application [system-application];
      dynamic-application-groups [system-application-group];
      ssl-encryption (any | yes | no);
    }
    then {
      (deny [block-message] | permit | reject [block-message]);
    }
  }
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 to include the **ssl-encryption** and **reject** options. The **block-message** options added in Junos OS Release 12.1X45-D10.

Description Configure the set of rules for the application firewall.

Options *rule-set-name*—Name of the rule set.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring an Application Group for Application Firewall on page 116](#)

security-zone

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
security-zone zone-name {
  address-book {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
      range-address lower-limit to upper-limit;
      wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
      address address-name;
      address-set address-set-name;
      description text;
    }
  }
  advance-policy-based-routing;
  application-tracking;
  description text;
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
  }
  system-services service-name {
    except;
  }
}
interfaces interface-name {
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
  }
  system-services service-name {
    except;
  }
}
screen screen-name;
tcp-rst;
}
```

Hierarchy Level [edit security zones]

Release Information Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description	Define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.
Options	<p><i>zone-name</i> —Name of the security zone.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Security Zones and Interfaces Overview • Example: Configuring Application Firewall Rule Sets Within a Security Policy on page 112

server-certificate (Services)

Supported Platforms	SRX Series , vSRX
Syntax	server-certificate <i>server-certificate</i> ;
Hierarchy Level	[edit services ssl termination profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify the local certificate identifier. This statement is supported on the SRX1500, SRX5400, SRX5600, and SRX5800 devices and vSRX.
Options	<i>server-certificate</i> —Specify the name of the local certificate identifier.
Required Privilege Level	<p>services—To view this statement in the configuration.</p> <p>services-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring SSL Proxy on page 83 • Firewall User Authentication Overview

session-update-interval

Supported Platforms [SRX Series, vSRX](#)

Syntax `session-update-interval session-update-interval;`

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure the interval between session update messages for long-lived sessions being monitored by AppTrack. Byte count, packet count, and start and end times are updated and logged when the amount of time between session start or the previous update and the current time exceeds the interval.

Options *session-update-interval*—Minutes between updates.
Default: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring AppTrack on page 127](#)

size (Services)

Supported Platforms [SRX Series, vSRX](#)

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 Proxy on page 83](#)
- [Firewall User Authentication Overview](#)

ssl (Services)

Supported Platforms [SRX Series, vSRX](#)

```
Syntax  ssl {
        initiation {
            profile profile-name {
                actions {
                    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 Proxy on page 83](#)
- [Firewall User Authentication Overview](#)

ssl-encryption

Supported Platforms	SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, vSRX
Syntax	ssl-encryption (any no yes);
Hierarchy Level	[edit security application-firewall rule-sets <i>rule-set-name</i> rule <i>rule-name</i> 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.
Options	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Configuring SSL Proxy on page 83

ssl-proxy (Application Services)

Supported Platforms [SRX Series](#)

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 security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation

- [Configuring SSL Proxy on page 83](#)

statistics (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
statistics {  
    interval interval-number;  
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the interval, in minutes, for statistics collection.

Options *interval interval-number*—Length of time, in minutes, that application statistics are collected.

Range: 1 through 1440 minutes

Default: 1 minute



NOTE: For SRX Series devices, the maximum number of interval periods for which statistics are stored is 8.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- [Onbox Application Identification Statistics on page 69](#)

stream (Security Log)

Supported Platforms SRX Series, vSRX

Syntax

```
stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp |
        rtlog | pst-ds-lite | appqos | secintel);
    file {
        name file-name;
        size file-size;
        rotation max-rotation-number;
    }
    filter {
        threat-attack;
    }
    format (binary | sd-syslog | syslog | welf);
    host {
        ip-address;
        port port-number;
    }
    rate-limit {
        log-rate;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
}
```

Hierarchy Level [edit security log]

Release Information Statement modified in Junos OS Release 9.2.

Description Defines the TWAMP server configuration settings.

Options **stream**—Every stream can configure file or host.

Values:

- **category**—Type of events that may be logged.
- **file-name**—Specify the file name.
- **file-size**—Specify the file size.
 - SRX1500, SRX4100, and SRX4200- The default value is 25M and the range is 10M through 50M.
 - vSRX - The default value is 2M and the range is 1M through 3M.
- **rotation**—Configure the max file number for rotation.
 - The default value is 10 and the range is 2 through 19.
- **rate-limit**—Rate-limit for security logs.
 - The range is 1 through 65535 logs per second and the default value is 65535 .

- **filter**—Selects the filter to filter the logs to be logged.
- **format**—Specify the log stream format.
- **host**—Destination to send security logs.
- **severity**—Severity threshold for security logs.

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	<ul style="list-style-type: none"> • Example: Configuring AppTrack on page 127 • <i>category (Security Logging)</i>

termination (Services)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```

termination {
  profile profile-name {
    custom-ciphers [cipher];
    enable-flow-tracing;
    enable-session-cache;
    preferred-ciphers (custom | medium | strong | weak);
    protocol-version (all | tls1 | tls11 | tls12);
    server-certificate certificate-identifier;
  }
}
```

Hierarchy Level [edit services ssl]

Release Information Statement introduced in Junos OS Release 12.1X44-D10. The **protocol-version** statement is updated to include **tls11** and **tls12** from Junos OS Release 15.1X49-D30.

Description Specify the configuration for Secure Socket Layer (SSL) termination support service.

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 Proxy on page 83](#)
- *Firewall User Authentication Overview*

then (Security Application Firewall)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
then {
    (deny [block-message] | permit | reject [block-message]);
}
```

Hierarchy Level [edit security application-firewall rule-set *rule-set-name* rule *rule-name*]

Release Information Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 with the **reject** option. The **block-message** option added in Junos OS Release 12.1X45-D10.

Description Specify the action to be performed when traffic matches the associated match criteria.

Note that an application firewall is applied after a session has already been created by the security firewall. When traffic is rejected or denied by an application firewall, therefore, logs contain a session open message, a session reject or deny message, and a session close message.

- Options**
- **deny**—Block the traffic at the firewall. The device drops the packet. By default, no message is returned to the sender.
 - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for denied HTTP or HTTPS traffic. All other traffic is dropped silently.
 - **permit**—Permit traffic at the firewall.
 - **reject**—Block the traffic at the firewall. For TCP traffic, by default the device drops the packet and returns a TCP reset (RST) message to the source host. For UDP and other protocol traffic, by default the device drops the packet and returns an ICMP “destination unreachable, port unreachable” message to both the client and the server.
 - **block-message**—(Optional) In application firewall rules, provide information to the user regarding blocked traffic. Depending on the content of the **profile** option for this rule set, including the **block-message** option displays a default message or customized message, or redirects the user for rejected HTTP or HTTPS traffic. All other traffic is dropped as specified in the default action for the **reject** option.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring an Application Group for Application Firewall on page 116](#)

trusted-ca (Services)

Supported Platforms [SRX Series, vSRX](#)

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 Proxy on page 83](#)
 - [Firewall User Authentication Overview](#)

traceoptions (advanced policy-based routing)

Supported Platforms SRX Series, vSRX

Syntax

```

traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}

```

Hierarchy Level [edit security advance-policy-based-routing]

Release Information Statement introduced in Junos OS Release 15.1X49-D60.

Description Configure tracing operations for advanced policy-based routing.

Options

- file**—Configure the trace file options.

- filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. By default, the name of the file is the name of the process being traced.
- files *number***—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files

- match *regular-expression***—Refine the output to include lines that contain the regular expression.
- size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: **x K** to specify KB, **x m** to specify MB, or **x g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
 - **all**—Trace with all flags enabled
 - **compilation**—Trace rule set compilation events
 - **configuration**—Trace configuration events
 - **ipc**—Trace process inter communication events
 - **lookup**—Trace rule set lookup events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege	services—To view this statement in the configuration.
Level	services-control—To add this statement to the configuration.

- | | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152• Understanding Advanced Policy-Based Routing on page 149 |
|------------------------------|--|

traceoptions (Security Application Firewall)

Supported Platforms SRX Series, vSRX

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure trace options for the application firewall.

- Options**
- **file**—Configure the trace file options.
 - **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. By default, the name of the file is the name of the process being traced.
 - **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files
 - **match regular-expression**—Refine the output to include lines that contain the regular expression.
 - **size maximum-file-size**—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
- If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: **x K** to specify KB, **x m** to specify MB, or **x g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
 - **all**—Trace with all flags enabled
 - **compilation**—Trace rule set compilation events
 - **configuration**—Trace configuration events
 - **ipc**—Trace process inter communication events
 - **lookup**—Trace rule set lookup events
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Application Firewall Overview on page 107
------------------------------	---

traceoptions (Services Application Identification)

Supported Platforms SRX Series, vSRX

Syntax

```
traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag all;
  level (all | error | info | notice | verbose | warning)
  no-remote-trace;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure tracing operations for application identification services.

- Options**
- **file**—Configure the trace file options.
 - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
 - ***files number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file.0***, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files
 - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
 - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the ***trace-file*** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: **x K** to specify KB, **x m** to specify MB, or **x g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
 - all**—Trace with all flags enabled.
- **level**—Set the level of debugging the output option.
 - **all**—Match all levels.
 - **error**—Match error conditions.
 - **info**—Match informational messages.
 - **notice**—Match conditions that should be handled specially
 - **verbose**—Match verbose messages.
 - **warning**—Match warning messages.
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Understanding Application Identification Techniques on page 23
------------------------------	--

traceoptions (Services SSL)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level [brief | detail | extensive | verbose];
  no-remote-trace;
}
```

Hierarchy Level [edit services ssl]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the trace file information. This statement is supported on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX.

- 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.
 - **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 with all flags enabled
 - **compilation**—Trace rule set compilation events
 - **configuration**—Trace configuration events
 - **ipc**—Trace process inter communication events
 - **lookup**—Trace rule set lookup events
 - **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.

Required Privilege	services—To view this statement in the configuration.
Level	services-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Configuring SSL Proxy on page 83• <i>Firewall User Authentication Overview</i>
------------------------------	---

transport (Security Log)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
transport {
  protocol (udp | tcp | tls);
  tls-profile tls-profile-name;
  tcp-connections tcp-connections;
}
```

Hierarchy Level [edit security log]

Release Information Statement introduced in Junos OS Release 12.1X46-D25.

Description Configure security log transport options.

Options **protocol**—Specify the type of transport protocol to be used to log the data.

- **UDP**—Set the transport protocol to UDP.
- **TCP**—Set the transport protocol to TCP.
- **TLS**—Set the transport protocol to TLS.

Default: UDP.

tls-profile *tls-profile-name*—Specify the TLS profile name.

tcp-connections *tcp-connections*—Specify the number of TCP connections per SPU.

Range: 1 through 5.

Default: 1.

Required Privilege Level

security—To view this in the configuration.
security-control—To add this to the configuration.

Related Documentation

- [Understanding AppTrack on page 125](#)

whitelist (Services)

Supported Platforms [SRX Series, vSRX](#)

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.

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 Proxy on page 83](#)
- *Firewall User Authentication Overview*

whitelist-url-categories

Supported Platforms	SRX1500, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX550M, SRX5600, SRX5800, vSRX
Syntax	<code>whitelist-url-categories <i>url-category-list</i>;</code>
Hierarchy Level	[edit services ssl proxy profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1X49-D80.
Description	Specify the enhanced Web filtering URL categories to be whitelisted. The whitelisting feature is extended to include URL categories. Each URL category has a unique ID. The list of URL categories to be whitelisted is parsed and the corresponding category IDs are pushed to the Packet Forwarding Engine for each SSL forward proxy profile. The SSL forward proxy then determines through APIs whether to accept, and proxy, or to ignore the session.
Options	<i>url-category-list</i> —List of URL categories defined by enhanced Web filtering that need to be whitelisted.
Required Privilege Level	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • SSL Proxy Overview on page 73 • Configuring SSL Proxy on page 83 • show services ssl proxy statistics on page 370

zones

Supported Platforms [SRX Series, vSRX](#)

```
Syntax zones {
    functional-zone {
        management {
            description text;
            host-inbound-traffic {
                protocols protocol-name {
                    except;
                }
            }
            system-services service-name {
                except;
            }
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
}

security-zone zone-name {
    address-book {
        address address-name {
            ip-prefix {
                description text;
            }
            description text;
            dns-name domain-name {
                ipv4-only;
                ipv6-only;
            }
            range-address lower-limit to upper-limit;
            wildcard-address ipv4-address/wildcard-mask;
        }
        address-set address-set-name {
            address address-name;
            address-set address-set-name;
            description text;
        }
    }
    advance-policy-based-routing;
    application-tracking;
    description text;
    host-inbound-traffic {
        protocols protocol-name {
```

```

        except;
    }
    system-services service-name {
        except;
    }
}
interfaces interface-name {
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
}
screen screen-name;
tcp-rst;
}
}

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:

- Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.
- Security zone—Most common type of zone that is used as a building block in policies.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Zones and Interfaces Overview*
- *Supported System Services for Host Inbound Traffic*

CHAPTER 14

Operational Commands

- clear security application-firewall rule-set statistics
- clear security application-firewall rule-set statistics logical-system
- clear services application-identification application-statistics
- clear services application-identification application-statistics cumulative
- clear services application-identification application-statistics interval
- clear services application-identification application-system-cache (Junos OS)
- clear services application-identification counter (Values)
- clear services ssl proxy statistics
- request security pki ca-certificate ca-profile-group load
- request security pki local-certificate export
- request security pki local-certificate generate-self-signed
- request security pki local-certificate load
- request services application-identification application
- request services application-identification download
- request services application-identification download status
- request services application-identification group
- request services application-identification install
- request services application-identification install status
- request services application-identification proto-bundle-status
- request services application-identification uninstall
- request services application-identification uninstall status
- show class-of-service application-traffic-control counter
- show class-of-service application-traffic-control statistics rate-limiter
- show class-of-service application-traffic-control statistics rule
- show security advance-policy-based-routing statistics
- show security advance-policy-based-routing status
- show security advance-policy-based-routing profile
- show security application-firewall rule-set

- `show security application-firewall rule-set logical-system`
- `show security application-tracking counters`
- `show security flow session`
- `show security flow session application-firewall`
- `show security pki ca-certificate`
- `show security pki local-certificate (View)`
- `show security policies`
- `show services application-identification application`
- `show services application-identification application-system-cache (View)`
- `show services application-identification commit-status`
- `show services application-identification counter (AppSecure)`
- `show services application-identification group`
- `show services application-identification statistics applications`
- `show services application-identification statistics application-groups`
- `show services application-identification status`
- `show services application-identification version`
- `show services ssl proxy statistics`

clear security application-firewall rule-set statistics

Supported Platforms [SRX Series, vSRX](#)

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.

Required Privilege Level clear

Related Documentation • [show security application-firewall rule-set on page 310](#)

Output Fields This command produces no output.

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

Supported Platforms [SRX5400, SRX5600, SRX5800](#)

Syntax The master, or root, administrator can issue the following statements:

```
clear security application-firewall rule-set statistics [logical-system logical-system-name |  
all | root-logical-system]
```

The user logical system administrator can issue the following statement:

```
clear security application-firewall rule-set statistics all
```

Release Information Command introduced in Junos OS Release 11.4.

Description Clear all security application firewall rule set statistics.



NOTE: User logical system administrators can clear statistics only for the logical systems they can access. For information about master and user administrator roles in logical systems, see *Understanding the Master Logical System and the Master Administrator Role*.

Options *logical-system-name*—Name of a specific logical system.

all—(default) Clear all rule set statistics for a specific logical system or all logical systems.

root-logical-system—Clear application firewall rule set statistics on the root logical system (master administrator only).

Required Privilege Level clear

Related Documentation

- [show security application-firewall rule-set logical-system on page 313](#)

Output Fields This command produces no output.

clear services application-identification application-statistics

Supported Platforms [SRX Series, vSRX](#)

Syntax clear services application-identification application-statistics

Release Information Statement introduced in Junos OS Release 11.4.

Description Clears all Junos OS application statistics such as cumulative, interval, applications, and application groups.

Required Privilege Level clear

Related Documentation

- [show services application-identification statistics applications on page 362](#)
- [show services application-identification statistics application-groups on page 364](#)
- [clear services application-identification application-statistics interval on page 281](#)
- [clear services application-identification application-statistics cumulative on page 280](#)

Output Fields This command produces no output.

[clear services application-identification application-statistics cumulative](#)

Supported Platforms [SRX Series, vSRX](#)

Syntax `clear services application-identification application-statistics cumulative`

Release Information Statement introduced in Junos OS Release 11.4.

Description Clear all Junos OS application cumulative statistics.

Required Privilege Level clear

Related Documentation

- [show services application-identification statistics applications on page 362](#)
- [show services application-identification statistics application-groups on page 364](#)
- [clear services application-identification application-statistics on page 279](#)
- [clear services application-identification application-statistics interval on page 281](#)

Output Fields This command produces no output.

clear services application-identification application-statistics interval

Supported Platforms [SRX Series, vSRX](#)

Syntax clear services application-identification application-statistics interval

Release Information Statement introduced in Junos OS Release 11.4.

Description Clear all Junos OS application interval statistics.

Required Privilege Level clear

Related Documentation

- [show services application-identification statistics applications on page 362](#)
- [show services application-identification statistics application-groups on page 364](#)
- [clear services application-identification application-statistics on page 279](#)
- [clear services application-identification application-statistics cumulative on page 280](#)

Output Fields This command produces no output.

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

Supported Platforms [SRX Series, vSRX](#)

Syntax clear services application-identification application-system-cache
<node (*node-id* | all | local | primary) >

Release Information Command introduced in Junos OS Release 10.2. Command syntax updated in Junos OS Release 12.1.

Description Clear Junos OS application identification application system cache.

- Options**
- none—Clear the application system cache on the device.
 - **node**—(Optional) For chassis cluster configurations, clear application system cache on the specified nodes.
 - *node-id*—Specific node number
 - all—All nodes
 - local—Local node
 - primary—Primary node

Required Privilege Level clear

Related Documentation

- [show services application-identification application-system-cache \(View\) on page 353](#)

Output Fields This command produces no output.

clear services application-identification counter (Values)

Supported Platforms	SRX Series , vSRX
Syntax	clear services application-identification counter <ssl-encrypted-sessions>
Release Information	Command introduced in Junos OS Release 10.2. Command updated in Junos OS Release 12.1-X47-D15.
Description	Reset all the Junos OS application identification counter values.
Options	ssl-encrypted-sessions —Reset application identification counter values for SSL encrypted sessions.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show services application-identification counter (AppSecure) on page 356
List of Sample Output	clear services application-identification counter on page 283
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 ssl proxy statistics

Supported Platforms [SRX1500, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX550M, SRX5600, SRX5800](#)

Syntax `clear services ssl proxy statistics`

Release Information Command introduced in Junos OS Release 12.1.

Description Clear services SSL proxy statistics.

Options **none**—Clear the ssl proxy statistics.

Required Privilege Level clear

Related Documentation

- [show services ssl proxy statistics on page 370](#)

Output Fields This command produces no output.

request security pki ca-certificate ca-profile-group load

Supported Platforms	SRX Series, vSRX
Syntax	request security pki ca-certificate ca-profile-group load ca-group-name <i>ca-group-name</i> filename [<i>path/filename</i> default]
Release Information	Command introduced in Junos OS Release 12.1; default option added in Junos OS Release 12.1X47-D10.
Description	<p>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.</p> <p>Use this command to load the default certificates or to specify a path and filename of trusted CA certificates that you define.</p>
Options	<p>ca-group-name <i>ca-group-name</i>—Load the specified CA group profile.</p> <p>filename <i>path/filename</i>—Directory location and filename of the trusted CA certificates defined by you.</p> <p>filename default—Load the trusted CA certificates available by default.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • show security pki ca-certificate on page 331 • <i>Understanding Certificates and PKI</i>
List of Sample Output	request security pki ca-certificate ca-profile-group load (default) on page 285 request security pki ca-certificate ca-profile-group load (path/filename) on page 286
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate ca-profile-group load (default)

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name ca-default
filename default
```

```
Do you want to load this CA certificate ? [yes,no] (no) yes
Loading 157 certificates for group 'ca-default'.
ca-default_1: Loading done.
ca-default_2: Loading done.
ca-default_3: Loading done.
.....
```

Sample Output

request security pki ca-certificate ca-profile-group load (path/filename)

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name ca-manual  
filename /var/tmp/firefox-all.pem
```

```
Do you want to load this CA certificate ? [yes,no] (no) yes
```

```
Loading 196 certificates for group 'ca-manual'.
```

```
ca-manual_1_sysgen: Loading done.
```

```
ca-manual_2_sysgen: Loading done.
```

```
ca-manual_3_sysgen: Loading done.
```

```
ca-manual_4_sysgen: Loading done.
```

```
ca-manual_5_sysgen: Loading done.
```

```
ca-manual_6_sysgen: Loading done.
```

```
...
```

```
ca-manual_195_sysgen: Loading done.
```

```
ca-manual_196_sysgen: Loading done.
```

```
ca-profile-group 'ca-manual' successfully loaded. Success[193] Skipped[3]
```

request security pki local-certificate export

Supported Platforms [SRX Series, vSRX](#)

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 287](#)

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

Supported Platforms	SRX1500, SRX5400, SRX5600, SRX5800, vSRX
Syntax	<code>request security pki local-certificate generate-self-signed certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> ip-address <i>ip-address</i> email <i>email-address</i> subject <i>subject-distinguished-name</i></code>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Manually generate a self-signed certificate for the given distinguished name.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—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.</p> <p>email <i>email-address</i>—E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—IP address of the router.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none">• CN—Common name• OU—Organizational unit name• O—Organization name• ST—State• C—Country
Required Privilege Level	maintenance security
Related Documentation	<ul style="list-style-type: none">• <i>Requesting for and Installing a Digital Certificates on Your Router</i>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert  
subject cn=abc domain-name example.net email user1@example.net  
Self-signed certificate generated and loaded successfully
```


request security pki local-certificate load

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800, vSRX](#)

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 290](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification application [disable | enable]
predefined-application-name

Release Information Command introduced in Junos OS Release 11.4.

Description Disable, or enable a predefined application signature.

Options **disable**—(Optional) Disable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration.

The following conditions apply:

- You cannot disable a predefined application signature that is referenced by an active security policy or custom application signature. First modify or deactivate the policy or custom application signature.
- If you disable an application signature, for example, junos:HTTP, that has nested applications, the nested applications are not recognized.

enable—(Optional) Enable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration.

Required Privilege Level maintenance

Related Documentation • [show services application-identification application on page 349](#)

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification application disable

```
user@host> request services application-identification application disable junos:163
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Please wait while we are updating signatures ...
Disable application junos:163 succeed.
```

request services application-identification download

Supported Platforms [SRX Series, vSRX](#)

Syntax `request services application-identification download <version>;`

Release Information Statement introduced in Junos OS Release 10.2.
Statement modified in Junos OS Release 11.4.

Description Manually download the application package for Junos OS application identification. The application package is extracted from the IDP signature database and contains signature definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP.

Options **version**—(Optional) Download a specific version of the application package from the Juniper Networks security website. If you do not enter a version, the most recent version is downloaded.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification download status on page 293](#)
- [request services application-identification install on page 296](#)

List of Sample Output [request services application-identification download on page 292](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification download status

Release Information Statement introduced in Junos OS Release 10.2.
Statement modified in Junos OS Release 11.4.

Description Check the download status of the application signature package. The downloaded application package is saved under `/var/db/appid/sec-download/`.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification download on page 292](#)

List of Sample Output [request services application-identification download status on page 293](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax `request services application-identification group [copy | disable | enable]
predefined-application-group-name`

Release Information Command introduced in Junos OS Release 11.4.

Description Copy, disable, or enable a predefined application signature group.

Options **copy**—(Optional) Copy a predefined application signature group from the database to the configuration and change the name (for example, my:FTP). The ID and order are generated automatically. Do not name your custom application signature group with the **junos** prefix; this prefix is reserved for predefined application signature groups. You can copy the same predefined application signature group only once; duplicate custom signature groups are not allowed.



NOTE: In configuration mode, if an uncommitted action is pending, the **request services application-identification group copy** command fails.

disable—(Optional) Disable a predefined application signature group.



NOTE: You cannot disable a predefined application signature group that is referenced by an active security policy or custom application signature group. First modify or deactivate the policy or custom application signature group.

enable—(Optional) Enable a predefined application signature group.

predefined-application-group-name—Name of the predefined application signature group.

Required Privilege Level maintenance

Related Documentation

- [show services application-identification group on page 360](#)

Output Fields When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification group

```
user@host> request services application-identification group disable
junos:infrastructure:networking
Disable application group junos:infrastructure:networking succeed.
```

request services application-identification group

```
user@host> request services application-identification group enable
junos:infrastructure:networking
Enable application group junos:infrastructure:networking succeed.
```

request services application-identification group

```
user@host> request services application-identification group copy junos:infrastructure:networking
Please wait while we are copying group ...
Copy application group junos:infrastructure:networking succeed.
```

request services application-identification install

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification install

Release Information Statement introduced in Junos OS Release 11.4.

Description Install the downloaded predefined application signature package.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification install status on page 297](#)
- [request services application-identification download on page 292](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification install status

Release Information Statement introduced in Junos OS Release 11.4.

Description Display the status of the install operation.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification install on page 296](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification proto-bundle-status

Release Information Statement introduced in Junos OS Release 12.1X47-D10.

Description Display the status of the install operation of the protocol bundle.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification install on page 296](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification uninstall

Release Information Statement introduced in Junos OS Release 10.2. Statement modified in Junos OS Release 10.4. Statement modified in Junos OS Release 11.4.

Description Uninstall the predefined application package.

The uninstall operation will fail if any active security policies reference predefined application signatures or predefined application signature groups in the Junos OS configuration.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification install on page 296](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax request services application-identification uninstall status

Release Information Statement introduced in Junos OS Release 11.4.

Description Display the status of the uninstall operation.

Required Privilege Level maintenance

Related Documentation

- [request services application-identification uninstall on page 299](#)

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

Supported Platforms [SRX Series, vSRX](#)

Syntax `show class-of-service application-traffic-control counter`

Release Information Command introduced in Junos OS Release 11.4.

Description Display AppQoS DSCP marking and honoring statistics based on Layer 7 application classifiers.

Required Privilege Level view

Related Documentation

- [Example: Configuring AppQoS on page 141](#)

List of Sample Output [show class-of-service application-traffic-control counter on page 301](#)

Output Fields [Table 12 on page 301](#) 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 12: show class-of-service application-traffic-control counter Output Fields

Field Name	Field Description
pic	PIC number of the accumulated statistics. NOTE: The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Sessions processed	The number of sessions where the class of service was checked.
Sessions marked	The number of sessions marked based on application-aware DSCP marking.
Sessions honored	The number of sessions honored based on application-aware traffic honoring.
Sessions rate limited	The number of sessions that have been rate limited.
Client-to-server flows rate limited	The number of client-to-server flows that have been rate limited.
Server-to-client flows rate limited	The number of server-to-client flows that have been rate limited.

Sample Output

show class-of-service application-traffic-control counter

```
user@host> show class-of-service application-traffic-control counter
```

pic: 2/1	
Counter type	Value
Sessions processed	300
Sessions marked	200
Sessions honored	0
Sessions rate limited	100
Client-to-server flows rate limited	100
Server-to-client flows rate limited	70
pic: 2/0	
Counter type	Value
Sessions processed	400
Sessions marked	300
Sessions honored	0
Sessions rate limited	200
Client-to-server flows rate limited	200
Server-to-client flows rate limited	100

show class-of-service application-traffic-control statistics rate-limiter

Supported Platforms [SRX Series, vSRX](#)

Syntax `show class-of-service application-traffic-control statistics rate-limiter`

Release Information Command introduced in Junos OS Release 11.4.

Description Display AppQoS real-time run information about application rate limiting of current or recent sessions.

Required Privilege Level view

Related Documentation

- [Example: Configuring AppQoS on page 141](#)

List of Sample Output [show class-of-service application-traffic-control statistics rate-limiter on page 303](#)

Output Fields [Table 13 on page 303](#) 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 13: show class-of-service application-traffic-control statistics rate-limiter Output Fields

Field Name	Field Description
pic	PIC number. <i>NOTE:</i> The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Ruleset	The rule set applied on the session.
Application	The application match for applying the rule set.
Client-to-server	The rate limiter applied from client to server.
Rate(kbps)	The rate in the client-to-server direction
Server-to-client	The rate limiter applied from server to client.
Rate(kbps)	The rate in the server-to-client direction.

Sample Output

show class-of-service application-traffic-control statistics rate-limiter

```
user@host> show class-of-service application-traffic-control statistics rate-limiter
```

```
pic: 2/1
Ruleset      Application Client-to-server Rate(kbps)  Server-to-client
Rate(kbps)
my-ruleset-1 HTTP      my-http-c2s-r1  10000000    my-http-s2c-r1
20000000
my-ruleset-2 HTTP      my-http-c2s-r1-2 20000000    my-http-s2c-r1-2
30000000
my-ruleset-2 FTP       my-ftp-c2s-r1   50000       my-ftp-s2c-r1
50000
...
```

```
pic: 2/0
Ruleset      Application Client-to-server Rate(kbps)  Server-to-client
Rate(kbps)
my-ruleset-1 HTTP      my-http-c2s-r1  10000000    my-http-s2c-r1
20000000
my-ruleset-2 HTTP      my-http-c2s-r1-2 20000000    my-http-s2c-r1-2
30000000
my-ruleset-2 FTP       my-ftp-c2s-r1   50000       my-ftp-s2c-r1
50000
```

show class-of-service application-traffic-control statistics rule

Supported Platforms [SRX Series, vSRX](#)

Syntax show class-of-service application-traffic-control statistics rule

Release Information Command introduced in Junos OS Release 11.4.

Description Display AppQoS counters identifying rule hits.

Required Privilege Level view

Related Documentation

- [Example: Configuring AppQoS on page 141](#)

List of Sample Output [show class-of-service application-traffic-control statistics rule on page 305](#)

Output Fields [Table 14 on page 305](#) 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 14: show class-of-service application-traffic-control statistics rule Output Fields

Field Name	Field Description
pic	PIC number where the rule is applied. NOTE: The PIC number is always displayed as 0 for for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Ruleset	The rule set containing the rule.
Rule	The rule to which the statistic applies.
Hits	The number of times a match for the rule was encountered.

Sample Output

show class-of-service application-traffic-control statistics rule

```

user@host> show class-of-service application-traffic-control statistics rule
pic: 2/0
  Ruleset      Rule           Hits
  my-ruleset-1 ftp-rule       100
  my-ruleset-1 http-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	http-rule	300
my-ruleset-2	telnet-rule	400
my-ruleset-2	smtp-rule	500

show security advance-policy-based-routing statistics

Supported Platforms [SRX Series, vSRX](#)

Syntax show security advance-policy-based-routing statistics

Release Information Command introduced in Junos OS Release 15.1X49-D60.

Description Display the statistics counter for APBR.

Required Privilege Level view

Related Documentation

- [Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152](#)

Output Fields [Table 15 on page 307](#) 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 15: show security advance-policy-based-routing statistics

Field Name	Field Description
Session Processed	The number of sessions processed for the application-based routing.
ASC Success	The number of times the presence of an entry in the application system cache (ASC) is found.
Rule match success	The number of times the application traffic matches the APBR profile.
Route modified	The number of times the APBR is applied for the session.
AppID Requested	The number of times AppID was consulted to identify application traffic.

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 status

Supported Platforms [SRX Series, vSRX](#)

Syntax show security advance-policy-based-routing status

Release Information Command introduced in Junos OS Release 15.1X49-D60.

Description Display the status for advanced policy-based routing (APBR).

Required Privilege Level view

Related Documentation

- [Example: Configuring Advanced Policy-Based Routing for Application-Aware Traffic Management Solution on page 152](#)

Sample Output

show security advance-policy-based-routing status

```
user@host> show security advance-policy-based-routing status
Advance Policy Based Routing is enabled.
```

show security advance-policy-based-routing profile

Supported Platforms [SRX Series, vSRX](#)

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 on page 152](#)

Output Fields [Table 16 on page 309](#) 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 16: show security advance-policy-based-routing profile

Field Name	Field Description
pic	PIC number of the accumulated statistics. <i>NOTE:</i> The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Profile	The name of the advanced policy-based (APBR) routing profile.
Zone	The zone on which APBR profile is applied to.

Sample Output

show security advance-policy-based-routing profile

```
user@host> show security advance-policy-based-routing profile

pic: 0/0
Profile    Zone
Profile1   trust
```

show security application-firewall rule-set

Supported Platforms [SRX Series, vSRX](#)

Syntax `show security application-firewall rule-set (<rule-set-name> | all)`

Release Information Command introduced in Junos OS Release 11.1. Updated in Junos OS Release 12.1X44-D10 with output format changes. Updated in Junos OS Release 12.1X45-D10 with redirection counters.

Description Display information about the specified rule set defined in the application firewall.

Options *rule-set-name*—Name of the rule set.
all—Display information about all the application firewall rule sets.

Required Privilege Level view

Related Documentation

- [clear security application-firewall rule-set statistics on page 277](#)

List of Sample Output [show security application-firewall rule-set my_ruleset1 on page 311](#)
[show security application-firewall rule-set all on page 311](#)

Output Fields [Table 17 on page 310](#) 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 17: show security application-firewall rule-set Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.
Logical system	Name of the logical system of the rule set.
Profile	The redirect profile to be used for rules requiring redirection for reject or deny actions.

Table 17: show security application-firewall rule-set Output Fields (*continued*)

Field Name	Field Description
Rule	<p>Name of the rule</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • permit • deny • reject • redirect • Number of sessions matched—Number of sessions matched with the application firewall rule. • Number of sessions redirected—Number of sessions redirected by the application firewall rule.
Default rule	<p>The default rule applied when the identified application is not specified in any rules of the rule set.</p> <ul style="list-style-type: none"> • Number of sessions matched—Number of sessions matched with the application firewall default rule. • Number of sessions redirected—Number of sessions redirected by the application firewall rule.
Number of sessions with appid pending	Number of sessions that are pending application identification processing

Sample Output

show security application-firewall rule-set my_ruleset1

```

user@host>show security application-firewall rule-set my_ruleset1
Rule-set: my_ruleset1
  Rule: rule1
    Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
    Dynamic Application Groups: junos:web, junos:chat
    SSL-Encryption: any
    Action: deny or redirect
    Number of sessions matched: 10
    Number of sessions redirected: 10
  Default rule: permit
    Number of sessions matched: 200
    Number of sessions redirected: 0
  Number of sessions with appid pending: 2

```

Sample Output

show security application-firewall rule-set all

```

user@host> show security application-firewall rule-set all

```

```
Rule-set: appfw
  Logical system: root-logical-system
  Profile: lsy2_pf555
  Rule: 2
    Dynamic Applications: junos:HTTP
    SSL-Encryption: any
    Action:deny or redirect
    Number of sessions matched: 2
    Number of sessions redirected: 2
  Rule: 1
    Dynamic Applications: junos:FTP
    SSL-Encryption: any
    Action:permit
    Number of sessions matched: 0
    Number of sessions redirected: 0
  Default rule:permit
    Number of sessions matched: 0
    Number of sessions redirected: 0
  Number of sessions with appid pending: 0
```

show security application-firewall rule-set logical-system

Supported Platforms [SRX Series, vSRX](#)

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*.

Options *rule-set-name*—Name of a specific rule set.

logical-system-name—Name of a specific logical system.

all—(default) Display all rule sets for all logical systems. The user logical system administrator can display all rule sets only for the logical system they can access.

root-logical-system—Display application firewall rule set information for the root logical system (master administrator only).

Required Privilege Level view

Related Documentation

- [clear security application-firewall rule-set statistics logical-system on page 278](#)

List of Sample Output [show security application-firewall rule-set logical-system all on page 314](#)
[show security application-firewall rule-set all on page 315](#)

Output Fields Table 18 on page 314 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 18: show security application-firewall rule-set logical-system Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.
Logical system	Name of the logical system.
Rule	<p>Name of the rule.</p> <ul style="list-style-type: none"> • Dynamic applications—Name of the applications. • Dynamic application groups—Name of the application groups. • Action—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following: <ul style="list-style-type: none"> • permit • deny • Number of sessions matched—Number of sessions matched with the application firewall rule.
Default rule	<p>The default rule applied when the identified application is not specified in any rules of the rule set.</p> <ul style="list-style-type: none"> • Number of sessions matched—Number of sessions matched with the application firewall default rule.
Number of sessions with appid pending	Number of sessions that are pending with the application ID processing.

Sample Output

show security application-firewall rule-set logical-system all

```
root@host> show security application-firewall rule-set logical-system all
```

```

Rule-set: root_rs1
  Logical system: root-logical-system
  Rule: r1
    Dynamic Applications: junos:FTP
    Action: permit
    Number of sessions matched: 10
  Default rule: deny
    Number of sessions matched: 100
  Number of sessions with appid pending: 4

Rule-set: root_rs2
  Logical system: root-logical-system
  Rule: r1
    Dynamic Application Groups: junos:web
    Action: permit
    Number of sessions matched: 20
  Default rule: deny

```

Number of sessions matched: 100
Number of sessions with appid pending: 10

show security application-firewall rule-set all

```
root@host> show security application-firewall rule-set all

Rule-set: ls-product-design-rs1
  Logical system: ls-product-design
  Rule: r1
    Dynamic Applications: junos:TELNET
    Action:permit
    Number of sessions matched: 10
  Default rule:deny
    Number of sessions matched: 100
  Number of sessions with appid pending: 2

Rule-set: ls-product-design-rs1
  Logical system: ls-product-design
  Rule: r2
    Dynamic Application Groups: junos:web
    Action:permit
    Number of sessions matched: 20
  Default rule:deny
    Number of sessions matched: 200
  Number of sessions with appid pending: 4

Rule-set: ls-product-design-rs2
  Logical system: ls-product-design
  Rule: r1
    Dynamic Applications: junos:FACEBOOK-ACCESS
    Action:deny
    Number of sessions matched: 40
  Default rule:permit
    Number of sessions matched: 400
  Number of sessions with appid pending: 10
```

show security application-tracking counters

Supported Platforms [SRX Series, vSRX](#)

Syntax `show security application-tracking counters`

Release Information Command introduced in Junos OS Release 10.2.

Description Display the status of AppTrack counters.

Required Privilege Level view

Related Documentation

- [Understanding AppTrack on page 125](#)
- [Example: Configuring AppTrack on page 127](#)

Output Fields [Table 19 on page 316](#) 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 19: show security application-tracking counters

Field Name	Field Description
Session create messages	The number of log messages generated when a session was created.
Session close messages	The number of log messages generated when a session was closed.
Session volume updates	The number of log messages generated when an update interval was exceeded.
Session route updates	The number of log messages generated when an egress interface was selected based on application carried in the session by APBR.
Failed messages	The number of messages that were not generated due to memory or session constraints.

Sample Output

show security application-tracking counters

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

```
Application tracking counters:
```

AppTrack counter type	Value
Session create messages	1
Session close messages	1
Session volume updates	0
Session route updates	1
Failed messages	0

show security flow session

Supported Platforms [SRX Series, vSRX](#)

Syntax `show security flow session [brief | extensive | summary]`

Release Information Command introduced in Junos OS Release 8.5. Support for filter and view options added in Junos OS Release 10.2.
Application firewall, dynamic application, and logical system filters added in Junos OS Release 11.2.
Policy ID filter added in Junos OS Release 12.3X48-D10.
Support for connection tag added in Junos OS Release 15.1X49-D40.

Description Display information about all currently active security sessions on the device.



NOTE: For the normal flow sessions, the `show security flow session` command displays bytes counters based on IP header length. However for sessions in Express Path mode, the statistics is collected from IOC2 and IOC3 ASIC hardware engine, and includes full packet length with L2 headers. Because of this, the output displays slightly larger bytes counters for sessions in Express Path mode than 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 advanced-anti-malware option, see the [Sky Advanced Threat Prevention CLI Reference Guide](#).

application—Predefined application name

application-firewall—Application firewall enabled

application-firewall-rule-set—Application firewall enabled with the specified rule set

application-traffic-control—Application traffic control session

application-traffic-control-rule-set—Application traffic control rule set name and rule name

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

policy-id—Display session information based on policy ID; the range is 1 through 4,294,967,295

protocol—IP protocol number

resource-manager—Resource manager

root-logical-system—Display root logical system as default

security-intelligence—Display security intelligence sessions

services-offload—Display services offload sessions

session-identifier—Display session with specified session identifier

source-port—Source port

source-prefix—Source IP prefix

tunnel—Tunnel sessions

- **brief | extensive | summary**—Display the specified level of output.
- **none**—Display information about all active sessions.

Required Privilege Level

view

Related Documentation

- *Juniper Networks Devices Processing Overview*
- *clear security flow session all*

List of Sample Output

[show security flow session on page 322](#)
[show security flow session brief on page 322](#)
[show security flow session extensive on page 322](#)
[show security flow session summary on page 323](#)

Output Fields [Table 20 on page 320](#) lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 20: show security flow session Output Fields

Field Name	Field Description	Level of Output
Session ID	Number that identifies the session. Use this ID to get more information about the session.	brief extensive none
If	Interface name.	brief none
State	Status of security flow session.	brief extensive none
Conn Tag	A 32-bit connection tag that uniquely identifies the GPRS tunneling protocol, user plane (GTP-U) and the Stream Control Transmission Protocol (SCTP) sessions. The connection tag for GTP-U is the tunnel endpoint identifier (TEID) and for SCTP is the vTag. The connection ID remains 0 if the connection tag is not used by the sessions.	brief extensive none
CP Session ID	Number that identifies the central point session. Use this ID to get more information about the central point session.	brief extensive none
Policy name	Name and ID of the policy that the first packet of the session matched.	brief extensive none
Timeout	Idle timeout after which the session expires.	brief extensive none
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).	brief extensive none

Table 20: show security flow session Output Fields (*continued*)

Field Name	Field Description	Level of Output
Bytes	Number of received and transmitted bytes.	brief
		extensive
		none
Pkts	Number of received and transmitted packets.	brief
		extensive
		none
Total sessions	Total number of sessions.	brief
		extensive
		none
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).	brief
		extensive
		none
Status	Session status.	extensive
Flag	Internal flag depicting the state of the session, used for debugging purposes.	extensive
Source NAT pool	The name of the source pool where NAT is used.	extensive
Dynamic application	Name of the application.	extensive
Application traffic control rule-set	AppQoS rule set for this session.	extensive
Rule	AppQoS rule for this session.	extensive
Maximum timeout	Maximum session timeout.	extensive
Current timeout	Remaining time for the session unless traffic exists in the session.	extensive
Session State	Session state.	extensive
Start time	Time when the session was created, offset from the system start time.	extensive
Unicast-sessions	Number of unicast sessions.	Summary
Multicast-sessions	Number of multicast sessions.	Summary

Table 20: show security flow session Output Fields (*continued*)

Field Name	Field Description	Level of Output
Services-offload-sessions	Number of services-offload sessions.	Summary
Failed-sessions	Number of failed sessions.	Summary
Sessions-in-use	Number of sessions in use. <ul style="list-style-type: none"> Valid sessions Pending sessions Invalidated sessions Sessions in other states 	Summary
Maximum-sessions	Maximum number of sessions permitted.	Summary

Sample Output

show security flow session

```

root> show security flow session
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 56, Valid
  In: 203.0.113.1/1000 --> 203.0.113.11/2000;udp, Conn Tag: 0x0, If: reth1.0,
Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.11/2000 --> 203.0.113.1/1000;udp, Conn Tag: 0x0, If: reth0.0,
Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1

```

show security flow session brief

```

root> show security flow session brief
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 62, Valid
  In: 203.0.113.11/1000 --> 203.0.113.1/2000;udp, Conn Tag: 0x0, If: reth1.0,
Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp, Conn Tag: 0x0, If: reth0.0,
Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1

```

show security flow session extensive

```

root> show security flow session extensive
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Status: Normal, State: Active
Flags: 0x8000040/0x18000000/0x12000003
Policy name: SG/4
Source NAT pool: Null, Application: junos-gprs-gtp-v0-udp/76
Dynamic application: junos:UNKNOWN,
Encryption: Unknown

```

```

Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 90, Current timeout: 54
Session State: Valid
Start time: 6704, Duration: 35
  In: 203.0.113.11/1000 --> 201.11.0.100/2000;udp,
    Conn Tag: 0x0, Interface: reth1.0,
    Session token: 0x6, Flag: 0x40000021
    Route: 0x86053c2, Gateway: 201.10.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 86
    CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp,
    Conn Tag: 0x0, Interface: reth0.0,
    Session token: 0x7, Flag: 0x50000000
    Route: 0x86143c2, Gateway: 203.0.113.11, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
    CP Session ID: 10320276
Total sessions: 1

```

show security flow session summary

```

root> show security flow session summary
Flow Sessions on FPC10 PIC1:
Unicast-sessions: 1
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456

Flow Sessions on FPC10 PIC2:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456

Flow Sessions on FPC10 PIC3:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456

```


show security flow session application-firewall

Supported Platforms [SRX Series, vSRX](#)

Syntax show security flow session application-firewall
 < dynamic-application (*dyn-app-name* | junos:UNKNOWN) >
 < dynamic-application-group (*dyn-app-group* | junos:UNASSIGNED) >
 < application-firewall-rule-set *rule-set-name* >
 < rule *rule-name* >
 < brief | extensive | summary >

Release Information Command introduced in Junos OS Release 11.2.

Description Display all sessions where application firewall is enabled.

Include options to filter the output and display only those enabled sessions with the specified features.

- Options**
- **dynamic-application** (*dyn-app-name* | junos:UNKNOWN)—Display only those enabled sessions with the specified dynamic application. Enter **junos:UNKNOWN** to display all enabled sessions where no dynamic application can be determined.
 - **dynamic-application-group** (*dyn-app-group* | junos:UNASSIGNED)— Display only those enabled session with the specified dynamic application group. Enter **junos:UNASSIGNED** to display all enabled sessions where no dynamic application group can be determined.
 - **application-firewall-rule-set** *rule-set-name*—Display only those enabled sessions that match the specified rule set.
 - **rule** *rule-name*—Display only those enabled sessions that match the specified rule.
 - **brief | extensive | summary**—Specify the level of detail for the display.
- The output fields for the **brief** and **summary** options are the same as those of the **show security flow session** command. Only the **extensive** display is different and is shown in the following output table and examples.

Required Privilege Level view

- Related Documentation**
- [Example: Configuring an Application Group for Application Firewall on page 116](#)
 - [show security flow session on page 318](#)

List of Sample Output [show security flow session application-firewall extensive on page 327](#)
[show security flow session application-firewall dynamic-application junos:FTP extensive on page 327](#)
[show security flow session application-firewall dynamic-application junos:UNKNOWN extensive on page 328](#)

[show security flow session application-firewall dynamic-application-group junos:WEB extensive on page 329](#)

[show security flow session application-firewall application-firewall-rule-set rule-set1 extensive on page 329](#)

Output Fields Table 21 on page 326 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 21: show security flow session application-firewall extensive Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to display more information about a session.
Status	Session status.
State	Current state of the session: Active, Pending, Closed, Unknown.
Flag	Internal flag depicting the state of the session. It is used for debugging purposes.
Policy name	The name of the policy that permitted the traffic.
Source NAT pool	The name of the source pool where NAT is used.
Dynamic application	Name of the dynamic application of the session. If the dynamic application has yet to be determined, the output indicates Pending. If the dynamic application cannot be determined, the output indicates junos:UNKNOWN.
Dynamic application group	Name of the dynamic application group of the session. If the dynamic application cannot be determined, the output indicates junos:UNASSIGNED.
Dynamic nested application	Name of the dynamic nested application of the session if one exists. If the dynamic nested application is yet to be determined, the output indicates Pending. If the dynamic nested application cannot be determined, the output indicates junos:UNKNOWN.
Application firewall rule-set	Name of the rule set that the session matched.
Rule	Name of the rule that the session matched. If the match has not yet been made, the output indicates Pending. If the rule has been deleted since the match was made, the output indicates the rule is invalid.
Maximum timeout	Maximum amount of idle time allowed for the session.
Current timeout	Number of seconds that the current session has been idle.
Session State	Session state.
Start time	Time when the session was created. Start time is indicated as an offset from the system start time.

Table 21: show security flow session application-firewall extensive Output Fields (*continued*)

Field Name	Field Description
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets, and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions per PIC that fit the display criteria.

Sample Output

show security flow session application-firewall extensive

The displayed information is similar to the **show security flow session** output but includes dynamic application and application firewall details for the session.

```

user@host> show security flow session application-firewall extensive
Flow Sessions on FPC9 PIC0:

    Session ID: 3729, Status: Normal, State: Active
    Policy name: self-traffic-policy/1
    Source NAT pool: Null
    Dynamic application: junos:HTTP, Dynamic nested application:
junos:FACEBOOK-ACCESS
    Application firewall rule-set: rule-set1, Rule: rule2
    Maximum timeout: 300, Current timeout: 276
    Session State: Valid
    Start time: 18292, Duration: 603536
    In: 192.0.2.1/1 --> 203.0.113.1/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
    Out: 203.0.113.1/1 --> 192.0.2.1/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xffffd0000, Gateway: 203.0.113.13, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

    Total sessions: 1

```

show security flow session application-firewall dynamic-application junos:FTP extensive

Entering a specific dynamic application in the command line filters the output and displays only those sessions with the specified application.

```

user@host> show security flow session application-firewall dynamic-application junos:FTP
extensive

```

Flow Sessions on FPC3 PIC0:

```
Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
Dynamic application: junos:FTP
Application firewall rule-set: rule-set1, Rule: rule1
Maximum timeout: 300, Current timeout: 276
Session State: Valid
Start time: 18292, Duration: 603536
  In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
  Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xffffd0000, Gateway: 203.0.113.13, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
```

Total sessions: 1

show security flow session application-firewall dynamic-application junos:UNKNOWN extensive

Using the keyword **junos:UNKNOWN** displays those enabled sessions where the dynamic application cannot be determined.

```
user@host> show security flow session application-firewall dynamic-application junos:UNKNOWN
extensive
```

Flow Sessions on FPC9 PIC0:

```
Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
Dynamic application: junos:UNKNOWN
Application firewall rule-set: rule-set1, Rule: rule1
Maximum timeout: 300, Current timeout: 276
Session State: Valid
Start time: 18292, Duration: 603536
  In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
  Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xffffd0000, Gateway: 203.0.113.13, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
```

```
Session ID: 180013339, Policy name: policy1/4, Timeout: 1776, Valid
Dynamic application: junos:HTTP, Dynamic nested application: junos:UNKNOWN

Application firewall rule-set: rule-set1, Rule: rule1
Maximum timeout: 300, Current timeout: 276
```

```

Session State: Valid
Start time: 18292, Duration: 603536
  In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
    Interface: reth1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 21043, Bytes: 1136322
  Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 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 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: 1

```

show security flow session application-firewall application-firewall-rule-set rule-set1 extensive

Specifying a rule set name reduces the display to only those sessions matching the specified rule set.

```

user@host> show security flow session application-firewall application-firewall-rule-set rule-set1
extensive

```

Flow Sessions on FPC9 PIC0:

Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
Dynamic application: junos:FTP
Application firewall rule-set: rule-set1, Rule: rule1
Maximum timeout: 300, Current timeout: 276
Session State: Valid
Start time: 18292, Duration: 603536
In: 192.0.2.4/1 --> 203.0.113.13/1;pim,
Interface: reth1.0,
Session token: 0x1c0, Flag: 0x0x21
Route: 0x0, Gateway: 192.0.2.4, Tunnel: 0
Port sequence: 0, FIN sequence: 0,
FIN state: 0,
Pkts: 21043, Bytes: 1136322
Out: 203.0.113.13/1 --> 192.0.2.4/1;pim,
Interface: .local..0,
Session token: 0x80, Flag: 0x0x30
Route: 0xffffd0000, 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: 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 pki ca-certificate

Supported Platforms [SRX5400, SRX5600, SRX5800, vSRX](#)

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 332](#)
[show security pki ca-certificate detail on page 333](#)

Output Fields [Table 22 on page 331](#) 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 22: show security pki ca-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	detail
Serial number	Unique serial number of the digital certificate.	detail
Issued by	Authority that issued the digital certificate.	none brief
Issued to	Device that was issued the digital certificate.	none brief

Table 22: show security pki ca-certificate Output Fields (*continued*)

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	All levels
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption(1024 bits) .	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .	detail
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show security pki ca-certificate

```

user@host> show security pki ca-certificate
Certificate identifier: abc
Issued to: example, Issued by: exmple
Validity:
  Not before: 2005 Oct 18th, 23:54:22 GMT
  Not after: 2025 Oct 19th, 00:24:22 GMT
Public key algorithm: rsaEncryption(1024 bits)

```

```

Certificate identifier: entrust
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

```

```

Certificate identifier:abe
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

```

show security pki ca-certificate detail

```

user@host> show security pki ca-certificate detail
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
    ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
    42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
    da:eb:10:27:bd:46:34:33

```

Signature algorithm: sha1WithRSAEncryption
Fingerprint:
 bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
 23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
Distribution CRL:
 C=us, O=example, CN=CRL1
 http://CA-1/CRL/example_us_crlfile.crl
Use for key: Key encipherment
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925b
Issuer:
 Organization: example, Country: us
Subject:
 Organization: example, Country: us, Common name: First Officer
Validity:
 Not before: 2005 Oct 18th, 23:55:59 GMT
 Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
 ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
 d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
 00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
 e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
 90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
 b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
 af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
 ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
 C=us, O=example, CN=CRL1
 http://CA-1/CRL/example_us_crlfile.crl
Use for key: Digital signature

show security pki local-certificate (View)

Supported Platforms [SRX Series, vSRX](#)

Syntax show security pki local-certificate
 < **brief** | **detail** >
 < certificate-id *certificate-id-name* >
 <system-generated>

Release Information Command modified in Junos OS Release 9.1. Subject string output field added in Junos OS Release 12.1X44-D10.

Description Display information about the local digital certificates, corresponding public keys, and the automatically generated self-signed certificate configured on the device.

- Options**
- **none**—Display basic information about all configured local digital certificates, corresponding public keys, and the automatically generated self-signed certificate.
 - **brief** | **detail**—(Optional) Display the specified level of output.
 - certificate-id *certificate-id-name* —(Optional) Display information about only the specified local digital certificates and corresponding public keys.
 - **system-generated**—Display information about the automatically generated self-signed certificate.

Required Privilege Level view

- Related Documentation**
- *clear security pki local-certificate (Device)*
 - *request security pki local-certificate generate-self-signed (Security)*

List of Sample Output [show security pki local-certificate certificate-id hello on page 337](#)
[show security pki local-certificate certificate-id hello detail on page 337](#)
[show security pki local-certificate system-generated on page 338](#)
[show security pki local-certificate system-generated detail on page 338](#)
[show security pki local-certificate certificate-id mycert - \(local certificate enrolled online using SCEP\) on page 339](#)
[show security pki local-certificate certificate-id mycert detail - \(local certificate enrolled online using SCEP\) on page 339](#)

Output Fields [Table 23 on page 336](#) 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 23: show security pki local-certificate Output Fields

Field Name	Field Description
Certificate identifier	Name of the digital certificate.
Certificate version	Revision number of the digital certificate.
Serial number	Unique serial number of the digital certificate.
Issued to	Device that was issued the digital certificate.
Issued by	Authority that issued the digital certificate.
Issuer	<p>Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:</p> <ul style="list-style-type: none"> • Organization—Organization of origin. • Organizational unit—Department within an organization. • Country—Country of origin. • Locality—Locality of origin. • Common name—Name of the authority.
Subject	<p>Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:</p> <ul style="list-style-type: none"> • Organization—Organization of origin. • Organizational unit—Department within an organization. • Country—Country of origin. • Locality—Locality of origin. • Common name—Name of the authority. • Serial number—Serial number of the device. <p>If the certificate contains multiple subfield entries, all entries are displayed.</p>
Subject string	Subject field as it appears in the certificate.
Alternate subject	Domain name or IP address of the device related to the digital certificate.
Validity	<p>Time period when the digital certificate is valid. Values are:</p> <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid.
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption(1024 bits) .
Public key verification status	Public key verification status: Failed or Passed . The detail output also provides the verification hash.
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .

Table 23: show security pki local-certificate Output Fields (*continued*)

Field Name	Field Description
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.
Use for key	Use of the public key, such as Certificate signing, CRL signing, Digital signature, or Data encipherment.

Sample Output

show security pki local-certificate certificate-id hello

```

user@host> show security pki local-certificate certificate-id hello
Certificate identifier: hello
  Issued to: cn1, Issued by: DC = local, DC = demo, CN = domain-example-WIN-CA
  Validity:
    Not before: 08- 8-2012 17:02
    Not after: 08- 8-2014 17:02
  Public key algorithm: rsaEncryption(1024 bits)

```

Sample Output

show security pki local-certificate certificate-id hello detail

```

user@host> show security pki local-certificate certificate-id hello detail
Certificate identifier: hello
  Certificate version: 3
  Serial number: 61ba9da000000000d72e
  Issuer:
    Common name: Example-CA,
    Domain component: local, Domain component: demo
  Subject:
    Organization: o1, Organization: o2,
    Organizational unit: ou1, Organizational unit: ou2, Country: US, State: CA,
    Locality: Sunnyvale, Common name: cn1, Common name: cn2,
    Domain component: dc1, Domain component: dc2
  Subject string:
    C=Example, DC=dc1, DC=dc2, ST=CA, L=Sunnyvale, O=o1, O=o2, OU=ou1, OU=ou2,
    CN=cn1, CN=cn2
  Alternate subject: "user@example.net", user.example.net, 192.0.2.1
  Validity:
    Not before: 08- 8-2012 17:02
    Not after: 08- 8-2014 17:02
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:b4:14:01:d5:4f:79:87:d5:bb:e6:5e:c1:14
    97:da:b4:40:ad:1a:77:3e:ec:2e:68:8e:e4:93:a3:fe:7c:0b:58:af
    e1:20:27:82:ca:8d:6f:f0:97:d1:ad:fe:df:6c:cb:3c:b0:4f:cc:dd
    ac:d8:69:3f:3c:59:b5:2a:c6:83:e8:b3:94:5e:0a:2d:cd:e2:b0:15
    3e:97:a7:8a:4e:fb:59:f7:20:4c:ba:a8:80:3e:ba:be:69:ef:2b:32
    e4:1a:1c:24:53:1b:d5:c3:aa:d4:25:73:96:76:ea:49:d4:da:7e:3e
    0c:c6:6b:22:43:cb:04:84:0d:25:33:07:6b:49:41:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Distribution CRL:

```

```

    ldap:///Example-CA,CN=cn-win,CN=CDP,CN=Public%20Key
%20Services,CN=Services,CN=Configuration,DC=demo,DC=local?certificateRevocationList?base?
objectClass=cRLDistributionPoint
    http://example.example.net/CertEnroll/Example-CA.crl
Use for key: Key encipherment, Digital signature, 1.3.6.1.5.5.8.2.2,
1.3.6.1.5.5.8.2.2
Fingerprint:
    76:a8:5f:65:b4:bf:bd:10:d8:56:82:65:ff:0d:04:3a:a5:e9:41:dd (sha1)
    8f:99:a4:15:98:10:4b:b6:1a:3d:81:13:93:2a:ac:e7 (md5)
Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started

```

Sample Output

show security pki local-certificate system-generated

```

user@host> show security pki local-certificate system-generated
Certificate identifier: system-generated
    Issued to: JN10B9390AGB, Issued by: CN = JN10B9390AGB, CN = system generated,
CN = self-signed
    Validity:
        Not before: 10-30-2009 23:02
        Not after: 10-29-2014 23:02
    Public key algorithm: rsaEncryption(1024 bits)

```

Sample Output

show security pki local-certificate system-generated detail

```

user@host> show security pki local-certificate system-generated detail
Certificate identifier: system-generated
    Certificate version: 3
    Serial number: e90d42ebd14ef954b3e48c2eed5b30fb
    Issuer:
        Common name: JN10B9390AGB, Common name: system generated, Common name:
self-signed
    Subject:
        Common name: JN10B9390AGB, Common name: system generated, Common name:
self-signed
    Subject string:
        CN=JN10B9390AGB, CN=system generated, CN=self-signed
    Validity:
        Not before: 10-30-2009 23:02
        Not after: 10-29-2014 23:02
    Public key algorithm: rsaEncryption(1024 bits)
        30:81:89:02:81:81:00:cb:c8:3f:e6:d3:e5:ca:9d:dc:2d:e9:ca:c7
        5f:b1:f5:3a:f0:1c:a7:55:43:0f:ef:fd:1c:fe:29:09:d5:37:d0:fa
        d6:ee:bc:b8:3f:58:d4:31:fb:96:4f:4f:cc:a9:1a:8f:2e:1b:50:6f
        2b:88:34:74:b2:6d:ad:94:b5:dd:3d:80:87:56:d0:42:50:4d:ac:d7
        8c:21:06:2d:07:1e:f4:d0:c7:85:2e:25:60:ad:1b:b5:b2:d2:1d:c8
        79:67:8c:56:06:04:75:6e:be:4e:99:b8:07:e6:9a:11:fe:b5:ec:c0
        1e:68:da:47:99:1b:b2:c8:07:ab:cd:6e:fe:c1:fd:02:03:01:00:01
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
        be:1f:21:13:71:cd:9d:de:7a:41:d7:4c:52:8d:3e:d6:ba:db:75:96 (sha1)
        ba:fc:90:4b:5f:a8:66:a3:b9:64:89:9f:e2:45:b5:84 (md5)
    Auto-re-enrollment:
        Status: Disabled
        Next trigger time: Timer not started

```

Sample Output

show security pki local-certificate certificate-id mycert - (local certificate enrolled online using SCEP)

```
user@host> show security pki local-certificate certificate-id mycert
Certificate identifier: mycert
  Issued to: bubba, Issued by: DC = local, DC = demo, CN = domain-example-WIN-CA

Validity:
  Not before: 11-15-2012 18:58
  Not after: 11-15-2014 18:58
  Public key algorithm: rsaEncryption(1024 bits)
```

Sample Output

show security pki local-certificate certificate-id mycert detail - (local certificate enrolled online using SCEP)

```
user@host> show security pki local-certificate certificate-id mycert detail
Certificate identifier: mycert
  Certificate version: 3
  Serial number: 1f00b50a000000013ad2
  Issuer:
    Common name: Example-CA,
    Domain component: local, Domain component: demo
  Subject:
    Organization: example, Organizational unit: SSD, Country: US,
    Common name: host1, Serial number: SRX240-11152012
  Subject string:
    serialNumber=SRX240-11152012, C=US, O=example, OU=SSD, CN=host1
  Alternate subject: "user@example.net", user.example.net, 192.0.2.1
  Validity:
    Not before: 11-15-2012 18:58
    Not after: 11-15-2014 18:58
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:e3:e5:ae:c0:82:af:db:94:01:2f:56:46:50
    7d:3d:0b:0c:f0:1f:1d:7d:c3:aa:d4:4c:a0:cd:23:8b:3f:47:05:ee
    7b:65:42:a0:dc:c4:ac:a7:b6:a6:9f:5c:ea:d8:22:b0:bf:03:75:09
    be:fa:77:cb:d6:67:19:e6:80:fa:a5:7c:93:af:96:66:9f:cc:45:d5
    eb:ab:c1:f0:32:a6:d9:27:1b:80:bb:57:ec:31:a2:e0:2b:e1:42:c0
    92:8a:9b:ed:a6:d2:ec:7c:84:5a:8a:d9:96:a7:7e:40:c3:80:0e:f4
    d6:a2:5d:78:93:3b:7d:d5:8a:f5:de:fb:bc:0d:6d:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Distribution CRL:
    ldap:///Example-CA,CN=cn-win,CN=CDP,CN=Public%20Key%20Services,
    CN=Services,CN=Configuration,DC=demo,DC=local?certificateRevocationList?
    base?objectClass=cRLDistributionPoint
    http://example.example.net/CertEnroll/Example-CA.crl
  Use for key: Key encipherment, Digital signature, 1.3.6.1.5.5.8.2.2,
  1.3.6.1.5.5.8.2.2
  Fingerprint:
    1f:2f:a9:22:a8:d5:a9:36:cc:c4:bd:81:59:9d:9c:58:bb:40:15:72 (sha1)
    51:27:e4:d5:29:90:f7:85:9e:67:84:a1:75:d1:5b:16 (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```

show security policies

Supported Platforms [SRX Series, vSRX](#)

Syntax **show security policies**
none
<detail>
policy-name *policy-name*
<global>

Release Information Command modified in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 10.2. Support for wildcard addresses added in Junos OS Release 11.1. Support for global policy added in Junos OS Release 11.4. Support for services offloading added in Junos OS Release 11.4. Support for source-identities added in Junos OS Release 12.1. The **Description** output field added in Junos OS Release 12.1. Support for negated address added in Junos OS Release 12.1X45-D10. The output fields for Policy Statistics expanded, and the output fields for the **global** and **policy-name** options expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Output field and description for **source-end-user-profile** option added in Junos OS Release 15.1x49-D70. Output field and description for **dynamic-applications** option added in Junos OS Release 15.1x49-D100.

Description Display a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy.

- Options**
- **none**—Display basic information about all configured policies.
 - **detail**—(Optional) Display a detailed view of all of the policies configured on the device.
 - **policy-name *policy-name***—(Optional) Display information about a specified policy.
 - **global**—(Optional) Display information about global policies.

Required Privilege Level view

- Related Documentation**
- [Security Policies Overview](#)
 - [Understanding Security Policy Rules](#)
 - [Understanding Security Policy Elements](#)

List of Sample Output [show security policies on page 344](#)
[show security policies \(Dynamic Applications\) on page 344](#)
[show security policies policy-name detail on page 345](#)
[show security policies \(Services-Offload\) on page 346](#)
[show security policies \(Device Identity\) on page 346](#)
[show security policies detail on page 346](#)

[show security policies detail \(TCP Options\) on page 347](#)
[show security policies policy-name \(Negated Address\) on page 347](#)
[show security policies policy-name detail \(Negated Address\) on page 348](#)
[show security policies global on page 348](#)

Output Fields Table 24 on page 341 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 24: show security policies Output Fields

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
Description	Description of the applicable policy.
State	Status of the policy: <ul style="list-style-type: none"> • enabled: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • disabled: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	Internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
source-end-user-profile	Name of the device identity profile (referred to as end-user-profile in the CLI) that contains attributes, or characteristics of a device. Specification of the device identity profile in the source-end-user-profile field is part of the device identity feature. If a device matches the attributes specified in the profile and other security policy parameters, then the security policy's action is applied to traffic issuing from the device.
Source addresses (excluded)	Name of the source address excluded from the policy.
Destination addresses (excluded)	Name of the destination address excluded from the policy.

Table 24: show security policies Output Fields (*continued*)

Field Name	Field Description
Source identities	One or more user roles specified for a policy.
Applications	<p>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</p> <ul style="list-style-type: none"> • IP protocol: The Internet protocol used by the application—for example, TCP, UDP, ICMP. • ALG: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If application-protocol ignore is configured, ignore is displayed. Otherwise, 0 is displayed. However, even if this command shows ALG: 0, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when application-protocol ignore is not configured for custom applications. • Inactivity timeout: Elapsed time without activity after which the application is terminated. • Source port range: The low-high source port range for the session application.
Dynamic Applications	Application identification based layer 7 dynamic applications.
Destination Address Translation	<p>Status of the destination address translation traffic:</p> <ul style="list-style-type: none"> • drop translated—Drop the packets with translated destination addresses. • drop untranslated—Drop the packets without translated destination addresses.
Application Firewall	<p>An application firewall includes the following:</p> <ul style="list-style-type: none"> • Rule-set—Name of the rule set. • Rule—Name of the rule. <ul style="list-style-type: none"> • Dynamic applications—Name of the applications. • Dynamic application groups—Name of the application groups. • Action—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following: <ul style="list-style-type: none"> • permit • deny • Default rule—The default rule applied when the identified application is not specified in any rules of the rule set.

Table 24: show security policies Output Fields (*continued*)

Field Name	Field Description
Action or Action-type	<ul style="list-style-type: none"> The action taken in regard to a packet that matches the policy's tuples. Actions include the following: <ul style="list-style-type: none"> permit firewall-authentication tunnel ipsec-vpn <i>vpn-name</i> pair-policy <i>pair-policy-name</i> source-nat pool <i>pool-name</i> pool-set <i>pool-set-name</i> interface destination-nat <i>name</i> deny reject services-offload
Session log	Session log entry that indicates whether the at-create and at-close flags were set at configuration time to log session information.
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.
Policy statistics	<ul style="list-style-type: none"> Input bytes—The total number of bytes presented for processing by the device. <ul style="list-style-type: none"> Initial direction—The number of bytes presented for processing by the device from the initial direction. Reply direction—The number of bytes presented for processing by the device from the reply direction. Output bytes—The total number of bytes actually processed by the device. <ul style="list-style-type: none"> Initial direction—The number of bytes from the initial direction actually processed by the device. Reply direction—The number of bytes from the reply direction actually processed by the device. Input packets—The total number of packets presented for processing by the device. <ul style="list-style-type: none"> Initial direction—The number of packets presented for processing by the device from the initial direction. Reply direction—The number of packets presented for processing by the device from the reply direction. Output packets—The total number of packets actually processed by the device. <ul style="list-style-type: none"> Initial direction—The number of packets actually processed by the device from the initial direction. Reply direction—The number of packets actually processed by the device from the reply direction. Session rate—The total number of active and deleted sessions. Active sessions—The number of sessions currently present because of access control lookups that used this policy. Session deletions—The number of sessions deleted since system startup. Policy lookups—The number of times the policy was accessed to check for a match.

Table 24: show security policies Output Fields (*continued*)

Field Name	Field Description
Per policy TCP Options	Configured syn and sequence checks, and the configured TCP MSS value for the initial direction and /or the reverse direction.

Sample Output

show security policies

```

user@host> show security policies
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
  Source addresses:
    sa-1-ipv4: 198.51.100.11/24
    sa-2-ipv6: 2001:db8:a0b:12f0::1/32
    sa-3-ipv6: 2001:db8:a0b:12f0::22/32
    sa-4-wc: 203.0.113.1/255.255.0.255
  Destination addresses:
    da-1-ipv4: 2.2.2.2/24
    da-2-ipv6: 2001:db8:a0b:12f0::8/32
    da-3-ipv6: 2001:db8:a0b:12f0::9/32
    da-4-wc: 192.168.22.11/255.255.0.255
  Source identities: role1, role2, role4
  Applications: any
  Action: permit, application services, log, scheduled
  Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
  Source addresses:
    sa-1-ipv4: 198.51.100.11/24
    sa-2-ipv6: 2001:db8:a0b:12f0::1/32
    sa-3-ipv6: 2001:db8:a0b:12f0::22/32
  Destination addresses:
    da-1-ipv4: 2.2.2.2/24
    da-2-ipv6: 2001:db8:a0b:12f0::1/32
    da-3-ipv6: 2001:db8:a0b:12f0::9/32
  Source identities: role1, role4
  Applications: any
  Action: deny, scheduled

```

show security policies (Dynamic Applications)

```

user@host> show security policies
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
  Source addresses: any
  Destination addresses: any
  Applications: any
  Dynamic Applications: junos:YAHOO
  Action: deny, log
Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
  Source addresses: any
  Destination addresses: any
  Applications: any
  Dynamic Applications: junos:web, junos:web:social-networking:facebook,
junos:TFTP, junos:QQ
  Action: permit, log
Policy: p3, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 3
  Source addresses: any

```

```

Destination addresses: any
Applications: any
Dynamic Applications: junos:HTTP, junos:SSL
Action: permit, application services, log

```

show security policies policy-name detail

```

user@host> show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
  sa-1-ipv4: 198.51.100.11/24
  sa-2-ipv6: 2001:db8:a0b:12f0::1/32
  sa-3-ipv6: 2001:db8:a0b:12f0::9/32
  sa-4-wc: 203.0.113.1/255.255.0.255
Destination addresses:
  da-1-ipv4: 192.0.2.0/24
  da-2-ipv6: 2001:db8:a0b:12f0::1/32
  da-3-ipv6: 2001:db8:a0b:12f0::9/32
  da-4-wc: 192.168.22.11/255.255.0.255
Source identities:
  role1
  role2
  role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Destination Address Translation: drop translated
Application firewall :
Rule-set: my_ruleset1
  Rule: rule1
    Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
    Dynamic Application groups: junos:web, junos:chat
    Action: deny
  Default rule: permit
Session log: at-create, at-close
Scheduler name: sch20
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
  Input bytes      : 18144      545 bps
    Initial direction: 9072      272 bps
    Reply direction  : 9072      272 bps
  Output bytes     : 18144      545 bps
    Initial direction: 9072      272 bps
    Reply direction  : 9072      272 bps
  Input packets    : 216        6 pps
    Initial direction: 108        3 bps
    Reply direction  : 108        3 bps
  Output packets   : 216        6 pps
    Initial direction: 108        3 bps
    Reply direction  : 108        3 bps
  Session rate     : 108        3 sps
  Active sessions  : 93
  Session deletions: 15
  Policy lookups    : 108

```

show security policies (Services-Offload)

```
user@host> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload, count
From zone: untrust, To zone: trust
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload
```

show security policies (Device Identity)

```
user@host> show security policies
From zone: trust, To zone: untrust
  Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0,
Sequence number: 1
    Source addresses: any
    Destination addresses: any
    source-end-user-profile: marketing-profile
    Applications: any
    Action: permit
```

show security policies detail

```
user@host> show security policies detail
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Source identities:
    role1
    role2
    role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input bytes      : 18144      545 bps
    Initial direction: 9072       272 bps
    Reply direction  : 9072       272 bps
```

```

Output bytes      :          18144          545 bps
  Initial direction:          9072          272 bps
  Reply direction  :          9072          272 bps
Input packets     :           216           6 pps
  Initial direction:          108           3 bps
  Reply direction  :          108           3 bps
Output packets    :           216           6 pps
  Initial direction:          108           3 bps
  Reply direction  :          108           3 bps
Session rate      :           108           3 sps
Active sessions   :            93
Session deletions :            15
Policy lookups    :           108

Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
5, Scope Policy: 0
Policy Type: Configured
Description: The policy p2 is for the sales team
Sequence number: 1
From zone: untrust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
  role1
  role2
  role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

show security policies detail (TCP Options)

```

user@host> show security policies policy-name policy1 detail
node0:
-----
Policy: policy1, action-type: permit, State: enabled, Index: 7, Scope Policy: 0
Policy Type: Configured
Sequence number: 2
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: 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
Per policy TCP MSS: initial: 800, reverse: 900

```

show security policies policy-name (Negated Address)

```

user@host> show security policies policy-name p1

```

node0:

```
-----
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit
```

show security policies policy-name detail (Negated Address)

user@host> show security policies policy-name p1 detail

node0:

```
-----
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses(excluded):
  ad1(ad): 255.255.255.255/32
  ad2(ad): 198.51.100.1/24
  ad3(ad): 198.51.100.6 ~ 198.51.100.56
  ad4(ad): 192.0.2.8/24
  ad5(ad): 198.51.100.99 ~ 198.51.100.199
  ad6(ad): 203.0.113.9/24
  ad7(ad): 203.0.113.23/24
Destination addresses(excluded):
  ad13(ad2): 198.51.100.76/24
  ad12(ad2): 198.51.100.88/24
  ad11(ad2): 192.0.2.23 ~ 192.0.2.66
  ad10(ad2): 192.0.2.93
  ad9(ad2): 203.0.113.76 ~ 203.0.113.106
  ad8(ad2): 203.0.113.199
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
```

show security policies global

user@host> show security policies global policy-name Pa

node0:

```
-----
Global policies:
Policy: Pa, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
From zones: zone1, zone2
To zones: zone3, zone4 Source addresses: any
Destination addresses: any
Applications: any
Action: permit
```

show services application-identification application

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification application (detail | summary)`

Release Information Command introduced in Junos OS Release 11.4.

Description Display detailed information about a specified application signature, detailed information about all application signatures, or a summary of the existing application signatures.

Options **detail** —Display detailed information for all application signatures.
summary—Display summary information for all application signatures.

Required Privilege Level view

Related Documentation

- [request services application-identification application on page 291](#)

List of Sample Output [show services application-identification application summary on page 350](#)
[show services application-identification application detail on page 351](#)
[show services application-identification application detail \(Custom Applications\) on page 352](#)

Output Fields [Table 25 on page 349](#) lists shows the output details for the **show services application-identification application detail** command.

Table 25: show services application-identification application summary Output Fields

Field Name	Field Description
Application(s)	The number of applications present.
Application	Name of the custom application.
Disabled	The status of the application and whether the mapping method is currently used to identify this application.
ID	The unique ID number of an application. ID numbers 1 through 32,767 are automatically generated for applications; these IDs do not change. ID numbers for custom applications use 16,777,216 to 33,554,431.
Order	Number used to specify priority when multiple applications match the traffic. The lowest order number takes the highest priority.

Table 26 on page 350 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 26: show services application-identification application Output Fields

Field Name	Field Description
Application Name	Name of the application.
Application Type	The basic application type, such as HTTP.
Description	A description of the application.
Application ID	The unique ID number of an application signature. ID numbers 1 through 32,767 are automatically generated for application; these IDs do not change. ID numbers for custom applications use 16,777,216 to 33,554,431.
Priority	Priority over other signature applications.
Order	Number used to specify priority when multiple patterns are matched for the same session. The lowest order number takes the highest priority.
Disabled	The status of the application and whether the mapping method is currently used to identify this application.
Number of Parent Group(s)	Total number of parent groups in this application signature group or cluster.
Application Group	Name of the application signature group associated with this application signature. Must be a unique name with a maximum length of 32 characters.
Application Tags	General information about this application type, for example, associated risk factors, technology, type of traffic, and so on. Support of application signature tags is dependent on the version of the loaded signature database. Please refer to the Juniper Networks security portal for further information.
Layer-7 Protocol(s)	List of applications or protocols over which this application can be sent.
Port Mapping: Default ports	The default port for this application type.

Sample Output

show services application-identification application summary

```

user@host> show services application-identification application summary
Application(s): 3616
  Applications      Disabled      ID      Order
  junos:SLACKER    No           1179    1
  junos:GOOGLE-TRUSTED-STORE    No           2819    5
  junos:AMJILT     No           2272    4

```

junos:DSI	No	2644	3
junos:HLN	No	2096	2
junos:ETSI-LI	No	537	1
junos:CRAZYSALOON	No	1720	5
junos:EKSISOZLUK	No	2436	4
junos:SABAH	No	2574	3
junos:AFREECA	No	2373	2
junos:SENEWEB	No	2068	1
junos:DIINO	No	776	5
junos:CARE2	No	376	4
junos:MOBAGE	No	1456	3
junos:CARTOONNETWORK	No	982	2
junos:AVATARS-UNITED	No	363	1
junos:CONVIVA	No	2015	5
junos:DREAMORA	No	1725	4
junos:ELWATANNEWS	No	2381	3
junos:REUTERS	No	1044	2
junos:BABYCENTER	No	364	1
junos:SOUTHWEST	No	289	5
junos:ONEDIO	No	2517	4
.....			
.....			

show services application-identification application detail

```

user@host> show services application-identification application detail junos:FTP

Application Name: junos:FTP
Application type: FTP
Description: This signature detects the File Transfer Protocol (FTP), which
provides facilities for transferring files to and from remote computer systems.
It usually runs on TCP port 21.
Application ID: 45
Priority: high
Order: 0
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:file-servers

```

```
Application Tags:
  characteristic      : Supports File Transfer
  characteristic      : Known Vulnerabilities
  characteristic      : Capable of Tunneling
  risk                : 3
  subcategory         : File-Servers
  category            : Infrastructure
Layer-7 Protocol(s):
  Protocol: TCP        / 205
  Protocol: SPDY       / 1469
  Protocol: SOCKS5     / 193
  Protocol: SOCKS4     / 192
  Protocol: HTTPS      / 68
  Protocol: HTTP2      / 2553
  Protocol: HTTP       / 67
Port Mapping:
  Default ports: TCP/21
Signature:
  Port range: N/A
  Client-to-server
  Order: 1
```

show services application-identification application detail (Custom Applications)

```
user@host> show services application-identification application detail example1
```

```
Application Name: example1
```

```
Application type: EXAMPLE1
```

```
Description: N/A
```

```
Application ID: 16777216
```

```
Priority: high
```

```
Order: 65500
```

```
Disabled: No
```

```
Layer-7 Protocol(s):
```

```
  Protocol: tcp        / tcp
```

```
  Port range: N/A
```

```
  Member(s): 1
```

```
    Member m01
```

```
      Context: stream
```

```
      Pattern: pat1
```

```
      Direction: CTS
```

show services application-identification application-system-cache (View)

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification application-system-cache`

Release Information Command introduced in Junos OS Release 10.2. Command updated in Junos OS Release 12.1X47-D10. Output updated in Junos OS Release 12.1X47-D15.

Description Display application ID from default port/protocol binding or from the application system cache.

Required Privilege Level view

Related Documentation

- [clear services application-identification application-system-cache \(Junos OS\) on page 282](#)

List of Sample Output [show services application-identification application-system-cache on page 354](#)

Output Fields [Table 27 on page 353](#) lists 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 27: show services application-identification application-system-cache Output Fields

Field Name	Field Description
application-cache	On or Off status of the application cache.
nested-application-cache	On or Off status of the nested application cache.
cache-unknown-result	On or Off status for caching unknown results.
cache-entry-timeout	The number of seconds the mapping information is saved.
pic	PIC number of the accumulated statistics.
Logical system name	Name of a specific logical system.
IP address	IP address.
Port	Port number.
Protocol	Type of protocol.
Application	Name of the application.

Table 27: show services application-identification application-system-cache Output Fields (continued)

Field Name	Field Description
Encrypted	Yes or No to identify the traffic as encrypted or not.

Sample Output

show services application-identification application-system-cache

```
user@host> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
  nested-application-cache: on
  cache-unknown-result: on
  cache-entry-timeout: 3600 seconds
  pic: 1/0
  Logical system name: root-logical-system
  IP address: 192.0.2.1                                Port: 443    Protocol:
TCP
  Application: SSL                                       Encrypted: Yes

  pic: 1/1
  Logical system name: root-logical-system
  IP address: 192.0.2.2                                Port: 80     Protocol:
TCP
  Application: HTTP                                       Encrypted: No
```

show services application-identification commit-status

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification commit-status]`

Release Information Command introduced in Junos OS Release 15.1X49-D40.

Description Display information about the commit status. Because the custom signatures commit is performed asynchronously, the command output shows the current status of your configuration commit.

Required Privilege Level view

Related Documentation

- [request services application-identification application on page 291](#)

List of Sample Output

- [show services application-identification commit-status on page 355](#)
- [show services application-identification commit-status on page 355](#)
- [show services application-identification commit-status on page 355](#)

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)

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification counter
<ssl-encrypted-sessions>`

Release Information Command introduced in Junos OS Release 10.2. Output updated in Junos OS Release 12.1X47-D10. Command and output updated in Junos OS Release 12.1X47-D15.

Description Display the status of all Junos OS application identification counter values per SPU.

Options `ssl-encrypted-sessions`—Display counters for SSL encrypted sessions.

Required Privilege Level view

Related Documentation

- [clear services application-identification counter \(Values\) on page 283](#)

List of Sample Output [show services application-identification counter on page 358](#)
[show services application-identification counter ssl-encrypted-sessions on page 358](#)

Output Fields [Table 28 on page 356](#) 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 28: show services application-identification counter Output Fields

Field Name	Field Description
PIC	PIC number of the accumulated statistics. <i>NOTE:</i> The PIC number is always displayed as 0 for SRX300, SRX320, SRX340, and SRX345 devices.
Unknown applications	Number of unknown applications.
Encrypted unknown applications	Number of encrypted unknown applications.
Cache hits	Number of sessions that matched the application in the AI cache.
Cache misses	Number of sessions that did not find the application in the AI cache.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.

Table 28: show services application-identification counter Output Fields (*continued*)

Field Name	Field Description
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.
Client-to-server encrypted packets processed	Number of client-to-server encrypted packets processed.
Server-to-client encrypted packets processed	Number of server-to-client encrypted packets processed.
Client-to-server encrypted bytes processed	Number of client-to-server encrypted payload bytes processed.
Server-to-client layer encrypted bytes processed	Number of server-to-client encrypted payload bytes processed.
Sessions bypassed due to resource allocation failure	Number of sessions bypassed due to resource allocation failure.
Segment case 1 - New segment to left	TCP segments contained before the previous segment.
Segment case 2 - New segment overlap right	TCP segments that start before the previous segment and are contained in it.
Segment case 3 - Old segment overlapped	TCP segments that start before the previous segment and extend beyond it.
Segment case 4 - New segment overlapped	TCP segments that start and end within the previous segment.
Segment case 5 - New segment overlap left	TCP segments that start within the previous segments and extend beyond it.
Segment case 6 - New segment overlap left	TCP segments that start after the previous segment. This is the normal case.

Sample Output

show services application-identification counter

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

pic: 6/0
Counter type                                     Value
Unknown applications                             5
Encrypted unknown applications                     0
Cache hits                                         0
Cache misses                                       8
Client-to-server packets processed                678
Server-to-client packets processed                 0
Client-to-server bytes processed                  83577
Server-to-client bytes processed                   0
Client-to-server encrypted packets processed      0
Server-to-client encrypted packets processed      0
Client-to-server encrypted bytes processed        0
Server-to-client encrypted bytes processed        0
Sessions bypassed due to resource allocation failure 0
Segment case 1 - New segment to left              0
Segment case 2 - New segment overlap right        0
Segment case 3 - Old segment overlapped           0
Segment case 4 - New segment overlapped           0
Segment case 5 - New segment overlap left         0
Segment case 6 - New segment to right             0
```

Sample Output

show services application-identification counter ssl-encrypted-sessions

```
user@host> show services application-identification counter ssl-encrypted-sessions

pic: 1/0
Counter type                                     Value
AI cache hits                                     0
AI cache hits by nested application               0
AI cache misses                                    0
AI matches                                         0
AI uni-matches                                    0
AI no-matches                                     0
AI partial matches                                0
AI no-partial matches                             0
Sessions that triggered Appid create session API  0
Sessions that do not incur signature match or decoding 0
Sessions that incur signature match or decoding    0
Client-to-server packets processed                 0
Server-to-client packets processed                 0
Client-to-server layer-7 bytes processed           0
Server-to-client layer-7 bytes processed           0
Terminal first data packets on both direction     0
pic: 1/1
Counter type                                     Value
AI cache hits                                     0
AI cache hits by nested application               0
AI cache misses                                    0
AI matches                                         0
AI uni-matches                                    0
AI no-matches                                     0
```

AI partial matches	0
AI no-partial matches	0
Sessions that triggered Appid create session API	0
Sessions that do not incur signature match or decoding	0
Sessions that incur signature match or decoding	0
Client-to-server packets processed	0
Server-to-client packets processed	0
Client-to-server layer-7 bytes processed	0
Server-to-client layer-7 bytes processed	0
Terminal first data packets on both direction	0

show services application-identification group

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification group [detail application-group name | summary]`

Release Information Command introduced in Junos OS Release 11.4.

Description Display detailed or summary information about a specified application signature group or all application signature groups. Both custom and predefined application signature groups can be displayed.

Options **detail *application-group name***—(Optional) Display detailed information for the specified application signature group.

summary—(Optional) Display summary information for all application signature groups.

Required Privilege Level view

Related Documentation

- [request services application-identification group on page 294](#)

List of Sample Output [show services application-identification group summary on page 361](#)
[show services application-identification group detail on page 361](#)

Output Fields [Table 29 on page 360](#) 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 29: show services application-identification group Output Fields

Field Name	Field Description
Description	Description of the specified application in the detailed display.
Group ID or ID	The unique ID number of an application signature or application signature group. ID numbers 1 through 32,767 are automatically generated for predefined application signatures and application signature groups; these IDs do not change. ID numbers for custom application signatures and application signature groups use ID numbers 32,768 to 65,534.
Disabled	The status of the application signature group and whether the signature method is currently used to identify this application. The default is No.
Application Group(s)	The application signature groups present.
Applications	The application signatures associated with this application signature group.

Sample Output

show services application-identification group summary

```
user@host> show services application-identification group summary
Application Group(s): 24
Application Groups                               Disabled  ID
my:enterprise                                   No        32770
junos:enterprise:voip                           No         25
junos:peer-to-peer:voip                         No         24
junos:peer-to-peer:chat                         No         23
junos:peer-to-peer:file-sharing                 No         22
...
```

show services application-identification group detail

```
user@host> show services application-identification group detail junos:social-networking
Group Name: junos:social-networking
Group ID: 36
Description: N/A
Disabled: No
Number of Applications: 0
Number of Sub-Groups: 2
Number of Parent-Groups: 1
Sub Groups:
  junos:social-networking:applications
  junos:social-networking:business
```

show services application-identification statistics applications

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification statistics applications <interval interval-number>`

Release Information Command introduced in Junos OS Release 11.4. Command updated in Junos OS Release 12.1.

Description Display application usage statistics.

- Options**
- **none**—Display cumulative session and byte statistics per application. Statistics are displayed in alphabetical order.
 - **interval *interval-number***—(Optional) Display interval statistics per application. Interval statistics are displayed in Top-N format, such that the first application displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval. The previous interval is 2, and the least current (oldest) is 8.

Required Privilege Level view

- Related Documentation**
- [statistics \(Services\) on page 256](#)
 - [clear services application-identification application-statistics on page 279](#)

List of Sample Output [show services application-identification statistics applications on page 363](#)
[show services application-identification statistics applications interval 3 on page 363](#)

Output Fields [Table 30 on page 362](#) 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 30: show services application-identification statistics applications Output Fields

Field Name	Field Description
Application	Name of the application.
Sessions	Number of sessions for the application.
Bytes	Size of the application in bytes.
<p>NOTE: When an SRX Series device is operating in chassis cluster mode (Active/Active mode - Z mode), the show services application-identification statistics applications command output does not provide complete statistics for bytes count for the session in application/application group statistics. This is because, ingress and egress traffic byte counts are updated separately on the primary and secondary nodes in the chassis cluster setup for a given application.</p>	

Table 30: show services application-identification statistics applications Output Fields
(continued)

Field Name	Field Description
Encrypted	Yes or No identifying the traffic as encrypted or not.

Sample Output

show services application-identification statistics applications

```

user@host> show services application-identification statistics applications

Last Reset: 2014-02-19 00:38:01 PST
Application      Sessions      Bytes
Encrypted
                SYSLOG        2            18610
No

```

show services application-identification statistics applications interval 3

```

user@host> show services application-identification statistics applications interval 8

Interval Start: 2014-02-19 21:10:29 PST
Elapsed time: 00:07:14

```

show services application-identification statistics application-groups

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification statistics application-groups <interval
interval-number>`

Release Information Command introduced in Junos OS Release 11.4.

Description Display application group usage statistics.

- Options**
- **none**—Display cumulative session and byte statistics per application group. Statistics are displayed in alphabetical order.
 - **interval interval-number**— (Optional) Display interval statistics per application group. Interval statistics are displayed in Top-N format, such that the first application group displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval. The previous interval is 2, and the least current (oldest) is 8.

Required Privilege Level view

- Related Documentation**
- [statistics \(Services\) on page 256](#)
 - [clear services application-identification application-statistics on page 279](#)

List of Sample Output [show services application-identification statistics application-groups on page 365](#)
[show services application-identification statistics application-groups interval 8 on page 365](#)

Output Fields [Table 31 on page 364](#) 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 31: show services application-identification statistics application-groups Output Fields

Field Name	Field Description
Application Group	Displays the name of the application group.
Sessions	Displays the number of sessions for the application group.

Table 31: show services application-identification statistics application-groups Output Fields (continued)

Field Name	Field Description
Kilo Bytes	Displays the size of the application group in kilobytes. NOTE: When an SRX Series device is operating in Chassis Cluster mode (Active/Active mode - Z mode), the show services application-identification statistics application-groups command output does not provide complete statistics for bytes count for the session in application/application group statistics. This is because, ingress and egress traffic byte counts are updated separately on the primary and secondary nodes in the chassis cluster setup for a given application.

Sample Output

show services application-identification statistics application-groups

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

```
Last Reset: 2014-02-19 00:38:01 PST
```

Application Group	Sessions	Kilo Bytes
junos:infrastructure	2	18
junos:encryption	1	2
junos:infrastructure:monitoring	2	18

show services application-identification statistics application-groups interval 8

```
user@host> show services application-identification statistics application-groups interval 8
```

```
Interval Start: 2014-02-19 21:07:29 PST
```

```
Elapsed time: 00:07:15
```

show services application-identification status

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification status`

Release Information Command introduced in Junos OS Release 12.1X47-D10.

Description Display detailed information about application identification status.

Required Privilege Level view

Related Documentation

- [request services application-identification application on page 291](#)

List of Sample Output [show services application-identification status on page 367](#)
[show services application-identification status \(DPI Performance Mode Enabled\) on page 368](#)

Output Fields [Table 32 on page 366](#) 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 32: show services application-identification status Output Fields

Field Name	Field Description
Status	Status of application identification: Enabled or Disabled .
Sessions under app detection	Sessions undergoing application identification detection.
Engine Version	Application identification detector engine version.
Max TCP session packet memory	Maximum number of TCP sessions that application identification maintains.
Force packet plugin	Force packet plugin status: Enabled or Disabled .
Force stream plugin	Force stream plugin status: Enabled or Disabled .
DPI Performance mode	DPI performance mode status. This field is displayed only if the DPI performance mode is enabled.
Statistics collection interval	Frequency (in minutes) for collecting statistics.
Status	Status of application system cache: Enabled or Disabled .

Table 32: show services application-identification status Output Fields
(continued)

Field Name	Field Description
Negative cache status	Status on the number of sessions that reach the Unknown cache entry: Enabled or Disabled .
Max Number of entries in cache	Maximum number of cache entries.
Cache timeout	Idle timeout after which the cache entries expires.
Download Server CGI	Name of the server from where protocol bundle was downloaded.
Auto Update	Status of auto update to receive protocol bundle updates from the server: Enabled or Disabled .
Status	Status of protocol bundle: Active or Free .
Version	Version of protocol bundle.
Session	The number of active sessions.

Sample Output

show services application-identification status

```

user@host> show services application-identification status
pic: 5/0

Application Identification
  Status                               Enabled
  Sessions under app detection         0
  Engine Version                       4.18.1-20 (build date Feb 15 2014)
  Max TCP session packet memory        30000
  Force packet plugin                  Disabled
  Force stream plugin                  Disabled
  Statistics collection interval        1 (in minutes)

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

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

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

```

Sample Output

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

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

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

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

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

[show services application-identification version](#)

Supported Platforms [SRX Series, vSRX](#)

Syntax `show services application-identification version`

Release Information Command introduced in Junos OS Release 10.2.

Description Display the Junos OS application package version.

Required Privilege Level view

Related Documentation

- [request services application-identification download on page 292](#)

List of Sample Output [show services application-identification version on page 369](#)

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 ssl proxy statistics

Supported Platforms [SRX1500, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX550M, SRX5600, SRX5800, vSRX](#)

Syntax `show services ssl proxy statistics`

Release Information Command introduced in Junos OS Release 12.1.

Description Display information about the SSL proxy statistics.



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 **none**—Display summary information about SSL proxy.

Required Privilege Level view

Related Documentation • [clear services ssl proxy statistics on page 284](#)

List of Sample Output [show services ssl proxy statistics on page 371](#)

Output Fields [Table 33 on page 370](#) 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 33: show services ssl proxy statistics Output Fields

Field Name	Field Description
Sessions matched	The number of proxy sessions that are matched.
Sessions bypassed: non SSL	The number of proxy sessions that are bypassed because the non SSL sessions limit was exceeded
Sessions bypassed: memory overflow	The number of proxy sessions that are bypassed because the memory usage limit per session was reached.
sessions bypassed: low memory	The number of proxy sessions that are bypassed because of low memory on Packet Forwarding Engine.
Sessions created	The number of proxy sessions that are newly created.
Sessions ignored	The number of proxy sessions that are ignored.

Table 33: show services ssl proxy statistics Output Fields (*continued*)

Field Name	Field Description
Sessions active	The number of proxy sessions that are active.
Sessions dropped	The number of proxy sessions that are dropped.
Sessions whitelisted	The number of sessions that are whitelisted. Whitelists comprise addresses or domain names that you want to exempt from the SSL proxy processing.
whitelisted url category match	Whitelists comprise url hostnames that you want to exempt from the SSL proxy processing.

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

```

