



Junos[®] OS

Logical Systems and Tenant Systems Feature Guide for Security Devices



Modified: 2018-09-24

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 Logical Systems and Tenant Systems Feature Guide for Security Devices
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://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	xvii
	Documentation and Release Notes	xvii
	Using the Examples in This Manual	xvii
	Merging a Full Example	xviii
	Merging a Snippet	xviii
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxii
	Opening a Case with JTAC	xxii
Chapter 1	Overview	23
	Logical Systems and Tenant Systems Overview	23
Chapter 2	Logical Systems	25
	Logical Systems Overview	25
	Understanding Logical Systems for SRX Series Services Gateways	26
	Features and Limitations of Logical Systems	29
	Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices	30
	Understanding the Interconnect Logical System and Logical Tunnel Interfaces	31
	Understanding Packet Flow in Logical Systems for SRX Series Devices	32
	Understanding Junos OS SRX Series Services Gateways Architecture	34
	Session Creation for Devices Running Logical Systems	35
	Understanding Flow on Logical Systems	35
	Understanding Packet Classification	36
	Handling Pass-Through Traffic for Logical Systems	36
	Handling Self-Traffic	37
	Understanding Session and Gate Limitation Control	39
	Understanding Sessions	39
	About Configuring Sessions	39
	Master Logical Systems Overview	40
	Understanding the Master Logical Systems and the Master Administrator Role	40
	SRX Series Logical Systems Master Administrator Configuration Tasks Overview	41
	Example: Configuring Multiple VPLS Switches and LT Interfaces for Logical Systems	44

User Logical Systems Overview	60
User Logical Systems Configuration Overview	61
Understanding User Logical Systems and the User Logical System Administrator Role	63
Setting Up a Logical System	64
Example: Configuring Root Password for Logical Systems	64
Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System	65
Security Profiles for Logical Systems	73
Understanding Logical Systems Security Profiles (Master Administrators Only)	73
Logical Systems Security Profiles	74
How the System Assesses Resources Assignment and Use Across Logical Systems	75
Cases: Assessments of Reserved Resources Assigned Through Security Profiles	76
Example: Configuring Logical Systems Security Profiles (Master Administrators Only)	79
Example: Configuring User Logical Systems Security Profiles	87
Example: Configuring Security log stream for Logical Systems	92
CPU Allocation for Logical Systems	96
Understanding CPU Allocation and Control	96
CPU Control	97
Reserved CPU Utilization Quota for Logical Systems	97
CPU Control Target	98
Shared CPU Resources and CPU Quotas	98
Monitoring CPU Utilization	100
Example: Configuring CPU Utilization (Master Administrators Only)	100
Routing and Interfaces for Master Logical Systems	103
Understanding Logical Systems Interfaces and Routing Instances	104
Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Master Administrators Only)	105
Example: Configuring OSPF Routing Protocol for the Master Logical Systems	114
Routing, Interfaces, and NAT for User Logical Systems	117
Understanding Logical Systems Network Address Translation	117
Example: Configuring Network Address Translation for a User Logical Systems	118
Example: Configuring Interfaces and Routing Instances for a User Logical Systems	121
Example: Configuring OSPF Routing Protocol for a User Logical Systems	124
Security Zones in Logical Systems	128
Understanding Logical Systems Zones	128
Example: Configuring User Logical Systems	130
Example: Configuring Security Zones for a User Logical Systems	141

User Authentication for Logical Systems	144
Example: Configuring Access Profiles (Master Administrators Only)	144
Example: Configuring Security Features for the Master Logical Systems	146
Understanding Logical System Firewall Authentication	152
Example: Configuring Firewall Authentication for a User Logical System	154
Understanding Integrated User Firewall support in a Logical System	158
Limitation of using user firewall authentication	158
Example: Configuring Integrated User Firewall Identification Management for a User Logical System	158
Security Policies for Logical Systems	166
Understanding Logical Systems Security Policies	167
Security Policies in Logical Systems	167
Application Timeouts	167
Security Policy Allocation	168
Example: Configuring Security Policies in a User Logical Systems	168
Screen Options for User Logical Systems	172
Understanding Logical Systems Screen Options	172
Example: Configuring Screen Options for a User Logical Systems	172
VPNs in Logical Systems	174
Understanding Route-Based VPN Tunnels in Logical Systems	175
Example: Configuring IKE and IPsec SAs for a VPN Tunnel (Master Administrators Only)	176
Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems	180
UTM for Logical Systems	184
Understanding UTM Features in Logical Systems	184
Example: Configuring UTM for the Master Logical System	185
Example: Configuring UTM for a User Logical System	193
IDP for Logical Systems	201
IDP in Logical Systems Overview	202
IDP Policies	202
Limitation	203
IDP Installation and Licensing for Logical Systems	203
Understanding IDP Features in Logical Systems	204
Rulebases	204
Protocol Decoders	204
SSL Inspection	204
Inline Tap Mode	205
Multi-Detectors	205
Logging and Monitoring	205
Example: Configuring an IDP Policy for the Master Logical Systems	206
Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System	212
Example: Enabling IDP in a User Logical System Security Policy	214
Example: Configuring an IDP Policy for a User Logical System	217
ALG for Logical Systems	223
Understanding Application Layer Gateway (ALG) in Logical Systems	223
Enabling and Disabling ALG for Logical System	224
Example: Enabling FTP ALG in a Logical System	227

Application Security in Logical Systems	235
Understanding Logical Systems Application Identification Services	235
Understanding Logical Systems Application Firewall Services	236
Example: Configuring Application Firewall Services for a Master Logical Systems	237
Understanding Logical Systems Application Tracking Services	242
Example: Configuring Application Firewall Services for a User Logical System	242
Example: Configuring AppTrack for a User Logical Systems	246
IPv6 for Logical Systems	249
IPv6 Addresses in Logical Systems Overview	249
Understanding IPv6 Dual-Stack Lite in Logical Systems	250
Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems (Master Administrators Only)	251
Example: Configuring IPv6 Zones for a User Logical Systems	259
Example: Configuring IPv6 Security Policies for a User Logical Systems	263
Example: Configuring IPv6 Dual-Stack Lite for a User Logical Systems	266
ICAP Redirects for Logical Systems	268
ICAP Redirect Support for Logical Systems	268
Limitations of SSL Proxy with Logical Systems	269
Example: Configuring ICAP Redirect Service on SRX Devices	269
Logical Systems in a Chassis Cluster	274
Understanding Logical Systems in the Context of Chassis Cluster	274
Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (Master Administrators Only)	275
Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) (Master Administrators Only)	308
Example: Deleting a Logical System	342
Troubleshooting Logical Systems	345
Understanding Security Logs and Logical Systems	345
Limitations	346
Understanding Data Path Debugging for Logical Systems	346
Performing Tracing for Logical Systems (Master Administrators Only)	347
Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only)	352
Chapter 3 Tenant Systems	353
Tenant Systems Overview	353
Understanding Tenant Systems	354
Differences Between Logical Systems and Tenant Systems	354
Use Cases for Logical Systems and Tenant Systems	355
Deployment Scenarios for Multitenant Systems	355
Benefits of Tenant Systems	356
Roles and Responsibilities of Master Administrator, Tenant System Administrator, and Tenant System User	356

Tenant System Capacity	357
Tenant System Configuration Overview	358
Configuring a Routing Instance for a Tenant System	359
Example: Configuring Tenant Systems	360
Understanding Tenant System Security Profiles (Master Administrators Only)	364
Tenant Systems Security Profiles	364
Understanding How the System Assesses Resources Assignment and Use Across the Tenant Systems	365
Cases: Assessments of Reserved Resources Assigned Through Security Profiles	366
Example: Configuring Tenant Systems Security Profiles (Master Administrators Only)	369
Security Zones for Tenant Systems	377
Understanding Zones for Tenant Systems	377
Example: Configuring Zones in the Tenant System	378
Flow for Tenant Systems	381
Session Creation for Devices Running Tenant Systems	381
Understanding Packet Classification	382
Understanding the VPLS Switch and Logical Tunnel Interfaces	382
Handling Pass-Through Traffic for Tenant Systems	383
Handling Self-Traffic	384
Understanding Session and Gate Limitation Control	385
About Configuring Sessions	386
Configuring Logical Systems and Tenant Systems Interconnect with Multiple VPLS Switches	386
Configuring tenant systems Interconnect with Logical Tunnel Interface point-to-point connection	394
Configuring Logical System and Tenant System Interconnect with a Logical Tunnel Interface point-to-point connection	400
Firewall Authentication for Tenant Systems	406
Understanding Tenant System Firewall Authentication	406
Configuring Firewall Authentication for a Tenant System	408
Security Policies for Tenant Systems	419
Understanding Security Policies for Tenant Systems	419
Application Timeouts	419
Security Policy Allocation	419
Example: Configuring Security Policies in the Tenant System	420
Screen Options for Tenant Systems	424
Understanding Tenant System Screen Options	424
Example: Configuring Screen Options for a Tenant System	424
NAT for Tenant Systems	429
Understanding Network Address Translation for Tenant systems	429
Example: Configuring Network Address Translation for the Tenant Systems	430
ALG for Tenant Systems	436
Understanding ALG Support for Tenant System	436
Enabling and Disabling ALG for Tenant System	437
Example: Configuring ALG in Tenant System	440

	Security Log for Tenant Systems	445
	Understanding of Security Log for Tenant Systems	445
	Example: Configure Security Log for Tenant Systems	446
Chapter 4	Configuration Statements	451
	address-book	453
	address-book (System)	455
	alg	456
	anti-spam (Logical System Security Feature Profile)	458
	anti-virus (Logical System Security Feature Profile)	460
	appfw-profile (System)	462
	appfw-rule	463
	appfw-rule-set	464
	application-firewall	465
	application-tracking	466
	auth-entry	467
	cluster (Chassis)	468
	content-filtering (Logical System Security Feature Profile)	470
	cpu	472
	datapath-debug	473
	dslite-software-initiator	475
	file (System Logging)	476
	firewall-authentication (Security)	478
	firewall-authentication (tenants)	479
	web-authentication	480
	pass-through	481
	flow (Security Flow)	482
	flow-gate	484
	flow-session	485
	idp (Security)	487
	idp (logical-systems)	496
	idp-policy	496
	ike (Security)	497
	ipsec (Security)	500
	log (Security)	503
	logical-system (System Security Profile)	507
	logical-systems	508
	logical-systems (All)	510
	nat	511
	nat-cone-binding	515
	nat-destination-pool	516
	nat-destination-rule	517
	nat-interface-port-ol (System)	518
	nat-nopat-address	519
	nat-pat-address	520
	nat-pat-portnum	521
	nat-port-ol-ipnumber	522
	nat-rule-referenced-prefix (System)	523
	nat-source-pool	524

	nat-source-rule	525
	nat-static-rule	526
	policies	527
	policy (System Security Profile)	532
	policy-with-count	533
	profile (Access)	534
	purging	535
	root-authentication	536
	root-logical-system	537
	scheduler (System Security Profile)	538
	screen (Security)	539
	security-profile	543
	security-profile-resources	546
	stream (logical-systems security log)	547
	softwires	548
	web-filtering (Logical System Security Feature Profile)	549
	zone (System Security Profile)	553
	zones	554
Chapter 5	Operational Commands	557
	clear security application-firewall rule-set statistics logical-system	560
	clear security dns-cache	561
	clear security firewall-authentication users	562
	clear security firewall-authentication history	564
	clear security idp attack table	566
	clear security idp counters ips	567
	clear security idp counters pdf-decoder	568
	clear security idp counters ssl-inspection	569
	clear security idp counters memory	570
	clear security idp counters memory	571
	clear security idp counters tcp-reassembler	572
	clear security idp counters application-identification	573
	clear security idp counters action	574
	clear security idp counters dfa	575
	clear security idp counters flow	576
	clear security idp counters log	577
	clear security idp counters http-decoder	578
	clear security idp counters packet-log	579
	clear security idp counters packet	580
	clear security idp counters policy-manager	581
	clear security flow session tenant	582
	request security datapath-debug capture start	583
	request security datapath-debug capture stop	584
	set chassis cluster cluster-id node node-number reboot	585
	show chassis cluster status	586
	show log	589
	show route tenant	593
	show security application-firewall rule-set	595
	show security application-firewall rule-set logical-system	598

show security application-tracking counters	601
show security alg status logical-system	602
show security datapath-debug capture	605
show security datapath-debug counter	606
show security dns-cache	607
show security firewall-authentication history	609
show security firewall-authentication users	612
show security flow session	615
show security flow session tenant	622
show security idp logical system	624
show security idp attack table	625
show security idp counters action	626
show security idp counters application-identification	628
show security idp counters memory	632
show security idp counters ssl-inspection	634
show security idp counters pdf-decoder	636
show security idp counters log	638
show security idp counters ips	642
show security idp counters dfa	646
show security idp counters flow	648
show security idp counters http-decoder	655
show security idp counters packet-log	657
show security idp counters packet	659
show security idp counters policy-manager	663
show security idp counters tcp-reassembler	665
show security idp logical-system policy-association	669
show security idp policies	670
show security idp policy-commit-status	671
show security idp policy-templates-list	672
show security idp security-package-version	673
show security ike security-associations	675
show security ipsec security-associations	685
show security match-policies	699
show security nat destination rule	705
show security nat destination summary	709
show security nat source rule	712
show security nat source summary	716
show security nat static rule	719
show security policies	723
show security screen statistics	735
show services user-identification authentication-table	745
show system security-profile	759
show system security-profile scheduler	765
show system security-profile security-log-stream-number detail logical-system all	768
show system security-profile security-log-stream-number logical-system all . .	770
show system security-profile security-log-stream-number summary	772
show security softwires	774
show security zones	775

List of Figures

Chapter 2	Logical Systems	25
	Figure 1: Understanding Logical Systems	27
	Figure 2: Logical Systems, Their Virtual Routers, and Their Interfaces	33
	Figure 3: Configuring the interconnect logical systems	45
	Figure 4: Configuring the interconnect logical systems with VPLS switches	46
	Figure 5: SRX Series Device Configured for Logical Systems	66
	Figure 6: Configuring Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers	107
	Figure 7: Configuring IPv6 Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers	253
	Figure 8: Logical Systems in a Chassis Cluster	278
	Figure 9: Logical Systems in a Chassis Cluster (IPv6)	311
Chapter 3	Tenant Systems	353
	Figure 10: Tenant Systems	354
	Figure 11: Tenant Systems, Their Virtual Routers, and Their Interfaces	383
	Figure 12: Configuring the interconnected logical systems and tenant systems with multiple VPLS switches.	387
	Figure 13: Configuring the interconnect tenant systems with a point-to-point connection LT interface	394
	Figure 14: Configuring the interconnect between logical systems and tenant systems with a point-to-point connection LT interface	401
	Figure 15: Topology for Tenant System	410

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xix
	Table 2: Text and Syntax Conventions	xix
Chapter 2	Logical Systems	25
	Table 3: Security Profiles Used for Reserved Resource Assessments	77
	Table 4: Reserved Resource Allocation Assessment Across Logical Systems	78
	Table 5: Resource Information for a User Logical System	88
	Table 6: CPU Utilization Scenario 1	99
	Table 7: CPU Utilization Scenario 2	99
	Table 8: CPU Utilization Scenario 3	100
	Table 9: Logical Systems, Security Profiles, and Reserved CPU Quotas	101
	Table 10: User Logical System Static NAT Configuration	119
	Table 11: User Logical System Interface and Routing Instance Configuration . . .	122
	Table 12: ls-marketing-dept Logical System Configuration	130
	Table 13: ls-accounting-dept Logical System Configuration	131
	Table 14: User Logical System Zone and Address Book Configuration	141
	Table 15: Access Profile Configuration	145
	Table 16: root-logical-system Security Feature Configuration	147
	Table 17: User Logical System Firewall Authentication Configuration	155
	Table 18: User Logical System Security Policies Configuration	169
	Table 19: User Logical System Screen Options Configuration	173
	Table 20: Logical System VPN Tunnel Configuration	176
	Table 21: User Logical System Route-Based VPN Configuration	181
	Table 22: UTM Configuration Type, Steps, and Parameters	186
	Table 23: UTM Configuration Type, Steps, and Parameters	194
	Table 24: IDP Configuration for the Master Logical System	207
	Table 25: User Logical System Zone and Address Book Configuration	260
	Table 26: User Logical System Security Policies Configuration	263
	Table 27: ICAP Redirect Configuration Parameters	270
Chapter 3	Tenant Systems	353
	Table 28: Differences Between Logical Systems and Tenant Systems	354
	Table 29: Deployment Scenarios with Respect to Tenant Systems	355
	Table 30: Roles and Responsibilities With Respect to Tenant Systems	356
	Table 31: Tenant Systems Capacity	357
	Table 32: Tenant System Configuration	361
	Table 33: Security Profiles Used for Reserved Resource Assessments	367
	Table 34: Reserved Resource Allocation Assessment Across Tenant Systems	368
	Table 35: Security Profiles for Logical Systems	369

Chapter 5

Table 36: Security Zones Parameters	379
Table 37: Firewall Authentication Options	407
Table 38: Firewall Configuration for the Tenant System	409
Table 39: Security Policies Parameters	420
Table 40: Tenant System NAT Configuration	430
Table 41: Comparison of Logging Stream Number	445
Operational Commands	557
Table 42: show chassis cluster status Output Fields	586
Table 43: show route summary Output Fields	593
Table 44: show security application-firewall rule-set Output Fields	595
Table 45: show security application-firewall rule-set logical-system Output Fields	599
Table 46: show security application-tracking counters	601
Table 47: show security dns-cache Output Fields	607
Table 48: show security firewall-authentication history Output Fields	610
Table 49: show security firewall-authentication users Output Fields	613
Table 50: show security flow session Output Fields	617
Table 51: show security flow session tenant	622
Table 52: show security idp attack table Output Fields	625
Table 53: show security idp counters action Output Fields	626
Table 54: show security idp counters application-identification Output Fields	628
Table 55: show security idp counters memory Output Fields	632
Table 56: show security idp counters ssl-inspection Output Fields	634
Table 57: show security idp counters pdf-decoder Output Fields	636
Table 58: show security idp counters log Output Fields	638
Table 59: show security idp counters ips Output Fields	642
Table 60: show security idp counters dfa Output Fields	646
Table 61: show security idp counters flow Output Fields	648
Table 62: show security idp counters http-decoder Output Fields	655
Table 63: show security idp counters packet Output Fields	659
Table 64: show security idp counters policy-manager Output Fields	663
Table 65: show security idp counters tcp-reassembler Output Fields	665
Table 66: show security idp logical-system policy-association Output Fields	669
Table 67: show security idp security-package-version Output Fields	673
Table 68: show security ike security-associations Output Fields	676
Table 69: show security ipsec security-associations	687
Table 70: show security match-policies Output Fields	701
Table 71: show security nat destination rule Output Fields	706
Table 72: show security nat destination summary Output Fields	709
Table 73: show security nat source rule Output Fields	713
Table 74: show security nat source summary Output Fields	717
Table 75: show security nat static rule Output Fields	720
Table 76: show security policies Output Fields	725
Table 77: show security screen statistics Output Fields	736
Table 78: show system security-profile Output Fields	761
Table 79: show security-profile scheduler Output Fields	765

Table 80: show system security-profile security-log-stream-number summary Output Fields	768
Table 81: show system security-profile security-log-stream-number logical-system all Output Fields	770
Table 82: show system security-profile security-log-stream-number summary Output Fields	772
Table 83: show security zones Output Fields	776

About the Documentation

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

Documentation and Release Notes

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

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

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

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

```
system {
  scripts {
    commit {
      file ex-script.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 xix](#) 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 xix](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<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.	<code>stub <default-metric metric>;</code>
(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.	<code>broadcast multicast</code> <code>(string1 string2 string3)</code>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<code>rsvp { # Required for dynamic MPLS only</code>
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	<code>community name members [community-ids]</code>
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	}
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

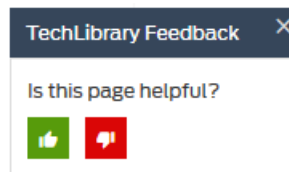
Table 2: Text and Syntax Conventions (continued)

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

Documentation Feedback

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

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



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Overview

- [Logical Systems and Tenant Systems Overview on page 23](#)

Logical Systems and Tenant Systems Overview

With the Junos operating system (Junos OS) on SRX Series device, you can partition a single security device into multiple logical devices that can perform independent tasks. Because logical systems perform a subset of the tasks once handled by the main device, logical systems offer an effective way to maximize the use of a single security platform.

A complex network design requires multiple layers of switches, routers, and security devices, which might lead to challenges in maintenance, configuration, and operation. To reduce such complexity, Juniper Networks supports logical systems. Logical systems perform a subset of the actions of the main device and have their own unique routing tables, interfaces, policies, and routing instances.

For SRX Series devices, you can partition a single device into following secure contexts:

- Logical systems
- Tenant systems

Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. A tenant system provides logical partitioning of the SRX device into multiple domains similar to logical systems and provides high scalability.

CHAPTER 2

Logical Systems

- [Logical Systems Overview on page 25](#)
- [Master Logical Systems Overview on page 40](#)
- [User Logical Systems Overview on page 60](#)
- [Setting Up a Logical System on page 64](#)
- [Security Profiles for Logical Systems on page 73](#)
- [CPU Allocation for Logical Systems on page 96](#)
- [Routing and Interfaces for Master Logical Systems on page 103](#)
- [Routing, Interfaces, and NAT for User Logical Systems on page 117](#)
- [Security Zones in Logical Systems on page 128](#)
- [User Authentication for Logical Systems on page 144](#)
- [Security Policies for Logical Systems on page 166](#)
- [Screen Options for User Logical Systems on page 172](#)
- [VPNs in Logical Systems on page 174](#)
- [UTM for Logical Systems on page 184](#)
- [IDP for Logical Systems on page 201](#)
- [ALG for Logical Systems on page 223](#)
- [Application Security in Logical Systems on page 235](#)
- [IPv6 for Logical Systems on page 249](#)
- [ICAP Redirects for Logical Systems on page 268](#)
- [Logical Systems in a Chassis Cluster on page 274](#)
- [Example: Deleting a Logical System on page 342](#)
- [Troubleshooting Logical Systems on page 345](#)

Logical Systems Overview

Logical systems enable you to partition a single device into multiple secure contexts that perform independent tasks. For more information, see the following topics:

- [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)
- [Features and Limitations of Logical Systems on page 29](#)

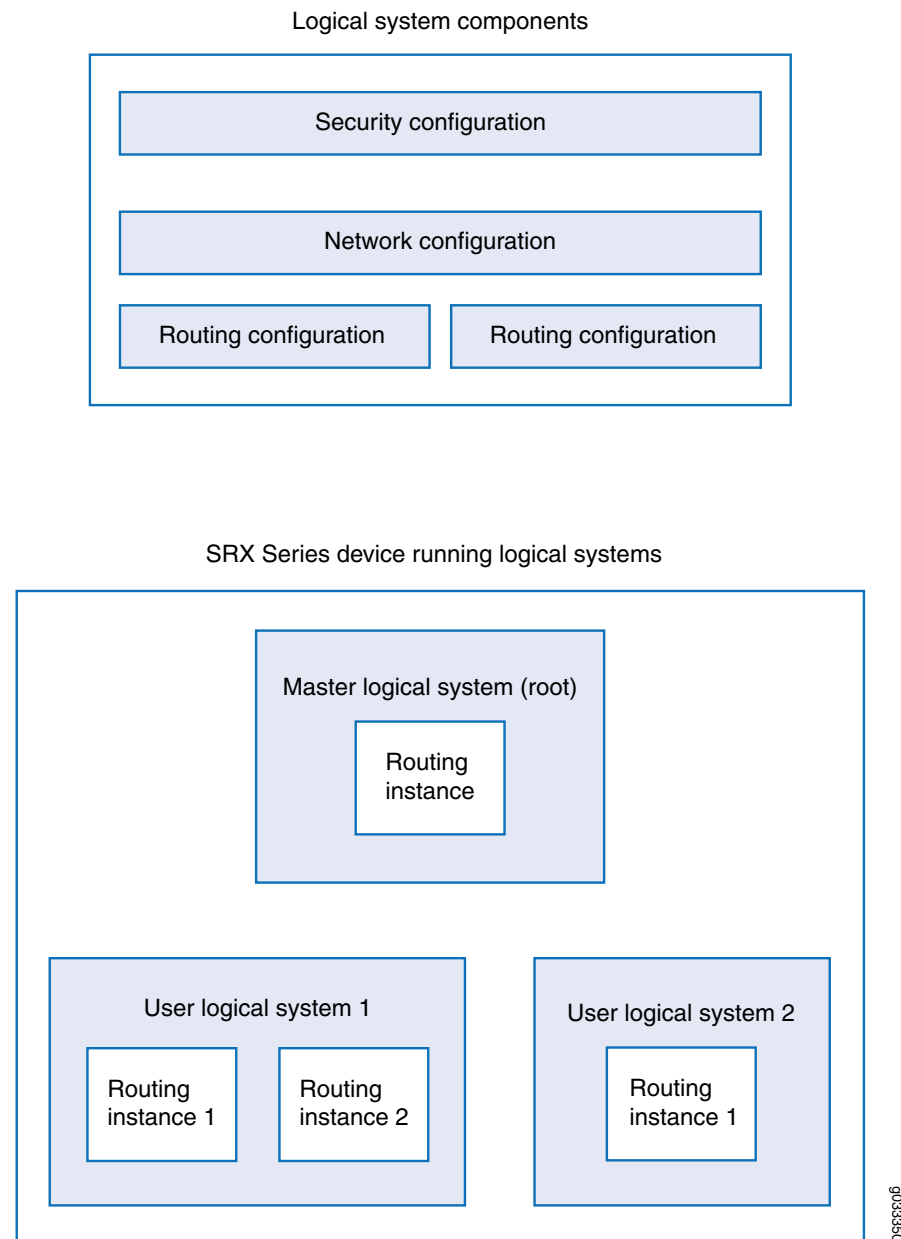
- [Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices on page 30](#)
- [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)
- [Understanding Packet Flow in Logical Systems for SRX Series Devices on page 32](#)

Understanding Logical Systems for SRX Series Services Gateways

Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. By transforming an SRX Series device into a multitenant logical systems device, you can give various departments, organizations, customers, and partners—depending on your environment—private use of portions of its resources and a private view of the device. Using logical systems, you can share system and underlying physical machine resources among discrete user logical systems and the master logical system.

The top part of [Figure 1 on page 27](#) shows the three main configuration components of a logical system. The lower part of the figure shows a single device with a master logical system and discrete user logical systems.

Logical systems include both master and user logical systems and their administrators. The roles and responsibilities of the master administrator and those of a user logical system administrator differ greatly. This differentiation of privileges and responsibilities is considered role-based administration and control.

Figure 1: Understanding Logical Systems

Logical systems on SRX Series devices offer many benefits, allowing you to:

- Curtail costs. Using logical systems, you can reduce the number of physical devices required for your company. Because you can consolidate services for various groups of users on a single device, you reduce both hardware costs and power expenditure.
- Create many logical systems on a single device and provision resources and services for them quickly. Because services are converged, it is easier for the master, or root, administrator to manage a single device configured for logical systems than it is to manage many discrete devices.

You can deploy an SRX Series device running logical systems in many environments, in particular, in the enterprise and in the data center.

- In the enterprise, you can create and provision logical systems for various departments and groups.

You can configure logical systems to enable communication among groups sharing the device. When you create logical systems for various departments on the same device, users can communicate with one another without traffic leaving the device if you have configured an interconnect logical system to serve as an internal switch. For example, members of the product design group, the marketing department, and the accounting department sharing an SRX Series Services Gateway running logical systems can communicate with one another just as they could if separate devices were deployed for their departments. You can configure logical systems to interconnect through *logical tunnel* (*lt-0/0/0*) internal interfaces. The *lt-0/0/0* interfaces on the interconnect logical system connect to an *lt-0/0/0* interface that you configure for each logical system. The interconnect logical system switches traffic between logical systems. The SRX Series device running logical systems provides for high, fast interaction among all logical systems created on the device when an interconnect logical system is used.

Logical systems on the same device can also communicate with one another directly through ports on the device, as if they were separate devices. Although this method allows for direct connections between logical systems, it consumes more resources—you must configure interfaces and an external switch—and therefore it is more costly.

- In the data center, as a service provider, you can deploy an SRX Series device running logical systems to offer your customers secure and private user logical systems and discrete use of the device's resources.

For example, one corporation might require 10 user logical systems and another might require 20. Because logical systems are secure, private, and self-contained, data belonging to one logical system cannot be viewed by administrators or users of other logical systems. That is, employees of one corporation cannot view the logical systems of another corporation.



NOTE: To use the internal switch, which is optional, you must also configure an interconnect logical system. The interconnect logical system does not require an administrator.



NOTE: This feature requires a license. To understand more about SRX Series devices license, see [Software Feature Licenses for SRX Series Devices](#). Please refer to the [Juniper Licensing Guide](#) for general information about License Management. Please refer to the product [Data Sheets](#) for details, or contact your Juniper Account Team or Juniper Partner.

See Also • [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)

- [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

Features and Limitations of Logical Systems

This topic covers basic information about the features and limitations of logical systems.

- By default, logical systems deliver a master logical system, which exists at the root level. You can purchase licenses for logical systems that you intend to create, with the total not exceeding 32.
- You can configure up to 32 security profiles, from 1 through 32, with ID 0 reserved for the internally configured default security profile. When the maximum number of security profiles is reached, if you want to add a new security profile, you must first delete one or more existing security profiles, commit the configuration, and then create the new security profile and commit it. You cannot add a new security profile and remove an existing one within a single configuration commit.

If you want to add more than one new security profile, the same rule is true. You must first delete the equivalent number of existing security profiles, commit the configuration, and then create the new security profiles and commit the configuration.

- You can configure one or more master administrators to oversee administration of the device and the logical systems they configure.

As master administrator for an SRX Series Services Gateway running logical systems, you have root control over the device, its resources, and the logical systems that you create. You allocate security, networking, and routing resources to user logical systems. You can configure one logical system to serve as an interconnect logical system virtual private LAN service (VPLS) switch. The interconnect logical system, which is not mandatory, does not require security resources. However, if you configure an interconnect logical system, you must bind a dummy security profile to it. The master administrator configures it and all `lt-0/0/0` interfaces for it.

- A user logical system can have one or more administrators, referred to as user logical system administrators. The master administrator creates login accounts for these administrators and assigns them to a user logical system. Currently, the master administrator must configure all user logical system administrators. The first assigned user logical administrator cannot configure additional user logical system administrators for his or her logical system. As a user logical system administrator, you can configure the resources assigned to your user logical system, including logical interfaces assigned by the master administrator, routing instances and their routes, and security components. You can display configuration information only for your logical system.
- A logical system can include more than one routing instance based on available system resources.
- You cannot configure class of service on `lt-0/0/0` interfaces.
- The trace and debug features are supported at the root level only.
- Commit rollback is supported at the root level only.

- Quality-of-service (QoS) classification across interconnected logical systems does not work.
- The master administrator can configure Application Layer Gateways (ALGs) at the root level. The configuration is inherited by all user logical systems. ALGs can also be configured discretely for user logical systems.
- The master administrator can configure IDP policies at the root level and then apply an IDP policy to a user logical system.
- Only the master administrator can create user accounts and login IDs for users for all logical systems. The master administrator creates these user accounts at the root level and assigns them to the appropriate user logical systems.
- The same name cannot be used in two separate logical systems. For example, if logical-system1 includes a user with Bob configured as the username, then other logical systems on the device cannot include a user with the username Bob.
- Configuration for users for all logical systems and all user logical systems administrators must be performed at the root level by the master administrator. A user logical system administrator cannot create other user logical system administrators or user accounts for their logical systems.
- Some of the scaling parameters are different for SRX1500 devices. For example, you can configure a maximum of 512 zones under a logical system.

- See Also**
- [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)
 - [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices

This topic provides licensing information for SRX Series devices running logical systems and tenant systems.

Starting in Junos OS Release 18.3R1, an SRX Series device running logical systems or tenant systems includes three licenses by default. One license for a master logical system and the other two licenses for user-defined logical system or tenant system. The system does not allow you to configure additional logical systems or tenant systems if the number of logical systems and tenant systems exceeds the number of available licenses. In the earlier releases, the system allowed you to configure an additional logical system even if the number of logical systems exceeds the number of available licenses, but with a warning message of non-licensed logical-systems do not pass traffic. You can purchase licenses for additional logical systems and tenant systems that you intend to create. If you intend to configure an interconnect logical system or interconnect tenant system to use as a switch, it also requires separate licenses.

We enforce that you do not configure more logical systems or tenant systems than the number of licenses you have purchased. If the number of logical systems or tenant

systems that you attempt to configure exceeds the number of licenses that you have purchased, then the system displays an error message similar to the following:

```
user@host> commit
error: 2 more multitenancy license(s) are needed!
error: configuration check-out failed
```

You can use the **show system license status all-logical-systems-tenants** or **show system license usage** commands to view the active logical systems and tenant systems on the device.

```
user@host> show system license status all-logical-systems-tenants
```

```
logical system name  license status
root-logical-system  enabled
LSYS2                enabled
LSYS0                enabled
LSYS11               enabled
LSYS12               enabled
LSYS23               enabled
TSYS1                enabled
TSYS2                enabled
TSYS3                enabled
```

```
user@host> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
logical-system	9	11	0	2019-05-18 08:00:00 CST

When you use SRX Series devices running logical systems or tenant systems in a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems or tenant systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

- See Also**
- [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)
 - [Understanding Tenant Systems on page 63](#)
 - *Understanding Chassis Cluster Licensing Requirements*
 - *Installing Licenses on the SRX Series Devices in a Chassis Cluster*
 - *Verifying Licenses on an SRX Series Device in a Chassis Cluster*

Understanding the Interconnect Logical System and Logical Tunnel Interfaces

This topic covers the interconnect logical system that serves as an internal virtual private LAN service (VPLS) switch connecting one logical system on the device to another. The topic also explains how logical tunnel (lt-0/0/0) interfaces are used to connect logical systems through the interconnect logical system.

A device running logical systems can use an internal VPLS switch to pass traffic without it leaving the device. The interconnect logical system switches traffic across logical systems that use it. Although a virtual switch is used typically, it is not mandatory. If you choose to use a virtual switch, you must configure the interconnect logical system. There can be only one interconnect logical system on a device.

For communication between logical systems on the device to occur, you must configure an `lt-0/0/0` interface on each logical system that will use the internal switch, and you must associate it with its peer `lt-0/0/0` interface on the interconnect logical system, effectively creating a logical tunnel between them. You define a peer relationship at each end of the tunnel when you configure the logical system's `lt-0/0/0` interfaces.

You might want all logical systems on the device to be able to communicate with one another without using an external switch. Alternatively, you might want some logical systems to connect across the internal switch but not all of them.

The interconnect logical system does not require security resources assigned to it through a security profile. However, you must assign a dummy security profile containing no resources to the interconnect logical system. Otherwise you will not be able to successfully commit the configuration for it.



WARNING: If you configure an `lt-0/0/0` interface in any user logical system or the master logical system and you do not configure an interconnect logical system containing a peer `lt-0/0/0` interface for it, the commit will fail.

An SRX Series device running logical systems can be used in a chassis cluster. Each node has the same configuration, including the interconnect logical system.

When you use SRX Series devices running logical systems within a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

- See Also**
- [Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\) on page 105](#)
 - [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)
 - [Understanding Logical Systems in the Context of Chassis Cluster on page 274](#)

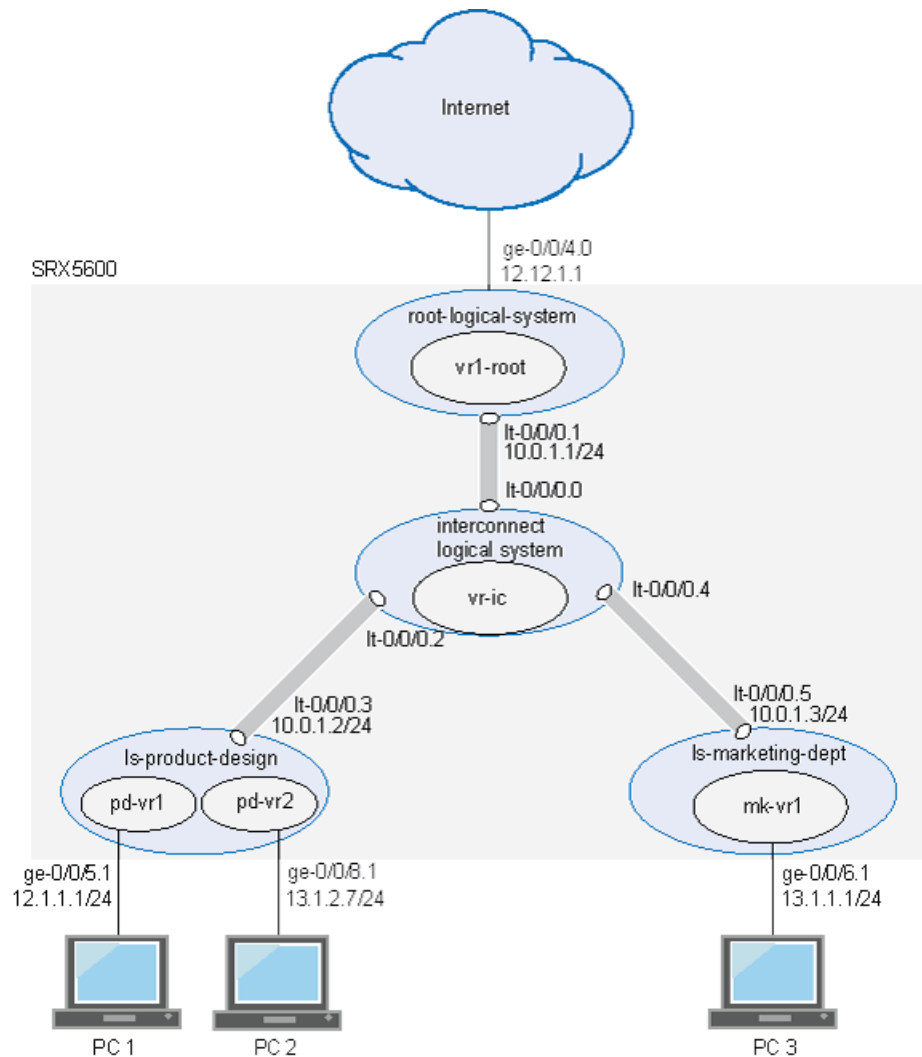
Understanding Packet Flow in Logical Systems for SRX Series Devices

This topic explains how packets are processed in flow sessions on SRX Series devices running logical systems. It describes how an SRX Series device running logical systems handles pass-through traffic in a single logical system and between logical systems. It also covers self-traffic as self-initiated traffic within a logical system and self-traffic terminated on another logical system. Before addressing logical systems, the topic provides basic information about the SRX Series architecture in with respect to packet

processing and sessions. Finally, it addresses sessions and how to change session characteristics.

The concepts explained in this example rely on the topology shown in [Figure 2 on page 33](#).

Figure 2: Logical Systems, Their Virtual Routers, and Their Interfaces



- [Understanding Junos OS SRX Series Services Gateways Architecture on page 34](#)
- [Session Creation for Devices Running Logical Systems on page 35](#)
- [Understanding Flow on Logical Systems on page 35](#)
- [Understanding Packet Classification on page 36](#)
- [Handling Pass-Through Traffic for Logical Systems on page 36](#)
- [Handling Self-Traffic on page 37](#)
- [Understanding Session and Gate Limitation Control on page 39](#)

- [Understanding Sessions on page 39](#)
- [About Configuring Sessions on page 39](#)

Understanding Junos OS SRX Series Services Gateways Architecture

Junos OS is a distributed parallel processing high throughput and high performance system. The distributed parallel processing architecture of the services gateways includes multiple processors to manage sessions and run security and other services processing. This architecture provides greater flexibility and allows for high throughput and fast performance.

The SRX5000 line devices include I/O cards (IOC) and Services Processing Cards (SPCs) that each contain processing units that process a packet as it traverses the device. A Network Processing Unit (NPU) runs on an IOC. An IOC has one or more NPUs. One or more Services Processing Units (SPUs) run on an SPC.

These processing units have different responsibilities. All flow-based services for a packet are executed on a single SPU. Otherwise, however, the lines are not clearly divided in regard to the kinds of services that run on these processors. (For details on flow-based processing, see *Understanding Traffic Processing on Security Devices*.)

For example:

- An NPU processes packets discretely. It performs sanity checks and applies some screens that are configured for the interface, such as denial-of-service (DoS) screens, to the packet.
- An SPU manages the session for the packet flow and applies security features and other services to the packet. It also applies packet-based stateless firewall filters, classifiers, and traffic shapers to the packet.
- The system uses one processor as a central point to take care of arbitration and allocation of resources and distribute sessions in an intelligent way. The central point assigns an SPU to be used for a particular session when the first packet of its flow is processed.

These discrete, cooperating parts of the system, including the central point, each store the information identifying whether a session exists for a stream of packets and the information against which a packet is matched to determine if it belongs to an existing session.

This architecture allows the device to distribute processing of all sessions across multiple SPUs. It also allows an NPU to determine if a session exists for a packet, to check the packet, and to apply screens to it. How a packet is handled depends on whether it is the first packet of a flow.

Flow-based packet processing treats related packets, or a stream of packets, in the same way. Packet treatment depends on characteristics that are established for the first packet of the packet stream when the flow session is established. Most packet processing occurs within a flow. For the distributed processing architecture of the services gateway, some packet-based processing, such as traffic shaping, occurs on the NPU. Some packet-based processing, such as application of classifiers to a packet, occurs on the SPU.

Configuration settings that determine the fate of a packet—such as the security policy that applies to it, Application Layer Gateway (ALG)s configured for it, if NAT should be applied to translate the packet's source and/or destination IP address—are assessed for the first packet of a flow.

Session Creation for Devices Running Logical Systems

Session establishment for SRX Series devices running logical systems differs in minor ways from that of SRX series devices not running logical systems. Despite the complexities that logical systems introduce, traffic is handled in a manner similar to how it is handled on SRX Series devices not running logical systems. Flow-based packet processing, which is stateful, requires the creation of sessions. In considering flow based processing and session establishment for logical systems, it helps to think of each logical system on the device as a discrete device with respect to session establishment.

A session is created, based on routing and other classification information, to store information and allocate resources for a flow. Basically, a session is established when traffic enters a logical system interface, route lookup is performed to identify the next hop interface, and policy lookup is performed.

Optionally, logical systems enable you to configure an internal software switch. This virtual private LAN switch (VPLS) is implemented as an interconnect logical system. It enables both transit traffic and traffic terminated at a logical system to pass between logical systems. To enable traffic to pass between logical systems, logical tunnel (lt-0/0/0) interfaces across the interconnect logical system are used.

Communication between logical systems across the interconnect logical system requires establishment of two sessions: one for traffic that enters a logical system and exits its lt-0/0/0 interface, and one for traffic that enters the lt-0/0/0 interface of another logical system and either exits the device through one of its physical interface or is destined for it.



NOTE: Packet sequence occurs at the ingress and the egress interfaces. Packets traveling between logical systems might not be processed in the order in which they were received on the physical interface.

Understanding Flow on Logical Systems

To understand how traffic is handled for logical systems, it is helpful to consider each logical system as a discrete device.



NOTE: Traffic is processed for the master logical system in the same way as it is for user logical systems on the device.



NOTE: On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 Series devices, J-Flow version 5, version 8, and version 9 are not supported on logical systems.

Understanding Packet Classification

Packet classification is assessed the same way for SRX Series devices running with or without logical systems. Filters and class-of-service features are typically associated with an interface to influence which packets are allowed to transit the system and to apply special actions to packets as needed. (Within a flow, some packet-based processing also takes place on an SPU.)

Packet classification is based on the incoming interface and performed at the ingress point. Traffic for a dedicated interface is classified to the logical system that contains that interface. Within the context of a flow, packet classification is based on both the physical interface and the logical interface.

Handling Pass-Through Traffic for Logical Systems

For SRX Series devices not running logical systems, pass-through traffic is traffic that enters and exits a device. You can think of pass-through traffic for logical systems similarly, but as having a larger dimension as a result of the nature of a multitenant device. For SRX Series devices running logical systems, pass-through traffic can exist within a logical system or between logical systems.

- [Pass-Through Traffic Within a Logical System on page 36](#)
- [Pass-Through Traffic Between Logical Systems on page 37](#)

Pass-Through Traffic Within a Logical System

For pass-through traffic within a logical system, traffic comes in on an interface belonging to one of the logical system's virtual routing instances, and it is sent to another of its virtual routing instances. To exit the device, the traffic is sent out an interface belonging to the second virtual routing instance. The traffic does not transit between logical systems but rather enters and exits the device in a single logical system. Pass-through traffic within a logical system is transmitted according to the routing tables in each of its routing instances.

Consider how pass-through traffic is handled within a logical system given the topology shown in [Figure 2 on page 33](#).

- When a packet arrives on interface ge-0/0/5, it is identified as belonging to the ls-product-design logical system.
- Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1 with pd-vr2 identified as the next hop.
- A second route lookup is performed in pd-vr2 to identify the egress interface to use—in this case— ge-0/0/8.
- The packet is sent out ge-0/0/8 to the network.
- The security policy lookup is performed in ls-product-design, and one session is established.

Pass-Through Traffic Between Logical Systems

Pass-through traffic between logical systems is complicated by the fact that each logical system has an ingress and an egress interface that the traffic must transit. It is as if traffic were coming into and going out from two devices.

Two sessions must be established for pass-through traffic between logical systems. (Note that policy lookup is performed in both logical systems).

- On the incoming logical system, one session is set up between the ingress interface (a physical interface) and its egress interface (an `lt-0/0/0` interface).
- On the egress logical system, another session is set up between the ingress interface (the `lt-0/0/0` interface of the second logical system) and its egress interface (a physical interface).

Consider how pass-through traffic is handled across logical systems in the topology shown in [Figure 2 on page 33](#).

- A session is established in the incoming logical system.
 - When a packet arrives on interface `ge-0/0/5`, it is identified as belonging to the `ls-product-design` logical system.
 - Because `ge-0/0/5` belongs to the `pd-vr1` routing instance, route lookup is performed in `pd-vr1`.
 - As a result of the lookup, the egress interface for the packet is identified as `lt-0/0/0.3` with the next hop identified as `lt-0/0/0.5`, which is the ingress interface in the `ls-marketing-dept`.
 - A session is established between `ge-0/0/5` and `lt-0/0/0.3`.
- A session is established in the outgoing logical system.
 - The packet is injected into the flow again from `lt-0/0/0.5`, and the logical system context identified as `ls-marketing-dept` is derived from the interface.
 - Packet processing continues in the `ls-marketing-dept` logical system.
 - To identify the egress interface, route lookup for the packet is performed in the `mk-vr1` routing instances.
 - The outgoing interface is identified as `ge-0/0/6`, and the packet is transmitted from the interface to the network.

Handling Self-Traffic

Self-traffic is traffic that originates in a logical system on the device and is either sent out to the network from that logical system or is terminated on another logical system on the device.

Self-Initiated Traffic

Self-initiated traffic is generated from a source logical system context and forwarded directly to the network from the logical system interface.

The following process occurs:

- When a packet is generated in a logical system, a process for handling the traffic is started in the logical system.
- Route lookup is performed to identify the egress interface, and a session is established.
- The logical system performs a policy lookup and processes the traffic accordingly.
- If required, a management session is set up.

Consider how self-initiated traffic is handled across logical systems given the topology shown in [Figure 2 on page 33](#).

- A packet is generated in the ls-product-design logical system, and a process for handling the traffic is started in the logical system.
- Route lookup performed in pd-vr2 to identifies the egress interface as ge-0/0/8.
- A session is established.
- The packet is transmitted to the network from ge-0/0/8.

Traffic Terminated on a Logical System

When a packet enters the device on an interface belonging to a logical system and the packet is destined for another logical system on the device, the packet is forwarded between the logical systems in the same manner as is pass-through traffic. However, route lookup in the second logical system identifies the local egress interface as the packet destination. Consequently the packet is terminated on the second logical system as self-traffic.

- For terminated self-traffic, two policy lookups are performed, and two sessions are established.
 - On the incoming logical system, one session is set up between the ingress interface (a physical interface) and its egress interface (an lt-0/0/0 interface).
 - On the destination logical system, another session is set up between the ingress interface (the lt-0/0/0 interface of the second logical system) and the local interface.

Consider how terminated self-traffic is handled across logical systems in the topology shown in [Figure 2 on page 33](#).

- A session is established in the incoming logical system.
 - When a packet arrives on interface ge-0/0/5, it is identified as belonging to the ls-product-design logical system.
 - Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1.
 - As a result of the lookup, the egress interface for the packet is identified as lt-0/0/0.3 with the next hop identified as lt-0/0/0.5, the ingress interface in the ls-marketing-dept.
- A session is established between ge-0/0/5 and lt-0/0/0.3.

- A management session is established in the destination logical system.
 - The packet is injected into the flow again from lt-0/0/0.5, and the logical system context identified as ls-marketing-dept is derived from the interface.
 - Packet processing continues in the ls-marketing-dept logical system.
 - Route lookup for the packet is performed in the mk-vr1 routing instance. The packet is terminated in the destination logical system as self-traffic.
- A management session is established.

Understanding Session and Gate Limitation Control

The logical systems flow module provides session and gate limitation to ensure that these resources are shared fairly among the logical systems. Resources allocation and limitations for each logical system are specified in the security profile bound to the logical system.

- For session limiting, the system checks the first packet of a session against the maximum number of sessions configured for the logical system. If the maximum is reached, the device drops the packet and logs the event.
- For gate limiting, the device checks the first packet of a session against the maximum number of gates configured for the logical system. If the maximum number of gates for a logical system is reached, the device rejects the gate open request and logs the event.

Understanding Sessions

Sessions are created based on routing and other classification information to store information and allocate resources for a flow. You can change some characteristics of sessions, such as when a session is terminated. For example, you might want to ensure that a session table is never entirely full to protect against an attacker's attempt to flood the table and thereby prevent legitimate users from starting sessions.

About Configuring Sessions

Depending on the protocol and service, a session is programmed with a timeout value. For example, the default timeout for TCP is 1800 seconds. The default timeout for UDP is 60 seconds. When a flow is terminated, it is marked as invalid, and its timeout is reduced to 10 seconds. If no traffic uses the session before the service timeout, the session is aged out and freed to a common resource pool for reuse.

You can affect the life of a session in the following ways:

- Age out sessions, based on how full the session table is.
- Set an explicit timeout for aging out TCP sessions.
- Configure a TCP session to be invalidated when it receives a TCP RST (reset) message.
- You can configure sessions to accommodate other systems as follows:
 - Disable TCP packet security checks.

- Change the maximum segment size.

- See Also**
- [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)
 - [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

Master Logical Systems Overview

Master logical systems can create a user logical system and configure the security resources of the user logical system. Master logical systems assign the logical interfaces to the user logical systems. For more information, see the following topics:

- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
- [SRX Series Logical Systems Master Administrator Configuration Tasks Overview on page 41](#)
- [Example: Configuring Multiple VPLS Switches and LT Interfaces for Logical Systems on page 44](#)

Understanding the Master Logical Systems and the Master Administrator Role

When, as a master administrator, you initialize an SRX Series device running logical systems, a master logical system is created at the root level. You can log in to the device as root and change the root password.

By default, all system resources are assigned to the master logical system, and the master administrator allocates them to the user logical systems.

As master administrator, you manage the device and all its logical systems. You also manage the master logical system and configure its assigned resources. There can be more than one master administrator managing a device running logical systems.

- The master administrator's role and main responsibilities include:
 - Creating user logical systems and configuring their administrators. You can create one or more user logical system administrators for each user logical system.
 - Creating login accounts for users for all logical systems and assigning them to the appropriate logical systems.
 - Configuring an interconnect logical system if you want to allow communication between logical systems on the device. The interconnect logical system acts as an internal switch. It does not require an administrator.

To configure an interconnect logical system, you configure lt-0/0/0 interfaces between the interconnect logical system and each logical system. These peer interfaces effectively allow for establishment of tunnels.

- Configuring security profiles to provision portions of the system's security resources to user logical systems and the master logical system.

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



NOTE: A user logical system administrator can configure interface, routing, and security resources allocated to his logical system.

- Creating logical interfaces to assign to user logical systems. (The user logical system administrator configures logical interfaces assigned to his logical system.)
- Viewing and managing user logical systems, as required, and deleting user logical systems. When a user logical system is deleted, its allocated reserved resources are released for use by other logical systems.
- Configuring IDP, AppTrack, application identification, and application firewall features. The master administrator can also use trace and debug at the root level, and he can perform commit rollbacks. The master administrator manages the master logical system and configures all the features that a user logical system administrator can configure for his or her own logical systems including routing instances, static routes, dynamic routing protocols, zones, security policies, screens, and firewall authentication.

- See Also**
- [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)
 - [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)
 - [Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\) on page 105](#)

SRX Series Logical Systems Master Administrator Configuration Tasks Overview

This topic describes the master administrator's tasks in the order in which they are performed.

An SRX Series device running logical systems is managed by a master administrator. The master administrator has the same capabilities as the root administrator of an SRX Series device not running logical systems. However, the master administrator's role and responsibilities extend beyond those of other SRX Series device administrators because an SRX Series device running logical systems is partitioned into discrete logical systems, each with its own resources, configuration, and management concerns. The master administrator is responsible for creating these user logical systems and provisioning them with resources.

For an overview of the master administrator's role and responsibilities, see "[Understanding the Master Logical Systems and the Master Administrator Role](#)" on page 40.

As the master administrator, you perform the following tasks to configure an SRX Series device running logical systems:

1. Configure a root password. Initially the master administrator logs in to the device as the root user without needing to specify a password. After you log in to the device, you must define a root password for later use.

See [“Example: Configuring Root Password for Logical Systems”](#) on page 64 for configuration information.

2. Create user logical systems and their administrators and users. Optionally, create an interconnect logical system.

For each user logical system that you want to configure on the device, you must create a logical system, define one or more administrators for it, and add users to it.

The master administrator configures login accounts for user logical system administrators and users and associates them with the user logical system. A user logical system can have more than one administrator; the master administrator must define and add all user logical system administrators and add them to their user logical systems.

The master administrator adds users to user logical systems on behalf of the user logical system administrator. For example, if you have created a user logical system for the product design department, you must create user accounts for the users who belong to that department and associate them with the user logical system. The user logical system administrator does not have the ability to do this. Rather, the user logical administrator tells you the user accounts that you must create and add for his logical system.

- For configuration information, see [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65
 - For information on user logical system administrators, see [“Understanding User Logical Systems and the User Logical System Administrator Role”](#) on page 63.
 - For information on the interconnect logical system, see [“Understanding the Interconnect Logical System and Logical Tunnel Interfaces”](#) on page 31.
3. Configure one or more security profiles. Security profiles assign security resources to logical systems. You can assign a single security profile to more than one logical system if you intend to allocate the same kinds and amounts of resources to them.
 - For configuration information, see [“Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\)”](#) on page 79.
 - For information on security profiles, see [“Understanding Logical Systems Security Profiles \(Master Administrators Only\)”](#) on page 73.
 4. Configure interfaces, routing instances, and static routes for logical systems, as appropriate.
 - If you plan to use an interconnect logical system, configure its logical tunnel interfaces and add them to its virtual routing instance.
 - Configure interfaces for the master logical system. Optionally, create its logical tunnel interface to allow it to communicate with other logical systems on the device. Create a virtual routing instance for the master logical system and add its interfaces

and static routes to it. Also configure logical interfaces for user logical systems with VLAN tagging.



NOTE: The master administrator tells the user logical system administrators which interfaces are assigned to their logical systems. It is the user logical system administrator's responsibility to configure their interfaces.

- Optionally, configure logical tunnel interfaces for any user logical systems that you want to allow to communicate with one another using the internal VPLS switch. VPLS is a virtual private network (VPN) technology. It allows point-to-point layer 2 tunnels connectivity.

By creating a VPLS type routing-instance (RI), we define a VPLS switch. VPLS switch behaves like a L2 ethernet switch. We assign multiple LT IFLs to the VPLS switch. Each LT IFL have encapsulation ethernet-vpls and this behaves as L2 switch port. To connect to the VPLS switch, each logical system creates a LT IFL and assigns to a port of the VPLS switch.

Starting with Junos OS Release 18.2R1, it is not required to define a dedicated interconnect logical system for including VPLS switch. For ease, VPLS switch is defined in root logical system. This approach is enabled by configuring multiple VPLS switches and LT IFLs per logical system.

When one LT logical interface connects to a VPLS switch, the routing engine assigns VPLS switch unique MAC address from MAC address pool of the LT interface. This determines the number of LT IFLs that connect a VPLS switch.

- For configuration information, see [“Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\)”](#) on page 105.
 - For information about the interconnect logical system and logical tunnel (lt-0/0/0) interfaces, see [“Understanding the Interconnect Logical System and Logical Tunnel Interfaces”](#) on page 31.
5. Enable CPU utilization control and configure the CPU control target and reserved CPU quotas for logical systems. See [“Example: Configuring CPU Utilization \(Master Administrators Only\)”](#) on page 100.
 6. Optionally, configure dynamic routing protocols for the master logical system. See [“Example: Configuring OSPF Routing Protocol for the Master Logical Systems”](#) on page 114
 7. Configure zones, security policies, and security features for the master logical system. See [“Example: Configuring Security Features for the Master Logical Systems”](#) on page 146.

8. Configure IDP for the master logical system. See [“Example: Configuring an IDP Policy for the Master Logical Systems” on page 206](#).
9. Configure application firewall services on the master logical system. See [“Understanding Logical Systems Application Firewall Services” on page 236](#) and [“Example: Configuring Application Firewall Services for a Master Logical Systems” on page 237](#).
10. Configure a route-based VPN to secure traffic between a logical system and a remote site. See [“Example: Configuring IKE and IPsec SAs for a VPN Tunnel \(Master Administrators Only\)” on page 176](#).

See Also • [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

Example: Configuring Multiple VPLS Switches and LT Interfaces for Logical Systems

This example shows how to interconnect multiple logical systems. This is achieved by configuring multiple logical systems with a Logical Tunnel (LT) interface point-to-point connection (Encapsulation Ethernet, Encapsulation Frame-Relay and Virtual Private LAN Service switch). More than one LT interface under a logical system and multiple VPLS switches are configured to pass the traffic without leaving an SRX Series device. The frame-relay encapsulation adds data-link connection identifier (DLCI) information to the given frame.

- [Requirements on page 44](#)
- [Overview on page 44](#)
- [Configuration on page 46](#)
- [Verification on page 59](#)

Requirements

This example uses an SRX Series device running Junos OS with logical system.

Before you begin:

- Read the [“SRX Series Logical Systems Master Administrator Configuration Tasks Overview” on page 41](#) to understand how and where this procedure fits in the overall master administrator configuration process.
- Read the [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#)
- Read the [“Understanding the Interconnect Logical System and Logical Tunnel Interfaces” on page 31](#)

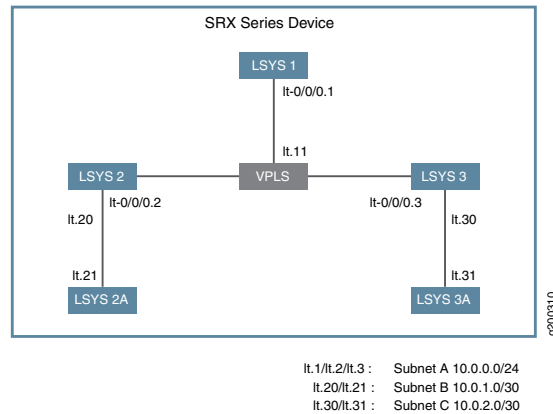
Overview

In this example, we configure multiple LT interfaces and multiple VPLS switches under one logical system.

In this example, we also configure interconnect multiple logical systems with LT interface point-to-point connection (Encapsulation Ethernet and Encapsulation Frame-Relay).

Figure 3 on page 45 shows the topology for interconnecting logical systems.

Figure 3: Configuring the interconnect logical systems



- For the interconnect logical system with LT interface point-to-point connection (encapsulation ethernet), the example configures logical tunnel interfaces Lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems.

The interconnect logical systems Lt-0/0/0 interfaces are configured with Ethernet as the encapsulation type. The corresponding peer Lt-0/0/0 interfaces in the logical systems are configured with Ethernet as the encapsulation type. A security profile is assigned to the logical systems.

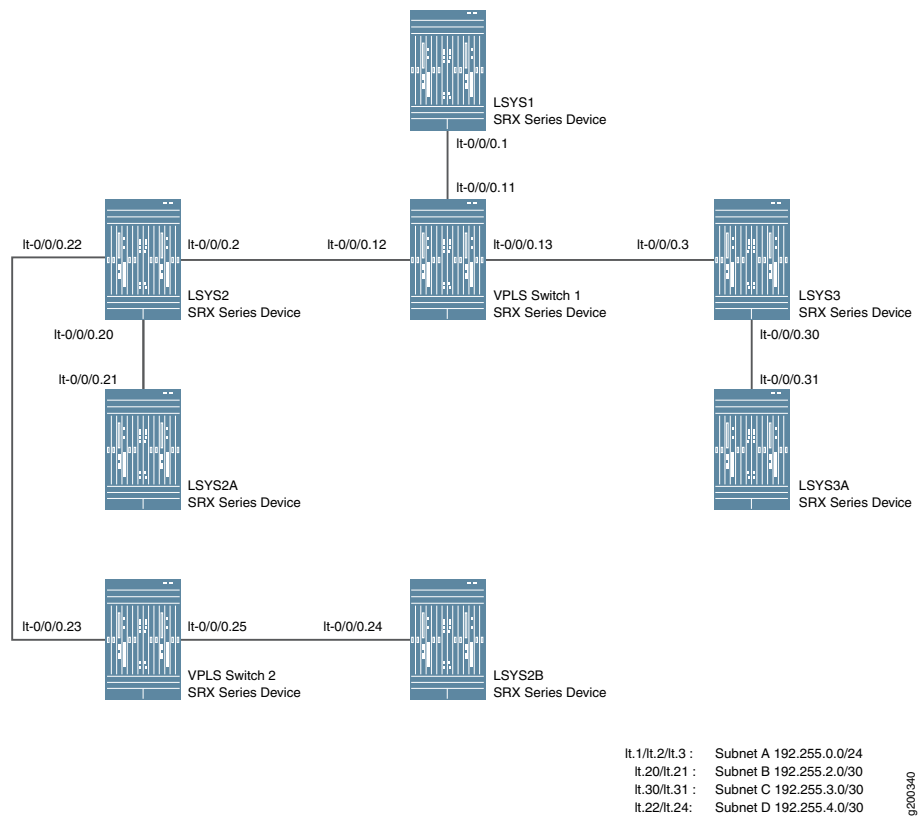
- For the interconnect logical systems with LT interface point-to-point connection (encapsulation frame-relay), this example configures logical tunnel interfaces Lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems.

The interconnect logical systems Lt-0/0/0 interfaces are configured with frame-relay as the encapsulation type. The corresponding peer Lt-0/0/0 interfaces in the logical systems are configured with frame-relay as the encapsulation type. A security profile is assigned to the logical systems.

- For interconnect logical systems with multiple VPLS switches, this example configures logical tunnel interfaces Lt-0/0/0 with ethernet-vpls as the encapsulation type. The corresponding peer Lt-0/0/0 interfaces and security-profiles are assigned to the logical systems. The routing instance for the VPLS switch-1 and VPLS switch-2 are also assigned to the logical systems.

Figure 4 on page 46 shows the topology for interconnect logical systems with VPLS switches.

Figure 4: Configuring the interconnect logical systems with VPLS switches



NOTE: Multiple LT interfaces can be configured within a logical system.

Configuration

To configure interfaces for the logical system, perform these tasks:

- [Configuring Logical Systems Interconnect with Logical Tunnel Interface point-to-point connection \(Encapsulation Ethernet\) on page 46](#)
- [Configuring Logical Systems Interconnect with Logical Tunnel Interface point-to-point connection \(Encapsulation Frame-Relay\) on page 50](#)
- [Configuring Logical Systems Interconnect with Multiple VPLS Switches on page 54](#)

Configuring Logical Systems Interconnect with Logical Tunnel Interface point-to-point connection (Encapsulation Ethernet)

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 system security-profile SP-user logical-system LSYS2
set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 peer-unit 21
set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 family inet address 192.255.2.1/30
set logical-systems LSYS2 security zones security-zone LT interfaces lt-0/0/0.20
set system security-profile SP-user logical-system LSYS2A
set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 encapsulation ethernet
set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 peer-unit 20
set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 family inet address 192.255.2.2/30
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT match
  source-address any
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT match
  destination-address any
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT match
  application any
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT then
  permit
set logical-systems LSYS2A security policies default-policy permit-all
set logical-systems LSYS2A security zones security-zone LT host-inbound-traffic
  system-services all
set logical-systems LSYS2A security zones security-zone LT host-inbound-traffic protocols
  all
set logical-systems LSYS2A security zones security-zone LT interfaces lt-0/0/0.21

```

Step-by-Step Procedure

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

1. Define a security profile and assign to a logical system.

```

[edit]
user@host# set system security-profile SP-user logical-system LSYS2

```
2. Set the LT interface as encapsulation ethernet in the logical system.

```

[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 encapsulation
  ethernet

```
3. Configure a peer relationship for logical systems LSYS2.

```

[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 peer-unit 21

```
4. Specify the IP address for the LT interface.

```

[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 family inet
  address 192.255.2.1/30

```
5. Set the security zone for the LT interface.

```

[edit]

```

```
user@host# set logical-systems LSYS2 security zones security-zone LT interfaces
lt-0/0/0.20
```

6. Define a security profile and assign to a logical system.

```
[edit]
user@host# set system security-profile SP-user logical-system LSYS2A
```

7. Set the LT interface as encapsulation ethernet in the logical system 2A.

```
[edit]
user@host# set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 encapsulation
ethernet
```

8. Configure a peer relationship for logical systems LSYS2A.

```
[edit]
user@host# set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 peer-unit 20
```

9. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 family inet
address 192.255.2.2/30
```

10. Configure a security policy that permits traffic from the LT zone to the LT policy LT zone.

```
[edit]
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT
policy LT match source-address any
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT
policy LT match destination-address any
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT
policy LT match application any
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT
policy LT then permit
```

11. Configure a security policy that permits traffic from default-policy.

```
[edit]
user@host# set logical-systems LSYS2A security policies default-policy permit-all
```

12. Configure security zones.

```
[edit]
user@host# set logical-systems LSYS2A security zones security-zone LT
host-inbound-traffic system-services all
user@host# set logical-systems LSYS2A security zones security-zone LT
host-inbound-traffic protocols all
user@host# set logical-systems LSYS2A security zones security-zone LT interfaces
lt-0/0/0.21
```


- Results**
- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS2** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS2
interfaces {
  lt-0/0/0 {
    unit 20 {
      encapsulation ethernet;
      peer-unit 21;
      family inet {
        address 192.255.2.1/30;
      }
    }
    unit 22 {
      encapsulation ethernet;
      peer-unit 23;
      family inet {
        address 192.255.4.1/30;
      }
    }
  }
}
security {
  zones {
    security-zone LT {
      interfaces {
        lt-0/0/0.22;
        lt-0/0/0.20;
      }
    }
  }
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS2A** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS2A
interfaces {
  lt-0/0/0 {
    unit 21 {
      encapsulation ethernet;
      peer-unit 20;
      family inet {
        address 192.255.2.2/30;
      }
    }
  }
}
security {
  policies {
    from-zone LT to-zone LT {
      policy LT {
```

```

        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
default-policy {
    permit-all;
}
}
zones {
    security-zone LT {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            lt-0/0/0.21;
        }
    }
}
}

```

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

Configuring Logical Systems Interconnect with Logical Tunnel Interface point-to-point connection (Encapsulation Frame-Relay)

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 system security-profile SP-user logical-system LSYS3A
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 encapsulation frame-relay
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 dlci 16
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 peer-unit 31
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 family inet address 192.255.3.1/30
set logical-systems LSYS3 security zones security-zone LT interfaces lt-0/0/0.30
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 encapsulation frame-relay
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 dlci 16
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 peer-unit 30
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 family inet address 192.255.3.2/30
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match
    source-address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match
    destination-address any

```

```

set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match
  application any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT then
  permit
set logical-systems LSYS3A security policies default-policy permit-all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic
  system-services all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic protocols
  all
set logical-systems LSYS3A security zones security-zone LT interfaces lt-0/0/0.31

```

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*.

1. Define a security profile and assign to a logical system.

```

[edit]
user@host# set system security-profile SP-user logical-system LSYS3A

```
2. Set the LT interface as encapsulation frame-relay in the logical system.

```

[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 encapsulation
  frame-relay

```
3. Configure the logical tunnel interface by including the dlci.

```

[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 dlci 16

```
4. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```

[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 peer-unit 31

```
5. Specify the IP address for the LT interface.

```

[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 family inet
  address 192.255.3.1/30

```
6. Set the security zone for the LT interface.

```

[edit]
user@host# set logical-systems LSYS3 security zones security-zone LT interfaces
  lt-0/0/0.30

```
7. Set the LT interface as encapsulation frame-relay in the logical system.

```

[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 encapsulation
  frame-relay

```

8. Configure the logical tunnel interface by including the dlcI.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 dlcI 16
```

9. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 peer-unit 30
```

10. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 family inet
address 192.255.3.2/30
```

11. Configure a security policy that permits traffic from the LT zone to the LT policy LT zone.

```
[edit]
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT
policy LT match source-address any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT
policy LT match destination-address any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT
policy LT match application any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT
policy LT then permit
```

12. Configure a security policy that permits traffic from default-policy.

```
[edit]
user@host# set logical-systems LSYS3A security policies default-policy permit-all
```

13. Configure security zones.

```
[edit]
user@host# set logical-systems LSYS3A security zones security-zone LT
host-inbound-traffic system-services all
user@host# set logical-systems LSYS3A security zones security-zone LT
host-inbound-traffic protocols all
user@host# set logical-systems LSYS3A security zones security-zone LT interfaces
lt-0/0/0.31
```

- Results**
- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS3** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS3
interfaces {
  lt-0/0/0 {
```

```

    unit 30 {
        encapsulation frame-relay;
        dlci 16;
        peer-unit 31;
        family inet {
            address 192.255.3.1/30;
        }
    }
}
}
security {
    zones {
        security-zone LT {
            interfaces {
                lt-0/0/0.30;
            }
        }
    }
}
}

```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS3A** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show logical-systems LSYS3A

interfaces {
    lt-0/0/0 {
        unit 31 {
            encapsulation frame-relay;
            dlci 16;
            peer-unit 30;
            family inet {
                address 192.255.3.2/30;
            }
        }
    }
}
security {
    policies {
        from-zone LT to-zone LT {
            policy LT {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        default-policy {
            permit-all;
        }
    }
}

```

```

    }
    zones {
        security-zone LT {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                lt-0/0/0.31;
            }
        }
    }
}

```

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

Configuring Logical Systems Interconnect with Multiple VPLS Switches

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 interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 11 peer-unit 1
set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 12 peer-unit 2
set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 13 peer-unit 3
set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 23 peer-unit 22
set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 25 peer-unit 24
set routing-instances vpls-switch-1 instance-type vpls
set routing-instances vpls-switch-1 interface lt-0/0/0.11
set routing-instances vpls-switch-1 interface lt-0/0/0.12
set routing-instances vpls-switch-1 interface lt-0/0/0.13
set routing-instances vpls-switch-2 instance-type vpls
set routing-instances vpls-switch-2 interface lt-0/0/0.23
set routing-instances vpls-switch-2 interface lt-0/0/0.25
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address 192.255.0.1/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 peer-unit 12
set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 family inet address 192.255.0.2/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 peer-unit 23
set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 family inet address 192.255.4.1/30
set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 peer-unit 13

```

```

set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 family inet address 192.255.0.3/24
set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 encapsulation ethernet
set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 peer-unit 25
set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 family inet address 192.255.4.2/30
set system security-profile SP-user policy maximum 100
set system security-profile SP-user policy reserved 50
set system security-profile SP-user zone maximum 60
set system security-profile SP-user zone reserved 10
set system security-profile SP-user flow-session maximum 100
set system security-profile SP-user flow-session reserved 50
set system security-profile SP-user logical-system LSYS1
set system security-profile SP-user logical-system LSYS2
set system security-profile SP-user logical-system LSYS3
set system security-profile SP-user logical-system LSYS2B

```

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*.

1. Configure the lt-0/0/0 interfaces.

```

[edit]
user@host# set interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 11 peer-unit 1
user@host# set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 12 peer-unit 2
user@host# set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 13 peer-unit 3
user@host# set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 23 peer-unit 22
user@host# set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 25 peer-unit 24

```

2. Configure the routing instance for the VPLS switches and add interfaces to it.

```

[edit]
user@host# set routing-instances vpls-switch-1 instance-type vpls
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.11
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.12
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.13
user@host# set routing-instances vpls-switch-2 instance-type vpls
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.23
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.25

```

3. Configure LSYS1 with lt-0/0/0.1 interface and peer lt-0/0/0.11.

```

[edit]
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation
  ethernet
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address
  192.255.0.1/24

```

4. Configure LSYS2 with lt-0/0/0.2 interface and peer lt-0/0/0.12.

```
[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 encapsulation
    ethernet
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 peer-unit 12
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 family inet address
    192.255.0.2/24
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 encapsulation
    ethernet
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 peer-unit 23
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 family inet
    address 192.255.4.1/30
```

5. Configure LSYS3 with lt-0/0/0.3 interface and peer lt-0/0/0.13

```
[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 encapsulation
    ethernet
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 peer-unit 13
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 family inet address
    192.255.0.3/24
```

6. Configure LSYS2B with lt-0/0/0 interface and peer-unit 24.

```
[edit]
user@host# set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 encapsulation
    ethernet
user@host# set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 peer-unit 25
user@host# set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 family inet
    address 192.255.4.2/30
```

7. Assign security-profile for logical-systems.

```
[edit]
user@host# set system security-profile SP-user policy maximum 100
user@host# set system security-profile SP-user policy reserved 50
user@host# set system security-profile SP-user zone maximum 60
user@host# set system security-profile SP-user zone reserved 10
user@host# set system security-profile SP-user flow-session maximum 100
user@host# set system security-profile SP-user flow-session reserved 50
user@host# set system security-profile SP-user logical-system LSYS1
user@host# set system security-profile SP-user logical-system LSYS2
user@host# set system security-profile SP-user logical-system LSYS3
user@host# set system security-profile SP-user logical-system LSYS2B
```

- Results**
- From configuration mode, confirm your configuration by entering the **show interfaces lt-0/0/0**, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it

```
[edit]
user@host# show interfaces lt-0/0/0
unit 11 {
    encapsulation ethernet-vpls;
    peer-unit 1;
```



```
}
unit 12 {
    encapsulation ethernet-vpls;
    peer-unit 2;
}
unit 13 {
    encapsulation ethernet-vpls;
    peer-unit 3;
}
unit 23 {
    encapsulation ethernet-vpls;
    peer-unit 22;
}
unit 25 {
    encapsulation ethernet-vpls;
    peer-unit 24;
}
```

- From configuration mode, confirm your configuration by entering the **show routing-instances** command. 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
vpls-switch-1 {
    instance-type vpls;
    interface lt-0/0/0.11;
    interface lt-0/0/0.12;
    interface lt-0/0/0.13;
}
vpls-switch-2 {
    instance-type vpls;
    interface lt-0/0/0.23;
    interface lt-0/0/0.25;
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS1** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS1
interfaces {
    lt-0/0/0 {
        unit 1 {
            encapsulation ethernet;
            peer-unit 11;
            family inet {
                address 192.255.0.1/24;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS2** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS2
interfaces {
  lt-0/0/0 {
    unit 2 {
      encapsulation ethernet;
      peer-unit 12;
      family inet {
        address 192.255.0.2/24;
      }
    }
    unit 22 {
      encapsulation ethernet;
      peer-unit 23;
      family inet {
        address 192.255.4.1/30;
      }
    }
  }
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS3**, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS3
interfaces {
  lt-0/0/0 {
    unit 3 {
      encapsulation ethernet;
      peer-unit 13;
      family inet {
        address 192.255.0.3/24;
      }
    }
  }
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS2B**, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS2B
interfaces {
  lt-0/0/0 {
    unit 24 {
      encapsulation ethernet;
      peer-unit 25;
      family inet {
        address 192.255.4.2/30;
      }
    }
  }
}
```

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

```
[edit]
user@host# show system security-profile
SP-user {
  policy {
    maximum 100;
    reserved 50;
  }
  zone {
    maximum 60;
    reserved 10;
  }
  flow-session {
    maximum 100;
    reserved 50;
  }
  logical-system [ LSYS1 LSYS2 LSYS3 LSYS2B ];
}
```

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 the Security-Profile for all Logical-systems on page 59](#)
- [Verifying the LT Interfaces for all Logical systems on page 60](#)

Verifying the Security-Profile for all Logical-systems

Purpose Verify security profile for each logical systems.

Action From operational mode, enter the **show system security-profile security-log-stream-number logical-system all** command.

```
user@host> show system security-profile security-log-stream-number logical-system
all
```

logical system name	security profile name	usage	reserved	maximum
root-logical-system	Default-Profile	2	0	2000
LSYS1	SP-user	1	10	60
LSYS2	SP-user	1	10	60
LSYS2B	SP-user	1	10	60
LSYS3	SP-user	1	10	60

Meaning The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Verifying the LT Interfaces for all Logical systems

Purpose Verify interfaces for logical systems.

Action From operational mode, enter the **show interfaces lt-0/0/0 terse** command.

```
user@host> show interfaces lt-0/0/0 terse
```

Interface	Admin	Link	Proto	Local	Remote
lt-0/0/0	up	up			
lt-0/0/0.1	up	up	inet	192.255.0.1/24	
lt-0/0/0.2	up	up	inet	192.255.0.2/24	
lt-0/0/0.3	up	up	inet	192.255.0.3/24	
lt-0/0/0.11	up	up	vpls		
lt-0/0/0.12	up	up	vpls		
lt-0/0/0.13	up	up	vpls		
lt-0/0/0.22	up	up	inet	192.255.4.1/30	
lt-0/0/0.23	up	up	vpls		
lt-0/0/0.24	up	up	inet	192.255.4.2/30	
lt-0/0/0.25	up	up	vpls		
lt-0/0/0.32767	up	up			

Meaning The output provides the status of LT interfaces. All the LT interfaces are up.

- See Also**
- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)
 - [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)
 - [SRX Series Logical Systems Master Administrator Configuration Tasks Overview on page 41](#)

User Logical Systems Overview

A user logical system enables you to configure zones, security policies, logical interfaces and security resources assigned to its own user logical system. For more information, see the following topics:

- [User Logical Systems Configuration Overview on page 61](#)
- [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

User Logical Systems Configuration Overview

When the master administrator creates a user logical system, he assigns a user logical system administrator to manage it. A user logical system can have multiple user logical system administrators.

As a user logical system administrator, you can access and view resources in your user logical system but not those of other user logical systems or the master logical system. You can configure resources allocated to your user logical system, but you cannot modify the numbers of allocated resources.

The following procedure lists the tasks that the user logical system administrator performs to configure resources in the user logical system:

1. Log in to the user logical system with the login and password configured by the master administrator:
 - a. Telnet or SSH to the management IP address configured on the device. Log in to the user logical system with the administrator login and password provided by the master administrator.

You enter a UNIX shell in the user logical system configured by the master administrator.

- b. The presence of the > prompt indicates the CLI has started. The prompt is preceded by a string that contains your username, the hostname of the router, and the name of the user logical system. When the CLI starts, you are at the top level in operational mode. You enter configuration mode by entering the **configure** operational mode command. The CLI prompt changes from `user@host: logical-system>` to `user@host: logical-system#`.

To exit the CLI and return to the UNIX shell, enter the **quit** command.

2. Configure the logical interfaces assigned to the user logical system by the master administrator. Configure one or more routing instances and the routing protocols and options within each instance. See [“Example: Configuring Interfaces and Routing Instances for a User Logical Systems” on page 121](#).
3. Configure security resources for the user logical system:
 - a. Create zones for the user logical system and bind the logical interfaces to the zones. Address books can be created that are attached to zones for use in policies. See [“Example: Configuring Security Zones for a User Logical Systems” on page 141](#).
 - b. Configure screen options at the zone level. See [“Example: Configuring Screen Options for a User Logical Systems” on page 172](#).
 - c. Configure security policies between zones in the user logical system. See [“Example: Configuring Security Policies in a User Logical Systems” on page 168](#).

Custom applications or application sets can be created for specific types of traffic. To create a custom application, use the **application** configuration statement at the `[edit applications]` hierarchy level. To create an application set, use the **application-set** configuration statement at the `[edit applications]` hierarchy level.

- d. Configure firewall authentication. The master administrator creates access profiles in the master logical system. See [“Example: Configuring Access Profiles \(Master Administrators Only\)”](#) on page 144.

The user logical system administrator then configures a security policy that specifies firewall authentication for matching traffic and configures the type of authentication (pass-through or Web authentication), default access profile, and success banner. See [“Example: Configuring Firewall Authentication for a User Logical System”](#) on page 154.

- e. Configure a route-based VPN tunnel to secure traffic between a user logical system and a remote site. The master administrator assigns a secure tunnel interface to the user logical system and configures IKE and IPsec SAs for the VPN tunnel. See [“Example: Configuring IKE and IPsec SAs for a VPN Tunnel \(Master Administrators Only\)”](#) on page 176.

The user logical system administrator then configures a route-based VPN tunnel. See [“Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems”](#) on page 180.

- f. Configure Network Address Translation (NAT). See [“Example: Configuring Network Address Translation for a User Logical Systems”](#) on page 118.

- g. Configure and assigning a predefined IDP policy to the user logical system. The master administrator configures IDP policies at the root level and specifies an IDP policy in the security profile that is bound to a logical system. See [“Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System”](#) on page 212.

The user logical system administrator then enables IDP in a security policy. See [“Example: Enabling IDP in a User Logical System Security Policy”](#) on page 214.

- h. Configure and enable an IDP policy at the user logical system. See [“Example: Configuring an IDP Policy for a User Logical System”](#) on page 217
- i. Display or clear application system cache (ASC) entries. See [“Understanding Logical Systems Application Identification Services”](#) on page 235.
- j. Configure application firewall services on a user logical system. See [“Understanding Logical Systems Application Firewall Services”](#) on page 236 and [“Example: Configuring Application Firewall Services for a User Logical System”](#) on page 242.
- k. Configure the AppTrack application tracking tool. See [“Example: Configuring AppTrack for a User Logical Systems”](#) on page 246.

- See Also**
- [Example: Configuring User Logical Systems](#) on page 130
 - [Understanding User Logical Systems and the User Logical System Administrator Role](#) on page 63

Understanding User Logical Systems and the User Logical System Administrator Role

Logical systems allow a master administrator to partition an SRX Series device into discrete contexts called user logical systems. User logical systems are self-contained, private contexts, separate both from one another and from the master logical system. A user logical system has its own security, networking, logical interfaces, routing configurations, and one or more user logical system administrators.

When the master administrator creates a user logical system, he assigns one or more user logical system administrators to manage it. A user logical system administrator has a view of the device that is limited to his logical system. Although a user logical system is managed by a user logical system administrator, the master administrator has a global view of the device and access to all user logical systems. If necessary, the master administrator can manage any user logical system on the device.

The role and responsibilities of a user logical system administrator differ from those of the master administrator. As a user logical system administrator, you can access, configure, and view the configuration for your user logical system resources, but not those of other user logical systems or the master logical system.

As a user logical system administrator, you can:

- Configure zones, address books, security policies, user lists, custom services, and so forth, for your user logical system environment, based on the resources allocated to it.

For example, if the master administrator allocates 40 zones to your user logical system, you can configure and administer those zones, but you cannot change the allocated number.

- Configure routing instances and assign allotted interfaces to them. Create static routes and add them to your routing instances. Configure routing protocols.
- Configure, enable, and monitor application firewall policy on your user logical system.
- Configure AppTrack.
- View all assigned logical interfaces and configure their attributes. The attributes that you configure for logical interfaces for your user logical system cannot be seen by other user logical system administrators.
- Run operational commands for your user logical system.

- See Also**
- [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)
 - [Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\) on page 105](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)

Setting Up a Logical System

- [Example: Configuring Root Password for Logical Systems on page 64](#)
- [Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System on page 65](#)

Example: Configuring Root Password for Logical Systems

- [Requirements on page 64](#)
- [Overview on page 64](#)
- [Configuration on page 64](#)

Requirements

Before you begin, read “[SRX Series Logical Systems Master Administrator Configuration Tasks Overview](#)” on [page 41](#) to understand how this task fits into the overall configuration process.

The example uses an SRX5600 device running Junos OS with logical systems.

Overview

The Junos OS software is installed on the router before it is delivered from the factory. When you power on your router, it is ready for you to configure. Initially you log in as *root* user without using a password.

After you log in, you can configure a password for the root user, or, in logical systems terms, the master administrator. The master administrator has root privileges over the device.

Configuration

- [Configuring the Root Password on page 64](#)

Configuring the Root Password

Step-by-Step Procedure

- Configure a root password for the device.
`user@host# set system root-authentication Talk22rt6`

See Also

- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
- [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System

This example shows how to create user logical systems and assign administrators to them. It shows how to add users to a user logical system. And the example shows how to create an interconnect logical system, which is optional.



NOTE: Only the master administrator can create user login accounts for administrators and users. If a user logical system administrator wants to add users to his logical system, he must convey the information to the master administrator, who will add the users.

- [Requirements on page 65](#)
- [Overview on page 65](#)
- [Configuration on page 66](#)
- [Verification on page 72](#)

Requirements

The example uses an SRX5600 device running Junos OS with logical systems.

Overview

Before you begin, read “[SRX Series Logical Systems Master Administrator Configuration Tasks Overview](#)” on [page 41](#) to understand how this task fits into the overall configuration process.

This example is for a company that includes product design, marketing, and accounting departments. The company wants to curtail hardware and energy costs, but not at the risk of exposing data across departments or to the Internet.

Each department has its own security requirements in regard both to other departments and to the Internet. To meet its requirements for cost control without forfeiting security, the company deploys the SRX5600 device. The master administrator configures three user logical systems giving each department a logical device that is private and fully secured.

This topic covers how to:

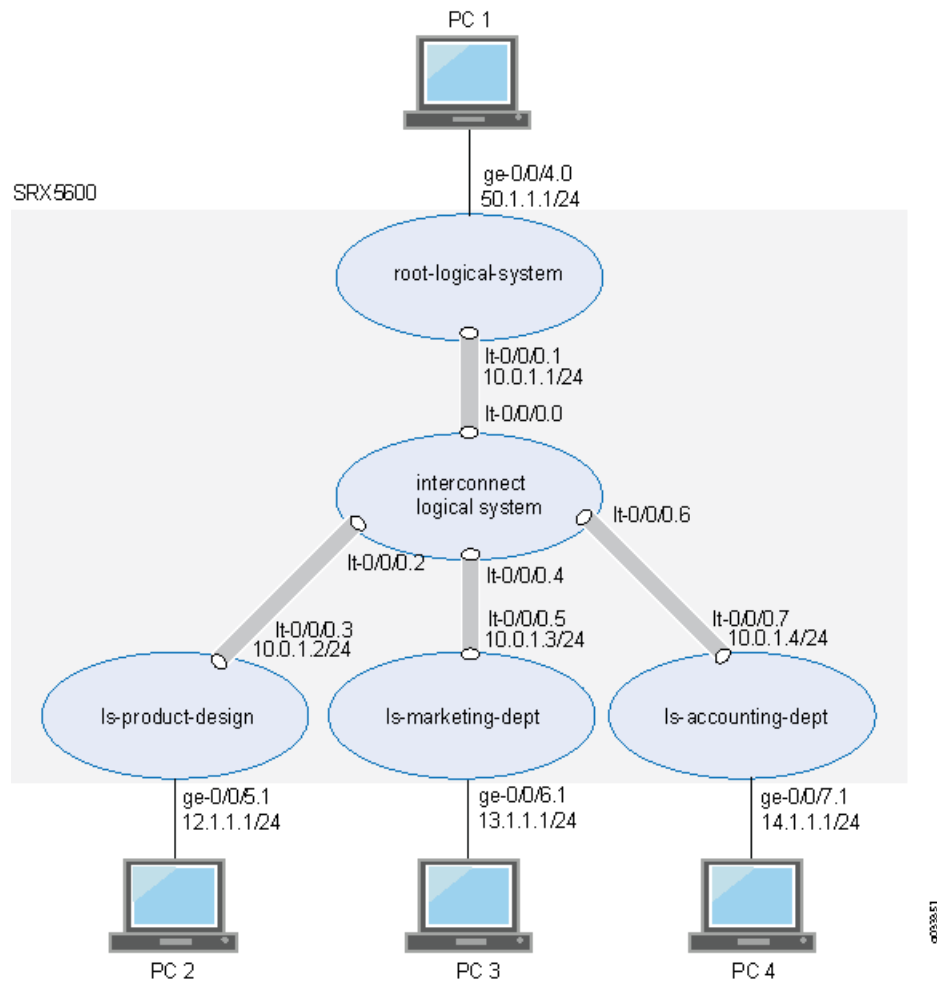
- Create user logical systems and an interconnect logical system that is used as an internal VPLS switch to allow traffic to pass from one logical system to another.
- Create administrators for user logical systems other than the interconnect logical system. A user logical system can have more than one administrator. The interconnect logical system does not require an administrator.
- Add users to a user logical system.



NOTE: This example shows how to configure only two users—`lsdesignuser1` and `lsdesignuser2`. In reality, every user logical system will include many users that would require configurations similar to those shown in this example.

Figure 5 on page 66 shows an SRX5600 device deployed and configured for logical systems. The configuration examples reflect this deployment.

Figure 5: SRX Series Device Configured for Logical Systems



Configuration

- Configuring User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System on page 67

Configuring User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System

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 logical-systems ls-product-design
set system login class ls-design-admin logical-system ls-product-design
set system login class ls-design-admin permissions all
set system login user lsdesignadmin1 full-name lsdesignadmin1
set system login user lsdesignadmin1 class ls-design-admin
set system login user lsdesignadmin1 authentication encrypted-password "$ABC123"
set system login class ls-design-user logical-system ls-product-design
set system login class ls-design-user permissions view
set system login user lsdesignuser1 full-name lsdesignuser1
set system login user lsdesignuser1 class ls-design-user
set system login user lsdesignuser1 authentication encrypted-password "$ABC123"
set system login user lsdesignuser2 full-name lsdesignuser2
set system login user lsdesignuser2 class ls-design-user
set system login user lsdesignuser2 authentication encrypted-password "$ABC123"
set logical-systems ls-marketing-dept
set system login class ls-marketing-admin logical-system ls-marketing-dept
set system login class ls-marketing-admin permissions all
set system login user lsmarketingadmin1 class ls-marketing-admin
set system login user lsmarketingadmin1 full-name lsmarketingadmin1
set system login user lsmarketingadmin1 authentication encrypted-password "$ABC123"
set system login user lsmarketingadmin2 full-name lsmarketingadmin2
set system login user lsmarketingadmin2 class ls-marketing-admin
set system login user lsmarketingadmin2 authentication encrypted-password "$ABC123"
set logical-systems ls-accounting-dept
set system login class ls-accounting-admin logical-system ls-accounting-dept
set system login class ls-accounting-admin permissions all
set system login user lsaccountingadmin1 full-name lsaccountingadmin1
set system login user lsaccountingadmin1 class ls-accounting-admin
set system login user lsaccountingadmin1 authentication encrypted-password "$ABC123"
set logical-systems interconnect-logical-system
```

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

1. Create the first user logical system and define its administrator.
 - a. Create the user logical system.

```
[edit]
user@host# set logical-systems ls-product-design
```

- b. Assign the user login class to the user logical system.

```
[edit system]
user@host# set login class ls-design-admin logical-system ls-product-design
```

- c. Create the login class to give the user logical system administrator full permission over the user logical system.

```
[edit system]
user@host# set login class ls-design-admin permissions all
```

- d. Assign a full name to the user logical system administrator.

```
[edit system]
user@host# set login user lsdesignadmin1 full-name lsdesignadmin1
```

- e. Associate the login class with the user logical system administrator to allow the administrator to log in to the user logical system.

```
[edit system]
user@host# set login user lsdesignadmin1 class ls-design-admin
```

- f. Create a user login password for the user logical system administrator.

```
[edit system]
user@host# set login user lsdesignadmin1 authentication plain-text-password
New password: Talk1234
Retype new password: Talk1234
```

- 2. Configure the first user for the logical system.

- a. Configure the user login class and assign it to the user logical system.

```
[edit system]
user@host# set login class ls-design-user logical-system ls-product-design
```

- b. To give the first user the ability to see the logical system's resources and settings but not change them, assign **view** as the permission to the login class.

```
[edit system]
user@host# set login class ls-design-user permissions view
```

- c. Assign a full name to the logical system user.

```
[edit system]
user@host# set login user lsdesignuser1 full-name lsdesignuser1
```

- d. Associate the login class with the user to allow the user to log in to the user logical system.

```
user@host# set login user lsdesignuser1 class ls-design-user
```

- e. Create a user login password for the user.

```
[edit system]
user@host# set login user lsdesignuser1 authentication plain-text-password
New password: Talk4234
```

Retype new password: Talk4234

3. Create the second user for logical system ls-product-design.

- a. Assign a full name to the user.

```
[edit system]
user@host# set login user lsdesignuser2 full-name lsdesignuser2
```

- b. Associate the user with the login class to allow the user to log in to the user logical system.

```
user@host# set login user lsdesignuser2 class ls-design-user
```

- c. Create a user login password.

```
[edit system]
user@host# set login user lsdesignuser2 authentication plain-text-password
New password: Talk9234
Retype new password: Talk9234
```

4. Create the second user logical system and define its administrator.

- a. Create the user logical system.

```
[edit]
user@host# set logical-systems ls-marketing-dept
```

- b. Configure the user login class and assign it to the user logical system.

```
[edit system]
user@host# set login class ls-marketing-admin logical-system ls-marketing-dept
```

- c. To give the user logical system administrator control over the user logical system, assign **all** as the permissions to the login class.

```
[edit system]
user@host# set login class ls-marketing-admin permissions all
```

- d. Assign a full name to the user logical system administrator.

```
[edit system]
user@host# set login user lsmarketingadmin1 full-name lsmarketingadmin1
```

- e. Associate the user logical system administrator with the login class to allow the administrator to log in to the user logical system.

```
[edit system]
user@host# set login user lsmarketingadmin1 class ls-marketing-admin
```

- f. Create a user login password for the user logical system administrator.

```
[edit system]
user@host# set login user lsmarketingadmin1 authentication plain-text-password
```

New password: Talk2345
 Retype new password: Talk2345

5. Create a second user logical system administrator for the ls-marketing-dept logical system.

- a. Assign a full name to the user logical system administrator.

```
[edit system]
user@host# set login user lsmarketingadmin2 full-name lsmarketingadmin2
```

- b. Associate the user logical system administrator with the login class to allow the administrator to log in to the user logical system.

```
[edit system]
user@host# set login lsmarketingadmin2 class ls-marketing-admin
```

- c. Create a user login password for the user logical system administrator.

```
[edit system]
user@host# set login user lsmarketingadmin2 authentication plain-text-password
New password: Talk6345
Retype new password: Talk6345
```

6. Create the third user logical system and define its administrator.

- a. Create the user logical system.

```
[edit]
user@host# set logical-systems ls-accounting-dept
```

- b. Configure the user login class and assign it to the user logical system.

```
[edit system]
user@host# set login class ls-accounting-admin logical-system
ls-accounting-dept
```

- c. To give the user logical system administrator control over the user logical system, assign permissions to the login class.

```
[edit system]
user@host# set login class ls-accounting-admin permissions all
```

- d. Assign a full name to the user logical system administrator.

```
[edit system]
user@host# set login user lsaccountingadmin1 full-name lsaccountingadmin1
```

- e. Associate the user logical system administrator with the login class to allow the administrator to log in to the user logical system.

```
[edit system]
user@host# set login user lsaccountingadmin1 class ls-accounting-admin
```

- f. Create a login password for the user logical system administrator.

```
[edit system]
user@host# set login user lsaccountingadmin1 authentication
plain-text-password
New password: Talk5678
Retype new password: Talk5678
```

7. Configure an interconnect logical system to allow logical systems to pass traffic from one to another.

```
user@host# set logical-systems interconnect-logical-system
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems** command to verify that the logical systems were created. Also enter the **show system login class** command for each class that you defined.

To ensure that the logical systems administrators were created, enter the **show system login user** command.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show logical-systems ?
interconnect-logical-system;
ls-accounting-dept;
ls-marketing-dept;
ls-product-design;

user@host# show system login class ls-design-admin
logical-system ls-product-design;
permissions all;

user@host# show system login class ls-design-user
logical-system ls-product-design
permissions view;

user@host# show system login class ls-marketing-admin
logical-system ls-marketing-dept;
permissions all;

user@host# show system login class ls-accounting-admin
logical-system ls-accounting-dept;
permissions all;

user@host# show system login user ?
lsaccountingadmin1 lsaccountingadmin1
lsdesignadmin1 lsdesignadmin1
lsdesignuser2 lsdesignuser2
lsmarketingadmin1 lsmarketingadmin1
lsmarketingadmin2 lsmarketingadmin2
```

Verification

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

- [Verifying User Logical Systems and Login Configurations from the Master Logical System on page 72](#)
- [Verifying User Logical Systems and Login Configurations Using Telnet on page 72](#)

Verifying User Logical Systems and Login Configurations from the Master Logical System

Purpose Verify that the user logical systems exist and that you, as the master administrator, can enter them from root. Return from a user logical system to the master logical system.

Action From operational mode, enter the following command:

```
root@host> set cli logical-system ls-product-design
Logical system:ls-product-design
root@host:ls-product-design>

root@host:ls-product-design> clear cli logical-system
Cleared default logical system
root@host>

root@host> set cli logical-system ls-marketing-dept
Logical system:ls-marketing-dept
root@host:ls-marketing-dept>

root@host:ls-marketing-dept> clear cli logical-system
Cleared default logical system
root@host>

root@host> set cli logical-system ls-accounting-dept
Logical system:ls-accounting-dept
root@host:ls-accounting-dept>

root@host:ls-accounting-dept> clear cli logical-system
Cleared default logical system
root@host>
```

Verifying User Logical Systems and Login Configurations Using Telnet

Purpose Verify that the user logical systems you created exist and that the administrators' login IDs and passwords that you created are correct.

Action Use Telnet to log in to each user logical system as its user administrator would do.

1. Run Telnet specifying the IP address of your SRX Series device. For example:

```
telnet 10.11.11.19
```
2. Enter the login ID and password for the administrator for one of the user logical systems that you created. After you log in, the prompt shows the administrator name. Notice how this result differs from the result produced when you log in to the user logical

system from the master logical system at root. Repeat this procedure for all of your user logical systems.

```
login: lsdesignadmin1
Password: Talk1234
lsdesignadmin1@host: ls-product-design>
```

- See Also**
- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)
 - [Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\) on page 105](#)

- Related Documentation**
- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

Security Profiles for Logical Systems

Security profiles for logical systems allows you to scan the applications for threats, such as viruses, malware, spyware, and attacks. Security profile is applied to scan traffic after the application or category is allowed by the security policy. For more information, see the following topics:

- [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)
- [Example: Configuring User Logical Systems Security Profiles on page 87](#)
- [Example: Configuring Security log stream for Logical Systems on page 92](#)

Understanding Logical Systems Security Profiles (Master Administrators Only)

Logical systems allow you to virtually divide a supported SRX Series device into multiple devices, isolating one from another, securing them from intrusion and attacks, and protecting them from faulty conditions outside their own contexts. To protect logical systems, security resources are configured in a manner similar to how they are configured for a discrete device. However, as the master administrator, you must allocate the kinds and amounts of security resources to logical systems. The logical system administrator allocates resources for his own logical system.

An SRX Series device running logical systems can be partitioned into user logical systems, an interconnect logical system, if desired, and the default master logical system. When the system is initialized, the master logical system is created at the root level. All system resources are assigned to it, effectively creating a default master logical system security profile. To distribute security resources across logical systems, the master administrator

creates security profiles that specify the kinds and amounts of resources to be allocated to a logical system that the security profile is bound to. Only the master administrator can configure security profiles and bind them to logical systems. The user logical system administrator configures these resources for his or her logical system.

Logical systems are defined largely by the resources allocated to them, including security components, interfaces, routing instances, static routes, and dynamic routing protocols. When the master administrator configures a user logical system, he binds a security profile to it. Any attempt to commit a configuration for a user logical system without a security profile bound to it will fail.

This topic includes the following sections:

- [Logical Systems Security Profiles on page 74](#)
- [How the System Assesses Resources Assignment and Use Across Logical Systems on page 75](#)
- [Cases: Assessments of Reserved Resources Assigned Through Security Profiles on page 76](#)

Logical Systems Security Profiles

As master administrator, you can configure a single security profile to assign resources to a specific logical system, use the same security profile for more than one logical system, or use a mix of both methods. You can configure up to 32 security profiles on an SRX Series device running logical systems. When you reach the limit, you must delete a security profile and commit the configuration change before you can create and commit another security profile. In many cases fewer security profiles are needed because you might bind a single security profile to more than one logical system.

Security profiles allow you to:

- Share the device's resources, including policies, zones, addresses and address books, flow sessions, and various forms of NAT, among all logical systems appropriately. You can dedicate various amounts of a resource to the logical systems and allow them to compete for use of the free resources.

Security profiles protect against one logical system exhausting a resource that is required at the same time by other logical systems. Security profiles protect critical system resources and maintain a fair level of performance among user logical systems when the device is experiencing heavy traffic flow. They defend against one user logical system dominating the use of resources and depriving other user logical systems of them.

- Configure the device in a scalable way to allow for future creation of additional user logical systems.

You must delete a logical system's security profile before you delete that logical system.

How the System Assesses Resources Assignment and Use Across Logical Systems

To provision a logical system with security resources, you, as a master administrator, configure a security profile that specifies for each resource:

- A reserved quota that guarantees that the specified resource amount is always available to the logical system.
- A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize 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 must compete for global resources.

If a reserved quota is not configured for a resource, the default value is 0. If a maximum allowed quota is not configured for a resource, the default value is the global system quota for the resource (global system quotas are platform-dependent). The master administrator must configure appropriate maximum allowed quota values in the security profiles so the maximum resource usage of a specific logical system does not negatively impact other logical systems configured on the device. The master administrator must configure the appropriate maximum-allowed quota values in the security profiles so that the maximum resource usage of a specific logical system does not negatively impact other logical systems configured on the device.

The system maintains a count of all allocated resources that are reserved, used, and made available again when a logical system is deleted. This count determines whether resources are available to use for new logical systems or to increase the amount of the resources allocated to existing logical systems through their security profiles.

When a user logical system is deleted, its reserved resource allocations are released for use by other logical systems.

Resources configured in security profiles are characterized as static modular resources or dynamic resources. For static resources, we recommend setting a maximum quota for a resource equal or close to the amount specified as its reserved quota, to allow for scalable configuration of logical systems. A high maximum quota for a resource might give a logical system greater flexibility through access to a larger amount of that resource, but it would constrain the amount available to allocate to a new user logical system.

The difference between reserved and maximum allowed amounts for a dynamic resource is not important because dynamic resources are aged out and do not deplete the pool available for assignment to other logical systems.

The following resources can be specified in a security profile:

- Security policies, including schedulers
- Security zones
- Addresses and address books for security policies

- Application firewall rule sets
- Application firewall rules
- Firewall authentication
- Flow sessions and gates
- NAT, including:
 - Cone NAT bindings
 - NAT destination rule
 - NAT destination pool
 - NAT IP address in source pool without Port Address Translation (PAT)



NOTE: IPv6 addresses in IPv6 source pools without PAT are not included in security profiles.

- NAT IP address in source pool with PAT
- NAT port overloading
- NAT source pool
- NAT source rule
- NAT static rule



NOTE: All resources except flow sessions are static.

You can modify a logical system security profile dynamically while the security profile is assigned to other logical systems. However, to ensure that the system resource quota is not exceeded, the system takes the following actions:

- If a static quota is changed, system daemons that maintain logical system counts for resources specified in security profiles revalidate the security profile. This check identifies the number of resources assigned across all logical systems to determine whether the allocated resources, including their increased amounts, are available.

These quota checks are the same quota checks that the system performs when you add a new user logical system and bind a security profile to it. They are also performed when you bind a different security profile from the security profile that is presently assigned to it to an existing user logical system (or the master logical system).

- If a dynamic quota is changed, no check is performed, but the new quota is imposed on future resource usage.

Cases: Assessments of Reserved Resources Assigned Through Security Profiles

To understand how the system assesses allocation of reserved resources through security profiles, consider the following three cases that address allocation of one resource, zones.

To keep the example simple, 10 zones are allocated in security-profile-1: 4 reserved zones and 6 maximum zones. This example assumes that the full maximum amount specified—six zones—is available for the user logical systems. The system maximum number of zones is 10.

These cases address configuration across logical systems. They test to see whether a configuration will succeed or fail when it is committed based on allocation of zones.

[Table 3 on page 77](#) shows the security profiles and their zone allocations.

Table 3: Security Profiles Used for Reserved Resource Assessments

Two Security Profiles Used in the Configuration Cases

security-profile-1

- zones reserved quota = 4
- zones maximum quota = 6

NOTE: Later the master administrator dynamically increases the reserved zone count specified in this profile.

master-logical-system-profile

- zones maximum quota = 10
- no reserved quota

[Table 4 on page 78](#) shows three cases that illustrate how the system assesses reserved resources for zones across logical systems based on security profile configurations.

- The configuration for the first case succeeds because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 8, which is less than the system maximum resource quota.
- The configuration for the second case fails because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 12, which is greater than the system maximum resource quota.
- The configuration for the third case fails because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 12, which is greater than the system maximum resource quota.

Table 4: Reserved Resource Allocation Assessment Across Logical Systems**Reserved Resource Quota Checks Across Logical Systems****Example 1: Succeeds**

This configuration is within bounds: $4+4+0=8$, maximum capacity =10.

Security Profiles Used

- The security profile security-profile-1 is bound to two user logical systems: user-logical-system-1 and user-logical-system-2.
- The master-logical-system-profile profile is used exclusively for the master logical system.
- user-logical-system-1 = 4 reserved zones.
- user-logical-system-2 = 4 reserved zones.
- master-logical-system = 0 reserved zones.

Example 2: Fails

This configuration is out of bounds: $4+4+4=12$, maximum capacity =10.

- user-logical-system-1 = 4 reserved zones.
- user-logical-system-2 = 4 reserved zones.
- master-logical-system = 0 reserved zones.
- new-user-logical-system = 4 reserved zones.

Security Profiles

- The security profile security-profile-1 is bound to two user logical systems: user-logical-system-1 and user-logical-system-2.
- The master-logical-system-profile is bound to the master logical system and used exclusively for it.
- The master administrator configures a new user logical system called new-user-logical-system and binds security-profile-1 to it.

Example 3: Fails

This configuration is out of bounds: $6+6=12$, maximum capacity =10.

The master administrator modifies the reserved zones quota in security-profile-1, increasing the count to 6.

- user-logical-system-1 = 6 reserved zones.
- user-logical-system-2 = 6 reserved zones.
- master-logical-system = 0 reserved zones.

- See Also**
- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)
 - [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

Example: Configuring Logical Systems Security Profiles (Master Administrators Only)

This example shows how a master administrator configures three logical system security profiles to assign to user logical systems and the master logical system to provision them with security resources.

- [Requirements on page 79](#)
- [Overview on page 79](#)
- [Configuration on page 79](#)
- [Verification on page 86](#)

Requirements

The example uses an SRX5600 device running Junos OS with logical systems.

Before you begin, read “[SRX Series Logical Systems Master Administrator Configuration Tasks Overview](#)” on page 41 to understand how this task fits into the overall configuration process.

Overview

This example shows how to configure security profiles for the following logical systems:

- The root-logical-system logical system. The security profile master-profile is assigned to the master, or root, logical system.
- The ls-product-design logical system. The security profile ls-design-profile is assigned to the logical system.
- The ls-marketing-dept logical system. The security profile ls-accnt-mrkt-profile is assigned to the logical system.
- The ls-accounting-dept logical system. The security profile ls-accnt-mrkt-profile is assigned to the logical system.
- The interconnect-logical-system, if you use one. You must assign a dummy, or null, security profile to it.

This configuration relies on the deployment shown in “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on page 65.

Configuration

- [Configuring Logical System Security Profiles on page 79](#)

Configuring Logical System Security Profiles

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 system security-profile master-profile policy maximum 65
```

```
set system security-profile master-profile policy reserved 60
set system security-profile master-profile zone maximum 22
set system security-profile master-profile zone reserved 17
set system security-profile master-profile flow-session maximum 3000
set system security-profile master-profile flow-session reserved 2100
set system security-profile master-profile icap-redirect-profile maximum 64
set system security-profile master-profile icap-redirect-profile reserved 30
set system security-profile master-profile nat-nopat-address maximum 115
set system security-profile master-profile nat-nopat-address reserved 100
set system security-profile master-profile nat-static-rule maximum 125
set system security-profile master-profile nat-static-rule reserved 100
set system security-profile master-profile idp
set system security-profile master-profile root-logical-system
set system security-profile ls-accnt-mrkt-profile policy maximum 65
set system security-profile ls-accnt-mrkt-profile policy reserved 60
set system security-profile ls-accnt-mrkt-profile zone maximum 22
set system security-profile ls-accnt-mrkt-profile zone reserved 17
set system security-profile ls-accnt-mrkt-profile flow-session maximum 2500
set system security-profile ls-accnt-mrkt-profile flow-session reserved 2000
set system security-profile master-profile icap-redirect-profile maximum 64
set system security-profile master-profile icap-redirect-profile reserved 30
set system security-profile ls-accnt-mrkt-profile nat-nopat-address maximum 125
set system security-profile ls-accnt-mrkt-profile nat-nopat-address reserved 100
set system security-profile ls-accnt-mrkt-profile nat-static-rule maximum 125
set system security-profile ls-accnt-mrkt-profile nat-static-rule reserved 100
set system security-profile ls-accnt-mrkt-profile logical-system ls-marketing-dept
set system security-profile ls-accnt-mrkt-profile logical-system ls-accounting-dept
set system security-profile ls-design-profile policy maximum 50
set system security-profile ls-design-profile policy reserved 40
set system security-profile ls-design-profile zone maximum 10
set system security-profile ls-design-profile zone reserved 5
set system security-profile ls-design-profile flow-session maximum 2500
set system security-profile ls-design-profile flow-session reserved 2000
set system security-profile master-profile icap-redirect-profile maximum 64
set system security-profile master-profile icap-redirect-profile reserved 30
set system security-profile ls-design-profile nat-nopat-address maximum 120
set system security-profile ls-design-profile nat-nopat-address reserved 100
set system security-profile ls-design-profile logical-system ls-product-design
set system security-profile interconnect-profile logical-system
interconnect-logical-system
```

**Step-by-Step
Procedure**

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

Create three security profiles.

1. Create the first security profile.
 - a. Specify the number of maximum and reserved policies.

```
[edit system security-profile]
user@host# set master-profile policy maximum 65 reserved 60
```
 - b. Specify the number of maximum and reserved zones.


```
[edit system security-profile]
user@host# set master-profile zone maximum 22 reserved 17
```

- c. Specify the number of maximum and reserved sessions.

```
[edit system security-profile]
user@host# set master-profile flow-session maximum 3000 reserved 2100
```

- d. Specify the number of maximum and reserved ICAP redirect profiles

```
[edit system security-profile]
user@host# set master-profile icap-redirect-profile maximum 64 reserved 30
```

- e. Specify the number of maximum and reserved source NAT no-PAT addresses and static NAT rules.

```
[edit system security-profile]
user@host# set master-profile nat-nopat-address maximum 115 reserved 100
user@host# set master-profile nat-static-rule maximum 125 reserved 100
```

- f. Enable intrusion detection and prevention (IDP). You can enable IDP only for the master (root) logical system.

```
[edit system security-profile]
user@host# set idp
```

- g. Bind the security profile to the logical system.

```
[edit system security-profile]
user@host# set master-profile root-logical-system
```

2. Create the second security profile.

- a. Specify the number of maximum and reserved policies.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile policy maximum 65 reserved 60
```

- b. Specify the number of maximum and reserved zones.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile zone maximum 22 reserved 17
```

- c. Specify the number of maximum and reserved sessions.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile flow-session maximum 2500 reserved
2000
```

- d. Specify the number of maximum and reserved ICAP redirect profiles

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile icap-redirect-profile maximum 64 reserved
30
```

- e. Specify the number of maximum and reserved source NAT no-PAT addresses.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile nat-nopat-address maximum 125 reserved
100
```

- f. Specify the number of maximum and reserved static NAT rules.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile nat-static-rule maximum 125 reserved 100
```

- g. Bind the security profile to two logical systems.

```
[edit system]
user@host# set security-profile ls-accnt-mrkt-profile logical-system
ls-marketing-dept
user@host# set security-profile ls-accnt-mrkt-profile logical-system
ls-accounting-dept
```

3. Create the third security profile.

- a. Specify the number of maximum and reserved policies.

```
[edit system security-profile]
user@host# set ls-design-profile policy maximum 50 reserved 40
```

- b. Specify the number of maximum and reserved zones.

```
[edit system security-profile]
user@host# set ls-design-profile zone maximum 10 reserved 5
```

- c. Specify the number of maximum and reserved sessions.

```
[edit system security-profile]
user@host# set ls-design-profile flow-session maximum 2500 reserved 2000
```

- d. Specify the number of maximum and reserved ICAP redirect profiles

```
[edit system security-profile]
user@host# set ls-design-profile icap-redirect-profile maximum 64 reserved 30
```

- e. Specify the number of maximum and reserved source NAT no-PAT addresses.

```
[edit system security-profile]
user@host# set ls-design-profile nat-nopat-address maximum 120 reserved 100
```

4. Bind the security profile to a logical system.

```
user@host# set system security-profile ls-design-profile logical-system
ls-product-design
```

5. Bind a null security profile to the interconnect logical system.

```
user@host# set system security-profile interconnect-profile logical-system
interconnect-logical-system
```

Results From configuration mode, confirm your configuration by entering the **show system security-profile** command to see all security profiles configured.

To see individual security profiles, enter the **show system security-profile master-profile**, the **show system security-profile ls-accnt-mrkt-profile** and, the **show system security-profile ls-design-profile** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show system security-profile
interconnect-profile {
  logical-system interconnect-logical-system;
}
ls-accnt-mrkt-profile {
  policy {
    maximum 65;
    reserved 60;
  }
  zone {
    maximum 22;
    reserved 17;
  }
  flow-session {
    maximum 2500;
    reserved 2000;
  }
  icap-redirect-profile {
    maximum 64;
    reserved 30;
  }
  nat-nopat-address {
    maximum 125;
    reserved 100;
  }
  nat-static-rule {
    maximum 125;
    reserved 100;
  }
  logical-system [ ls-marketing-dept ls-accounting-dept ];
}
ls-design-profile {
  policy {
    maximum 50;
    reserved 40;
  }
  zone {
    maximum 10;
    reserved 5;
  }
  flow-session {
    maximum 2500;
    reserved 2000;
  }
}
```

```
    }
    icap-redirect-profile {
        maximum 64;
        reserved 30;
    }
    nat-nopat-address {
        maximum 120;
        reserved 100;
    }
    nat-static-rule {
        maximum 125;
        reserved 100;
    }
    logical-system ls-product-design;
}
master-profile {
    policy {
        maximum 65;
        reserved 60;
    }
    zone {
        maximum 22;
        reserved 17;
    }
    flow-session {
        maximum 3000;
        reserved 2100;
    }
    icap-redirect-profile {
        maximum 64;
        reserved 30;
    }
    nat-nopat-address {
        maximum 115;
        reserved 100;
    }
    nat-static-rule {
        maximum 125;
        reserved 100;
    }
    root-logical-system;
}

user@host# show system security-profile master-profile
policy {
    maximum 65;
    reserved 60;
}
zone {
    maximum 22;
    reserved 17;
}
flow-session {
    maximum 3000;
    reserved 2100;
}
```

```
icap-redirect-profile {
  maximum 64;
  reserved 30;
}
nat-nopat-address {
  maximum 115;
  reserved 100;
}
nat-static-rule {
  maximum 125;
  reserved 100;
}
}
root-logical-system;

user@host# show system security-profile ls-accnt-mrkt-profile
policy {
  maximum 65;
  reserved 60;
}
zone {
  maximum 22;
  reserved 17;
}
flow-session {
  maximum 2500;
  reserved 2000;
}
icap-redirect-profile {
  maximum 64;
  reserved 30;
}
nat-nopat-address {
  maximum 125;
  reserved 100;
}
nat-static-rule {
  maximum 125;
  reserved 100;
}
}
logical-system [ ls-accounting-dept ls-marketing-dept ];

user@host# show system security-profile ls-design-profile
policy {
  maximum 50;
  reserved 40;
}
zone {
  maximum 10;
  reserved 5;
}
flow-session {
  maximum 2500;
  reserved 2000;
}
icap-redirect-profile {
  maximum 64;
  reserved 30;
}
```

```
}
nat-nopat-address {
    maximum 120;
    reserved 100;
}
nat-static-rule {
    maximum 125;
    reserved 100;
}
logical-system ls-product-design;
```

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

Verification

To confirm that the security resources that you allocated for logical systems have been assigned to them, follow this procedure for each logical system and for all its resources.

- [Verifying That Security Profile Resources Are Effectively Allocated for Logical Systems on page 86](#)

Verifying That Security Profile Resources Are Effectively Allocated for Logical Systems

Purpose Verify security resources for each logical system. Follow this process for all configured logical systems.

- Action**
1. Use Telnet to log in to each user logical system as its user logical system administrator.
Run Telnet, specifying the IP address of your SRX Series device. For example:

```
telnet 10.11.11.19
```

2. Enter the login ID and password for one of the user logical systems that you created.

```
login: lsmarketingadmin1
password: Talk2345
lsmarketingadmin1@host:ls-marketing-dept>
```

3. Enter the following statement to identify the resources configured for the profile.

```
lsmarketingadmin1@host:ls-marketing-dept> show system security-profile ?
```

4. Enter the following command at the resulting prompt. Do this for each feature configured for the profile.

```
lsmarketingadmin1@host:ls-marketing-dept> show system security-profile zone detail
logical system name : ls-marketing-dept
security profile name : ls-accnt-mrkt-profile
used amount : 0
reserved amount : 17
maximum quota : 22
```

- See Also**
- [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

Example: Configuring User Logical Systems Security Profiles

In this example, you configure the user logical systems security profiles. It provides the information about a resource allocated to the logical system in a security profile.



NOTE:

- The user logical system supports Layer 2 traffic and firewall session function on SRX4100 and SRX4200 devices.
- Layer 2 cross logical system traffic is not supported.

- [Requirements on page 88](#)
- [Overview on page 88](#)

- [Configuration on page 89](#)
- [Verification on page 91](#)

Requirements

This example uses an SRX4100 and SRX4200 devices running Junos OS with logical systems.

Before you begin:

- Understand the logical system configuration process. See [“User Logical Systems Configuration Overview” on page 61](#) to understand how this task fits into the overall configuration process.

Overview

Logical systems allow a master administrator to partition an SRX Series device into discrete contexts called user logical systems. User logical systems are self-contained, private contexts, separate both from one another and from the master logical system. A user logical system has its own security, networking, logical interfaces, routing configurations, and one or more user logical system administrators.

In this example, you configure security features for the user logical system described in [Table 5 on page 88](#). This configuration used by the user logical system administrator to display resource information for a user logical system.

Table 5: Resource Information for a User Logical System

Field Name	Field Description
MAC flags	Status of MAC address learning properties for each interface: <ul style="list-style-type: none"> • S—Static MAC address is configured • D—Dynamic MAC address is configured • L—Locally learned MAC address is configured • P—Persistent static • C—Control MAC • SE—MAC accounting is enabled • NM—Non-configured MAC • R—Locally learned MAC address is configured • O—Open vSwitch Database (OVSDb) MAC
Ethernet switching table	For learned entries, the time at which the entry was added to the Ethernet switching table.
Logical system	Name of the logical system
Routing instance	Name of the routing instance
VLAN name	Name of the VLAN
MAC address	MAC address or addresses learned on a logical interface

Table 5: Resource Information for a User Logical System (continued)

Field Name	Field Description
Age	This field is not supported
Logical interface	Name of the logical interface
RTR ID	ID of the routing device
NH Index	Software index of the next hop that is used to route the traffic for a given prefix.

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 system security-profile security-profile-name logical-system logical-system-name
set logical-systems logical-system-name interfaces xe-0/0/0 unit 0 family
  ethernet-switching interface-mode access
set logical-systems logical-system-name interfaces xe-0/0/0 unit 0 family
  ethernet-switching vlan members VLAN100
set logical-systems logical-system-name interfaces xe-0/0/1 unit 0 family
  ethernet-switching interface-mode access
set logical-systems logical-system-name interfaces xe-0/0/1 unit 0 family
  ethernet-switching vlan members VLAN100
set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family
  ethernet-switching interface-mode trunk
set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family
  ethernet-switching vlan members VLAN200
set logical-systems logical-system-name interfaces xe-0/0/1.0 unit 0 family
  ethernet-switching interface-mode trunk
set logical-systems logical-system-name interfaces xe-0/0/2.0 unit 0 family
  ethernet-switching vlan members vlan200
set logical-systems logical-system-name interfaces irb unit 22 family inet address
  10.11.11.150/24
set logical-systems logical-system-name security policies default-policy permit-all
set logical-systems logical-system-name security zones security-zone trust
  host-inbound-traffic system-services all
set logical-systems logical-system-name security zones security-zone trust
  host-inbound-traffic protocols all
set logical-systems logical-system-name security zones security-zone trust interfaces
  xe-0/0/2.0
set logical-systems logical-system-name security zones security-zone untrust
  host-inbound-traffic system-services all
set logical-systems logical-system-name security zones security-zone untrust
  host-inbound-traffic protocols all
set logical-systems logical-system-name security zones security-zone untrust interfaces
  xe-0/0/2.0
set logical-systems logical-system-name security zones security-zone untrust interfaces
  xe-0/0/3.0

```

```
set logical-systems logical-system-name vlans VLAN100 vlan-id 100
set logical-systems logical-system-name vlans VLAN100 l3-interface irb.22
```

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

To configure user logical systems security profiles:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
[edit]
admin@host> configure
admin@host#
```

2. Configure a security profile and assign it to a logical-system.

```
[edit system security-profile ]
admin@host# set system security-profile security-profile-name logical-system
```

3. Set the interfaces to the appropriate interface modes and specify that the logical interface that will receive the untagged data packets is a member of the native VLAN.

```
[edit logical-systems]
admin@host#set logical-systems logical-system-name interfaces xe-0/0/0 unit
0 family ethernet-switching interface-mode access
admin@host# set logical-systems logical-system-name interfaces xe-0/0/2 unit
0 family ethernet-switching vlan members VLAN100
admin@host#set logical-systems logical-system-name interfaces xe-0/0/1 unit 0
family ethernet-switching interface-mode access
admin@host# set logical-systems logical-system-name interfaces xe-0/0/3 unit
0 family ethernet-switching vlan members VLAN100
admin@host#set logical-systems logical-system-name interfaces xe-0/0/2 unit
0 family ethernet-switching interface-mode trunk
admin@host#set logical-systems logical-system-name interfaces xe-0/0/2 unit
0 family ethernet-switching vlan members VLAN100
admin@host#set logical-systems logical-system-name interfaces xe-0/0/1.0 unit
0 family ethernet-switching interface-mode trunk
admin@host#set logical-systems logical-system-name interfaces xe-0/0/2.0 unit
0 family ethernet-switching vlan members vlan200
```

4. Create the IRB interface and assign it an address in the subnet.

```
[edit interface]
admin@host# set interfaces irb unit 22 family inet address 10.11.11.150/24
```

5. Create the security policy to permit traffic from the trust zone to the untrust zone and assign interfaces to each zone.

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

```
admin@host# set security zones security-zone trust host-inbound-traffic
system-services all
admin@host# set security zones security-zone trust host-inbound-traffic protocols
all
admin@host# set security zones security-zone trust interfaces xe-0/0/2.0
admin@host# set security zones security-zone untrust host-inbound-traffic
system-services all
admin@host# set security zones security-zone untrust host-inbound-traffic protocols
all
admin@host# set security zones security-zone untrust interfaces xe-0/0/2.0
admin@host# set security zones security-zone untrust interfaces xe-0/0/3.0
```

6. Associate an IRB interface with the VLAN.

```
[edit logical-systems]
admin@host# set logical-systems logical-system-name vlans VLAN100 vlan-id 100
admin@host# set logical-systems logical-system-name vlans VLAN100 l3-interface
irb.22
```

Results

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

```
admin@host# show ethernet-switching table
ethernet-switching table {
  filter;
  inner-vlan;
  inter-switch-link;
  interface-mode;
  policer;
  recovery-timeout;
  storm-control;
  vlan;
  vlan-auto-sense;
  vlan-rewrite;
}
```

Verification

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

- [Verifying User Logical Systems Security Profiles Configuration on page 91](#)

Verifying User Logical Systems Security Profiles Configuration

Purpose Verify security policies information.

Action From operational mode, enter the **show ethernet-switching table** command.

```
admin@host> show ethernet-switching table
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent
static, C - Control MAC
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC,
O - ovsdb MAC)
```

```
Ethernet switching table : 1 entries, 1 learned
Logical system : LD2
Routing instance : default
  Vlan      MAC      MAC      Age      Logical
  NH      RTR
  name      address    flags      interface
  Index      ID
VLAN100      d4:04:ff:89:fd:30  D      -      xe-0/0/2.0
  0          0
```

Example: Configuring Security log stream for Logical Systems

This example shows how to configure a security profiles for a logical system.

- [Requirements on page 92](#)
- [Overview on page 92](#)
- [Configuration on page 92](#)
- [Verification on page 93](#)

Requirements

This example uses the SRX Series devices running Junos OS with logical systems.

Before you begin:

- Read “[SRX Series Logical Systems Master Administrator Configuration Tasks Overview](#)” on page 41 to understand how this task fits into the overall configuration process.
- See “[Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\)](#)” on page 79.

Overview

As master administrator, you can configure a single security profile to assign resources to a specific logical system. You can use the same security profile for more than one logical system, or use a mix of both methods. The **set logical-system LSYS1 security log** command is introduced for logging support on SRX Series devices.

Configuration

- [Configuring Logical System Security Profiles logical-system on page 93](#)
- [Results on page 93](#)

Configuring Logical System Security Profiles logical-system

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 system security-profile p1 security-log-stream-number reserved 1
set system security-profile p1 security-log-stream-number maximum 2
set system security-profile p1 logical-system LSYS1
```

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

1. Configure a security profile and specify the number of maximum and reserved policies..

```
[edit system]
user@host# set security-profile p1 security-log-stream-number reserved 1
user@host# set security-profile p1 security-log-stream-number maximum 2
```

2. Assign the configured security profile to LSYS1.

```
user@host# set security-profile p1 logical-system LSYS1
```

Results

From configuration mode, confirm your configuration by entering the **show system security-profile** command to see all security profiles configured.

```
[edit]
user@host# show system security-profile
p1 {
  security-log-stream-number {
    maximum 2;
    reserved 1;
  }
  logical-system LSYS1;
}
```

Verification

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

- [Verifying Security Profile Resources for Logical Systems on page 94](#)
- [Verifying security-log-stream-number for logical-systems on page 94](#)
- [Verifying security-log-stream-number summary for logical-systems on page 95](#)
- [Verifying security-log-stream-number detail for logical-systems on page 95](#)

Verifying Security Profile Resources for Logical Systems

Purpose Verify the security resources for each logical system.

Action From operational mode, enter the **show system security-profile all-resource**, **show system security-profile security-log-stream-number logical-system all**, **show system security-profile security-log-stream-number summary**, or **show system security-profile security-log-stream-number detail logical-system all** command to see the output:

show system security-profile all-resource

```
user@host> show system security-profile all-resource
```

resource	usage	reserved	maximum
[logical system name: root-logical-system]			
[security profile name: Default-Profile]			
address-book	0	0	512
auth-entry	0	0	2147483647
cpu on CP	0.00%	1.00%	80.00%
cpu on SPU	0.00%	1.00%	80.00%
flow-gate	0	0	524288
flow-session	2	0	6291456
nat-cone-binding	0	0	65536
nat-destination-pool	0	0	4096
nat-destination-rule	0	0	8192
nat-nopat-address	0	0	1048576
nat-pat-address	0	0	2048
nat-port-ol-ipnumber	0	0	4
nat-rule-referenced-prefix	0	0	1048576
nat-source-pool	0	0	2048
nat-source-rule	0	0	8192
nat-static-rule	0	0	20480
policy	0	0	40000
policy-with-count	0	0	1024
scheduler	0	0	64
zone	0	0	512

Meaning The sample outputs displays information about the resources allocated to the logical system in a security profile. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

Verifying security-log-stream-number for logical-systems

Purpose Verify the security-log-stream-number for each logical system.

Action From operational mode, enter the **show system security-profile security-log-stream-number logical-system all** command to see the output:

show system security-profile security-log-stream-number logical-system all

```
user@host> show system security-profile security-log-stream-number logical-system all
logical system name  security profile name  usage  reserved  maximum
root-logical-system  Default-Profile        1       0         3
LSYS1                sp1                     0       1         3
LSYS2                sp2                     1       0         3
```

Meaning The sample output displays the information about a resource allocated to the logical system in a security profile with security profile name. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

Verifying security-log-stream-number summary for logical-systems

Purpose Verify the security-log-stream-number summary.

Action From operational mode, enter the **show system security-profile security-log-stream-number summary** command to see the output:

show system security-profile security-log-stream-number summary

```
user@host> show system security-profile security-log-stream-number summary
global used amount      : 0
global maximum quota    : 32
global available amount : 32
total logical systems   : 1
total security profiles : 0
heaviest usage / user   : 0 / root-logical-system
lightest usage / user   : 0 / root-logical-system
```

Meaning The sample output displays the summary information about the resource for all logical systems.

Verifying security-log-stream-number detail for logical-systems

Purpose Verify the security-log-stream-number detail.

Action From operational mode, enter the **show system security-profile security-log-stream-number detail logical-system all** command to see the output:

show system security-profile security-log-stream-number detail logical-system all

```
user@host> show system security-profile security-log-stream-number detail logical-system all
logical system name      : root-logical-system
security profile name    : Default-Profile
used amount              : 0
reserved amount          : 0
maximum quota            : 8
logical system name      : lsys0
security profile name    : lsys_profile
used amount              : 0
reserved amount          : 0
maximum quota            : 8
logical system name      : lsys1
security profile name    : lsys_profile
used amount              : 0
reserved amount          : 0
maximum quota            : 8
logical system name      : lsys2
security profile name    : lsys_profile
used amount              : 0
reserved amount          : 0
maximum quota            : 8
```

Meaning The sample output displays the detailed level of output for all logical systems.

See Also • [security-profile-resources on page 546](#)

CPU Allocation for Logical Systems

The CPU allocation for logical systems assign the reserved CPU resources to a logical system used to calculate the amount of CPU usage based on the runtime utilization. For more information, see the following topics:

- [Understanding CPU Allocation and Control on page 96](#)
- [Example: Configuring CPU Utilization \(Master Administrators Only\) on page 100](#)

Understanding CPU Allocation and Control

When device CPU utilization is low, logical systems can acquire and use CPU resources above their allocated reserve quotas as long as the system-wide utilization remains within a stable range. CPU utilization on a device should never reach 100 percent because a device running at 100 percent CPU utilization might be slow to respond to management or system events or be unable to handle traffic bursts.

CPU resources are used on a first-come first-served basis. Without controls, logical systems can compete for CPU resources and drive CPU utilization up to 100 percent. You

cannot rely on the configuration of static resources, such as security policies and zones, to directly control CPU usage because a logical system with small numbers of static resources allocated could still consume a large amount of CPU. Instead, the master administrator can enable CPU resource control and configure CPU utilization parameters for logical systems.



NOTE: Only the master administrator can enable CPU control and configure CPU utilization parameters. User logical system administrators can use the `show system security-profile cpu` command to view CPU utilization for their logical systems.

This topic includes the following sections:

- [CPU Control on page 97](#)
- [Reserved CPU Utilization Quota for Logical Systems on page 97](#)
- [CPU Control Target on page 98](#)
- [Shared CPU Resources and CPU Quotas on page 98](#)
- [Monitoring CPU Utilization on page 100](#)

CPU Control

The master administrator enables CPU control with the `cpu-control` configuration statement at the `[edit system security-profile resources]` hierarchy level.



NOTE: The `resources` security profile is a special security profile that contains global settings that apply to all logical systems in the device. Other security profiles configured by the master administrator are bound to specific logical systems.

When CPU control is enabled, the master administrator can then configure the following CPU utilization parameters:

- A reserved CPU quota is the percentage of CPU utilization that is guaranteed for a logical system.
- The CPU control target is the upper limit, in percent, for system-wide CPU utilization on the device under normal operating conditions.

Reserved CPU Utilization Quota for Logical Systems

A configured reserved CPU quota guarantees that a specified percentage of CPU is always available to a logical system. During runtime, CPU utilization by each logical system is measured every two seconds. The reserved CPU quota is used to calculate the amount of CPU each logical system can use based on the runtime utilization.

The master administrator specifies the reserved CPU quota in a logical system security profile with the `cpu reserved` configuration statement at the `[edit system security-profile`

profile-name] hierarchy level. The security profile is bound to one or more logical systems. Unlike other resources that are allocated to a logical system in a security profile, no maximum allowed quota can be configured for CPU utilization.

The Junos OS software checks to ensure that the sum of reserved CPU quotas for all logical systems on the device is less than 90 percent of the CPU control target value. If CPU control is enabled and reserved CPU quotas are not configured, the default reserved CPU quota for the master logical system is 1 percent and the default reserved CPU quota for user logical systems is 0 percent. The master administrator can configure reserved CPU quotas even if CPU control is not enabled. The master administrator can enable or disable CPU control without changing security profiles.



CAUTION: The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota because traffic loss could occur.

CPU Control Target

CPU control target is the upper limit, in percent, for CPU utilization on the device under normal operating conditions. If CPU utilization on the device surpasses the configured target value, the Junos OS software initiates controls to bring CPU utilization between the target value and 90 percent of the target value. For example, if the CPU control target value is 80 and CPU utilization on the device surpasses 80 percent, then controls are initiated to bring CPU utilization within the range of 72 (90 percent of 80) and 80 percent.

During runtime, CPU utilization by each logical system is measured every two seconds. Dropping packets reduces the CPU usage for a logical system. If the CPU usage of a logical system exceeds its quota, CPU utilization control drops the packets received on that logical system. The packet drop rate is calculated every two seconds based on CPU utilization of all logical systems.

The master administrator configures the CPU control target with the **cpu-control-target** configuration statement at the [**edit system security-profile resources**] hierarchy level. A stable level of CPU utilization should be relatively close to 100 percent but allow for bursts in CPU utilization. The master administrator should configure the CPU control target level based on an understanding of the usage pattern of the logical system's deployment on the device.

CPU control must be enabled for the Junos OS software to control CPU usage. If the master administrator enables CPU control without specifying a CPU control target value, the default CPU control target is 80 percent.

Shared CPU Resources and CPU Quotas

The sum of the reserved CPU quotas for all logical systems on the device must be less than 90 percent of the CPU control target; the difference is called the shared CPU resource. The shared CPU resource is dynamically allocated among the logical systems that need additional CPU. This means that a logical system can use more CPU than its reserved CPU quota.

The CPU quota for a logical system is the sum of its reserved CPU quota and its portion of the shared CPU resource. If multiple logical systems need more CPU resources, they split the shared CPU resource based on the relative weights of their reserved CPU quotas. Logical systems with larger reserved CPU quotas receive larger portions of the shared CPU resource. The goal for CPU control is to keep the actual CPU utilization of a logical system at its CPU quota. If a logical system's CPU needs are greater than its CPU quota, packets are dropped for that logical system.

The following scenarios illustrate CPU control for logical systems. In each scenario, the CPU control target value is 80, which means that CPU controls will keep the maximum system-wide CPU utilization between 72 and 80 percent. The reserved CPU quotas for the logical systems are configured as follows: master and lsys1 logical systems are 10 percent each and the lsys2 logical system is 5 percent.

CPU Utilization Scenario 1

In this scenario, each of the three logical systems needs 40 percent of CPU.

[Table 6 on page 99](#) shows the CPU quotas for each logical system. Because the CPU needed by each logical system is greater than its CPU quota, packets are dropped for each logical system.

Table 6: CPU Utilization Scenario 1

Logical System	Needed CPU	CPU Quotas	Packets Dropped?
master	40%	28.8%	Yes
lsys1	40%	28.8%	Yes
lsys2	40%	14.4%	Yes

CPU Utilization Scenario 2

In this scenario, the master logical system needs 25 percent of CPU while the two user logical systems need 40 percent. [Table 7 on page 99](#) shows the CPU quota for the master logical system is equal to the CPU it needs, so no packets are dropped for the master logical system and CPU control monitors the CPU utilization of the master logical system. Packets are dropped for lsys1 and lsys2.

Table 7: CPU Utilization Scenario 2

Logical System	Needed CPU	CPU Quotas	Packets Dropped?
master	25%	25%	No
lsys1	40%	31.3%	Yes
lsys2	40%	15.6%	Yes

CPU Utilization Scenario 3

In this scenario, the master and lsys2 logical systems need 5 percent and 3 percent of CPU, respectively, while lsys1 needs 40 percent. [Table 8 on page 100](#) shows system-wide

CPU utilization is 48 percent, which is less than 72 percent (90 percent of the CPU control target), so no packets are dropped and CPU control monitors all logical systems.

Table 8: CPU Utilization Scenario 3

Logical System	Needed CPU	CPU Quota	Packets Dropped?
master	5%	5%	No
lsys1	40%	40%	No
lsys2	3%	3%	No

Monitoring CPU Utilization

CPU utilization can be monitored by either the master administrator or the user logical system administrators. The master administrator can monitor CPU utilization for the master logical system, a specified user logical system, or all logical systems. User logical system administrators can only monitor CPU utilization for their logical system.

The **show system security-profile cpu** command shows the usage and drop rate in addition to the reserved CPU quota configured for the logical system. During runtime, CPU utilization by each logical system is measured every two seconds. The usage and drop rates displayed are the values at the interval prior to when the **show** command is run. If the **detail** option is not specified, the utilization of the central point (CP) and the average utilization of all services processing units (SPUs) is shown. The **detail** option displays the CPU utilization on each SPU.

The CPU utilization log file **lsys-cpu-utilization-log** contains utilization data for all logical systems on the device. Only the master administrator can view the log file with the **show log lsys-cpu-utilization-log** command.

- See Also**
- [Example: Configuring CPU Utilization \(Master Administrators Only\) on page 100](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)

Example: Configuring CPU Utilization (Master Administrators Only)

The master administrator can enable CPU control and configure CPU utilization parameters. This example shows how to enable CPU utilization control and configure CPU utilization quotas and a control target.

- [Requirements on page 101](#)
- [Overview on page 101](#)
- [Configuration on page 101](#)
- [Verification on page 103](#)

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role”](#) on page 40.
- Bind security profiles to the master logical system and user logical systems configured on the device. See [“Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\)”](#) on page 79.

Overview

In this example, you enable CPU control and set the CPU control target to be 85 percent. You allocate reserved CPU quotas to the logical systems shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65. The logical systems are bound to the security profiles shown in [Table 9](#) on page 101 and are assigned the reserved CPU quotas in the security profiles.

Table 9: Logical Systems, Security Profiles, and Reserved CPU Quotas

Logical System	Security Profile	Reserved CPU Quotas
root-logical-system (master)	master-profile	2 percent
ls-product-design	ls-design-profile	2 percent
ls-marketing-dept, ls-accounting-dept	ls-accnt-mrkt-profile	1 percent

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 system security-profile resources cpu-control
set system security-profile resources cpu-control-target 85
set system security-profile master-profile cpu reserved 2
set system security-profile ls-design-profile cpu reserved 2
set system security-profile ls-accnt-mrkt-profile cpu reserved 1
```

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

To configure CPU utilization control parameters:

1. Log in to the master logical system as the master administrator and enter configuration mode.

[edit]

```
admin@host> configure
admin@host#
```

2. Enable CPU control.

```
[edit system security-profile resources]
admin@host# set cpu-control
```

3. Configure the CPU control target.

```
[edit system security-profile resources]
admin@host# set cpu-control-target 85
```

4. Configure the reserved CPU quotas in the security profiles.

```
[edit system]
admin@host# set security-profile security-profile master-profile cpu reserved 2
admin@host# set security-profile security-profile ls-design-profile cpu reserved 2
admin@host# set security-profile security-profile ls-accnt-mrkt-profile cpu reserved
1
```

Results From configuration mode, confirm your configuration by entering the **show system security-profile** 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 (...).

```
[edit]
admin@host# show system security-profile
resources {
  cpu-control;
  cpu-control-target 85;
}
ls-accnt-mrkt-profile {
  ...
  cpu {
    reserved 1;
  }
  logical-system [ ls-marketing-dept ls-accounting-dept ];
}
ls-design-profile {
  ...
  cpu {
    reserved 2;
  }
  logical-system ls-product-design;
}
master-profile {
  ...
  cpu {
    reserved 2;
  }
}
```

```

    }
    logical-system root-logical-system;
}

```

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

Verification

Confirm that the configuration is working properly.

- [Verifying CPU Utilization on page 103](#)

Verifying CPU Utilization

Purpose Display the configured reserved CPU quota, the actual CPU usage, and the drop rate.

Action From operational mode, enter the **show system security-profile cpu logical-system all** command.

```

admin@host> show system security-profile cpu logical-system all
CPU control: TRUE
CPU control target: 85.00%
logical system name  profile name  CPU name  usage(%)  reserved(%)
drop rate(%)
root-logical-system  master-profile CP          0.10%      2.00%
0.00%
root-logical-system  master-Profile SPU         0.25%      2.00%
0.00%
ls-product-design    ls-design-profile CP       0.53%      2.00%
0.00%
ls-product-design    ls-design-profile SPU       0.26%      2.00%
0.00%
ls-marketing-dept    ls-acct-mrkt-profile CP    0.10%      1.00%
0.00%
ls-marketing-dept    ls-acct-mrkt-profile SPU    0.15%      1.00%
0.00%
ls-accounting-dept    ls-acct-mrkt-profile CP    0.23%      1.00%
0.00%
ls-accounting-dept    ls-acct-mrkt-profile SPU    0.34%      1.00%
0.00%

```

- See Also**
- [Understanding CPU Allocation and Control on page 96](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)

Routing and Interfaces for Master Logical Systems

Logical systems enables you to configure the interfaces, routing instances and the routing protocol. The master logical system administrator can display or clear the routing protocol parameters for all logical systems whereas the administrator for the user logical system

can display or clear the protocol parameters for their own logical system. For more information, see the following topics:

- [Understanding Logical Systems Interfaces and Routing Instances on page 104](#)
- [Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\) on page 105](#)
- [Example: Configuring OSPF Routing Protocol for the Master Logical Systems on page 114](#)

Understanding Logical Systems Interfaces and Routing Instances

Logical interfaces on the device are allocated among the user logical systems by the master administrator. The user logical system administrator configures the attributes of the interfaces, including IP addresses, and assigns them to routing instances and zones.

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. There can be multiple routing tables for a single routing instance—for example, unicast IPv4, unicast IPv6, and multicast IPv4 routing tables can exist in a single routing instance. Routing protocol parameters and options control the information in the routing tables.

Interfaces and routing instances can be configured in the master logical system and in user logical systems. Configuring an interface or routing instance in a logical system is the same as configuring an interface or routing instance on a device that is not configured for logical systems. Any routing instance created within a logical system is only applicable to that logical system.

The default routing instance, master, refers to the main inet.0 routing table in the logical system. The master routing instance is reserved and cannot be specified as a routing instance. Routes are installed in the master routing instance by default, unless a routing instance is specified. Configure global routing options and protocols for the master routing instance by including statements at the **[edit protocols]** and **[edit routing-options]** hierarchy levels in the logical system.

You can configure only virtual router routing instance type in a user logical system. Only one virtual private LAN service (VPLS) routing instance type can be configured on the device and it must be in the interconnect logical system.

The user logical system administrator can configure and view all attributes for an interface or routing instance in a user logical system. All attributes of an interface or routing instance in a user logical system are also visible to the master administrator.

Multicast is a “one source, many destinations” method of traffic distribution, which means the destinations needing to receive the information from a particular source receive the traffic stream. The master and user logical system administrators can configure a logical system to support multicast applications. The same multicast configurations to configure a device as a node in a multicast network can be used in a logical system.

- See Also**
- [Example: Configuring Interfaces and Routing Instances for a User Logical Systems on page 121](#)

- [User Logical Systems Configuration Overview on page 61](#)
- [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Master Administrators Only)

This topic covers configuration of interfaces, static routes, and routing instances for the master and interconnect logical systems. It also covers configuration of logical tunnel interfaces for user logical systems.

- [Requirements on page 105](#)
- [Overview on page 105](#)
- [Configuration on page 107](#)
- [Verification on page 113](#)

Requirements

The example uses an SRX5600 device running Junos operating system (Junos OS) with logical systems.

Before you begin:

- Read “[SRX Series Logical Systems Master Administrator Configuration Tasks Overview](#)” on [page 41](#) to understand how and where this procedure fits in the overall master administrator configuration process.
- Read “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on [page 65](#)
- [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)

Overview

This scenario shows how to configure interfaces for the logical systems on the device, including an interconnect logical system.

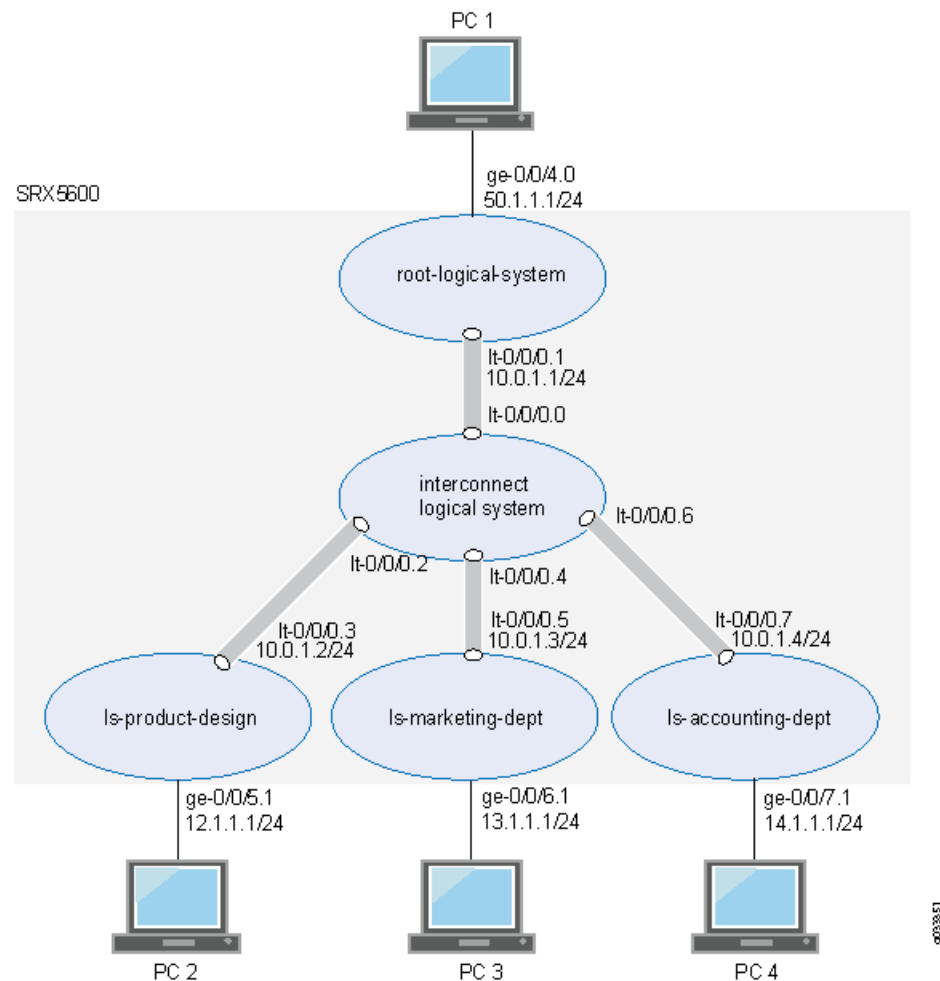
- For the interconnect logical system, the example configures logical tunnel interfaces lt-0/0/0.0, lt-0/0/0.2, lt-0/0/0.4, and lt-0/0/0.6. The example configures a routing instance called vr-ic and assigns the interfaces to it.

Because the interconnect logical system acts as a virtual switch, it is configured as a virtual private LAN service (VPLS) routing instance type. The interconnect logical system's lt-0/0/0 interfaces are configured with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the master and user logical systems are configured with Ethernet as the encapsulation type.

- lt-0/0/0.0 connects to lt-0/0/0.1 on the root logical system.
- lt-0/0/0.2 connects to lt-0/0/0.3 on the ls-product-design logical system.
- lt-0/0/0.4 connects to lt-0/0/0.5 on the ls-marketing-dept logical system.
- lt-0/0/0.6 connects to lt-0/0/0.7 on the ls-accounting-dept logical system.
- For the master logical system, called root-logical-system, the example configures ge-0/0/4.0 and assigns it to the vr1-root routing instance. The example configures lt-0/0/0.1 to connect to lt-0/0/0.0 on the interconnect logical system and assigns it to the vr1-root routing instance. The example configures static routes to allow for communication with other logical systems and assigns them to the vr1-root routing instance.
- For the ls-product-design logical system, the example configures lt-0/0/0.3 to connect to lt-0/0/0.2 on the interconnect logical system.
- For the ls-marketing-dept logical system, the example configures lt-0/0/0.5 to connect to lt-0/0/0.4 on the interconnect logical system.
- For the ls-accounting-dept logical system, the example configures lt-0/0/0.7 to connect to lt-0/0/0.6 on the interconnect logical system.

[Figure 6 on page 107](#) shows the topology for this deployment including virtual routers and their interfaces for all logical systems.

Figure 6: Configuring Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers



Configuration

This topic explains how to configure interfaces for logical systems.

- [Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System on page 107](#)
- [Configuring Interfaces, a Routing Instance, and Static Routes for the Master Logical System on page 109](#)
- [Configuring Logical Tunnel Interfaces for the User Logical Systems on page 111](#)

Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System

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 logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 0 encapsulation
  ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 2 encapsulation
  ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 4 encapsulation
  ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 6 encapsulation
  ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 6 peer-unit 7
set logical-systems interconnect-logical-system routing-instances vr-ic instance-type
  vpls
set logical-systems interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.0
set logical-systems interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.2
set logical-systems interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.4
set logical-systems interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.6
```

**Step-by-Step
Procedure**

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

To configure the interconnect system lt-0/0/0 interfaces and routing instances:

1. Configure the lt-0/0/0 interfaces.

```
[edit logical-systems]
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 0 encapsulation
  ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 0 peer-unit 1
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 2 encapsulation
  ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 2 peer-unit 3
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 4 encapsulation
  ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 4 peer-unit 5
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 6 encapsulation
  ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 6 peer-unit 7
```

2. Configure the routing instance for the interconnect logical system and add its lt-0/0/0 interfaces to it.

```
[edit logical-systems]
user@host# set interconnect-logical-system routing-instances vr-ic instance-type
  vpls
user@host# set interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.0
user@host# set interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.2
```

```
user@host# set interconnect-logical-system routing-instances vr-ic interface
lt-0/0/0.4
user@host# set interconnect-logical-system routing-instances vr-ic interface
lt-0/0/0.6
```

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

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

```
user@host# show logical-systems interconnect-logical-system
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
    }
    unit 4 {
      encapsulation ethernet-vpls;
      peer-unit 5;
    }
    unit 6 {
      encapsulation ethernet-vpls;
      peer-unit 7;
    }
  }
}
routing-instances {
  vr-ic {
    instance-type vpls;
    interface lt-0/0/0.0;
    interface lt-0/0/0.2;
    interface lt-0/0/0.4;
    interface lt-0/0/0.6;
  }
}
```

Configuring Interfaces, a Routing Instance, and Static Routes for the Master Logical System

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 interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 600
set interfaces ge-0/0/4 unit 0 family inet address 50.1.1.1/24
```

```
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/6 vlan-tagging
set interfaces ge-0/0/7 vlan-tagging
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet address 10.0.1.1/24
set routing-instances vr1-root instance-type virtual-router
set routing-instances vr1-root interface ge-0/0/4.0
set routing-instances vr1-root interface lt-0/0/0.1
set routing-instances vr1-root routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
set routing-instances vr1-root routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
set routing-instances vr1-root routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
```

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 the master logical system interfaces:

1. Configure the master (root) logical and lt-0/0/0.1 interfaces.

```
[edit interfaces]
user@host# set ge-0/0/4 vlan-tagging
user@host# set ge-0/0/4 unit 0 vlan-id 600
user@host# set ge-0/0/4 unit 0 family inet address 50.1.1.1/24
user@host# set lt-0/0/0 unit 1 encapsulation ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet address 10.0.1.1/24
```

2. Configure the interfaces for other logical systems to support VLAN tagging.

```
[edit interfaces]
user@host# set ge-0/0/5 vlan-tagging
user@host# set ge-0/0/6 vlan-tagging
user@host# set ge-0/0/7 vlan-tagging
```

3. Configure a routing instance for the master logical system, assign its interfaces to it, and configure static routes for it.

```
[edit routing-instances]
user@host# set vr1-root instance-type virtual-router
user@host# set vr1-root interface ge-0/0/4.0
user@host# set vr1-root interface lt-0/0/0.1
user@host# set vr1-root routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
user@host# set vr1-root routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
user@host# set vr1-root routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
```

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

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

```

ge-0/0/4 {
  vlan-tagging;
  unit 0 {
    vlan-id 600;
    family inet {
      address 50.1.1.1/24;
    }
  }
}
ge-0/0/5 {
  vlan-tagging;
}
ge-0/0/6 {
  vlan-tagging;
}
ge-0/0/7 {
  vlan-tagging;
}
lt-0/0/0 {
  unit 1 {
    encapsulation ethernet;
    peer-unit 0;
    family inet {
      address 10.0.1.1/24;
    }
  }
}

[edit]
user@host# show routing-instances
vr1-root {
  instance-type virtual-router;
  interface ge-0/0/4.0;
  interface lt-0/0/0.1;
  routing-options {
    static {
      route 14.1.1.0/24 next-hop 10.0.1.4;
      route 12.1.1.0/24 next-hop 10.0.1.2;
      route 13.1.1.0/24 next-hop 10.0.1.3;
    }
  }
}

```

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

Configuring Logical Tunnel Interfaces for the User Logical Systems

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 logical-systems ls-product-design interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems ls-product-design interfaces lt-0/0/0 unit 3 peer-unit 2

```

```
set logical-systems ls-product-design interfaces lt-0/0/0 unit 3 family inet address
  10.0.1.2/24
set logical-systems ls-marketing-dept interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems ls-marketing-dept interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems ls-marketing-dept interfaces lt-0/0/0 unit 5 family inet address
  10.0.1.3/24
set logical-systems ls-accounting-dept interfaces lt-0/0/0 unit 7 encapsulation ethernet
set logical-systems ls-accounting-dept interfaces lt-0/0/0 unit 7 peer-unit 6
set logical-systems ls-accounting-dept interfaces lt-0/0/0 unit 7 family inet address
  10.0.1.4/24
```

**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*.

1. Configure the lt-0/0/0 interface for the first user logical system:

```
[edit logical-systems]
user@host# set ls-product-design interfaces lt-0/0/0 unit 3 encapsulation ethernet
user@host# set ls-product-design interfaces lt-0/0/0 unit 3 peer-unit 2
user@host# set ls-product-design interfaces lt-0/0/0 unit 3 family inet address
  10.0.1.2/24
```

2. Configure the lt-0/0/0 interface for the second user logical system.

```
[edit logical-systems]
user@host# set ls-marketing-dept interfaces lt-0/0/0 unit 5 encapsulation ethernet
user@host# set ls-marketing-dept interfaces lt-0/0/0 unit 5 peer-unit 4
user@host# set ls-marketing-dept interfaces lt-0/0/0 unit 5 family inet address
  10.0.1.3/24 face
```

3. Configure the lt-0/0/0 interface for the third user logical system.

```
[edit logical-systems]
user@host# set ls-accounting-dept interfaces lt-0/0/0 unit 7 encapsulation ethernet
user@host# set ls-accounting-dept interfaces lt-0/0/0 unit 7 peer-unit 6
user@host# set ls-accounting-dept interfaces lt-0/0/0 unit 7 family inet address
  10.0.1.4/24
```

Results

From configuration mode, confirm your configuration by entering the **show logical-systems ls-product-design interfaces lt-0/0/0**, **show logical-systems ls-marketing-dept interfaces lt-0/0/0**, and **show logical-systems ls-accounting-dept interfaces lt-0/0/0** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show logical-systems ls-product-design interfaces lt-0/0/0
lt-0/0/0 {
  unit 3 {
    encapsulation ethernet;
    peer-unit 2;
    family inet {
      address 10.0.1.2/24;
```



```
    }  
  }  
}  
user@host# show logical-systems ls-marketing-dept interfaces lt-0/0/0  
lt-0/0/0 {  
  unit 5 {  
    encapsulation ethernet;  
    peer-unit 4;  
    family inet {  
      address 10.0.1.3/24;  
    }  
  }  
}  
}  
user@host# show logical-systems ls-accounting-dept interfaces lt-0/0/0  
lt-0/0/0 {  
  unit 7 {  
    encapsulation ethernet;  
    peer-unit 6;  
    family inet {  
      address 10.0.1.4/24;  
    }  
  }  
}  
}
```

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 That the Static Routes Configured for the Master Administrator Are Correct on page 113](#)

Verifying That the Static Routes Configured for the Master Administrator Are Correct

Purpose Verify if you can send data from the master logical system to the other logical systems.

Action From operational mode, use the **ping** command.

- See Also**
- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)
 - [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)

Example: Configuring OSPF Routing Protocol for the Master Logical Systems

This example shows how to configure OSPF for the master logical system.

- [Requirements on page 114](#)
- [Overview on page 114](#)
- [Configuration on page 114](#)
- [Verification on page 116](#)

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See [“Example: Configuring Root Password for Logical Systems” on page 64](#).
- Configure logical interfaces ge-0/0/4.0 and lt-0/0/0.1 for the master logical system and assign them to the vr1-root routing instance. See [“Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\)” on page 105](#).

Overview

In this example, you configure OSPF for the master logical system, called root-logical-system, shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

This example enables OSPF routing on the ge-0/0/4.0 and lt-0/0/0.1 interfaces in the master logical system. You configure the following routing policies to export routes from the Junos OS routing table into OSPF in the vr1-root routing instance:

- ospf-redirect-direct—Routes learned from directly connected interfaces.
- ospf-redirect-static—Static routes.
- ospf-to-ospf—Routes learned from OSPF.

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 policy-options policy-statement ospf-redirect-direct from protocol direct
set policy-options policy-statement ospf-redirect-direct then accept
set policy-options policy-statement ospf-redirect-static from protocol static
set policy-options policy-statement ospf-redirect-static then accept
set policy-options policy-statement ospf-to-ospf from protocol ospf
set policy-options policy-statement ospf-to-ospf then accept
set routing-instances vr1-root protocols ospf export ospf-redirect-direct
```

```

set routing-instances vr1-root protocols ospf export ospf-redist-static
set routing-instances vr1-root protocols ospf export ospf-to-ospf
set routing-instances vr1-root protocols ospf area 0.0.0.1 interface ge-0/0/4.0
set routing-instances vr1-root protocols ospf area 0.0.0.1 interface lt-0/0/0.1

```

Step-by-Step Procedure

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

To configure OSPF for the master logical system:

1. Log in to the master logical system as the master administrator and enter configuration mode.

```

admin@host> configure
admin@host#

```

2. Create routing policies that accept routes.

```

[edit policy-options]
admin@host# set policy-statement ospf-redist-direct from protocol direct
admin@host# set policy-statement ospf-redist-direct then accept
admin@host# set policy-statement ospf-redist-static from protocol static
admin@host# set policy-statement ospf-redist-static then accept
admin@host# set policy-statement ospf-to-ospf from protocol ospf
admin@host# set policy-statement ospf-to-ospf then accept

```

3. Apply the routing policies to routes exported from the Junos OS routing table into OSPF.

```

[edit routing-instances]
admin@host# set vr1-root protocols ospf export ospf-redist-direct
admin@host# set vr1-root protocols ospf export ospf-redist-static
admin@host# set vr1-root protocols ospf export ospf-to-ospf

```

4. Enable OSPF on the logical interfaces.

```

[edit routing-instances]
admin@host# set vr1-root protocols ospf area 0.0.0.1 interface ge-0/0/4.0
admin@host# set vr1-root protocols ospf area 0.0.0.1 interface lt-0/0/0.1

```

Results From configuration mode, confirm your configuration by entering the **show policy-options** and **show routing-instances** 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]
admin@host# show policy-options
policy-statement ospf-redist-direct {

```

```

        from protocol direct;
        then accept;
    }
    policy-statement ospf-redist-static {
        from protocol static;
        then accept;
    }
    policy-statement ospf-to-ospf {
        from protocol ospf;
        then accept;
    }
    [edit]
admin@host# show routing-instances
vr1-root {
    ...
    protocols {
        ospf {
            export [ ospf-redist-direct ospf-to-ospf ospf-redist-static ];
            area 0.0.0.1 {
                interface lt-0/0/0.1;
                interface ge-0/0/4.0;
            }
        }
    }
}

```

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

Verification

Confirm that the configuration is working properly.

- [Verifying OSPF Interfaces on page 116](#)
- [Verifying OSPF Neighbors on page 116](#)
- [Verifying OSPF Routes on page 117](#)

Verifying OSPF Interfaces

Purpose Verify OSPF-enabled interfaces.

Action From the CLI, enter the **show ospf interface instance vr1-root** command.

```

admin@host> show ospf interface instance vr1-root

```

Interface	State	Area	DR ID	BDR ID	Nbrs
lt-0/0/0.1	DR	0.0.0.0	10.0.1.1	0.0.0.0	0
ge-0/0/4.0	DR	0.0.0.1	10.0.1.1	0.0.0.0	0

Verifying OSPF Neighbors

Purpose Verify OSPF neighbors.

Action From the CLI, enter the **show ospf neighbor instance vr1-root** command.

```
admin@host> show ospf neighbor instance vr1-root
Address  Interface  State  ID      Pri  Dead
10.0.1.2  plt0.3    Full   0.0.0.0  128   39
```

Verifying OSPF Routes

Purpose Verify OSPF routes.

Action From the CLI, enter the **show ospf route instance vr1-root** command.

```
admin@host> show ospf route instance vr1-root
Topology default Route Table:

Prefix          Path  Route  NH      Metric NextHop      Nexthop
                Type  Type   Type                    Interface  Address/LSP
10.0.1.0/24      Intra Network IP          1 1t-0/0/0.1
12.12.1.0/24     Intra Network IP          1 ge-0/0/4.0
```

- See Also**
- [Understanding Logical Systems Interfaces and Routing Instances on page 104](#)
 - [Example: Configuring OSPF Routing Protocol for a User Logical Systems on page 124](#)
 - *OSPF Feature Guide*

Routing, Interfaces, and NAT for User Logical Systems

The user logical system enables you to configure routing protocols, interfaces and NAT. Routing protocols handles all routing messages. NAT is a mechanism to translate the IP address of a computer or group of computers into a single public address when the packets are sent out to the internet. For more information, see the following topics:

- [Understanding Logical Systems Network Address Translation on page 117](#)
- [Example: Configuring Network Address Translation for a User Logical Systems on page 118](#)
- [Example: Configuring Interfaces and Routing Instances for a User Logical Systems on page 121](#)
- [Example: Configuring OSPF Routing Protocol for a User Logical Systems on page 124](#)

Understanding Logical Systems Network Address Translation

Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either or both source and destination addresses in a packet may be translated. NAT can include the translation of port numbers as well as IP addresses.

Any combination of static, destination, or source NAT can be configured in the root or user logical systems. Configuring NAT in a logical system is the same as configuring NAT

in a root system. The master administrator can configure and monitor NAT in the master logical system as well as any user logical system.

Starting in Junos OS Release 18.2R1, the NAT functionality is supported for logical systems on SRX4100, and SRX4200 devices in addition to existing support on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

For each user logical system, the master administrator can configure the maximum and reserved numbers for the following NAT resources:

- Source NAT pools and destination NAT pools
- IP addresses in source NAT pools with and without port address translation
- Rules for source, destination, and static NAT
- Persistent NAT bindings
- IP addresses that support port overloading

From a user logical system, the user logical system administrator can use the operational command **show system security-profile** with a NAT option to view the number of NAT resources allocated to the user logical system.



NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of NAT resources applied to the master logical system. The number of resources configured in the master logical system count toward the maximum number of NAT resources available on the device.

From a user logical system, the user logical system administrator can use the **show security nat** command to view the information about NAT for the user logical system. From the master logical system, the master administrator can use the same command to view information for the master logical system, a specific user logical system, or all logical systems.

- See Also**
- [Example: Configuring Network Address Translation for a User Logical Systems on page 118](#)
 - [User Logical Systems Configuration Overview on page 61](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Introduction to NAT](#)

Example: Configuring Network Address Translation for a User Logical Systems

This example shows how to configure static NAT for a user logical system.

- [Requirements on page 119](#)
- [Overview on page 119](#)

- [Configuration on page 119](#)
- [Verification on page 121](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Use the **show system security-profile nat-static-rule** command to see the static NAT resources allocated to the logical system.
- Configure security policies. See [“Example: Configuring Security Policies in a User Logical Systems” on page 168](#).

Overview

This example configures the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

Devices in the ls-product-design-untrust zone access a specific host in the ls-product-design-trust zone by way of the address 12.1.1.200/32. For packets that enter the ls-product-design logical system from the ls-product-design-untrust zone with the destination IP address 12.1.1.200/32, the destination IP address is translated to the 12.1.1.100/32. This example configures the static NAT described in [Table 10 on page 119](#).

Table 10: User Logical System Static NAT Configuration

Feature	Name	Configuration Parameters
Static NAT rule set	rs1	<ul style="list-style-type: none"> • Rule r1 to match packets from the ls-product-design-untrust zone with destination address 12.1.1.200/32. • Destination IP address in matching packets is translated to 12.1.1.100/32.
Proxy ARP		Address 12.1.1.200 on interface lt-0/0/0.3.

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 nat static rule-set rs1 from zone ls-product-design-untrust
set security nat static rule-set rs1 rule r1 match destination-address 12.1.1.200/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 12.1.1.100/32
set security nat proxy-arp interface lt-0/0/0.3 address 12.1.1.200/32
```

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

To configure NAT in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a static NAT rule set.

```
[edit security nat static]
lsdesignadmin1@host:ls-product-design# set rule-set rs1 from zone
ls-product-design-untrust
```

3. Configure a rule that matches packets and translates the destination address in the packets.

```
[edit security nat static]
lsdesignadmin1@host:ls-product-design# set rule-set rs1 rule r1 match
destination-address 12.1.1.200/32
lsdesignadmin1@host:ls-product-design# set rule-set rs1 rule r1 then static-nat prefix
12.1.1.100/32
```

4. Configure proxy ARP.

```
[edit security nat]
lsdesignadmin1@host:ls-product-design# set proxy-arp interface lt-0/0/0.3 address
12.1.1.200/32
```

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

```
lsdesignadmin1@host:ls-product-design# show security nat
static {
  rule-set rs1 {
    from zone ls-product-design-untrust;
    rule r1 {
      match {
        destination-address 12.1.1.200/32;
      }
      then {
        static-nat prefix 12.1.1.100/32;
      }
    }
  }
}
proxy-arp {
  interface lt-0/0/0.3 {
```



```
        address {  
            12.1.1.200/32;  
        }  
    }  
}
```

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 Static NAT Configuration on page 121](#)
- [Verifying NAT Application to Traffic on page 121](#)

Verifying Static NAT Configuration

Purpose Verify that there is traffic matching the static NAT rule set.

Action From operational mode, enter the **show security nat static rule** command. View the Translation hits field to check for traffic that matches the rule.

Verifying NAT Application to Traffic

Purpose Verify that NAT is being applied to the specified traffic.

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

See Also

- [User Logical Systems Configuration Overview on page 61](#)
- [Understanding Logical Systems Network Address Translation on page 117](#)
- *Static NAT Configuration Overview*

Example: Configuring Interfaces and Routing Instances for a User Logical Systems

This example shows how to configure interfaces and routing instances for a tenant system.

- [Requirements on page 121](#)
- [Overview on page 122](#)
- [Configuration on page 122](#)

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).

- Determine which logical interfaces and, optionally, which logical tunnel interfaces are allocated to your user logical system by the master administrator. The master administrator configures the logical tunnel interfaces. See [“Understanding the Master Logical Systems and the Master Administrator Role”](#) on page 40.

Overview

This example configures the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65.

This example configures the interfaces and routing instances described in [Table 11](#) on page 122.

Table 11: User Logical System Interface and Routing Instance Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/5.1	<ul style="list-style-type: none"> • IP address 12.1.1.1/24 • VLAN ID 700
Routing instance	pd-vr1	<ul style="list-style-type: none"> • Instance type: virtual router • Includes interfaces ge-0/0/5.1 and lt-0/0/0.3 • Static routes: <ul style="list-style-type: none"> • 13.1.1.0/24 next-hop 10.0.1.3 • 14.1.1.0/24 next-hop 10.0.1.4 • 12.12.1.0/24 next-hop 10.0.1.1

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 interfaces ge-0/0/5 unit 1 family inet address 12.1.1.1/24
set interfaces ge-0/0/5 unit 1 vlan-id 700
set routing-instances pd-vr1 instance-type virtual-router
set routing-instances pd-vr1 interface ge-0/0/5.1
set routing-instances pd-vr1 interface lt-0/0/0.3
set routing-instances pd-vr1 routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
set routing-instances pd-vr1 routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
set routing-instances pd-vr1 routing-options static route 12.12.1.0/24 next-hop 10.0.1.1
```

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

To configure an interface and a routing instance in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure the logical interface for a user logical system.

```
[edit interfaces]
lsdesignadmin1@host:ls-product-design# set ge-0/0/5 unit 1 family inet address
12.1.1.1/24
lsdesignadmin1@host:ls-product-design# set ge-0/0/5 unit 1 vlan-id 700
```

3. Configure the routing instance and assign interfaces.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 instance-type virtual-router
lsdesignadmin1@host:ls-product-design# set pd-vr1 interface ge-0/0/5.1
lsdesignadmin1@host:ls-product-design# set pd-vr1 interface lt-0/0/0.3
```

4. Configure static routes.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 routing-options static route
13.1.1.0/24 next-hop 10.0.1.3
lsdesignadmin1@host:ls-product-design# set pd-vr1 routing-options static route
14.1.1.0/24 next-hop 10.0.1.4
lsdesignadmin1@host:ls-product-design# set pd-vr1 routing-options static route
12.12.1.0/24 next-hop 10.0.1.1
```

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



NOTE: The master administrator configures the lt-0/0/0.3 interface. Thus, the lt-0/0/0.3 configuration appears in the **show interfaces** output even though you did not configure this item.

```
lsdesignadmin1@host:ls-product-design# show interfaces
ge-0/0/5 {
  unit 1 {
    vlan-id 700;
    family inet {
      address 12.1.1.1/24;
    }
  }
}
```

```
    }  
  }  
}  
lt-0/0/0 {  
  unit 3 {  
    encapsulation ethernet;  
    peer-unit 2;  
    family inet {  
      address 10.0.1.2/24;  
    }  
  }  
}  
lsdesignadmin1@host:ls-product-design# show routing-instances  
pd-vr1 {  
  instance-type virtual-router;  
  interface ge-0/0/5.1;  
  interface lt-0/0/0.3;  
  routing-options {  
    static {  
      route 13.1.1.0/24 next-hop 10.0.1.3;  
      route 14.1.1.0/24 next-hop 10.0.1.4;  
      route 12.12.1.0/24 next-hop 10.0.1.1;  
    }  
  }  
}
```

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

- See Also**
- [User Logical Systems Configuration Overview on page 61](#)
 - [Understanding Logical Systems Interfaces and Routing Instances on page 104](#)

Example: Configuring OSPF Routing Protocol for a User Logical Systems

This example shows how to configure OSPF for a user logical system.

- [Requirements on page 124](#)
- [Overview on page 125](#)
- [Configuration on page 125](#)
- [Verification on page 127](#)

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Configure logical interface ge-0/0/5.1. Assign ge-0/0/5.1 and lt-0/0/0.3 to the pd-vr1 routing instance. See [“Example: Configuring Interfaces and Routing Instances for a User Logical Systems” on page 121](#).

Overview

In this example, you configure OSPF for the ls-product-design user logical system, shown in “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on page 65.

This example enables OSPF routing on the ge-0/0/5.1 and lt-0/0/0.3 interfaces in the ls-product-design user logical system. You configure the following routing policies to export routes from the Junos OS routing table into OSPF in the pd-vr1 routing instance:

- ospf-redirect-direct—Routes learned from directly connected interfaces.
- ospf-redirect-static—Static routes.
- ospf-to-ospf—Routes learned from OSPF.

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 policy-options policy-statement ospf-redirect-direct from protocol direct
set policy-options policy-statement ospf-redirect-direct then accept
set policy-options policy-statement ospf-redirect-static from protocol static
set policy-options policy-statement ospf-redirect-static then accept
set policy-options policy-statement ospf-to-ospf from protocol ospf
set policy-options policy-statement ospf-to-ospf then accept
set routing-instances pd-vr1 protocols ospf export ospf-redirect-direct
set routing-instances pd-vr1 protocols ospf export ospf-redirect-static
set routing-instances pd-vr1 protocols ospf export ospf-to-ospf
set routing-instances pd-vr1 protocols ospf area 0.0.0.1 interface ge-0/0/5.1
set routing-instances pd-vr1 protocols ospf area 0.0.0.1 interface lt-0/0/0.3
```

Step-by-Step Procedure

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

To configure OSPF for the user logical system:

1. Log in to the user logical system as the user logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Create routing policies that accept routes.

```
[edit policy-options]
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redirect-direct
from protocol direct
```

```
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-direct
then accept
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-static
from protocol static
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-static
then accept
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-to-ospf from
protocol ospf
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-to-ospf then
accept
```

3. Apply the routing policies to routes exported from the Junos OS routing table into OSPF.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf export
ospf-redist-direct
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf export
ospf-redist-static
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf export
ospf-to-ospf
```

4. Enable OSPF on the logical interfaces.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf area 0.0.0.1
interface ge-0/0/5.1
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf area 0.0.0.1
interface lt-0/0/0.3
```

Results From configuration mode, confirm your configuration by entering the **show policy-options** and **show routing-instances** 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]
lsdesignadmin1@host:ls-product-design# show policy-options
policy-statement ospf-redist-direct {
    from protocol direct;
    then accept;
}
policy-statement ospf-redist-static {
    from protocol static;
    then accept;
}
policy-statement ospf-to-ospf {
    from protocol ospf;
    then accept;
}
[edit]
```

```

lsdesignadmin1@host:ls-product-design# show routing-instances
pd-vr1 {
  ...
  protocols {
    ospf {
      export [ ospf-redist-direct ospf-to-ospf ospf-redist-static ];
      area 0.0.0.1 {
        interface lt-0/0/0.3;
        interface ge-0/0/5.1;
      }
    }
  }
}

```

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

Verification

Confirm that the configuration is working properly.

- [Verifying OSPF Interfaces on page 127](#)
- [Verifying OSPF Neighbors on page 127](#)
- [Verifying OSPF Routes on page 127](#)

Verifying OSPF Interfaces

Purpose Verify OSPF-enabled interfaces.

Action From the CLI, enter the **show ospf interface instance pd-vr1** command.

```

lsdesignadmin1@host:ls-product-design> show ospf interface instance pd-vr1

```

Interface	State	Area	DR ID	BDR ID	Nbrs
lt-0/0/0.3	DR	0.0.0.0	10.0.1.2	0.0.0.0	0
ge-0/0/5.1	DR	0.0.0.1	10.0.1.2	0.0.0.0	0

Verifying OSPF Neighbors

Purpose Verify OSPF neighbors.

Action From the CLI, enter the **show ospf neighbor instance pd-vr1** command.

```

lsdesignadmin1@host:ls-product-design> show ospf neighbor instance pd-vr1

```

Address	Interface	State	ID	Pri	Dead
10.0.1.1	pl0.1	Full	0.0.0.0	128	39

Verifying OSPF Routes

Purpose Verify OSPF routes.

Action From the CLI, enter the **show ospf route instance pd-vr1** command.

```
lsdesignadmin1@host:ls-product-design> show ospf route instance pd-vr1
Topology default Route Table:
```

Prefix	Path Type	Route Type	NH Type	Metric	NextHop Interface	Nexthop Address/LSP
10.0.1.0/24	Intra	Network	IP	1	1t-0/0/0.3	
12.12.1.0/24	Intra	Network	IP	1	ge-0/0/5.1	

- See Also**
- [Understanding Logical Systems Interfaces and Routing Instances on page 104](#)
 - [Example: Configuring OSPF Routing Protocol for the Master Logical Systems on page 114](#)
 - *OSPF Feature Guide*

- Related Documentation**
- [User Logical Systems Overview on page 60](#)

Security Zones in Logical Systems

Security zones are the building blocks for policies. Security zones are logical entities to which one or more interfaces are bound and provides a means of distinguishing groups of hosts (user logical systems and other hosts, such as servers), resources from one another in order to apply different security measures. For more information, see the following topics:

- [Understanding Logical Systems Zones on page 128](#)
- [Example: Configuring User Logical Systems on page 130](#)
- [Example: Configuring Security Zones for a User Logical Systems on page 141](#)

Understanding Logical Systems Zones

Security zones are logical entities to which one or more interfaces are bound. Security zones can be configured on the master logical system by the master administrator or on user logical systems by the user logical system administrator. On a logical system, the administrator can configure multiple security zones, dividing the network into network segments to which various security options can be applied.

The master administrator configures the maximum and reserved numbers of security zones for each user logical system. The user logical system administrator can then create security zones in the user logical system and assign interfaces to each security zone. From a user logical system, the user logical system administrator can use the **show system security-profile zones** command to view the number of security zones allocated to the user logical system and the **show interfaces** command to view the interfaces allocated to the user logical system.



NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of security zones applied to the master logical system. The number of zones configured in the master logical system count toward the maximum number of zones available on the device.

The master and user administrator can configure the following properties of a security zone in a logical system:

- Interfaces that are part of a security zone.
- Screen options—For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful.
- TCP-Reset—When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the synchronize flag set.
- Host inbound traffic—This feature specifies the kinds of traffic that can reach the device from systems that are directly connected to its interfaces. You can configure these parameters at the zone level, in which case they affect all interfaces of the zone, or at the interface level. (Interface configuration overrides that of the zone.)

There are no preconfigured security zones in the master logical system or user logical system.

The management functional zone (MGT) can only be configured for the master logical system. There is only one management interface per device and that interface is allocated to the master logical system.

The **all** interface can only be assigned to a zone in the master logical system by the master administrator.

The user logical system administrator can configure and view all attributes for a security zone in a user logical system. All attributes of a security zone in a user logical system are also visible to the master administrator.

- See Also**
- [Example: Configuring Security Zones for a User Logical Systems on page 141](#)
 - [User Logical Systems Configuration Overview on page 61](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Understanding Logical Systems Interfaces and Routing Instances on page 104](#)
 - [Security Zones Overview](#)

Example: Configuring User Logical Systems

This example shows the configuration of interfaces, routing instances, zones, and security policies for user logical systems.

- [Requirements on page 130](#)
- [Overview on page 130](#)
- [Configuration on page 132](#)
- [Verification on page 140](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Be sure you know which logical interfaces and optionally, which logical tunnel interface (and its IP address) are allocated to your user logical system by the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).

Overview

This example configures the ls-marketing-dept and ls-accounting-dept user logical systems shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

This example configures the parameters described in [Table 12 on page 130](#) and [Table 13 on page 131](#).

Table 12: ls-marketing-dept Logical System Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/6.1	<ul style="list-style-type: none"> • IP address 13.1.1.1/24 • VLAN ID 800
Routing instance	mk-vr1	<ul style="list-style-type: none"> • Instance type: virtual router • Includes interfaces ge-0/0/6.1 and lt-0/0/0.5 • Static routes: <ul style="list-style-type: none"> • 12.1.1.0/24 next-hop 10.0.1.2 • 14.1.1.0/24 next-hop 10.0.1.4 • 12.12.1.0/24 next-hop 10.0.1.1
Zones	ls-marketing-trust	Bind to interface ge-0/0/6.1.
	ls-marketing-untrust	Bind to interface lt-0/0/0.5
Address books	marketing-internal	<ul style="list-style-type: none"> • Address marketers: 13.1.1.0/24 • Attach to zone ls-marketing-trust

Table 12: *ls-marketing-dept* Logical System Configuration (continued)

Feature	Name	Configuration Parameters
	marketing-external	<ul style="list-style-type: none"> Address design: 12.1.1.0/24 Address accounting: 14.1.1.0/24 Address others: 12.12.1.0/24 Address set otherlsys: design, accounting Attach to zone ls-marketing-untrust
Policies	permit-all-to-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> From zone: ls-marketing-trust To zone: ls-marketing-untrust Source address: marketers Destination address: otherlsys Application: any
	permit-all-from-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> From zone: ls-marketing-untrust To zone: ls-marketing-trust Source address: otherlsys Destination address: marketers Application: any

Table 13: *ls-accounting-dept* Logical System Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/7.1	<ul style="list-style-type: none"> IP address 14.1.1.1/24 VLAN ID 900
Routing instance	acct-vr1	<ul style="list-style-type: none"> Instance type: virtual router Includes interfaces ge-0/0/7.1 and lt-0/0/0.7 Static routes: <ul style="list-style-type: none"> 12.1.1.0/24 next-hop 10.0.1.2 13.1.1.0/24 next-hop 10.0.1.3 12.12.1.0/24 next-hop 10.0.1.1
Zones	ls-accounting-trust	Bind to interface ge-0/0/7.1.
	ls-accounting-untrust	Bind to interface lt-0/0/0.7
Address books	accounting-internal	<ul style="list-style-type: none"> Address accounting: 14.1.1.0/24 Attach to zone ls-accounting-trust

Table 13: *ls-accounting-dept* Logical System Configuration (continued)

Feature	Name	Configuration Parameters
	accounting-external	<ul style="list-style-type: none"> Address design: 12.1.1.0/24 Address marketing: 13.1.1.0/24 Address others: 12.12.1.0/24 Address set otherlsys: design, marketing Attach to zone ls-accounting-untrust
Policies	permit-all-to-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> From zone: ls-accounting-trust To zone: ls-accounting-untrust Source address: accounting Destination address: otherlsys Application: any
	permit-all-from-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> From zone: ls-accounting-untrust To zone: ls-accounting-trust Source address: otherlsys Destination address: accounting Application: any

Configuration

- [Configuring the ls-marketing-dept User Logical System on page 132](#)
- [Configuring the ls-accounting-dept User Logical System on page 136](#)

Configuring the ls-marketing-dept User Logical System

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 interfaces ge-0/0/6 unit 1 family inet address 13.1.1.1/24
set interfaces ge-0/0/6 unit 1 vlan-id 800
set routing-instances mk-vr1 instance-type virtual-router
set routing-instances mk-vr1 interface ge-0/0/6.1
set routing-instances mk-vr1 interface lt-0/0/0.5
set routing-instances mk-vr1 routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
set routing-instances mk-vr1 routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
set routing-instances mk-vr1 routing-options static route 12.12.1.0/24 next-hop 10.0.1.1
set security zones security-zone ls-marketing-trust interfaces ge-0/0/6.1
set security zones security-zone ls-marketing-untrust interfaces lt-0/0/0.5
set security address-book marketing-external address design 12.1.1.0/24
set security address-book marketing-external address accounting 14.1.1.0/24
set security address-book marketing-external address others 12.12.1.0/24
set security address-book marketing-external address-set otherlsys address design
set security address-book marketing-external address-set otherlsys address accounting

```

```

set security address-book marketing-external attach zone ls-marketing-untrust
set security address-book marketing-internal address marketers 13.1.1.0/24
set security address-book marketing-internal attach zone ls-marketing-trust
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys match source-address marketers
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys match destination-address otherlsys
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys match application any
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys then permit
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys match source-address otherlsys
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys match destination-address marketers
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys match application any
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys 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 the Junos OS CLI User Guide.

To configure a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```

lsmarketingadmin1@host:ls-marketing-dept> configure
lsmarketingadmin1@host:ls-marketing-dept#

```

2. Configure the logical interface for a user logical system.

```

[edit interfaces]
lsmarketingadmin1@host:ls-marketing-dept# set ge-0/0/6 unit 1 family inet address
  13.1.1.1/24
lsmarketingadmin1@host:ls-marketing-dept# set ge-0/0/6 unit 1 vlan-id 800

```

3. Configure the routing instance and assign interfaces.

```

[edit routing-instances]
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 instance-type virtual-router
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 interface ge-0/0/6.1
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 interface lt-0/0/0.5

```

4. Configure static routes.

```

[edit routing-instances]
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 routing-options static route
  12.12.1.0/24 next-hop 10.0.1.2
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 routing-options static route
  14.1.1.0/24 next-hop 10.0.1.4

```

```
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 routing-options static route
12.12.1.0/24 next-hop 10.0.1.1
```

5. Configure security zones and assign interfaces to each zone.

```
[edit security zones]
lsmarketingadmin1@host:ls-marketing-dept# set security-zone ls-marketing-trust
interfaces ge-0/0/6.1
lsmarketingadmin1@host:ls-marketing-dept# set security-zone ls-marketing-untrust
interfaces lt-0/0/0.5
```

6. Create address book entries.

```
[edit security]
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-internal
address marketers 13.1.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
address design 12.1.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
address accounting 14.1.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
address others 12.12.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
address-set otherlsys address design
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
address-set otherlsys address accounting
```

7. Attach address books to zones.

```
[edit security]
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-internal
attach zone ls-marketing-trust
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
attach zone ls-marketing-untrust
```

8. Configure a security policy that permits traffic from the ls-marketing-trust zone to the ls-marketing-untrust zone.

```
[edit security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust]
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys
match source-address marketers
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys
match destination-address otherlsys
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys
match application any
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys then
permit
```

9. Configure a security policy that permits traffic from the ls-marketing-untrust zone to the ls-marketing-trust zone.

```
[edit security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust]
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
match source-address otherlsys
```

```

lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
match destination-address marketers
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
match application any
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
then permit

```

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

```

lsmarketingadmin1@host:ls-marketing-dept# show routing instances
mk-vr1 {
  instance-type virtual-router;
  interface ge-0/0/6.1;
  interface lt-0/0/0.5;
  routing-options {
    static {
      route 12.1.1.0/24 next-hop 10.0.1.2;
      route 14.1.1.0/24 next-hop 10.0.1.4;
      route 12.12.1.0/24 next-hop 10.0.1.1;
    }
  }
}
lsmarketingadmin1@host:ls-marketing-dept# show security
address-book {
  marketing-external {
    address product-designers 12.1.1.0/24;
    address accounting 14.1.1.0/24;
    address others 12.12.1.0/24;
    address-set otherlsys {
      address product-designers;
      address accounting;
    }
    attach {
      zone ls-marketing-untrust;
    }
  }
  marketing-internal {
    address marketers 13.1.1.0/24;
    attach {
      zone ls-marketing-trust;
    }
  }
}
policies {
  from-zone ls-marketing-trust to-zone ls-marketing-untrust {
    policy permit-all-to-otherlsys {
      match {
        source-address marketers;
        destination-address otherlsys;
        application any;
      }
      then {

```

```

        permit;
    }
}
}
from-zone ls-marketing-untrust to-zone ls-marketing-trust {
    policy permit-all-from-otherlsys {
        match {
            source-address otherlsys;
            destination-address marketers;
            application any;
        }
        then {
            permit;
        }
    }
}
}
zones {
    security-zone ls-marketing-trust {
        interfaces {
            ge-0/0/6.1;
        }
    }
    security-zone ls-marketing-untrust {
        interfaces {
            lt-0/0/0.5;
        }
    }
}
}

```

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

Configuring the ls-accounting-dept User Logical System

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 interfaces ge-0/0/7 unit 1 family inet address 14.1.1.1/24
set interfaces ge-0/0/7 unit 1 vlan-id 900
set routing-instances acct-vr1 instance-type virtual-router
set routing-instances acct-vr1 interface ge-0/0/7.1
set routing-instances acct-vr1 interface lt-0/0/0.7
set routing-instances acct-vr1 routing-options static route 12.12.1.0/24 next-hop 10.0.1.1
set routing-instances acct-vr1 routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
set routing-instances acct-vr1 routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
set security address-book accounting-internal address accounting 14.1.1.0/24
set security address-book accounting-internal attach zone ls-accounting-trust
set security address-book accounting-external address design 12.1.1.0/24
set security address-book accounting-external address marketing 13.1.1.0/24
set security address-book accounting-external address others 12.12.1.0/24
set security address-book accounting-external address-set otherlsys address design
set security address-book accounting-external address-set otherlsys address marketing
set security address-book accounting-external attach zone ls-accounting-untrust

```



```

set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
  permit-all-to-otherlsys match source-address accounting
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
  permit-all-to-otherlsys match destination-address otherlsys
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
  permit-all-to-otherlsys match application any
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
  permit-all-to-otherlsys then permit
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
  permit-all-from-otherlsys match source-address otherlsys
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
  permit-all-from-otherlsys match destination-address accounting
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
  permit-all-from-otherlsys match application any
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
  permit-all-from-otherlsys then permit
set security zones security-zone ls-accounting-trust interfaces ge-0/0/7.1
set security zones security-zone ls-accounting-untrust interfaces lt-0/0/0.7

```

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 user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```

lsaccountingadmin1@host:ls-accounting-dept> configure
lsaccountingadmin1@host:ls-accounting-dept#

```

2. Configure the logical interface for a user logical system.

```

[edit interfaces]
lsaccountingadmin1@host:ls-accounting-dept# set ge-0/0/7 unit 1 family inet
  address 14.1.1.1/24
lsaccountingadmin1@host:ls-accounting-dept# set ge-0/0/7 unit 1 vlan-id 900

```

3. Configure the routing instance and assign interfaces.

```

[edit routing-instances]
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 instance-type
  virtual-router
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 interface ge-0/0/7.1
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 interface lt-0/0/0.7

```

4. Configure static routes.

```

[edit routing-instances]
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 routing-options static
  route 12.1.1.0/24 next-hop 10.0.1.2
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 routing-options static
  route 13.1.1.0/24 next-hop 10.0.1.3

```

```
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 routing-options static
route 12.12.1.0/24 next-hop 10.0.1.1
```

5. Configure security zones and assign interfaces to each zone.

```
[edit security zones]
lsaccountingadmin1@host:ls-accounting-dept# set security-zone ls-accounting-trust
interfaces ge-0/0/7.1
lsaccountingadmin1@host:ls-accounting-dept# set security-zone
ls-accounting-untrust interfaces lt-0/0/0.7
```

6. Create address book entries.

```
[edit security]
lsaccountingadmin1@host:ls-accounting-dept# set address-book accounting-internal
address accounting 14.1.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
accounting-external address design 12.1.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
accounting-external address marketing 13.1.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
accounting-external address others 12.12.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
accounting-external address-set otherlsys address design
lsaccountingadmin1@host:ls-accounting-dept# set address-book
accounting-external address-set otherlsys address marketing
```

7. Attach address books to zones.

```
[edit security]
lsaccountingadmin1@host:ls-accounting-dept# set address-book accounting-internal
attach zone ls-accounting-trust
lsaccountingadmin1@host:ls-accounting-dept# set address-book
accounting-external attach zone ls-accounting-untrust
```

8. Configure a security policy that permits traffic from the ls-accounting-trust zone to the ls-accounting-untrust zone.

```
[edit security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust]
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
match source-address accounting
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
match destination-address otherlsys
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
match application any
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
then permit
```

9. Configure a security policy that permits traffic from the ls-accounting-untrust zone to the ls-accounting-trust zone.

```
[edit security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust]
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
match source-address otherlsys
```

```

lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
match destination-address accounting
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
match application any
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
then permit

```

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

```

lsaccountingadmin1@host:ls-accounting-dept# show routing-instances
acct-vr1 {
  instance-type virtual-router;
  interface ge-0/0/7.1;
  interface lt-0/0/0.7;
  routing-options {
    static {
      route 12.12.1.0/24 next-hop 10.0.1.1;
      route 12.1.1.0/24 next-hop 10.0.1.2;
      route 13.1.1.0/24 next-hop 10.0.1.3;
    }
  }
}
lsaccountingadmin1@host:ls-accounting-dept# show security
address-book {
  accounting-internal {
    address accounting 14.1.1.0/24;
    attach {
      zone ls-accounting-trust;
    }
  }
  accounting-external {
    address design 12.1.1.0/24;
    address marketing 13.1.1.0/24;
    address others 12.12.1.0/24;
    address-set otherlsys {
      address design;
      address marketing;
    }
    attach {
      zone ls-accounting-untrust;
    }
  }
}
policies {
  from-zone ls-accounting-trust to-zone ls-accounting-untrust {
    policy permit-all-to-otherlsys {
      match {
        source-address accounting;
        destination-address otherlsys;
        application any;
      }
      then {

```

```
        permit;
    }
}
}
from-zone ls-accounting-untrust to-zone ls-accounting-trust {
    policy permit-all-from-otherlsys {
        match {
            source-address otherlsys;
            destination-address accounting;
            application any;
        }
        then {
            permit;
        }
    }
}
}
}
zones {
    security-zone ls-accounting-trust {
        interfaces {
            ge-0/0/7.1;
        }
    }
    security-zone ls-accounting-untrust {
        interfaces {
            lt-0/0/0.7;
        }
    }
}
}
```

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 Policy Configuration on page 140](#)

Verifying Policy Configuration

Purpose Verify information about policies and rules.

Action From operational mode, enter the **show security policies detail** command to display a summary of all policies configured on the logical system.

- See Also**
- [User Logical Systems Configuration Overview on page 61](#)
 - [Understanding Logical Systems Interfaces and Routing Instances on page 104](#)
 - [Understanding Logical Systems Zones on page 128](#)
 - [Understanding Logical Systems Security Policies on page 167](#)

Example: Configuring Security Zones for a User Logical Systems

This example shows how to configure zones for a user logical system.

- [Requirements on page 141](#)
- [Overview on page 141](#)
- [Configuration on page 141](#)

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Use the **show system security-profile zones** command to see the zone resources allocated to the logical system.
- Logical interfaces for the user logical system must be configured. See [“Example: Configuring Interfaces and Routing Instances for a User Logical Systems” on page 121](#).

Overview

This example configures the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

This example creates the zones and address books described in [Table 14 on page 141](#).

Table 14: User Logical System Zone and Address Book Configuration

Feature	Name	Configuration Parameters
Zones	ls-product-design-trust	<ul style="list-style-type: none"> • Bind to interface ge-0/0/5.1. • TCP reset enabled.
	ls-product-design-untrust	<ul style="list-style-type: none"> • Bind to interface lt-0/0/0.3.
Address books	product-design-internal	<ul style="list-style-type: none"> • Address product-designers: 12.1.1.0/24 • Attach to zone ls-product-design-trust
	product-design-external	<ul style="list-style-type: none"> • Address marketing: 13.1.1.0/24 • Address accounting: 14.1.1.0/24 • Address others: 12.12.1.0/24 • Address set otherlsys: marketing, accounting • Attach to zone ls-product-design-untrust

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 address-book product-design-internal address product-designers 12.1.1.0/24
set security address-book product-design-internal attach zone ls-product-design-trust
set security address-book product-design-external address marketing 13.1.1.0/24
set security address-book product-design-external address accounting 14.1.1.0/24
set security address-book product-design-external address others 12.12.1.0/24
set security address-book product-design-external address-set otherlsys address
marketing
set security address-book product-design-external address-set otherlsys address
accounting
set security address-book product-design-external attach zone ls-product-design-untrust
set security zones security-zone ls-product-design-trust tcp-rst
set security zones security-zone ls-product-design-trust interfaces ge-0/0/5.1
set security zones security-zone ls-product-design-untrust interfaces lt-0/0/0.3
```

Step-by-Step Procedure

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

To configure zones in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security zone and assign it to an interface.

```
[edit security zones]
lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-trust
interfaces ge-0/0/5.1
```

3. Configure the TCP-Reset parameter for the zone.

```
[edit security zones security-zone ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set tcp-rst
```

4. Configure a security zone and assign it to an interface.

```
[edit security zones]
lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-untrust
interfaces lt-0/0/0.3
```

5. Create global address book entries.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
address product-designers 12.1.1.0/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address marketing 13.1.1.0/24
```

```

lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address accounting 14.1.1.0/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address others 12.12.1.0/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address-set otherlsys address marketing
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address-set otherlsys address accounting

```

6. Attach address books to zones.

```

[edit security]
lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
attach zone ls-product-design-trust
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
attach zone ls-product-design-untrust

```

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

```

lsdesignadmin1@host:ls-product-design# show security
address-book {
  product-design-internal {
    address product-designers 12.1.1.0/24;
    attach {
      zone ls-product-design-trust;
    }
  }
  product-design-external {
    address marketing 13.1.1.0/24;
    address accounting 14.1.1.0/24;
    address others 12.12.1.0/24;
    address-set otherlsys {
      address marketing;
      address accounting;
    }
    attach {
      zone ls-product-design-untrust;
    }
  }
}
zones {
  security-zone ls-product-design-trust {
    tcp-rst;
    interfaces {
      ge-0/0/5.1;
    }
  }
  security-zone ls-product-design-untrust {
    interfaces {
      lt-0/0/0.3;
    }
  }
}

```

```
}
```

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

- See Also**
- [Understanding Logical Systems Zones on page 128](#)
 - [User Logical Systems Configuration Overview on page 61](#)

- Related Documentation**
- [Example: Configuring Security Policies in a User Logical Systems on page 168](#)

User Authentication for Logical Systems

User authentication for logical systems enables to define firewall users and create policies that require the users to authenticate themselves through one of two authentication schemes: pass-through authentication or web authentication. For more information, see the following topics:

- [Example: Configuring Access Profiles \(Master Administrators Only\) on page 144](#)
- [Example: Configuring Security Features for the Master Logical Systems on page 146](#)
- [Understanding Logical System Firewall Authentication on page 152](#)
- [Example: Configuring Firewall Authentication for a User Logical System on page 154](#)
- [Understanding Integrated User Firewall support in a Logical System on page 158](#)
- [Example: Configuring Integrated User Firewall Identification Management for a User Logical System on page 158](#)

Example: Configuring Access Profiles (Master Administrators Only)

The master administrator is responsible for configuring access profiles in the master logical system. This example shows how to configure access profiles.

- [Requirements on page 144](#)
- [Overview on page 144](#)
- [Configuration on page 145](#)

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See “[Understanding the Master Logical Systems and the Master Administrator Role](#)” on page 40.
- Read *Firewall User Authentication Overview*.

Overview

This example configures an access profile for LDAP authentication for logical system users. This example creates the access profile described in [Table 15 on page 145](#).



NOTE: The master administrator creates the access profile.

Table 15: Access Profile Configuration

Name	Configuration Parameters
ldap1	<ul style="list-style-type: none"> • LDAP is used as the first (and only) authentication method. • Base distinguished name: <ul style="list-style-type: none"> • Organizational unit name (OU): people • Domain components (DC): example, com • A user's LDAP distinguished name is assembled through the use of a common name identifier, username, and base distinguished name. The common name identifier is user ID (UID). • The LDAP server address is 10.155.26.104 and is reached through port 389.

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.



NOTE: You must be logged in as the master administrator.

```
set access profile ldap1 authentication-order ldap
set access profile ldap1 ldap-options base-distinguished-name
  ou=people,dc=example,dc=com
set access profile ldap1 ldap-options assemble common-name uid
set access profile ldap1 ldap-server 10.155.26.104 port 389
```

Step-by-Step Procedure

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

To configure an access profile in the master logical system:

1. Log in to the master logical system as the master administrator and enter configuration mode.

```
admin@host> configure
admin@host#
```

2. Configure an access profile and set the authentication order.

```
[edit access profile ldap1]
admin@host# set authentication-order ldap
```

3. Configure LDAP options.

```
[edit access profile ldap1]
admin@host# set ldap-options base-distinguished-name
ou=people,dc=example,dc=com
admin@host# set ldap-options assemble common-name uid
```

4. Configure the LDAP server.

```
[edit access profile ldap1]
admin@host# set ldap-server 10.155.26.104 port 389
```

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

```
admin@host# show access profile ldap1
authentication-order ldap;
ldap-options {
  base-distinguished-name ou=people,dc=example,dc=com;
  assemble {
    common-name uid;
  }
}
ldap-server {
  10.155.26.104 port 389;
}
```

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

- See Also**
- [Example: Configuring Firewall Authentication for a User Logical System on page 154](#)
 - [Understanding Logical System Firewall Authentication on page 152](#)
 - [User Logical Systems Configuration Overview on page 61](#)

Example: Configuring Security Features for the Master Logical Systems

This example shows how to configure security features, such as zones, policies, and firewall authentication, for the master logical system.

- [Requirements on page 147](#)
- [Overview on page 147](#)
- [Configuration on page 148](#)
- [Verification on page 152](#)

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See [“Example: Configuring Root Password for Logical Systems”](#) on page 64.
- Use the **show system security-profile** command to see the resources allocated to the master logical system.
- Configure logical interfaces for the master logical system. See [“Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\)”](#) on page 105.
- Configure the access profile `ldap1` in the master logical system. The `ldap1` access profile is used for Web authentication of firewall users. See [“Example: Configuring Access Profiles \(Master Administrators Only\)”](#) on page 144.

Overview

In this example, you configure security features for the master logical system, called `root-logical-system`, shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65. This example configures the security features described in [Table 16 on page 147](#).

Table 16: root-logical-system Security Feature Configuration

Feature	Name	Configuration Parameter
Zones	<code>ls-root-trust</code>	Bind to interface <code>ge-0/0/4.0</code> .
	<code>ls-root-untrust</code>	Bind to interface <code>lt-0/0/0.1</code>
Address books	<code>root-internal</code>	<ul style="list-style-type: none"> • Address masters: <code>12.12.1.0/24</code> • Attach to zone <code>ls-root-trust</code>
	<code>root-external</code>	<ul style="list-style-type: none"> • Address design: <code>12.1.1.0/24</code> • Address accounting: <code>14.1.1.0/24</code> • Address marketing: <code>13.1.1.0/24</code> • Address set <code>usersys</code>: design, accounting, marketing • Attach to zone <code>ls-root-untrust</code>
Security policies	<code>permit-to-usersys</code>	Permit the following traffic: <ul style="list-style-type: none"> • From zone: <code>ls-root-trust</code> • To zone: <code>ls-root-untrust</code> • Source address: <code>masters</code> • Destination address: <code>usersys</code> • Application: any

Table 16: root-logical-system Security Feature Configuration (continued)

Feature	Name	Configuration Parameter
	permit-authorized-users	Permit the following traffic: <ul style="list-style-type: none"> • From zone: ls-root-untrust • To zone: ls-root-trust • Source address: userlsys • Destination address: masters • Application: junos-http, junos-https
Firewall authentication		<ul style="list-style-type: none"> • Web authentication • Authentication success banner "WEB AUTH LOGIN SUCCESS" • Default access profile ldap1
HTTP daemon		Activate on interface ge-0/0/4.0

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 address-book root-internal address masters 12.12.1.0/24
set security address-book root-internal attach zone ls-root-trust
set security address-book root-external address design 12.1.1.0/24
set security address-book root-external address accounting 14.1.1.0/24
set security address-book root-external address marketing 13.1.1.0/24
set security address-book root-external address-set userlsys address design
set security address-book root-external address-set userlsys address accounting
set security address-book root-external address-set userlsys address marketing
set security address-book root-external attach zone ls-root-untrust
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys match source-address masters
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys match destination-address userlsys
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys match application any
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys then permit
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match source-address userlsys
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match destination-address masters
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match application junos-http
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match application junos-https
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users then permit firewall-authentication web-authentication
set security zones security-zone ls-root-trust interfaces ge-0/0/4.0

```

```

set security zones security-zone ls-root-untrust interfaces lt-0/0/0.1
set system services web-management http interface ge-0/0/4.0
set access firewall-authentication web-authentication default-profile ldap1
set access firewall-authentication web-authentication banner success "WEB AUTH
LOGIN SUCCESS"

```

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

To configure zones and policies for the master logical system:

1. Log in to the master logical system as the master administrator and enter configuration mode.

```

admin@host> configure
admin@host#

```

2. Create security zones and assign interfaces to each zone.

```

[edit security zones]
admin@host# set security-zone ls-root-trust interfaces ge-0/0/4.0
admin@host# set security-zone ls-root-untrust interfaces lt-0/0/0.1

```

3. Create address book entries.

```

[edit security]
admin@host# set address-book root-internal address masters 12.12.1.0/24
admin@host# set address-book root-external address design 12.1.1.0/24
admin@host# set address-book root-external address accounting 14.1.1.0/24
admin@host# set address-book root-external address marketing 13.1.1.0/24
admin@host# set address-book root-external address-set userlsys address design
admin@host# set address-book root-external address-set userlsys address
accounting
admin@host# set address-book root-external address-set userlsys address
marketing

```

4. Attach address books to zones.

```

[edit security]
admin@host# set address-book root-internal attach zone ls-root-trust
admin@host# set address-book root-external attach zone ls-root-untrust

```

5. Configure a security policy that permits traffic from the ls-root-trust zone to the ls-root-untrust zone.

```

[edit security policies from-zone ls-root-trust to-zone ls-root-untrust]
admin@host# set policy permit-to-userlsys match source-address masters
admin@host# set policy permit-to-userlsys match destination-address userlsys
admin@host# set policy permit-to-userlsys match application any
admin@host# set policy permit-to-userlsys then permit

```

6. Configure a security policy that authenticates traffic from the ls-root-untrust zone to the ls-root-trust zone.

```
[edit security policies from-zone ls-root-untrust to-zone ls-root-trust]
admin@host# set policy permit-authorized-users match source-address userlsys
admin@host# set policy permit-authorized-users match destination-address masters
admin@host# set policy permit-authorized-users match application junos-http
admin@host# set policy permit-authorized-users match application junos-https
admin@host# set policy permit-authorized-users then permit firewall-authentication
web-authentication
```

7. Configure the Web authentication access profile and define a success banner.

```
[edit access]
admin@host# set firewall-authentication web-authentication default-profile ldap1
admin@host# set firewall-authentication web-authentication banner success "WEB
AUTH LOGIN SUCCESS"
```

8. Activate the HTTP daemon on the device.

```
[edit system]
admin@host# set services web-management http interface ge-0/0/4.0
```

Results From configuration mode, confirm your configuration by entering the **show security**, **show access**, and **show system services** 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]
admin@host# show security
...
address-book {
  root-internal {
    address masters 12.12.1.0/24;
    attach {
      zone ls-root-trust;
    }
  }
  root-external {
    address design 12.1.1.0/24;
    address accounting 14.1.1.0/24;
    address marketing 13.1.1.0/24;
    address-set userlsys {
      address design;
      address accounting;
      address marketing;
    }
    attach {
      zone ls-root-untrust;
    }
  }
}
```

```
}
}
policies {
  from-zone ls-root-trust to-zone ls-root-untrust {
    policy permit-to-userlsys {
      match {
        source-address masters;
        destination-address userlsys;
        application any;
      }
      then {
        permit;
      }
    }
  }
  from-zone ls-root-untrust to-zone ls-root-trust {
    policy permit-authorized-users {
      match {
        source-address userlsys;
        destination-address masters;
        application [ junos-http junos-https ];
      }
      then {
        permit {
          firewall-authentication {
            web-authentication;
          }
        }
      }
    }
  }
}
zones {
  security-zone ls-root-trust {
    interfaces {
      ge-0/0/4.0;
    }
  }
  security-zone ls-root-untrust {
    interfaces {
      lt-0/0/0.1;
    }
  }
}
[edit]
admin@host# show access
...
firewall-authentication {
  web-authentication {
    default-profile ldap1;
    banner {
      success "WEB AUTH LOGIN SUCCESS";
    }
  }
}
[edit]
```

```
admin@host# show system services
web-management {
  http {
    interface ge-0/0/4.0;
  }
}
```

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 Policy Configuration on page 152](#)

Verifying Policy Configuration

Purpose Verify information about policies and rules.

Action From operational mode, enter the **show security policies detail** command to display a summary of all policies configured on the logical system.

- See Also**
- [Understanding Logical Systems Zones on page 128](#)
 - [Understanding Logical Systems Security Policies on page 167](#)
 - [Understanding Logical System Firewall Authentication on page 152](#)

Understanding Logical System Firewall Authentication

A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall. Junos OS enables administrators to restrict and permit firewall users to access protected resources (different zones) behind a firewall based on their source IP address and other credentials.

The master administrator is responsible for configuring access profiles in the master logical system. Access profiles store usernames and passwords of users or point to external authentication servers where such information is stored. Access profiles configured at the master logical system are available to all user logical systems.

The master administrator configures the maximum and reserved numbers of firewall authentications for each user logical system. The user logical system administrator can then create firewall authentications in the user logical system. From a user logical system, the user logical system administrator can use the **show system security-profile auth-entry** command to view the number of authentication resources allocated to the user logical system.

To configure the access profile, the master administrator uses the **profile** configuration statement at the **[edit access]** hierarchy level in the master logical system. The access profile can also include the order of authentication methods, LDAP or RADIUS server options, and session options.

The user logical system administrator can then associate the access profile with a security policy in the user logical system. The user logical system administrator also specifies the type of authentication:

- With pass-through authentication, a host or a user from one zone tries to access resources on another zone using an FTP, a Telnet, or an HTTP client. The device uses FTP, Telnet, or HTTP to collect username and password information, and subsequent traffic from the user or host is allowed or denied based on the result of this authentication.
- With Web authentication, users use HTTP to connect to an IP address on the device that is enabled for Web authentication and are prompted for the username and password. Subsequent traffic from the user or host to the protected resource is allowed or denied based on the result of this authentication.

The user logical system administrator configures the following properties for firewall authentication in the user logical system:

- Security policy that specifies firewall authentication for matching traffic. Firewall authentication is specified with the **firewall-authentication** configuration statement at the **[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit]** hierarchy level.

Users or user groups in an access profile who are allowed access by the policy can optionally be specified with the client-match configuration statement. (If no users or user groups are specified, any user who is successfully authenticated is allowed access.)

For pass-through authentication, the access profile can optionally be specified and Web redirect (redirecting the client system to a webpage for authentication) can be enabled.

- Type of authentication (pass-through or Web authentication), default access profile, and success banner for the FTP, Telnet, or HTTP session. These properties are configured with the **firewall-authentication** configuration statement at the **[edit access]** hierarchy level.
- Host inbound traffic. Protocols, services, or both are allowed to access the logical system. The types of traffic are configured with the **host-inbound-traffic** configuration statement at the **[edit security zones security-zone zone-name]** or **[edit security zones security-zone zone-name interfaces interface-name]** hierarchy levels.

From a user logical system, the user logical system administrator can use the **show security firewall-authentication users** or **show security firewall-authentication history** commands to view the information about firewall users and history for the user logical system. From the master logical system, the master administrator can use the same commands to view information for the master logical system, a specific user logical system, or all logical systems.

- See Also**
- [Example: Configuring Access Profiles \(Master Administrators Only\) on page 144](#)
 - [Example: Configuring Firewall Authentication for a User Logical System on page 154](#)
 - [User Logical Systems Configuration Overview on page 61](#)

- [Understanding Logical Systems Security Profiles \(Master Administrators Only\)](#) on page 73
- [Firewall User Authentication Overview](#)

Example: Configuring Firewall Authentication for a User Logical System

This example shows how to configure firewall authentication for a user logical system.

- [Requirements](#) on page 154
- [Overview](#) on page 154
- [Configuration](#) on page 155
- [Verification](#) on page 157

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview”](#) on page 61.
- Use the **show system security-profiles auth-entry** command to see the firewall authentication entries allocated to the logical system.
- Access profiles must be configured in the master logical system by the master administrator. See [“Example: Configuring Access Profiles \(Master Administrators Only\)”](#) on page 144.

Overview

This example configures the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65.

In this example, users in the ls-marketing-dept and ls-accounting-dept logical systems are required to authenticate when initiating certain connections to the product designers subnet. This example configures the firewall authentication described in [Table 5](#) on page 88.



NOTE: This example uses the access profile configured in [“Example: Configuring Access Profiles \(Master Administrators Only\)”](#) on page 144 and address book entries configured in [“Example: Configuring Security Zones for a User Logical Systems”](#) on page 141.

Table 17: User Logical System Firewall Authentication Configuration

Feature	Name	Configuration Parameters
Security policy	permit-authorized-users NOTE: Policy lookup is performed in the order that the policies are configured. The first policy that matches the traffic is used. If you have previously configured a policy that permits traffic for the same from-zone, to-zone, source address, and destination address but with application any , the policy configured in this example would never be matched. (See "Example: Configuring Security Policies in a User Logical Systems" on page 168.) Therefore, this policy should be reordered so that it is checked first.	Permit firewall authentication for the following traffic: <ul style="list-style-type: none"> • From zone: ls-product-design-untrust • To zone: ls-product-design-trust • Source address: otherlsys • Destination address: product-engineers • Application: junos-h323 The ldap1 access profile is used for pass-through authentication.
Firewall authentication		<ul style="list-style-type: none"> • Pass-through authentication • HTTP login prompt "welcome" • Default access profile ldap1

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 ls-product-design-untrust to-zone ls-product-design-trust
policy permit-authorized-users match source-address otherlsys
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-authorized-users match destination-address product-designers
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-authorized-users match application junos-h323
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-authorized-users then permit firewall-authentication pass-through
access-profile ldap1
set access firewall-authentication pass-through default-profile ldap1
set access firewall-authentication pass-through http banner login "welcome"

```

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

To configure firewall authentication in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```

lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#

```

2. Configure a security policy that permits firewall authentication.

```
[edit security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users match
source-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users match
destination -address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users match
application junos-h323
lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users then
permit firewall-authentication pass-through access-profile ldap1
```

3. Reorder the security policies.

```
[edit]
lsdesignadmin1@host:ls-product-design# insert security policies from-zone
ls-product-design-untrust to-zone ls-product-design-trust policy
permit-authorized-users before policy permit-all-from-otherlsys
```

4. Configure firewall authentication.

```
[edit access firewall-authentication]
lsdesignadmin1@host:ls-product-design# set pass-through http banner login
"welcome"
lsdesignadmin1@host:ls-product-design# set pass-through default-profile ldap1
```

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

```
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
  policy permit-all-to-otherlsys {
    match {
      source-address product-designers;
      destination-address otherlsys;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone ls-product-design-untrust to-zone ls-product-design-trust {
  policy permit-authorized-users {
    match {
      source-address otherlsys;
      destination-address product-designers;
      application junos-h323;
    }
    then {
      permit {
        firewall-authentication {
```

```

        pass-through {
            access-profile ldap1;
        }
    }
}
}
}
}
policy permit-all-from-otherlsys {
    match {
        source-address otherlsys;
        destination-address product-designers;
        application any;
    }
    then {
        permit;
    }
}
}
lsdesignadmin1@host:ls-product-design# show access firewall-authentication
pass-through {
    default-profile ldap1;
    http {
        banner {
            login welcome;
        }
    }
}
}

```

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 Firewall User Authentication and Monitoring Users and IP Addresses on page 157](#)

Verifying Firewall User Authentication and Monitoring Users and IP Addresses

Purpose Display firewall authentication user history and verify the number of firewall users who successfully authenticated and firewall users who failed to log in.

Action From operational mode, enter these **show** commands.

```

lsdesignadmin1@host:ls-product-design> show security firewall-authentication history
lsdesignadmin1@host:ls-product-design> show security firewall-authentication history
    identifier id
lsdesignadmin1@host:ls-product-design> show security firewall-authentication users
lsdesignadmin1@host:ls-product-design> show security firewall-authentication users
    identifier id

```

- See Also**
- [Example: Configuring Access Profiles \(Master Administrators Only\) on page 144](#)
 - [Understanding Logical System Firewall Authentication on page 152](#)

- [User Logical Systems Configuration Overview on page 61](#)
- *Example: Configuring Pass-Through Authentication*

Understanding Integrated User Firewall support in a Logical System

Starting in Junos OS Release 18.3R1, the support for authentication sources is extended to include Local authentication, Active Directory (AD) authentication, and firewall authentication in addition to the existing support for authentication sources Juniper Identity Management Service (JIMS) and ClearPass authentication.

Starting in Junos OS Release 18.2R1, the support for user firewall authentication is enhanced using a shared model. In this model, user logical systems share user firewall configuration and authentication entries with the master logical system and the integrated user firewall authentication is supported in a user logical system.

In the shared model, user firewall related configuration is configured under master logical system, such as authentication source, authentication source priority, authentication entries timeout, and IP query or Individual query and so on. The user firewall provides user information service for an application in the SRX Series device, such as policy and logging. Traffic from a user logical system queries authentication tables from the master logical system.

The authentication tables are managed by a master logical system. The user logical systems share the authentication tables. Traffic from the master logical system and the user logical systems query the same authentication table. User logical systems enable the use of the source-identity in security policy.

For example, if the master logical system is configured with **employee** and the user logical system is configured with the source-identity **manager**, then the reference group of this authentication entry includes **employee** and **manager**. This reference group contains the same authentication entries from master logical system and user logical system.

Limitation of using user firewall authentication

Using user firewall authentication on tenant systems has the following limitation:

- The authentication entries are collected by the JIMS server based on the IP address from the customer network. If the IP addresses overlap, then the authentication entry changes when users login under different user logical systems.

- See Also**
- [Example: Configuring Integrated User Firewall Identification Management for a User Logical System on page 144](#)
 - [show services user-identification authentication-table on page 745](#)

Example: Configuring Integrated User Firewall Identification Management for a User Logical System

This example shows how to configure the SRX Series device's advanced query feature for obtaining user identity information from the Juniper Identity Management Service

(JIMS) and the security policy to match the source identity for a user logical system. In the root logical system, user firewall is configured with JIMS, and then the root logical system manages all of authentication entries coming from JIMS. In this example, all of user logical systems share their authentication entries with the root logical system.

- [Requirements on page 159](#)
- [Overview on page 159](#)
- [Configuration on page 160](#)
- [Verification on page 164](#)

Requirements

This example uses the following hardware and software components:

- SRX1500 devices operating in chassis clustering
- JIMS server
- Junos OS Release 18.2 R1

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#)
- Configure user logical systems `lsys1` and `lsys2`. See [“Example: Configuring User Logical Systems” on page 130](#)
- Configure security profile on master logical system and assign it to user logical systems `lsys1` and `lsys2`. See [“Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\)” on page 79](#)
- Configure interfaces and routing options on logical systems root logical system, user logical systems `lsys1`, and `lsys2`. See [“Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems \(Master Administrators Only\)” on page 105](#) and [“Example: Configuring Interfaces and Routing Instances for a User Logical Systems” on page 121](#)
- Configure security policies for a user logical systems. See [“Example: Configuring Security Policies in a User Logical Systems” on page 168](#)
- Configure zones for a user logical system. See [“Example: Configuring Security Zones for a User Logical Systems” on page 141](#)
- Configure logical systems in a basic active/passive chassis cluster. See [“Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(Master Administrators Only\)” on page 275](#)

Overview

In this example, you can configure JIMS with HTTPs connection on port 443 and primary server with IPv4 address on master logical system, policy `p1` with source-identity `"group1"` of `dc0` domain on logical system `lsys1`, policy `p1` with source-identity `"group1"` of `dc0`

domain on logical system lsys2, and send traffic from and through logical system lsys1 to logical system lsys2. You can view the authentication entries on master logical system and user logical systems (lsys1 and lsys2) even after rebooting the primary node.

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 logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
  lsys1_policy1 match source-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
  lsys1_policy1 match destination-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
  lsys1_policy1 match application any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
  lsys1_policy1 then permit
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
  lsys1_policy1 match source-identity "example.com\group1"
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
  lsys1_policy1 then permit
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust
  policy lsys1_policy2 match source-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust
  policy lsys1_policy2 match destination-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust
  policy lsys1_policy2 match application any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust
  policy lsys1_policy2 then permit
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust
  policy lsys1_policy3 match source-address any
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust
  policy lsys1_policy3 match destination-address any
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust
  policy lsys1_policy3 match application any
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust
  policy lsys1_policy3 then permit
set logical-systems lsys1 security policies policy-rematch
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust
  policy lsys2_policy1 match source-address any
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust
  policy lsys2_policy1 match destination-address any
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust
  policy lsys2_policy1 match application any
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust
  policy lsys2_policy1 match source-identity "example.com\group2"
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust
  policy lsys2_policy1 then permit
set logical-systems lsys2 security policies policy-rematch
set services user-identification identity-management connection connect-method https
set services user-identification identity-management connection port 443
set services user-identification identity-management connection primary address 192.0.2.5
set services user-identification identity-management connection primary client-id otest
```



```

set services user-identification identity-management connection primary client-secret
"$ABC123"
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
source-address any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
destination-address any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
application any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 then permit
set security policies policy-rematch
set security zones security-zone root_trust interfaces reth1.0 host-inbound-traffic
system-services all
set security zones security-zone root_trust interfaces reth1.0 host-inbound-traffic protocols
all
set security zones security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic
system-services all
set security zones security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic
protocols all
set firewall family inet filter impair-ldap term allow_all then accept

```

Configuring user firewall identification management

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

To configure user firewall identification management:

1. Log in to the master logical system as the master administrator and enter configuration mode.


```

user@host> configure
user@host#

```
2. Create logical systems.


```

[edit logical-systems]
user@host#set LSYS0
user@host#set LSYS1
user@host#set LSYS2

```
3. Configure a security policy `lsys1_policy1` with source-identity `group1` on logical system `lsys1` that permits traffic from `lsys1_trust` to `lsys1_trust`.


```

[edit security policies]
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match
source-address any
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match
destination-address any
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match
application any
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match
source-identity "example.com\group1"
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 then
permit

```

4. Configure a security policy `lsys1_policy2` that permits traffic from `lsys1_trust` to `lsys1_untrust`.

```
[edit security policies]
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2
match source-address any
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2
match destination-address any
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2
match application any
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2 then
permit
```

5. Configure a security policy `lsys1_policy3` that permits traffic from `lsys1_untrust` to `lsys1_trust`.

```
[edit security policies]
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3
match source-address any
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3
match destination-address any
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3
match application any
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3 then
permit
user@host#set policy-rematch
```

6. Configure security zone and assign interfaces to each zone.

```
[edit security zones]
user@host#set security-zone lsys1_trust interfaces reth2.0 host-inbound-traffic
system-services all
user@host#set security-zone lsys1_trust interfaces reth2.0 host-inbound-traffic
protocols all
user@host#set security-zone lsys1_trust interfaces lt-0/0/0.11 host-inbound-traffic
system-services all
user@host#set security-zone lsys1_trust interfaces lt-0/0/0.11 host-inbound-traffic
protocols all
user@host#set security-zone lsys1_untrust interfaces reth3.0 host-inbound-traffic
system-services all
user@host#set security-zone lsys1_untrust interfaces reth3.0 host-inbound-traffic
protocols all
```

7. Configure a security policy `lsys2_policy1` with source-identity `group1` that permits traffic from `lsys2_untrust` to `lsys2_untrust` on `lsys2`.

```
[edit security policies]
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1
match source-address any
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1
match destination-address any
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1
match application any
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1
match source-identity "example.com\group2"
```

```

user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1
then permit
user@host#set policy-rematch

```

8. Configure security zones and assign interfaces to each zone on lsys2.

```

[edit security zones]
user@host#set security-zone lsys2_untrust interfaces reth4.0 host-inbound-traffic
system-services all
user@host#set security-zone lsys2_untrust interfaces reth4.0 host-inbound-traffic
protocols all
user@host#set security-zone lsys2_untrust interfaces lt-0/0/0.21
host-inbound-traffic system-services all
user@host#set security-zone lsys2_untrust interfaces lt-0/0/0.21
host-inbound-traffic protocols all

```

9. Configure JIMS as the authentication source for advanced query requests with the primary address. The SRX Series device requires this information to contact the server.

```

[edit services user-identification identity-management]
user@host#set connection port 443
user@host#set connection connect-method https
user@host#set connection primary address 192.0.2.5
user@host#set connection primary client-id otest
user@host#set connection primary client-secret test
user@host#set authentication-entry-timeout 0

```

10. Configure security policies and zones on master logical system.

```

[edit security policies]
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match
source-address any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match
destination-address any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match
application any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 then
permit
user@host#set policy-rematch

```

11. Configure security zones and assign interfaces to each zone on master logical system.

```

[edit security zones]
user@host#set security-zone root_trust interfaces reth1.0 host-inbound-traffic
system-services all
user@host#set security-zone root_trust interfaces reth1.0 host-inbound-traffic
protocols all
user@host#set security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic
system-services all
user@host#set security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic
protocols all
user@host#set firewall family inet filter impair-ldap term allow_all then accept

```

Results

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

```
user@host# show services user-identification identity-management
connection {
  connect-method https;
  port 443;
  primary {
    address 192.0.2.5;
    client-id otest;
    client-secret "$ABC123"; ## SECRET-DATA
  }
}

user@host# show chassis cluster
reth-count 5;
control-ports {
  fpc 3 port 0;
  fpc 9 port 0;
}
redundancy-group 0 {
  node 0 priority 200;
  node 1 priority 1;
}
redundancy-group 1 {
  node 0 priority 100;
  node 1 priority 1;
}
redundancy-group 2 {
  node 0 priority 100;
  node 1 priority 1;
}
redundancy-group 3 {
  node 0 priority 100;
  node 1 priority 1;
}
redundancy-group 4 {
  node 0 priority 100;
  node 1 priority 1;
}
```

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

Verification

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

- [Verifying chassis cluster status and authentication entries on page 165](#)
- [Verifying chassis cluster status on page 165](#)

Verifying chassis cluster status and authentication entries

Purpose To verify authentication entries in a logical system.

Action To verify the configuration is working properly, enter the **show services user-identification authentication-table authentication-source identity-management logical-system all** command.

```
user@host> show services user-identification authentication-table authentication-source
identity-management logical-system all
node0:
```

```
-----
Logical System: root-logical-system
Domain: ad2012.jims.com
Total entries: 3
Source IP      Username      groups(Ref by policy)      state
2001:db8:aaaa: N/A                      Valid
2001:db8:aaaa: administrator          Valid
203.0.113.50   administrator          Valid
node1:
```

```
-----
Logical System: root-logical-system
Domain: ad2012.jims.com
Total entries: 3
Source IP      Username      groups(Ref by policy)      state
2001:db8:aaaa: N/A                      Valid
2001:db8:aaaa: administrator          Valid
203.0.113.50   administrator          Valid
```

Meaning The output displays the authentication entries that are shared from user logical system to root logical system.

Verifying chassis cluster status

Purpose Verify chassis cluster status after rebooting the primary node.

Action To verify the configuration is working properly, enter the **show chassis cluster status** command.

```
user@host> show chassis cluster status
```

```
Monitor Failure codes:
CS Cold Sync monitoring      FL Fabric Connection monitoring
GR GRES monitoring           HW Hardware monitoring
IF Interface monitoring      IP IP monitoring
LB Loopback monitoring       MB Mbuf monitoring
NH Nexthop monitoring       NP NPC monitoring
SP SPU monitoring           SM Schedule monitoring
CF Config Sync monitoring    RE Relinquish monitoring
Cluster ID: 6
Node  Priority Status      Preempt Manual  Monitor-failures
Redundancy group: 0 , Failover count: 0
node0 200    hold          no      no      None
node1 1      secondary     no      no      None
```

```

Redundancy group: 1 , Failover count: 0
node0 0      hold          no      no      CS
node1 1      secondary     no      no      None
Redundancy group: 2 , Failover count: 0
node0 0      hold          no      no      CS
node1 1      secondary     no      no      None
Redundancy group: 3 , Failover count: 0
node0 0      hold          no      no      CS
node1 1      secondary     no      no      None
Redundancy group: 4 , Failover count: 0
node0 0      hold          no      no      CS
node1 1      secondary     no      no      None

```

Meaning The output displays user identification management session existing on lsys1 and lsys2 after rebooting the primary node.

See Also

- [show services user-identification authentication-table on page 745](#)
- [Understanding Integrated User Firewall support in a Logical System on page 158](#)

Release History Table

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the support for authentication sources is extended to include Local authentication, Active Directory (AD) authentication, and firewall authentication in addition to the existing support for authentication sources Juniper Identity Management Service (JIMS) and ClearPass authentication.
18.2R1	Starting in Junos OS Release 18.2R1, the support for user firewall authentication is enhanced using a shared model. In this model, user logical systems share user firewall configuration and authentication entries with the master logical system and the integrated user firewall authentication is supported in a user logical system.

Related Documentation

- [Example: Configuring Security log stream for Logical Systems on page 92](#)

Security Policies for Logical Systems

Security policies are used to secure business and control access to LAN resources. Secure access is required both within the company across the LAN and in its interactions with external networks such as the Internet. Junos OS provides powerful network security features through its stateful firewall, application firewall, and user identity firewall. All three types of firewall enforcement are implemented through security policies. For more information, see the following topics:

- [Understanding Logical Systems Security Policies on page 167](#)
- [Example: Configuring Security Policies in a User Logical Systems on page 168](#)

Understanding Logical Systems Security Policies

- [Security Policies in Logical Systems on page 167](#)
- [Application Timeouts on page 167](#)
- [Security Policy Allocation on page 168](#)

Security Policies in Logical Systems

Security policies enforce rules for what traffic can pass through the firewall and actions that need to take place on the traffic as it passes through the firewall. From the perspective of security policies, traffic enters one security zone and exits another security zone.

By default, a logical system denies all traffic in all directions, including intra-zone and inter-zone directions. Through the creation of security policies, the logical system administrator can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from specified sources to specified destinations.

Security policies can be configured in the master logical system and in user logical systems. Configuring a security policy in a logical system is the same as configuring a security policy on a device that is not configured for logical systems. Any security policies, policy rules, address books, applications and application sets, and schedulers created within a logical system are only applicable to that logical system. Only predefined applications and application sets, such as **junos-ftp**, can be shared between logical systems.



NOTE: In a logical system, you cannot specify **global** as either the **from-zone** or the **to-zone** in a security policy.

The user logical system administrator can configure and view all attributes for security policies in a user logical system. All attributes of a security policy in a user logical system are also visible to the master administrator.

Application Timeouts

The application timeout value set for an application determines the session timeout. Application timeout behavior is the same in a logical system as at the root level. However, user logical system administrators can use predefined applications in security policies but cannot modify the timeout value of predefined applications. This is because the predefined applications are shared by the master logical system and all user logical systems, so the user logical system administrator is not allowed to change its behavior. Application timeout values are stored in the application entry database and in the corresponding logical system TCP and UDP port-based timeout tables.

If the application that is matched for the traffic has a timeout value, that timeout value is used. Otherwise, the lookup proceeds in the following order until an application timeout value is found:

1. The logical system TCP and UDP port-based timeout table is searched for a timeout value.
2. The root TCP and UDP port-based timeout table is searched for a timeout value.
3. The protocol-based default timeout table is searched for a timeout value.

Security Policy Allocation

The master administrator configures the maximum and reserved numbers of security policies for each user logical system. The user logical system administrator can then create security policies in the user logical system. From a user logical system, the user logical system administrator can use the **show system security-profile policy** command to view the number of security policies allocated to the user logical system.



NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of security policies applied to the master logical system. The number of policies configured in the master logical system count toward the maximum number of policies available on the device.

- See Also**
- [Example: Configuring Security Policies in a User Logical Systems on page 168](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [User Logical Systems Configuration Overview on page 61](#)
 - [Security Policies Overview](#)
 - [Understanding Policy Application Timeout Configuration and Lookup](#)

Example: Configuring Security Policies in a User Logical Systems

This example shows how to configure security policies for a user logical system.

- [Requirements on page 169](#)
- [Overview on page 169](#)
- [Configuration on page 169](#)
- [Verification on page 171](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Use the **show system security-profiles policy** command to see the security policy resources allocated to the logical system.
- Configure zones and address books. See [“Example: Configuring Security Zones for a User Logical Systems” on page 141](#).

Overview

This example configures the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

This example configures the security policies described in [Table 18 on page 169](#).

Table 18: User Logical System Security Policies Configuration

Name	Configuration Parameters
permit-all-to-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> • From zone: ls-product-design-trust • To zone: ls-product-design-untrust • Source address: product-designers • Destination address: otherlsys • Application: any
permit-all-from-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> • From zone: ls-product-design-untrust • To zone: ls-product-design-trust • Source address: otherlsys • Destination address: product-designers • Application: any

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 ls-product-design-trust to-zone ls-product-design-untrust
policy permit-all-to-otherlsys match source-address product-designers
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy permit-all-to-otherlsys match destination-address otherlsys
```

```
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy permit-all-to-otherlsys match application any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy permit-all-to-otherlsys then permit
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-all-from-otherlsys match source-address otherlsys
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-all-from-otherlsys match destination-address product-designers
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-all-from-otherlsys match application any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy permit-all-from-otherlsys 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 the Junos OS CLI User Guide.

To configure security policies in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security policy that permits traffic from the ls-product-design-trust zone to the ls-product-design-untrust zone.

```
[edit security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust]
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
source-address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
destination-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
application any
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys then
permit
```

3. Configure a security policy that permits traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone.

```
[edit security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
source-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
destination-address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
application any
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys 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.

```
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
  policy permit-all-to-otherlsys {
    match {
      source-address product-designers;
      destination-address otherlsys;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone ls-product-design-untrust to-zone ls-product-design-trust {
  policy permit-all-from-otherlsys {
    match {
      source-address otherlsys;
      destination-address product-designers;
      application any;
    }
    then {
      permit;
    }
  }
}
```

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 Policy Configuration on page 171](#)

Verifying Policy Configuration

Purpose Verify information about policies and rules.

Action From operational mode, enter the **show security policies detail** command to display a summary of all policies configured on the logical system.

- See Also**
- [Understanding Logical Systems Security Policies on page 167](#)
 - [User Logical Systems Configuration Overview on page 61](#)
 - [Troubleshooting Security Policies](#)

Screen Options for User Logical Systems

Screen options on SRX Series devices prevent attacks, such as IP address sweeps, port scans, denial of service (DOS) attacks, ICMP, UDP, and SYN floods. For more information, see the following topics:

- [Understanding Logical Systems Screen Options on page 172](#)
- [Example: Configuring Screen Options for a User Logical Systems on page 172](#)

Understanding Logical Systems Screen Options

Junos OS screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos OS then applies firewall policies, which can contain content filtering and IDP components, to the traffic that passes the screen filters.

All screen options available on the device are available in each logical system. Each user logical system administrator can configure screen options for their user logical system. The master administrator can configure screen options for the master logical system as well as all user logical systems.

The user logical system administrator can configure and view all screen options in a user logical system. All screen options in a user logical system are visible to the master administrator.

- See Also**
- [Example: Configuring Screen Options for a User Logical Systems on page 172](#)
 - [User Logical Systems Configuration Overview on page 61](#)
 - *Attack Detection and Prevention Overview*

Example: Configuring Screen Options for a User Logical Systems

This example shows how to configure screen options for a user logical system.

- [Requirements on page 172](#)
- [Overview on page 173](#)
- [Configuration on page 173](#)

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Configure zones for the user logical system. See [“Example: Configuring Security Zones for a User Logical Systems” on page 141](#).

Overview

This example configures the ls-product-design user logical system shown in “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on page 65.

You can limit the number of concurrent sessions to the same destination IP address in a user logical system. Setting a destination-based session limit can ensure that Junos OS allows only an acceptable number of concurrent connection requests—no matter what the source—to reach any one host. When the number of concurrent connection requests to an IP address surpasses the limit, Junos OS blocks further connection attempts to that IP address. This example creates the screen options described in [Table 19 on page 173](#).

Table 19: User Logical System Screen Options Configuration

Name	Configuration Parameters
limit-destination-sessions	<ul style="list-style-type: none"> Limits concurrent connection requests to destination IPs to 80. Applied to ls-product-design-untrust zone.

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 screen ids-option limit-destination-sessions limit-session destination-ip-based 80
set security zones security-zone ls-product-design-untrust screen limit-destination-sessions
```

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

To configure destination-based session limits in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a screen option for a destination-based session limit.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set screen ids-option
limit-destination-sessions limit-session destination-ip-based 80
```

3. Set the security zone for the screen option.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set zones security-zone
ls-product-design-untrust screen limit-destination-sessions
```

Results From configuration mode, confirm your configuration by entering the **show security screen** and **show security zone** 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 (...).

```
lsdesignadmin1@host:ls-product-design# show security screen
ids-option limit-destination-sessions {
  limit-session {
    destination-ip-based 80;
  }
}
lsdesignadmin1@host:ls-product-design# show security zones
security-zone ls-product-design-trust {
  ...
}
security-zone ls-product-design-untrust {
  screen limit-destination-sessions;
  ...
}
```

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

- See Also**
- [User Logical Systems Configuration Overview on page 61](#)
 - [Understanding Logical Systems Screen Options on page 172](#)

- Related Documentation**
- [IDP for Logical Systems on page 201](#)

VPNs in Logical Systems

A VPN is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. VPN prevents unauthorized access eavesdropping on the traffic, and allows the user to conduct work remotely. For more information, see the following topics:

- [Understanding Route-Based VPN Tunnels in Logical Systems on page 175](#)
- [Example: Configuring IKE and IPsec SAs for a VPN Tunnel \(Master Administrators Only\) on page 176](#)
- [Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems on page 180](#)

Understanding Route-Based VPN Tunnels in Logical Systems

A VPN connection can secure traffic that passes between a logical system and a remote site across a WAN. With route-based VPNs, you configure one or more security policies in a logical system to regulate the traffic flowing through a single IP Security (IPsec) tunnel. For each IPsec tunnel, there is one set of IKE and IPsec security associations (SAs) that must be configured at the root level by the master administrator.



NOTE: The external interface configured under the gateway configuration can only be a part of the root logical system.



NOTE: Only route-based VPNs are supported for logical systems. Policy-based VPNs are not supported.

In addition to configuring IKE and IPsec SAs for each VPN, the master administrator must also assign a secure tunnel (st0) interface to a user logical system. An st0 interface can only be assigned to a single user logical system. However, multiple user logical systems can each be assigned their own st0 interface.



NOTE: The st0 unit 0 interface should not be assigned to a logical system, as an SA cannot be set up for this interface.

The user logical system administrator can configure the IP address and other attributes of the st0 interface assigned to the user logical system. The user logical system administrator cannot delete an st0 interface assigned to their user logical system.

For route-based VPNs, a security policy refers to a destination address and not a specific VPN tunnel. For cleartext traffic in a user logical system to be sent to the VPN tunnel for encapsulation, the user logical system administrator must make the following configurations:

- Security policy that permits traffic to a specified destination.
- Static route to the destination with the st0 interface as the next hop.

When Junos OS looks up routes in the user logical system to find the interface to use to send traffic to the destination address, it finds a static route through the st0 interface. Traffic is routed to the VPN tunnel as long as the security policy action is permit.

The master logical system and a user logical system can share a route-based VPN tunnel. An st0 interface assigned to a user logical system can also be used by the master logical system. For the master logical system, the master administrator configures a security policy that permits traffic to the remote destination and a static route to the remote destination with the st0 interface as the next hop.

VPN monitoring is configured by the master administrator in the master logical system. For the VPN monitor source interface, the master administrator must specify the st0 interface; a physical interface for a user logical system cannot be specified.

- See Also**
- [Understanding Route-Based IPsec VPNs](#)
 - [User Logical Systems Configuration Overview](#) on page 61
 - [Example: Configuring IKE and IPsec SAs for a VPN Tunnel \(Master Administrators Only\)](#) on page 176
 - [Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems](#) on page 180

Example: Configuring IKE and IPsec SAs for a VPN Tunnel (Master Administrators Only)

The master administrator is responsible for assigning an st0 interface to a user logical system and configuring IKE and IPsec SAs at the root level for each VPN tunnel. This example shows how to assign an st0 interface to a user logical system and configure IKE and IPsec SA parameters.

- [Requirements](#) on page 176
- [Overview](#) on page 176
- [Configuration](#) on page 177
- [Verification](#) on page 180

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role”](#) on page 40.
- Read [Understanding Route-Based IPsec VPNs](#).

Overview

In this example you configure a VPN tunnel for the ls-product-design user logical system. This example configures the VPN tunnel parameters described in [Table 20 on page 176](#).

Table 20: Logical System VPN Tunnel Configuration

Feature	Name	Configuration Parameters
Tunnel interface	st0 unit 1	Assigned to ls-product-design logical system
IKE proposal	ike-phase1-proposal	<ul style="list-style-type: none"> • Preshared keys authentication • Diffie-Hellman group 2 • sha1 authentication algorithm • aes-128-cbc encryption algorithm

Table 20: Logical System VPN Tunnel Configuration (continued)

Feature	Name	Configuration Parameters
IKE policy		<ul style="list-style-type: none"> Main mode References IKE proposal ike-phase1-proposal ASCII preshared key 395psksecr3t
IKE gateway	ike-gw	<ul style="list-style-type: none"> External interface ge-0/0/3.0 References IKE policy ike-phase1-policy Address 2.2.2.2
IPsec proposal	ipsec-phase2-proposal	<ul style="list-style-type: none"> ESP protocol hmac-sha1-96 authentication algorithm aes-128-cbc encryption algorithm
IPsec policy	vpn-policy1	<ul style="list-style-type: none"> References ipsec-phase2-proposal perfect-forward-secrecy keys group2
VPN	ike-vpn	<ul style="list-style-type: none"> bind-interface st0.1 References ike-gw gateway References vpn-policy1 policy
VPN monitoring		<p>For ike-vpn VPN:</p> <ul style="list-style-type: none"> source-interface st0.1 destination-ip 4.0.0.1

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 logical-systems ls-product-design interfaces st0 unit 1
set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2
set security ike proposal ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-phase1-policy mode main
set security ike policy ike-phase1-policy proposals ike-phase1-proposal
set security ike policy ike-phase1-policy pre-shared-key ascii-text "$ABC123"
set security ike gateway ike-gw ike-policy ike-phase1-policy
set security ike gateway ike-gw address 2.2.2.2
set security ike gateway ike-gw external-interface ge-0/0/3.0
set security ipsec proposal ipsec-phase2-proposal protocol esp
set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group2
set security ipsec policy vpn-policy1 proposals ipsec-phase2-proposal
set security ipsec vpn ike-vpn bind-interface st0.1
set security ipsec vpn ike-vpn vpn-monitor source-interface st0.1

```

```
set security ipsec vpn ike-vpn vpn-monitor destination-ip 4.0.0.1
set security ipsec vpn ike-vpn ike gateway ike-gw
set security ipsec vpn ike-vpn ike ipsec-policy vpn-policy1
```

**Step-by-Step
Procedure**

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

To assign a VPN tunnel interface to a user logical system and configure IKE and IPsec SAs:

1. Log in to the master logical system as the master administrator and enter configuration mode.

```
[edit]
admin@host> configure
admin@host#
```

2. Assign a VPN tunnel interface.

```
[edit logical-systems ls-product-design]
admin@host# set interfaces st0 unit 1
```

3. Configure an IKE proposal.

```
[edit security ike]
admin@host# set proposal ike-phase1-proposal authentication-method
pre-shared-keys
admin@host# set proposal ike-phase1-proposal dh-group group2
admin@host# set proposal ike-phase1-proposal authentication-algorithm sha1
admin@host# set proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
```

4. Configure an IKE policy.

```
[edit security ike]
admin@host# set policy ike-phase1-policy mode main
admin@host# set policy ike-phase1-policy proposals ike-phase1-proposal
admin@host# set policy ike-phase1-policy pre-shared-key ascii-text 395psksecr3t
```

5. Configure an IKE gateway.

```
[edit security ike]
admin@host# set gateway ike-gw external-interface ge-0/0/3.0
admin@host# set gateway ike-gw ike-policy ike-phase1-policy
admin@host# set gateway ike-gw address 2.2.2.2
```

6. Configure an IPsec proposal.

```
[edit security ipsec]
admin@host# set proposal ipsec-phase2-proposal protocol esp
admin@host# set proposal ipsec-phase2-proposal authentication-algorithm
hmac-sha1-96
admin@host# set proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
```

7. Configure an IPsec policy.

```
[edit security ipsec]
admin@host# set policy vpn-policy1 proposals ipsec-phase2-proposal
admin@host# set policy vpn-policy1 perfect-forward-secrecy keys group2
```

8. Configure the VPN.

```
[edit security ipsec]
admin@host# set vpn ike-vpn bind-interface st0.1
admin@host# set vpn ike-vpn ike gateway ike-gw
admin@host# set vpn ike-vpn ike ipsec-policy vpn-policy1
```

9. Configure VPN monitoring.

```
[edit security ipsec]
admin@host# set vpn ike-vpn vpn-monitor source-interface st0.1
admin@host# set vpn ike-vpn vpn-monitor destination-ip 4.0.0.1
```

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

```
[edit]
admin@host# show interfaces
st0 {
  unit 1;
}
[edit]
admin@host# show security ike
proposal ike-phase1-proposal {
  authentication-method pre-shared-keys;
  dh-group group2;
  authentication-algorithm sha1;
  encryption-algorithm aes-128-cbc;
}
policy ike-phase1-policy {
  mode main;
  proposals ike-phase1-proposal;
  pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway ike-gw {
  ike-policy ike-phase1-policy;
  address 2.2.2.2;
  external-interface ge-0/0/3.0;
}
[edit]
admin@host# show security ipsec
proposal ipsec-phase2-proposal {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm aes-128-cbc;
}
policy vpn-policy1 {
```

```
perfect-forward-secrecy {
    keys group2;
}
proposals ipsec-phase2-proposal;
}
vpn ike-vpn {
    bind-interface st0.1;
    vpn-monitor {
        source-interface st0.1;
        destination-ip 4.0.0.1;
    }
    ike {
        gateway ike-gw;
        ipsec-policy vpn-policy1;
    }
}
```

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

Verification

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose Verify that the IKE and IPsec SA configuration is correct.

Action From operational mode, enter the **show security ike** and **show security ipsec** commands.

See Also

- [Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems on page 180](#)
- [Understanding Route-Based VPN Tunnels in Logical Systems on page 175](#)
- [User Logical Systems Configuration Overview on page 61](#)

Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems

This example shows how to configure a route-based VPN tunnel in a user logical system.

- [Requirements on page 180](#)
- [Overview on page 181](#)
- [Configuration on page 181](#)
- [Verification on page 183](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).

- Ensure that an st0 interface is assigned to the user logical system and IKE and IPsec SAs are configured at the root level by the master administrator. See [“Example: Configuring IKE and IPsec SAs for a VPN Tunnel \(Master Administrators Only\)”](#) on page 176.

Overview

In this example, you configure the ls-product-design user logical system as shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65.

You configure the route-based VPN parameters described in [Table 21](#) on page 181.

Table 21: User Logical System Route-Based VPN Configuration

Feature	Name	Configuration Parameters
Tunnel interface	st0 unit 1	<ul style="list-style-type: none"> • IPv4 protocol family (inet) • IP address 10.11.11.150/24
Static route		<ul style="list-style-type: none"> • Destination 192.168.168.0/24 • Next hop st0.1
Security policy	through-vpn	Permit the following traffic: <ul style="list-style-type: none"> • From zone: ls-product-design-trust • To zone: ls-product-design-untrust • Source address: any • Destination address: 192.168.168.0/24 • Application: any

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 interfaces st0 unit 1 family inet address 10.11.11.150/24
set routing-options static route 192.168.168.0/24 next-hop st0.1
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy through-vpn match source-address any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy through-vpn match destination-address 192.168.168.0/24
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy through-vpn match application any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
policy through-vpn 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 the Junos OS CLI User Guide.

To configure a route-based VPN tunnel in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
[edit]
lsdesignadmin1@host:ls-product-design>configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure the VPN tunnel interface.

```
[edit interfaces]
lsdesignadmin1@host:ls-product-design# set st0 unit 1 family inet address
10.11.11.150/24
```

3. Create a static route to the remote destination.

```
[edit routing-options]
lsdesignadmin1@host:ls-product-design# set static route 192.168.168.0/24 next-hop
st0.1
```

4. Configure a security policy to permit traffic to the remote destination.

```
[edit security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust]
lsdesignadmin1@host:ls-product-design# set policy through-vpn match
source-address any
lsdesignadmin1@host:ls-product-design# set policy through-vpn match
destination-address 192.168.168.0/24
lsdesignadmin1@host:ls-product-design# set policy through-vpn match application
any
lsdesignadmin1@host:ls-product-design# set policy through-vpn then permit
```

Results From configuration mode, confirm your configuration by entering the **show interfaces st0**, **show routing-options**, 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]
lsdesignadmin1@host:ls-product-design# show interfaces st0
unit 1 {
  family inet {
    address 10.11.11.150/24;
  }
}
lsdesignadmin1@host:ls-product-design# show routing-options
static {
  route 192.168.168.0/24 next-hop st0.1;
}
```

```
[edit]
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
  policy through-vpn {
    match {
      source-address any;
      destination-address 192.168.168.0/24;
      application any;
    }
    then {
      permit;
    }
  }
  ...
}
```

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

Verification

Confirm that the configuration is working properly.



NOTE: Before starting the verification process, you need to send traffic from a host in the user logical system to a host in the 192.168.168.0/24 network. For example, initiate a ping from a host in the 12.1.1.0/24 subnet in the ls-product-design user logical system to the host 192.168.168.10.

- [Verifying the IKE Phase 1 Status on page 183](#)
- [Verifying the IPsec Phase 2 Status on page 183](#)

Verifying the IKE Phase 1 Status

Purpose Verify the IKE Phase 1 status.

Action From operational mode, enter the **show security ike security-associations** command. After obtaining an index number from the command, use the **show security ike security-associations index *index_number* detail** command.

For sample outputs and meanings, see the “Verification” section of *Example: Configuring a Route-Based VPN*.

Verifying the IPsec Phase 2 Status

Purpose Verify the IPsec Phase 2 status.

Action From operational mode, enter the **show security ipsec security-associations** command. After obtaining an index number from the command, use the **show security ipsec security-associations index *index_number* detail** command.

For sample outputs and meanings, see the “Verification” section of *Example: Configuring a Route-Based VPN*.

- See Also**
- [Example: Configuring a Route-Based VPN](#).
 - [Understanding Route-Based VPN Tunnels in Logical Systems on page 175](#)
 - [User Logical Systems Configuration Overview on page 61](#)

- Related Documentation**
- [IPv6 Addresses in Logical Systems Overview on page 249](#)

UTM for Logical Systems

Unified threat management (UTM) provides multiple security features and services for SRX Series devices on the network, protecting users from security threats in a simplified way. UTM secures the logical systems from viruses, malware, or malicious attachments by scanning the incoming data using Deep Packet Inspection and prevents access to unwanted websites by installing Enhanced Web Filtering (EWf). For more information, see the following topics:

- [Understanding UTM Features in Logical Systems on page 184](#)
- [Example: Configuring UTM for the Master Logical System on page 185](#)
- [Example: Configuring UTM for a User Logical System on page 193](#)

Understanding UTM Features in Logical Systems

Unified Threat Management (UTM) in logical systems provides several security features such as antispam, antivirus, content filtering, and Web filtering to secure users from multiple Internet-borne threats. The advantage of UTM is streamlined installation and management of these multiple security capabilities. In logical systems the master administrator configures the UTM features for the master logical system. Configuring UTM features for logical systems is similar to configuring UTM features on a device that is not configured for logical systems.

The security features provided as part of the UTM solution are:

- **Antispam Filtering**—E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. The default antispam feature is configured at the master logical system and it is applicable for all the user logical systems.
- **Content Filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type. The default content filtering feature is configured at the master logical system and it is applicable for all the user logical systems.
- **Web Filtering**—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. The default Web filtering feature is configured at the

master logical system, and the user logical systems inherit these default Web filtering configuration.

- *Sophos Antivirus*—Sophos Antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. Sophos Antivirus is an in-the-cloud antivirus solution. The default antivirus feature is configured at the master logical system, and the user logical systems inherit these default antivirus configuration.

You must configure the custom objects for the Web filtering, anti-spam, and content filtering features before configuring the UTM features. You can configure custom objects for each user logical system.

The predefined UTM default policy parameters for Web filtering, content filtering, antivirus, and antispam profiles are configured at the master logical system. The user logical systems inherit the same antivirus and Web filtering features configured for the master logical system. The options such as **mime-whitelist** and **url-whitelist** in antivirus profile, and **address-blacklist** and **address-whitelist** in antispam profile can be configured at the following hierarchy levels, respectively:

- **[edit security utm feature-profile anti-virus sophos-engine profile]**
- **[edit security utm feature-profile anti-spam sbl profile]**

The options **url-whitelist** and **url-blacklist** are not supported in the Web filtering profile, you can use the custom category option to achieve the function.

Example: Configuring UTM for the Master Logical System

This example shows how to configure the UTM features antivirus, antispam, content filtering, and Web filtering in the master logical system. The master administrator is responsible for assigning the UTM features to the user logical systems.

- [Requirements on page 185](#)
- [Overview on page 186](#)
- [Configuration on page 186](#)
- [Verification on page 190](#)

Requirements

This example uses the following hardware and software components:

- SRX Series device configured with the logical systems.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand how to log in to the master logical system as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).
- Configure the interfaces, routing instances, and static routes for the master logical system. See [“Example: Configuring Interfaces, Routing Instances, and Static Routes](#)

for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Master Administrators Only)" on page 105.

Overview

By default, all system resources are assigned to the master logical system, and the master administrator allocates them to the user logical systems. The master administrator manages the device and the logical systems.

This example shows how to configure the UTM features described in [Table 22 on page 186](#) for the master logical system.

Table 22: UTM Configuration Type, Steps, and Parameters

Configuration Type	Configuration Description	Configuration Parameter
Custom objects	Configure the MIME (Multipurpose Internet Mail Extension) types (my_blockmime01) to decide which traffic is allowed to bypass various types of scanning	[multipart/ application/]
	Define a set of file extensions (my_fileextlist01) that are used in file extension scan mode (scan-by-extension)	[txt pl com zip]
	Configure a URL pattern list (black_list) of URLs or addresses that you want to block.	www.example.com
	Configure a custom URL category (cust_black) of URLs or addresses that you want to block.	black_list
Antispam	Configure the antispam type server-based spam block list (SBL).	sbl
Antivirus	Configure the antivirus type Sophos Antivirus (sophos-engine) profile (mysav) scan option to scan specific types of traffic.	uri-check
Web filtering	Specify an action for Enhanced Web Filtering (EWF) (juniper-enhanced) profile (myewf), for requests that experience internal errors in the Web filtering module.	log-and-permit

In this procedure, you define custom objects, configure feature profiles for UTM features (antispam, antivirus, content filtering, and Web filtering), configure a UTM policy and attach feature profiles, and apply the UTM policy to the security policy as an application service. For more information, see the *UTM Feature Guide for Security Devices*.

Configuration

CLI Quick Configuration To quickly configure this example, log in to the master logical system as the master administrator, 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 utm custom-objects mime-pattern my_blockmime01 value [ multipart/
application/ ]
set security utm custom-objects filename-extension my_fileextlist01 value [ txt pl com
zip ]
set security utm custom-objects url-pattern black_list value www.example.com
set security utm custom-objects custom-url-category cust_black value black_list
set security utm default-configuration anti-virus type sophos-engine
set security utm default-configuration web-filtering type juniper-enhanced
set security utm default-configuration web-filtering juniper-enhanced cache timeout
1800
set security utm default-configuration web-filtering juniper-enhanced cache size 0
set security utm default-configuration anti-spam type sbl
set security utm feature-profile anti-virus sophos-engine profile mysav scan-options
uri-check
set security utm feature-profile web-filtering juniper-enhanced profile myewf default
log-and-permit
set security utm utm-policy utm-p1 anti-virus http-profile mysav
set security utm utm-policy utm-p1 content-filtering http-profile junos-cf-defaults
set security utm utm-policy utm-p1 web-filtering http-profile myewf
set security utm utm-policy utm-p1 anti-spam smtp-profile junos-as-defaults
set security policies from-zone trust to-zone untrust policy p1 match source-address any
any
set security policies from-zone trust to-zone untrust policy p1 match application junos-http
set security policies from-zone trust to-zone untrust policy p1 then permit
application-services utm-policy utm-p1

```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the Junos OS CLI User Guide.

1. Log in to the master logical system as the master administrator and enter configuration mode.

```

admin@host> configure
admin@host#

```
2. Configure the custom objects for the master logical system.

```

[edit security utm custom-objects]
admin@host# set mime-pattern my_blockmime01 value [ multipart/ application/
]
admin@host# set filename-extension my_fileextlist01 value [ txt pl com zip ]
admin@host# set url-pattern black_list value www.example.com
admin@host# set custom-url-category cust_black value black_list

```
3. Define the UTM default configuration for the master logical system.

```

[edit security utm default-configuration]
admin@host# set anti-virus type sophos-engine
admin@host# set web-filtering type juniper-enhanced
admin@host# set web-filtering juniper-enhanced cache timeout 1800
admin@host# set web-filtering juniper-enhanced cache size 0
admin@host# set anti-spam type sbl

```

4. Configure the feature profile for the master logical system.

```
[edit security utm feature-profile]
admin@host# set anti-virus sophos-engine profile mysav scan-options uri-check
admin@host# set web-filtering juniper-enhanced profile myewf default
log-and-permit
```

5. Configure the UTM policy for the master logical system.

```
[edit security utm utm-policy]
admin@host# set utm-p1 anti-virus http-profile mysav
admin@host# set utm-p1 content-filtering http-profile junos-cf-defaults
admin@host# set utm-p1 web-filtering http-profile myewf
admin@host# set utm-p1 anti-spam smtp-profile junos-as-defaults
```

6. Configure the security policies for the master logical system.

```
[edit security policies]
admin@host# set from-zone trust to-zone untrust policy p1 match source-address
any
admin@host# set from-zone trust to-zone untrust policy p1 match
destination-address any
admin@host# set from-zone trust to-zone untrust policy p1 match application
junos-http
admin@host# set from-zone trust to-zone untrust policy p1 permit
application-services utm-policy utm-p1
```

Results

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

```
admin@host# show security
utm {
  custom-objects {
    mime-pattern {
      my_blockmime01 {
        value [ multipart/ application/ ];
      }
    }
    filename-extension {
      my_fileextlist01 {
        value [ txt pl com zip ];
      }
    }
    url-pattern {
      black_list {
        value www.example.com;
      }
    }
    custom-url-category {
      cust_black {
        value black_list;
      }
    }
  }
}
```

```

    }
  }
}
default-configuration {
  anti-virus {
    type sophos-engine;
  }
  web-filtering {
    type juniper-enhanced;
    juniper-enhanced {
      cache {
        timeout 1800;
        size 0;
      }
    }
  }
}
anti-spam {
  type sbl;
}
}
feature-profile {
  anti-virus {
    sophos-engine {
      profile mysav {
        scan-options {
          uri-check;
        }
      }
    }
  }
}
web-filtering {
  juniper-enhanced {
    profile myewf {
      default log-and-permit;
    }
  }
}
}
utm-policy utm-p1 {
  anti-virus {
    http-profile mysav;
  }
  content-filtering {
    http-profile junos-cf-defaults;
  }
  web-filtering {
    http-profile myewf;
  }
  anti-spam {
    smtp-profile junos-as-defaults;
  }
}
}
policies {
  from-zone trust to-zone untrust {
    policy p1 {

```

```
match {
  source-address any;
  destination-address any;
  application junos-http;
}
then {
  permit {
    application-services {
      utm-policy utm-p1;
    }
  }
}
}
```

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 Antivirus Configuration on page 190](#)
- [Verifying Antispam Configuration on page 191](#)
- [Verifying Content Filtering Configuration on page 192](#)
- [Verifying Web Filtering Configuration on page 192](#)

Verifying Antivirus Configuration

Purpose Verify that the antivirus feature is configured for the master logical system.

Action From operational mode, enter the **show security utm anti-virus statistics** command to view the details of the antivirus feature configured for the master logical system.

```
admin@host> show security utm anti-virus statistics
UTM Anti Virus statistics:
  MIME-whitelist passed:          0
  URL-whitelist passed:           0
  Session abort:                  0
  Scan Request:

      Total      Clean      Threat-found      Fallback
        9         7         1         1

Fallback:
           Log-and-Permit      Block      Permit
Engine not ready:      0         0         0
  Out of resources:    0         0         0
  Timeout:             0         0         0
Maximum content size:  1         0         0
Too many requests:    0         0         0
Others:               0         0         0
```

Meaning The output displays the antivirus statistics for the master logical system.

Verifying Antispam Configuration

Purpose Verify that the antispam feature is configured for the master logical system.

Action From operational mode, enter the **show security utm anti-spam statistics** command to view the details of the antispam feature configured for the master logical system.

```
admin@host> show security utm anti-spam statistics
UTM Anti Spam statistics:

Total connections:      1
Denied connections:    1
Total greetings:        0
Denied greetings:       0
Total e-mail scanned:  0
White list hit:         0
Black list hit:         0
Spam total:             0
Spam tagged:           0
Spam dropped:           0
DNS errors:             0
Timeout errors:         0
Return errors:          0
Invalid parameter errors: 0
```

Meaning The output displays the antispam statistics for the master logical system.

Verifying Content Filtering Configuration

Purpose Verify that the content filtering feature is configured for the master logical system.

Action From operational mode, enter the **show security utm content-filtering statistics** command to view the details of the content filtering feature configured for the master logical system.

```
admin@host> show security content-filtering statistics
Content-filtering-statistic:      Blocked
Base on command list:           0
Base on mime list:              1
Base on extension list:         0
ActiveX plugin:                 0
Java applet:                    0
EXE files:                      0
ZIP files:                      0
HTTP cookie:                    0
```

Meaning The output displays the content filtering statistics for the master logical system.

Verifying Web Filtering Configuration

Purpose Verify that the Web filtering feature is configured for the master logical system.

Action From operational mode, enter the **show security utm web-filtering statistics** command to view the details of the Web filtering feature configured for the master logical system.

```
admin@host> show security web-filtering statistics
UTM web-filtering statistics:
Total requests:                4
white list hit:                 1
Black list hit:                 1
Custom category permit:         1
Custom category block:          1
Custom category quarantine:      0
Custom category quarantine block: 0
Custom category quarantine permit: 0
Web-filtering sessions in total: 64000
Web-filtering sessions in use:   0
Fallback:                       log-and-permit      block
  Default                       0              0
  Timeout                       0              0
  Connectivity                   0              0
Too-many-requests               0              0
```

Meaning The output displays the Web filtering statistics for the master logical system.

Example: Configuring UTM for a User Logical System

This example shows how to configure the UTM features antivirus, antispyware, content filtering, and Web filtering for a user logical system. The master administrator creates a user logical system and assigns an administrator for managing the user logical system. A user logical system can have multiple user logical system administrators.

- [Requirements on page 193](#)
- [Overview on page 193](#)
- [Configuration on page 194](#)
- [Verification on page 198](#)

Requirements

This example uses the following hardware and software components:

- SRX Series device configured with the logical systems.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand the user logical system administrator role and functions. See [“Understanding User Logical Systems and the User Logical System Administrator Role” on page 63](#).
- Understand how to log in to the user logical system as an administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- This example shows how to configure the UTM features for the ls-product-design user logical system. To understand how to create the ls-product-design user logical system, see [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

Overview

The master administrator assigns the UTM features antivirus, antispyware, content filtering, and Web filtering to the user logical system. The user logical system administrator can configure and manage the UTM features for the user logical systems. The antispyware, antivirus and Web filtering features are configured in the master logical system are described in [Table 23 on page 194](#). All the user logical systems can use the same antispyware, antivirus and Web filtering features with the same profile.

Table 23: UTM Configuration Type, Steps, and Parameters

Configuration Type	Configuration Description	Configuration Parameter
Custom objects	Configure a URL pattern (url1) of URL patterns that bypass scanning.	<i>www.abc.com</i>
	Configure a custom URL category (cust1) of URLs or addresses list that bypass scanning.	<i>url1</i>
	Configure a custom message type (redirect-url) to redirect traffic destined for protected sources.	<i>http://www.example1.com.cn</i>
Antispam	Configure antispam profile (as1) spam action.	<i>block</i>
Antivirus	Configure antivirus profile (sav1) fallback option.	<i>log-and-permit</i>
	Configure antivirus profile (sav1) scan option.	<i>uri-check</i>
Web filtering	Configure Web filtering profile (ewf1) category (cust1) action.	<i>block</i>
	Configure Web filtering profile (ewf1) category (cust1) custom message.	<i>custmsg1</i>
	Configure Web filtering profile (ewf1) category (Enhanced_Search_Engines_and_Portals) action.	<i>block</i>
	Specify an action for Enhanced Web Filtering (EWF) (juniper-enhanced) profile (ewf1), for requests that experience internal errors in the Web filtering module.	<i>log-and-permit</i>

Configuration

CLI Quick Configuration

To quickly configure this example, log in to the ls-product-design user logical system as the administrator, 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 utm custom-objects url-pattern url1 value www.abc.com
set security utm custom-objects custom-url-category cust1 value url1
set security utm custom-objects custom-message cust-msg1 type redirect-url content
http://www.example1.com.cn
```

```

set security utm feature-profile anti-virus sophos-engine profile sav1 fallback-options
  default log-and-permit
set security utm feature-profile anti-virus sophos-engine profile sav1 scan-options
  uri-check
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 category cust1
  action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 category cust1
  custom-message custmsg1
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 category
  Enhanced_Search_Engines_and_Portals action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 default
  log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf2 default
  log-and-permit
set security utm feature-profile anti-spam sbl profile as1 spam-action block
set security utm utm-policy utm-p1 anti-virus http-profile sav1
set security utm utm-policy utm-p1 web-filtering http-profile juniper-enhanced
set security utm utm-policy utm-p1 anti-spam smtp-profile as1
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
  policy sec_policy match source-address any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
  policy sec_policy match destination-address any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
  policy sec_policy match application any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
  policy sec_policy then permit application-services utm-policy utm-p1

```

Step-by-Step Procedure

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

1. Log in to the ls-product-design user logical system as the administrator and enter configuration mode.

```

lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#

```

2. Configure the custom objects for the ls-product-design user logical system.

```

[edit security utm custom-objects]
lsdesignadmin1@host:ls-product-design# set url-pattern url1 value www.abc.com
lsdesignadmin1@host:ls-product-design# set custom-url-category cust1 value url1
lsdesignadmin1@host:ls-product-design# set custom-message cust-msg1 type
  redirect-url content http://www.example1.com.cn

```

3. Configure the feature profiles for the ls-product-design user logical system.

```

[edit security utm feature-profile]
lsdesignadmin1@host:ls-product-design# set anti-virus sophos-engine profile sav1
  fallback-options default log-and-permit
lsdesignadmin1@host:ls-product-design# set anti-virus sophos-engine profile sav1
  scan-options uri-check
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile
  ewf1 category cust1 action block

```

```

lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile
ewf1 category cust1 custom-message custmsg1
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile
ewf1 category Enhanced_Search_Engines_and_Portals action block
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile
ewf1 default log-and-permit
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile
ewf2 default log-and-permit
lsdesignadmin1@host:ls-product-design# set anti-spam sbl profile as1 spam-action
block

```

4. Configure the UTM policy for the ls-product-design user logical system.

```

[edit security utm utm-policy]
lsdesignadmin1@host:ls-product-design# set utm-p1 anti-virus http-profile sav1
lsdesignadmin1@host:ls-product-design# set utm-p1 web-filtering http-profile
juniper-enhanced
lsdesignadmin1@host:ls-product-design# set utm-p1 anti-spam smtp-profile as1

```

5. Configure the security policies for the ls-product-design user logical system.

```

[edit security policies]
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone
lsys1-untrust policy sec_policy match source-address any
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone
lsys1-untrust policy sec_policy match destination-address any
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone
lsys1-untrust policy sec_policy match application any
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone
lsys1-untrust policy sec_policy then permit application-services utm-policy utm-p1

```

Results

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

```

lsdesignadmin1@host:ls-product-design# show security
utm {
  custom-objects {
    url-pattern {
      url1 {
        value www.abc.com;
      }
    }
    custom-url-category {
      cust1 {
        value url1;
      }
    }
  }
  custom-message {
    cust-msg1 {
      type redirect-url;
      content http://www.example1.com.cn;
    }
  }
}

```

```

    }
  }
}
feature-profile {
  anti-virus {
    sophos-engine {
      profile sav1 {
        fallback-options {
          default log-and-permit;
        }
        scan-options {
          uri-check;
        }
      }
    }
  }
}
web-filtering {
  juniper-enhanced {
    profile ewf1 {
      category {
        cust1 {
          action block;
          custom-message custmsg1;
        }
        Enhanced_Search_Engines_and_Portals {
          action block;
        }
      }
      default log-and-permit;
    }
    profile ewf2 {
      default log-and-permit;
    }
  }
}
anti-spam {
  sbl {
    profile as1 {
      spam-action block;
    }
  }
}
utm-policy utm-p1 {
  anti-virus {
    http-profile sav1;
  }
  web-filtering {
    http-profile juniper-enhanced;
  }
  anti-spam {
    smtp-profile as1;
  }
}
}
policies {

```

```
from-zone ls-product-design-trust to-zone ls-product-design-untrust {  
  policy sec_policy {  
    match {  
      source-address any;  
      destination-address any;  
      application any;  
    }  
    then {  
      permit {  
        application-services {  
          utm-policy utm-p1;  
        }  
      }  
    }  
  }  
}
```

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 Antivirus Configuration on page 198](#)
- [Verifying Antispam Configuration on page 199](#)
- [Verifying Content Filtering Configuration on page 200](#)
- [Verifying Web Filtering Configuration on page 201](#)

Verifying Antivirus Configuration

Purpose Verify that the antivirus feature is configured for the ls-product-design user logical system.

Action From operational mode, enter the **show security utm anti-virus statistics** command to view the antivirus statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security utm anti-virus statistics
UTM Anti Virus statistics:
  MIME-whitelist passed:          0
  URL-whitelist passed:           0
  Session abort:                  0
  Scan Request:

      Total          Clean          Threat-found      Fallback
        9             7             1             1

Fallback:
           Log-and-Permit      Block      Permit
Engine not ready:      0          0          0
  Out of resources:    0          0          0
  Timeout:             0          0          0
Maximum content size:  1          0          0
Too many requests:    0          0          0
Others:
```

Meaning The output displays the antivirus statistics information for the ls-product-design user logical system.

Verifying Antispam Configuration

Purpose Verify that the antispam feature is configured for the ls-product-design user logical system.

Action From operational mode, enter the **show security utm anti-spam statistics** command to view the antispam statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security utm anti-spam statistics
UTM Anti Spam statistics:

Total connections:      1
Denied connections:    1
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:          0
Spam dropped:          0
DNS errors:            0
Timeout errors:       0
Return errors:         0
Invalid parameter errors: 0
```

Meaning The output displays the antispam statistics information for the ls-product-design user logical system.

Verifying Content Filtering Configuration

Purpose Verify that the content filtering feature is configured for the ls-product-design user logical system.

Action From operational mode, enter the **show security utm content-filtering statistics** command to view the content filtering statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security content-filtering statistics
Content-filtering-statistic:      Blocked
Base on command list:            0
Base on mime list:               1
Base on extension list:         0
ActiveX plugin:                  0
Java applet:                     0
EXE files:                       0
ZIP files:                       0
HTTP cookie:                     0
```

Meaning The output displays the content filtering statistics information for the ls-product-design user logical system.

Verifying Web Filtering Configuration

Purpose Verify that the Web filtering feature is configured for the ls-product-design user logical system.

Action From operational mode, enter the **show security utm web-filtering statistics** command to view the Web filtering statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security web-filtering statistics
UTM web-filtering statistics:
  Total requests:                4
  white list hit:                1
  Black list hit:                1
  Custom category permit:       1
  Custom category block:        1
  Custom category quarantine:    0
  Custom category quarantine block: 0
  Custom category quarantine permit: 0
  Web-filtering sessions in total: 64000
  Web-filtering sessions in use: 0
  Fallback:      log-and-permit      block
    Default      0                  0
    Timeout      0                  0
    Connectivity 0                  0
  Too-many-requests 0                0
```

Meaning The output displays the Web filtering statistics information for the ls-product-design user logical system.

IDP for Logical Systems

An Intrusion Detection and Prevention (IDP) policy in logical systems enables you to selectively enforce various attack detection and prevention techniques on the network traffic passing through your SRX Series. The SRX Series offer the same set of IDP signatures that are available on Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to secure networks against attacks. For more information, see the following topics:

- [IDP in Logical Systems Overview on page 202](#)
- [Understanding IDP Features in Logical Systems on page 204](#)
- [Example: Configuring an IDP Policy for the Master Logical Systems on page 206](#)
- [Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System on page 212](#)
- [Example: Enabling IDP in a User Logical System Security Policy on page 214](#)
- [Example: Configuring an IDP Policy for a User Logical System on page 217](#)

IDP in Logical Systems Overview

A Junos OS Intrusion Detection and Prevention (IDP) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through a logical system.

This topic includes the following sections:

- [IDP Policies on page 202](#)
- [Limitation on page 203](#)
- [IDP Installation and Licensing for Logical Systems on page 203](#)

IDP Policies

The master administrator configures IDP policies at the root level. Configuring an IDP policy for logical systems is similar to configuring an IDP policy on a device that is not configured for logical systems. This can include the configuration of custom attack objects.

IDP policy templates installed in root logical system are visible and used by all logical systems.

The master administrator then specifies an IDP policy in the security profile that is bound to a logical system. To enable IDP in a logical system, the master administrator or user logical system administrator configures a security policy that defines the traffic to be inspected and specifies the **permit application-services idp** action.

Although the master administrator can configure multiple IDP policies, a logical system can have only one active IDP policy at a time. For user logical systems, the master administrator can either bind the same IDP policy to multiple user logical systems or bind a unique IDP policy to each user logical system. To specify the active IDP policy for the master logical system, the master administrator can *either* reference the IDP policy in the security profile that is bound to the master logical system or use the **active-policy** configuration statement at the **[edit security idp]** hierarchy level.

The root administrator configures the number of maximum IDP sessions reservation for a root and user logical system. The number of IDP sessions that are allowed for a root logical system are defined using the command **set security idp max-sessions max-sessions** and the number of IDP sessions that are allowed for a user logical system are defined using the command **set security idp logical-system logical-system max-sessions max-sessions**.



NOTE: A commit error is generated if an IDP policy is both configured in the security profile that is bound to the master logical system and specified with the **active-policy** configuration statement. Use only one method to specify the active IDP policy for the master logical system.



NOTE: If you have configured more than one IDP policy in a security policy, then configuring default IDP policy configuration is mandatory.

A default IDP policy configuration is supported when multiple IDP policies are available. The default IDP policy is one of the multiple IDP policies. For more information about configuring multiple IDP policies and default IDP policy, see the *IDP Policy Selection for Unified Policies*.

The logical system administrator performs the following actions:

- Configure multiple IDP policies and attach to the firewall policies to be used by the user logical systems. If the IDP policy is not configured for a user logical system, the default IDP policy configured by the master administrator is used. The IDP policy is bound to the user logical systems through a logical systems security policy.
- Create or modify IDP policies for their user logical systems. The IDP policies are bound to user logical systems. When an IDP policy is changed, and commit succeeds, the existing sessions mapped to current active policy continue to use the old IDP combined policy. When an IDP policy is changed, and commit fails, only the logical system user that has initiated the commit change is notified about the commit failure.
- The logical system can create security zones in the user logical system and assign interfaces to each security zone. Zones that are specific to user logical systems cannot be referenced in IDP policies configured by the master administrator. The master administrator can reference zones in the master logical system in an IDP policy configured for the master logical system.
- View the attack statistics detected and IDP counters, attack table, and policy commit status by the individual logical system using the commands **show security idp counters**, **show security idp attack table**, **show security idp policies**, **show security idp policy-commit-status**, and **show security idp security-package-version**.

Limitation

- When a IDP policy is changed and compiled in a specific user logical system, this change is considered as a single global policy change and compiled for all policies of all the logical systems.

IDP Installation and Licensing for Logical Systems

An idp-sig license must be installed at the root level. Once IDP is enabled at the root level, it can be used with any logical system on the device.

A single IDP security package is installed for all logical systems on the device at the root level. The download and install options can only be executed at the root level. The same version of the IDP attack database is shared by all logical systems.

See Also • [User Logical Systems Configuration Overview on page 61](#)

- [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
- [IDP Policies Overview](#)

Understanding IDP Features in Logical Systems

This topic includes the following sections:

- [Rulebases on page 204](#)
- [Protocol Decoders on page 204](#)
- [SSL Inspection on page 204](#)
- [Inline Tap Mode on page 205](#)
- [Multi-Detectors on page 205](#)
- [Logging and Monitoring on page 205](#)

Rulebases

A single IDP policy can contain only one instance of any type of rulebase. The following IDP rulebases are supported for logical systems:

- The Intrusion prevention system (IPS) rulebase uses attack objects to detect known and unknown attacks. It detects attacks based on stateful signature and protocol anomalies.
- The application-level distributed denial-of-service (DDoS) rulebase defines parameters to protect servers such as DNS or HTTP. The application-level DDoS rulebase defines the source match condition for traffic that should be monitored and takes an action, such as drop the connection, drop the packet, or no action. It can also perform actions against future connections that use the same IP address.



NOTE: Status monitoring for IPS and application-level DDoS is global to the device and not on a per logical system basis.

Protocol Decoders

The Junos IDP module ships with a set of preconfigured protocol decoders. These protocol decoders have default settings for various protocol-specific contextual checks that they perform. The IDP protocol decoder configuration is global and applies to all logical systems. Only the master administrator at the root level can modify the settings at the `[edit security idp sensor-configuration]` hierarchy level.

SSL Inspection

IDP SSL inspection uses the Secure Sockets Layer (SSL) protocol suite to enable inspection of HTTP traffic encrypted in SSL.

SSL inspection configuration is global and applies to all logical systems on a device. SSL inspection can only be configured by the master administrator at the root level with the

ssl-inspection configuration statement at the [**edit security idp sensor-configuration**] hierarchy level.

Inline Tap Mode

The inline tap mode feature provides passive, inline detection of Application Layer threats for traffic matching security policies that have the IDP application service enabled. When a device is in inline tap mode, packets pass through firewall inspection and are also copied to the independent IDP module. This allows the packets to get to the next service module without waiting for IDP processing results.

Inline tap mode is enabled or disabled for all logical systems at the root level by the master administrator. To enable inline tap mode, use the **inline-tap** configuration statement at the [**edit security forwarding-process application-services maximize-idp-sessions**] hierarchy level. Delete the inline tap mode configuration to switch the device back to regular mode.



NOTE: The device must be restarted when switching to inline tap mode or back to regular mode.

Multi-Detectors

When a new IDP security package is received, it contains attack definitions and a detector. After a new policy is loaded, it is also associated with a detector. If the policy being loaded has an associated detector that matches the detector already in use by the existing policy, the new detector is not loaded and both policies use a single associated detector. But if the new detector does not match the current detector, the new detector is loaded along with the new policy. In this case, each loaded policy will then use its own associated detector for attack detection.

The version of the detector is common to all logical systems.

Logging and Monitoring

Status monitoring options are available to the master administrator only. All status monitoring options under the **show security idp** and **clear security idp** CLI operational commands present global information, but not on a per logical system basis.



NOTE: SNMP monitoring for IDP is not supported on logical systems.

IDP generates event logs when an event matches an IDP policy rule in which logging is enabled.

The logical systems identification is added to the following types of IDP traffic processing logs:

- Attack logs. The following example shows an attack log for the ls-product-design logical system:

```
Feb 22 14:06:00 aqgp01fw01 RT_IDP: %-IDP_ATTACK_LOG_EVENT_LS: Lsys A01:
IDP: At 1329883555, ANOMALY Attack log <10.1.128.200/33699->192.168.22.84/80>
for TCP protocol and service HTTP application NONE by rule 4 of rulebase
IPS in policy Policy1. attack: repeat=3, action=NONE, threat-severity=INFO,
name=HTTP:AUDIT:URL, NAT <0.0.0.0->0.0.0.0>, time-elapsed=0, inbytes=0,
outbytes=0, inpackets=0, outpackets=0,
intf:NSS-Mgmt:reth0.55->SIEM-MGMT:reth0.60, packet-log-id: 0 and misc-message
```



NOTE: In the IDP attack detection event log message (IDP_ATTACK_LOG_EVENT_LS), the time-elapsed, inbytes, outbytes, inpackets, and outpackets fields are not populated.

- IP action logs. The following example shows an IP action log for the ls-product-design logical system:

```
Oct 13 16:56:04 8.0.0.254 RT_IDP: IDP_ATTACK_LOG_EVENT_LS: IDP: In
ls-product-design at 1287014163, TRAFFIC Attack log
<25.0.0.1/34802->15.0.0.1/21> for TCP protocol and service SERVICE_NONE
application NONE by rule 1 of rulebase IPS in policy Recommended. attack:
repeat=0, action=TRAFFIC_IPACTION_NOTIFY, threat-severity=INFO, name=_, NAT
<0.0.0.0->0.0.0.0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0,
outpackets=0,
intf:ls-product-design-trust:ge-0/0/1.0->ls-product-design-untrust:plt0.3,
packet-log-id: 0 and misc-message -
```

- Application DDoS logs. The following example shows an application DDoS log for the ls-product-design logical system:

```
Oct 11 16:29:57 8.0.0.254 RT_IDP: IDP_APPDDOS_APP_ATTACK_EVENT_LS: DDOS
Attack in ls-product-design at 1286839797 on my-http,
<ls-product-design-untrust:ge-0/0/0.0:4.0.0.1:33738->ls-product-design-trust:ge-0/0/1.0:5.0.0.1:80>
for TCP protocol and service HTTP by rule 1 of rulebase DDOS in policy
Recommended. attack: repeats 0 action DROP threat-severity INFO,
connection-hit-rate 0, context-name http-url-parsed, hit-rate 6,
value-hit-rate 6 time-scope PEER time-count 2 time-period 10 secs, context
value: ascii: /abc.html hex: 2f 61 62 63 2e 68 74 6d 6c
```

- See Also**
- [Understanding IDP Policy Rule Bases](#)
 - [Understanding IDP Protocol Decoders](#)
 - [IDP SSL Overview](#)
 - [Understanding IDP Inline Tap Mode](#)
 - [Understanding Multiple IDP Detector Support](#)
 - [Understanding IDP Logging](#)

Example: Configuring an IDP Policy for the Master Logical Systems

This example shows how to configure an IDP policy in a master logical system.

- [Requirements on page 207](#)
- [Overview on page 207](#)

- [Configuration on page 208](#)
- [Verification on page 212](#)

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).
- Read [“IDP in Logical Systems Overview” on page 202](#).
- Use the **show system security-profile** command to see the resources allocated to the master logical system.

Overview

In this example you configure a custom attack that is used in an IDP policy. The IDP policy is specified in a security profile that is applied to the master logical system. IDP is then enabled in a security policy configured in the master logical system.

You configure the features described in [Table 24 on page 207](#).

Table 24: IDP Configuration for the Master Logical System

Feature	Name	Configuration Parameters
Custom attack	http-bf	<ul style="list-style-type: none"> • Severity critical • Detect three attacks between source and destination addresses of sessions. • Stateful signature attack type with the following characteristics: <ul style="list-style-type: none"> • location http-url-parsed • pattern .*juniper.* • client to server traffic
IPS rulebase policy	root-idp-policy	Match: <ul style="list-style-type: none"> • application default • http-bf custom attacks Action: <ul style="list-style-type: none"> • drop-connection • notification log-attacks
Logical system security profile	master-profile (previously configured and applied to root-logical-system)	Add IDP policy root-idp-policy.
Security policy	enable-idp	Enable IDP in a security policy that matches any traffic from the lsys-root-untrust zone to the lsys-root-trust zone.



NOTE: A logical system can have only one active IDP policy at a time. To specify the active IDP policy for the master logical system, the master administrator can reference the IDP policy in the security profile that is bound to the master logical system as shown in this example. Alternatively, the master administrator can use the active-policy configuration statement at the `[edit security idp]` hierarchy level.

A commit error is generated if an IDP policy is both configured in the security profile that is bound to the master logical system and specified with the active-policy configuration statement. Use only one method to specify the active IDP policy for the master logical system.

Configuration

- [Configuring a Custom Attack on page 208](#)
- [Configuring an IDP Policy for the Master Logical System on page 209](#)
- [Enabling IDP in a Security Policy on page 211](#)

Configuring a Custom Attack

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 idp custom-attack http-bf severity critical
set security idp custom-attack http-bf time-binding count 3
set security idp custom-attack http-bf time-binding scope peer
set security idp custom-attack http-bf attack-type signature context http-url-parsed
set security idp custom-attack http-bf attack-type signature pattern .*juniper.*
set security idp custom-attack http-bf attack-type signature direction client-to-server
```

Step-by-Step Procedure

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

To configure a custom attack object:

1. Log in to the master logical system as the master administrator and enter configuration mode.

```
[edit]
admin@host> configure
admin@host#
```

2. Create the custom attack object and set the severity level.

```
[edit security idp]
admin@host# set custom-attack http-bf severity critical
```


3. Configure attack detection parameters.

```
[edit security idp]
admin@host# set custom-attack http-bf time-binding count 3
admin@host# set custom-attack http-bf time-binding scope peer
```

4. Configure stateful signature parameters.

```
[edit security idp]
admin@host# set custom-attack http-bf attack-type signature context
http-url-parsed
admin@host# set custom-attack http-bf attack-type signature pattern .*juniper.*
admin@host# set custom-attack http-bf attack-type signature direction
client-to-server
```

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

```
[edit]
admin@host# show security idp custom-attack http-bf
severity critical;
time-binding {
  count 3;
  scope peer;
}
attack-type {
  signature {
    context http-url-parsed;
    pattern .*juniper.*;
    direction client-to-server;
  }
}
```

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

Configuring an IDP Policy for the Master Logical System

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 idp idp-policy root-idp-policy rulebase-ips rule 1 match application default
set security idp idp-policy root-idp-policy rulebase-ips rule 1 match attacks custom-attacks
http-bf
set security idp idp-policy root-idp-policy rulebase-ips rule 1 then action drop-connection
set security idp idp-policy root-idp-policy rulebase-ips rule 1 then notification log-attacks
set system security-profile master-profile idp-policy root-idp-policy
```

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 an IDP policy:

1. Create the IDP policy and configure match conditions.

```
[edit security idp]
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 match application
default
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 match attacks
custom-attacks http-bf
```

2. Configure actions for the IDP policy.

```
[edit security idp]
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 then action
drop-connection
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 then notification
log-attacks
```

3. Add the IDP policy to the security profile.

```
[edit system security-profile master-profile]
admin@host# set idp-policy lsys1-idp-policy
```

Results From configuration mode, confirm your configuration by entering the **show security idp idp-policy root-idp-policy** and **show system security-profile master-profile** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
admin@host# show security idp idp-policy root-idp-policy
rulebase-ips {
  rule 1 {
    match {
      application default;
      attacks {
        custom-attacks http-bf;
      }
    }
    then {
      action {
        drop-connection;
      }
      notification {
        log-attacks;
      }
    }
  }
}
admin@host# show system security-profile master-profile
```

```
...
idp-policy lsys1-idp-policy;
```

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

Enabling IDP in a Security Policy

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 lsys-root-untrust to-zone lsys-root-trust policy enable-idp
  match source-address any
set security policies from-zone lsys-root-untrust to-zone lsys-root-trust policy enable-idp
  match destination-address any
set security policies from-zone lsys-root-untrust to-zone lsys-root-trust policy enable-idp
  match application any
set security policies from-zone lsys-root-untrust to-zone lsys-root-trust policy enable-idp
  then permit application-services idp
```

Step-by-Step Procedure To enable IDP in a security policy:

1. Create the security policy and configure match conditions.


```
[edit security policies from-zone lsys-root-untrust to-zone lsys-root-trust]
admin@host# set policy enable-idp match source-address any
admin@host# set policy enable-idp match destination-address any
admin@host# set policy enable-idp match application any
```
2. Enable IDP.


```
[edit security policies from-zone lsys-root-untrust to-zone lsys-root-trust]
admin@host# set policy enable-idp then permit application-services idp
```

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.

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]
admin@host# show security policies
from-zone lsys-root-untrust to-zone lsys-root-trust {
  policy enable-idp {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
```

```
    permit {  
      application-services {  
        idp;  
      }  
    }  
  }  
}  
...  
}
```

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

Verification

Verifying Attack Matches

Purpose Verify that attacks are being matched in network traffic.

Action From operational mode, enter the **show security idp attack table** command.

```
admin@host> show security idp attack table  
IDP attack statistics:  
Attack name                               #Hits  
http-bf                                   1
```

See Also

- [IDP in Logical Systems Overview on page 202](#)
- [SRX Series Logical Systems Master Administrator Configuration Tasks Overview on page 41](#)

Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System

The master administrator can *either* download predefined IDP policies to the device or configure custom IDP policies at the root level using custom or predefined attack objects. The master administrator is responsible for assigning an IDP policy to a user logical system. This example shows how to assign a predefined IDP policy to a user logical system.

- [Requirements on page 212](#)
- [Overview on page 213](#)
- [Configuration on page 213](#)
- [Verification on page 214](#)

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).
- Read *IDP Policies Overview*.

- Assign the ls-design-profile security policy to the ls-product-design user logical system. See [“Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\)”](#) on page 79.
- Download predefined IDP policy templates to the device. See *Downloading and Using Predefined IDP Policy Templates (CLI Procedure)*.



NOTE: Activating a predefined IDP policy with the active-policy configuration statement at the [edit security idp] hierarchy level only applies to the master logical system. For a user logical system, the master administrator specifies the active IDP policy in the security profile that is bound to the user logical system.

Overview

The predefined IDP policy named Recommended contains attack objects recommended by Juniper Networks. All rules in the policy have their actions set to take the recommended action for each attack object. You add the Recommended IDP policy to the ls-design-profile, which is bound to the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System”](#) on page 65.

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 system security-profile ls-design-profile idp-policy Recommended
```

Step-by-Step Procedure

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

To add a predefined IDP policy to a security profile for a user logical system:

1. Log in to the master logical system as the master administrator and enter configuration mode.

```
[edit]
admin@host> configure
admin@host#
```

2. Add the IDP policy to the security profile.

```
[edit system security-profile]
admin@host# set ls-design-profile idp-policy Recommended
```

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

```
[edit]
admin@host# show security idp
  idp-policy Recommended {
    ...
  }
[edit]
admin@host# show system security-profile ls-design-profile
  policy {
    ...
  }
  idp-policy Recommended;
  logical-system ls-product-design;
```

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

Verification

Verifying the Configuration

Purpose Verify the IDP policy assigned to the logical system.

Action From operational mode, enter the **show security idp logical-system policy-association** command. Ensure that the IDP policy in the security profile that is bound to the logical system is correct.

```
admin@host> show security idp logical-system policy-association
Logical system      IDP policy
ls-product-design   Recommended
```

See Also

- [Example: Enabling IDP in a User Logical System Security Policy on page 214](#)
- [IDP in Logical Systems Overview on page 202](#)
- [User Logical Systems Configuration Overview on page 61](#)

Example: Enabling IDP in a User Logical System Security Policy

This example shows how to enable IDP in a security policy in a user logical system.

- [Requirements on page 215](#)
- [Overview on page 215](#)
- [Configuration on page 215](#)
- [Verification on page 217](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Use the **show system security-profiles idp-policy** command to see the security policy resources allocated to the logical system.
- Configure an IDP security policy for the user logical system as the master administrator. See [“Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System” on page 212](#).

Overview

In this example, you configure the ls-product-design user logical system as shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

You enable IDP in a security policy that matches any traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone. Enabling IDP in a security policy directs matching traffic to be checked against the IDP rulebases.



.....

NOTE: This example uses the IDP policy configured and assigned to the ls-product-design user logical system by the master administrator in [“Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System” on page 212](#).

.....

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 ls-product-design-untrust to-zone ls-product-design-trust
policy enable-idp match source-address any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy enable-idp match destination-address any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy enable-idp match application any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
policy enable-idp then permit application-services idp
```

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

To configure a security policy to enable IDP in a user logical system:

1. Log in to the logical system as the user logical system administrator and enter configuration mode.

```
[edit]
lsdesignadmin1@host:ls-product-design>configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security policy that matches traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone.

```
[edit security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy enable-idp match source-address
any
lsdesignadmin1@host:ls-product-design# set policy enable-idp match
destination-address any
lsdesignadmin1@host:ls-product-design# set policy enable-idp match application
any
```

3. Configure the security policy to enable IDP for matching traffic.

```
[edit security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy enable-idp then permit
application-services idp
```

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.

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]
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-untrust to-zone ls-product-design-trust {
  policy enable-idp {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          idp;
        }
      }
    }
  }
}
```



```

    }
  }
}
...
}

```

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

Verification

Verifying Attack Matches

Purpose Verify that attacks are being matched in network traffic.

Action From operational mode, enter the **show security idp attack table** command.

```

admin@host> show security idp attack table
IDP attack statistics:
  Attack name                               #Hits
  FTP:USER:ROOT                             1

```

- See Also**
- [Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System on page 212](#)
 - [IDP in Logical Systems Overview on page 202](#)
 - [User Logical Systems Configuration Overview on page 61](#)

Example: Configuring an IDP Policy for a User Logical System

This example shows how to configure and assign an IDP policy to a user logical system. After assigning the IDP policy, the traffic is sent from client to check for the attack detection on the configured custom attack.

- [Requirements on page 217](#)
- [Overview on page 218](#)
- [Configuration on page 218](#)
- [Verification on page 222](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 18.3R1 and later
- an SRX4200 device

Before you configure IDP policy on user logical system:

- Configure security zones. See [“Example: Configuring Security Zones for a User Logical Systems” on page 141](#).

Overview

In this example, you configure a custom attack that is used in an IDP policy. The IDP policy is specified and enabled using a security policy configured in the user logical system.

Configuration

To configure IDP in a user logical system:

- [Configuring a user logical system on page 218](#)
- [Configuring a Custom Attack on page 218](#)
- [Configuring an IDP Policy for the User Logical System on page 220](#)
- [Enabling IDP in a Security Policy on page 221](#)

Configuring a user logical system

Step-by-Step Procedure

To configure a user logical system:

1. Configure a user logical system.

```
[edit]
user@host# set logical-system LSYS1
```
2. Exit from the configuration mode and enter to the operational mode.

```
user@host# exit
```
3. Login as LSYS1 user to the user logical sytem and enter to configuration mode.

```
user@host> set cli logical-system LSYS1
user@host:LSYS1> edit
user@host:LSYS1#
```

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

```
[edit]
user@host# show logical-systems
LSYS1 {
}
```

Configuring a Custom Attack

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 idp custom-attack my-http severity info
set security idp custom-attack my-http attack-type signature protocol-binding application
  HTTP
set security idp custom-attack my-http attack-type signature context http-get-url
set security idp custom-attack my-http attack-type signature pattern .*test.*
set security idp custom-attack my-http attack-type signature direction any
```

Step-by-Step Procedure

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

To configure a custom attack object:

1. Log in to the user logical system as LSYS1 and enter configuration mode.

```
[edit]
user@host:LSYS1#
```

2. Create the custom attack object and set the severity level.

```
[edit security idp]
user@host:LSYS1# set custom-attack my-http severity info
```

3. Configure stateful signature parameters.

```
[edit security idp]
user@host:LSYS1# set custom-attack my-http attack-type signature
  protocol-binding application HTTP
user@host:LSYS1# set custom-attack my-http attack-type signature context
  http-get-url
user@host:LSYS1# set custom-attack my-http attack-type signature pattern .*test.*
user@host:LSYS1# set custom-attack my-http attack-type signature direction any
```

Results

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

```
[edit]
user@host:LSYS1# show security idp custom-attack my-http
severity info;
  attack-type {
    signature {
      protocol-binding {
        application HTTP;
      }
      context http-get-url;
      pattern .*test.*;
      direction any;
    }
  }
}
```

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

Configuring an IDP Policy for the User Logical System

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 idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match destination-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match application default
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks custom-attacks
  my-http
set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
```

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 an IDP policy:

1. Create the IDP policy and configure match conditions.

```
[edit security idp]
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match from-zone
  any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match source-address
  any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match to-zone any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match
  destination-address any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match application
  default
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks
  custom-attacks my-http
```

2. Configure actions for the IDP policy.

```
[edit security idp]
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 then action no-action
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 then notification
  log-attacks
```

Results From configuration mode, confirm your configuration by entering the **show security idp idp-policy idpengine** and **show system security-profile master-profile** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host:LSYS1# show security idp idp-policy idpengine
rulebase-ips {
  rule 1 {
    match {
      from-zone any;
      source-address any;
      to-zone any;
      destination-address any;
      application default;
      attacks {
        custom-attacks my-http;
      }
    }
    then {
      action {
        no-action;
      }
      notification {
        log-attacks;
      }
    }
  }
}

```

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

Enabling IDP in a Security Policy

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 z1 to-zone z2 policy p1 match source-address any
set security policies from-zone z1 to-zone z2 policy p1 match destination-address any
set security policies from-zone z1 to-zone z2 policy p1 match application any
set security policies from-zone z1 to-zone z2 policy p1 then permit application-services
idp-policy idpengine

```

Step-by-Step Procedure To enable IDP in a security policy:

1. Create the security policy and configure match conditions.

```

[edit security policies from-zone z1 to-zone z2]
user@host:LSYS1# set policy p1 match source-address any
user@host:LSYS1# set policy p1 match destination-address any
user@host:LSYS1# set policy p1 match application any

```

2. Enable IDP.

```

[edit security policies from-zone z1 to-zone z2]
user@host:LSYS1# set policy p1 then permit application-services idp-policy idpengine

```

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

```
[edit]
user@host:LSYS1# show security policies
from-zone z1 to-zone z2 {
  policy p1{
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          idp-policy idpengine;
        }
      }
    }
  }
}
```

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

Verification

To send traffic and check for attack detection from user logical system:

Verifying Attack Detection

Purpose Verify that attack detection is happening for the custom attack.

Action From operational mode, enter the **show security idp attack table** command.

```
user@host:LSYS1> show security idp policies
PIC : FPC 0 PIC 0:
ID   Name           Sessions   Memory    Detector
1    idpengine        0          188584    12.6.130180509

user@host:LSYS1> show security idp attack table
IDP attack statistics:

Attack name           #Hits
my-http                1
```

Meaning The output displays the attacks detected for the custom attack that is configured in the IDP policy in the user logical system LSYS1.

See Also • *IDP Policies Overview*

- [idp on page 496](#)

ALG for Logical Systems

An Application Layer Gateway (ALG) in logical systems enables the gateway to parse application layer payloads and take decisions whether to allow or deny traffic to the application server. ALGs supports the applications such as Transfer Protocol (FTP) and various IP protocols that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections. For more information, see the following topics:

- [Understanding Application Layer Gateway \(ALG\) in Logical Systems on page 223](#)
- [Enabling and Disabling ALG for Logical System on page 224](#)
- [Example: Enabling FTP ALG in a Logical System on page 227](#)

Understanding Application Layer Gateway (ALG) in Logical Systems

The master administrator can configure ALGs at the root level. The configuration is inherited by all user logical systems. ALGs can also be configured discretely for user logical systems. The ALG status is not inherited by all user logical systems. For a newly created logical system, the ALG consists of a default status. The FTP protocol ALG can be enabled or disabled for a specific logical system. The ICMP ALG protocol is enabled by default and is not provisioned to disable.



NOTE: When an SRX device is upgraded to 18.2 release, the ALG status in a logical system is changed when compared with previous status. This change affects the ALG traffic in the logical system. For example, before upgrade, H.323 ALG is configured to enable by root. So H.323 ALG is also enabled in lsys1. After upgrade to 18.2, H.323 ALG status in lsys1 is disabled because the default status for H.323 is disabled for a new logical system.



NOTE: You can enable a particular ALG for only one specific logical system.

By default, the following ALGs are enabled on a root logical system:

- DNS
- FTP
- MSRPC
- PPTP
- SUNRPC
- TALK
- TFTP

Starting in Junos OS Release 18.2R1, you can either enable or disable the ALGs configuration for each logical system individually, and view the status of the ALGs for all logical systems or specific logical system. All 12 data ALGs (DNS, FTP, TFTP, MSRPC, SUNRPC, PPTP, RSH, RTSP, TALK, SQL, IKE, and TWAMP) and four VOIP ALGs (SIP, H.323, MGCP, and SCCP) are supported on the logical systems.

- See Also**
- [show security alg status logical-system on page 602](#)
 - [Example: Enabling FTP ALG in a Logical System on page 227](#)
 - [alg on page 456](#)

Enabling and Disabling ALG for Logical System

This topic shows how to enable or disable the ALG status for each logical system.

1. By Default IKE ALG is disabled on the logical system. To enable this ALG, use the following command.
 - Enable IKE and ESP ALG with NAT.

```
[edit]
user@host# set logical-systems LSYS1 security alg ike-esp-nat enable
```
2. By default, the DNS, FTP, PPTP, SIP, SUNRPC and TWAMP ALGs are enabled on the logical system. To disable these ALGs, use the following commands.
 - Disable DNS ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg dns disable
```
 - Disable FTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg ftp disable
```
 - Disable H323 ALG.

```
[edit]
user@host# logical-systems LSYS1 security alg h323 disable
```
 - Disable MGCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg mgcp disable
```
 - Disable MSRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg msrpc disable
```
 - Disable PPTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg pptp disable
```
 - Disable RSH ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg rsh disable
```


- Disable RTSP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg rtsp disable
```

- Disable SCCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sccp disable
```

- Disable SIP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sip disable
```

- Disable SQL ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sql disable
```

- Disable SUNRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sunrpc disable
```

- Disable TALK ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg talk disable
```

- Disable TFTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg tftp disable
```

3. Configuring ALG functions in logical systems.

- Configure DNS ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg dns
```

- Configure FTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg ftp
```

- Configure H323 ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg h323
```

- Configure IKE and ESP ALG with NAT.

```
[edit]
user@host# set logical-systems LSYS1 security alg ike-esp-nat
```

- Configure MGCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg mgcp
```

- Configure MSRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg msrpc
```

- Configure PPTP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg pptp
```
- Configure RSH ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg rsh
```
- Configure RTSP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg rtsp
```
- Configure SCCP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg sccp
```
- Configure SIP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg sip
```
- Configure SQL ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg sql
```
- Configure SUNRPC ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg sunrpc
```
- Configure TALK ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg talk
```
- Configure TFTP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg tftp
```
- Configure TWAMP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg twamp
```
- Configure extended function for FTP ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg ftp allow-mismatch-ip-address
```
- Configure extended function for MSRPC ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg msrpc map-entry-timeout 10
```
- Configure extended function for SUNRPC ALG.

```
[edit]  
user@host# set logical-systems LSYS1 security alg sunrpc map-entry-timeout 10
```
- Configure extended function for SIP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sip retain-hold-resource
```

Example: Enabling FTP ALG in a Logical System

This example shows how to enable or disable an FTP ALG configuration in a logical system and send traffic based on FTP ALG configuration of the logical system individually.

- [Requirements on page 227](#)
- [Overview on page 227](#)
- [Configuration on page 227](#)
- [Verification on page 232](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See “[User Logical Systems Configuration Overview](#)” on page 61.

Overview

In this example, the ALG for FTP is configured to monitor and allow FTP traffic to be exchanged between the clients and the server on a logical system.

By default, the FTP ALG is enabled on the logical system.

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 system security-profile p1 policy maximum 100
set system security-profile p1 policy reserved 50
set system security-profile p1 zone maximum 100
set system security-profile p1 zone reserved 50
set system security-profile p1 flow-session maximum 6291456
set system security-profile p1 flow-session reserved 50
set system security-profile p1 flow-gate maximum 524288
set system security-profile p1 flow-gate reserved 50
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 routing-instances vr0 instance-type vpls
set logical-systems LSYS0 routing-instances vr0 interface lt-0/0/0.0
set system security-profile p1 logical-system LSYS0
set system security-profile p1 logical-system LSYS1
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 0
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address 10.0.0.0/8
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet address 198.51.100.0/24
set logical-systems LSYS1 interfaces ge-0/0/1 unit 0 family inet address 203.0.113.0/24
```

```
set logical-systems LSYS1 security zones security-zone LSYS1_tzone host-inbound-traffic
system-services all
set logical-systems LSYS1 security zones security-zone LSYS1_tzone host-inbound-traffic
protocol all
set logical-systems LSYS1 security zones security-zone LSYS1_tzone interfaces ge-0/0/0
set logical-systems LSYS1 security zones security-zone LSYS1_utzone host-inbound-traffic
system-services all
set logical-systems LSYS1 security zones security-zone LSYS1_utzone host-inbound-traffic
protocol all
set logical-systems LSYS1 security zones security-zone LSYS1_utzone interfaces ge-0/0/1
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone
policy p11 match source-address any
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone
policy p11 match destination-address any
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone
policy p11 match application junos-ftp
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone
policy p11 match application junos-ping
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone
policy p11 then permit
set logical-systems LSYS1 security policies default-policy deny-all
```

Configuring FTP ALG in a Logical System

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

To configure an ALG in a user logical system:

1. Configure a security profile.

```
[edit system security-profile]
user@host#set p1 policy maximum 100
user@host#set p1 policy reserved 50
user@host#set p1 zone maximum 100
user@host#set p1 zone reserved 50
user@host#set p1 flow-session maximum 6291456
user@host#set p1 flow-session reserved 50
user@host#set p1 flow-gate maximum 524288
user@host#set p1 flow-gate reserved 50
```

2. Configure the master logical system.

- a. Create the master logical system

```
[edit logical-systems]
user@host#set LSYS0
user@host#set LSYS1
```

- b. Configure interfaces for a master logical system and configure logical tunnel interfaces and routing instances to the LSYS0.

```
[edit interfaces]
user@host#set lt-0/0/0 unit 0 encapsulation ethernet-vpls
```

```

user@host#set lt-0/0/0 unit 0 peer-unit 1
user@host#set routing-instances vr0 instance-type vpls
user@host#set routing-instances vr0 interface lt-0/0/0.0

```

- c. Configure a security profile p1 and assign it to the root logical system LSYS0.

```

[edit system security-profile]
user@host#set p1 logical-system LSYS0

```

3. Configure a user logical system.

- a. Create the user logical system LSYS1

```

[edit logical-systems]
user@host#set LSYS1

```

- b. Configure user logical and logical tunnel interfaces to transfer traffic within the logical system.

```

[edit interfaces]
user@host#set ge-0/0/0 unit 0 family inet address 198.51.100.0/24
user@host#set ge-0/0/1 unit 0 family inet address 203.0.113.0/24
user@host#set lt-0/0/0 unit 1 encapsulation ethernet
user@host#set lt-0/0/0 unit 1 peer-unit 0
user@host#set lt-0/0/0 unit 1 family inet address 10.0.0.0/8

```

- c. Assign a security profile p1 to LSYS1.

```

[edit system security-profile]
user@host#set p1 logical-system LSYS1

```

- d. Configure security zones and assign interfaces to each zone.

```

[edit security zones]
user@host#set security-zone LSYS1_tzone host-inbound-traffic system-services
all
user@host#set security-zone LSYS1_tzone host-inbound-traffic protocol all
user@host#set security-zone LSYS1_tzone interfaces ge-0/0/0
user@host#set security-zone LSYS1_utzone host-inbound-traffic system-services
all
user@host#set security-zone LSYS1_utzone host-inbound-traffic protocol all
user@host#set security-zone LSYS1_utzone interfaces ge-0/0/1

```

4. Configure a security policy that permits FTP traffic from the LSYS1_tzone to LSYS1_utzone.

```

[edit security policies]
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p1 match
source-address any
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p1 match
destination-address any
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p1 match
application junos-ftp

```

```
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 match
application junos-ping
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 then permit
user@host#set default-policy deny-all
```

Results

From configuration mode, confirm the configuration for LSYS0 and LSYS1 by entering the **show logical-systems**. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host#show logical-systems LSYS0
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
    }
  }
}
routing-instances {
  vr0 {
    instance-type vpls;
    interface lt-0/0/0.0;
    interface lt-0/0/0.2;
  }
}

user@host#show logical-systems LSYS1
interfaces {
  lt-0/0/0 {
    unit 1 {
      encapsulation ethernet;
      peer-unit 0;
      family inet {
        address 10.0.1.1/24;
      }
    }
  }
  reth0 {
    unit 0 {
      family inet {
        address 198.51.100.0/24;
      }
    }
  }
}
security {
  alg {
    ftp;
  }
}
```

```
policies {
  from-zone LSYS1_tzone to-zone LSYS1_utzone {
    policy P11 {
      match {
        source-address any;
        destination-address any;
        application [ junos-ping junos-ftp ];
      }
      then {
        permit;
      }
    }
  }
  default-policy {
    deny-all;
  }
}
zones {
  security-zone LSYS1_tzone {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      reth0.0;
    }
  }
  security-zone LSYS1_utzone {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      lt-0/0/0.1;
    }
  }
}
```

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

Verification

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

- [Verify ALG status for user logical system on page 232](#)
- [Verify ALG status for all the logical systems on page 232](#)
- [Verifying Intra-Logical System Traffic on a Logical System on page 234](#)

Verify ALG status for user logical system

Purpose Verify alg status for FTP is enabled.

Action To verify the configuration is working properly, enter the **show security alg status logical-system LSYS1** command.

```
user@host> show security alg status logical-system LSYS1
```

ALG Status:

DNS	: Enabled
FTP	: Enabled
H323	: Disabled
MGCP	: Disabled
MSRPC	: Enabled
PPTP	: Enabled
RSH	: Disabled
RTSP	: Disabled
SCCP	: Disabled
SIP	: Enabled
SQL	: Disabled
SUNRPC	: Enabled
TALK	: Enabled
TFTP	: Enabled
IKE-ESP	: Disabled
TWAMP	: Disabled

Meaning The output displays the alg status for FTP Enabled for the logical system LSYS1.

Verify ALG status for all the logical systems

Purpose Verify the ALG status for all the logical systems on the device.

Action To verify the configuration is working properly, enter the **show security alg status logical-system all** command.

```
user@host> show security alg status logical-system all
```

Logical system: root-logical-system

ALG Status:

DNS	: Enabled
FTP	: Enabled
H323	: Disabled
MGCP	: Disabled
MSRPC	: Enabled
PPTP	: Enabled

RSH : Disabled
RTSP : Disabled
SCCP : Disabled
SIP : Disabled
SQL : Disabled
SUNRPC : Enabled
TALK : Enabled
TFTP : Enabled
IKE-ESP : Disabled
TWAMP : Disabled

Logical system: LSYS3

ALG Status:

DNS : Enabled
FTP : Enabled
H323 : Disabled
MGCP : Disabled
MSRPC : Enabled
PPTP : Enabled
RSH : Disabled
RTSP : Disabled
SCCP : Disabled
SIP : Enabled
SQL : Disabled
SUNRPC : Enabled
TALK : Enabled
TFTP : Enabled
IKE-ESP : Disabled
TWAMP : Disabled

Logical system: LSYS1

ALG Status:

DNS : Enabled
FTP : Enabled
H323 : Disabled
MGCP : Disabled
MSRPC : Enabled
PPTP : Enabled
RSH : Disabled
RTSP : Disabled
SCCP : Disabled
SIP : Enabled
SQL : Disabled
SUNRPC : Enabled
TALK : Enabled
TFTP : Enabled
IKE-ESP : Disabled
TWAMP : Disabled

Logical system: LSYS2

ALG Status:

DNS : Enabled
FTP : Enabled
H323 : Disabled
MGCP : Disabled
MSRPC : Enabled
PPTP : Enabled
RSH : Disabled
RTSP : Disabled
SCCP : Disabled
SIP : Enabled

```
SQL      : Disabled
SUNRPC   : Enabled
TALK     : Enabled
TFTP     : Enabled
IKE-ESP  : Disabled
TWAMP    : Disabled
```

```
Logical system: LSYS0
ALG Status:
```

```
DNS      : Enabled
FTP      : Enabled
H323     : Disabled
MGCP     : Disabled
MSRPC    : Enabled
PPTP     : Enabled
RSH      : Disabled
RTSP     : Disabled
SCCP     : Disabled
SIP      : Disabled
SQL      : Disabled
SUNRPC   : Enabled
TALK     : Enabled
TFTP     : Enabled
IKE-ESP  : Disabled
TWAMP    : Disabled
```

Meaning The output displays the ALG status for all the logical systems on the device.

Verifying Intra-Logical System Traffic on a Logical System

Purpose Verify the information about active resources, clients, groups, and sessions created through the resource manager.

Action From operational mode, enter the **show security resource-manager summary** command.

```
user@host> show security resource-manager summary
Active resource-manager clients   : 16
Active resource-manager groups    : 3
Active resource-manager resources : 26
Active resource-manager sessions  : 4
```

Meaning The output displays summary information about active resources, clients, groups, and sessions created through the resource manager.

See Also

- [Understanding Application Layer Gateway \(ALG\) in Logical Systems on page 223](#)
- [alg on page 456](#)
- [show security alg status logical-system on page 602](#)

- Related Documentation**
- [Security Zones in Logical Systems on page 128](#)

Application Security in Logical Systems

Application Security in logical systems enables to identify application traffic traversing your network regardless of port, protocol, and encryption, thereby providing greater visibility to control network traffic. The application security controls network traffic by setting and enforcing security policies based on accurate application information. For more information, see the following topics:

- [Understanding Logical Systems Application Identification Services on page 235](#)
- [Understanding Logical Systems Application Firewall Services on page 236](#)
- [Example: Configuring Application Firewall Services for a Master Logical Systems on page 237](#)
- [Understanding Logical Systems Application Tracking Services on page 242](#)
- [Example: Configuring Application Firewall Services for a User Logical System on page 242](#)
- [Example: Configuring AppTrack for a User Logical Systems on page 246](#)

Understanding Logical Systems Application Identification Services

Predefined and custom application signatures identify an application by matching patterns in the first few packets of a session. Identifying applications provides the following benefits:

- Allows Intrusion Detection and Prevention (IDP) to apply appropriate attack objects to applications running on nonstandard ports.
- Improves performance by narrowing the scope of attack signatures for applications without decoders.
- Enables you to create detailed reports using AppTrack on applications passing through the device.

With logical systems, predefined and custom application signatures are global resources that are shared by all logical systems. The master administrator is responsible for downloading and installing predefined Juniper Networks application signatures and creating custom application and nested application signatures to identify applications that are not part of the predefined database.

Application identification is enabled by default.

The application system cache (ASC) saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. Each user logical system has its own ASC. A user logical system administrator can display the ASC entries for their logical system with the **show services application-identification application-system-cache** command. A user logical system administrator can use the **clear services application-identification application-system-cache** command to clear the ASC entries for their logical system.

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

- Security services including security policies, application firewall (AppFW), application tracking (AppTrack), application quality of service (AppQoS), Juniper Sky ATP, IDP, and UTM do not use the ASC by default.
- Miscellaneous services including advanced policy-based routing (APBR) use the ASC for application identification by default.

For more information, see *Enabling or Disabling Application System Cache for Application Services*.

The master administrator can display or clear ASC entries for any logical system. The master administrator can also display or clear global counters with the **show services application-identification counter** and **clear services application-identification counter** commands.

Application signature package is installed at the global-level, that is shared by all user logical systems. The master logical system administrator can install or uninstall application signature package.

Starting in Junos OS Release 18.3R1, the application identification (AppID) support for logical systems include two new options to view and clear logical system statistics and logical system counters statistics.

The master logical system administrator can display or clear the statistics for all logical systems whereas the administrator for the user logical system can display or clear the statistics for their own logical system.

The user logical system administrator can view the AppID signature package status and version. Custom signatures configured by the master logical system administrator can be configured in the use logical system security policies.

You can view the status and version information about the AppID signature package status and version by using the commands **show services application-identification status** and **show services application-identification version**.

- See Also**
- *Understanding the Junos OS Application Identification Database*
 - *Example: Scheduling the Application Signature Package Updates*
 - *Example: Configuring Junos OS Application Identification Custom Application Signatures*
 - *Understanding IDP Application Identification*
 - *Understanding the Application System Cache*
 - *Verifying Application System Cache Statistics*

Understanding Logical Systems Application Firewall Services

An application firewall enables administrators of logical systems to create security policies for traffic based on application identification defined by application signatures. The application firewall provides additional security protection against

dynamic-application traffic that might not be adequately controlled by standard network firewall policies. The application firewall controls information transmission by allowing or blocking traffic originating from particular applications.

To configure an application firewall, you define a rule set that contains rules specifying the action to be taken on identified dynamic applications. The rule set is configured independently and assigned to a security policy. Each rule set contains at least two rules, a matched rule (consisting of match criteria and action) and a default rule.

- A matched rule defines the action to be taken on matching traffic. When traffic matches an application and other criteria specified in the rule, the traffic is allowed or blocked based on the action specified in the rule.
- A default rule is applied when traffic does not match any other rule in the rule set.

The master administrator can download a predefined application signature database from the Juniper Networks Security Engineering website or can define application signatures using the Junos OS configuration CLI. For more information about application identification and application signatures, see *Application Security Feature Guide for Security Devices*.

Configuring an application firewall on a logical system is the same process as configuring an application firewall on a device that is not configured with logical systems. However, the application firewall applies only to the logical system for which it is configured. The master administrator can configure, enable, and monitor application firewalls on the master logical system and all user logical systems on a device. User logical system administrators can configure, enable, and monitor application firewalls only on the user logical systems for which they have access.

- See Also**
- [Example: Configuring Application Firewall Services for a Master Logical Systems on page 237](#)
 - [Example: Configuring Application Firewall Services for a User Logical System on page 242](#)

Example: Configuring Application Firewall Services for a Master Logical Systems

This example describes how to configure application firewall services on the master, or root, logical system by a master administrator. Only the master administrator can configure, manage, and view configuration of the master logical system, in addition to all user logical systems.

After configuring application firewall rule sets and rules, the master administrator adds the application firewall rule set information to the security policy on the master logical system.

For information about configuring an application firewall within a security policy, see *Application Firewall Overview*.

- [Requirements on page 238](#)
- [Overview on page 238](#)

- [Configuration on page 239](#)
- [Verification on page 241](#)

Requirements

Before you begin:

- Verify that all interfaces, routing instances, and security zones have been configured on the master logical system.

See [“Example: Configuring Security Features for the Master Logical Systems” on page 146](#).

- Verify that application firewall resources (appfw-rule-set and appfw-rule) have been allocated in a security profile and bound to the master logical system through the `[system security-profile]` command. For application firewall resources, a security profile configuration allows 0 to 10,000 rule sets and 0 to 10,000 rules.



NOTE: The master administrator allocates various global system resources through a security profile configuration which is then bound to the various logical systems on the device. The master administrator owns this function and configures the security profile for all user logical systems as well as the master logical system.

For more information, see [“Understanding Logical Systems Security Profiles \(Master Administrators Only\)” on page 73](#).

-
- Log in to the master logical system as the master administrator.

For information about master administrator role functions, see [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).

Overview

In this example you create application firewall services on the master logical system, called root-logical-system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#).

This example creates the following application firewall configuration:

- Rule set, root-rs1, with rules r1 and r2. When r1 is matched, telnet traffic is allowed through the firewall. When r2 is matched, web traffic is allowed through the firewall.
- Rule set, root-rs2, with rule r1. When r1 is matched, example2 traffic is blocked by the firewall.

All rule sets require a default rule, which specifies whether to permit or deny traffic that is not specified in any rules of a rule set. The default-rule action (permit or deny) must be the opposite from the action that is specified for the other rule(s) in the rule set.

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 logical-systems root-logical-system security application-firewall rule-sets root-rs1
  rule r1 match dynamic-application junos:telnet
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
  rule r1 then permit
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
  rule r2 match dynamic-application-group junos:web
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
  rule r2 then permit
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
  default-rule deny
set logical-systems root-logical-system security application-firewall rule-sets root-rs2
  rule r1 match dynamic-application junos:facebook
set logical-systems root-logical-system security application-firewall rule-sets root-rs2
  rule r1 then deny
set logical-systems root-logical-system security application-firewall rule-sets root-rs2
  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 *Using the CLI Editor in Configuration Mode* in the Junos OS CLI User Guide.

To configure application firewall for a master logical system:

1. Log in to the master logical system as the master administrator. See [“Example: Configuring Root Password for Logical Systems” on page 64](#) and enter configuration mode.

```
admin@host> configure
admin@host#
```

2. Configure an application firewall rule set for root-logical-system.

```
[edit ]
admin@host# set logical-systems security application-firewall rule-sets root-rs1
```

3. Configure a rule for this rule set and specify which dynamic applications and dynamic application groups the rule should match.

```
[edit]
admin@host# set logical-systems security application-firewall rule-sets root-rs1
  rule r1 match dynamic-application telnet then permit
```

4. Configure the default rule for this rule set and specify the action to take when the identified dynamic application is not specified in any rules of the rule set.

```
[edit]
```

```
admin@host# set logical-systems security application-firewall rule-sets root-rs1
default-rule deny
```

5. Repeat these steps to configure another rule set, root-rs2, if desired.

Results From configuration mode, confirm your configuration by entering the **show security application-firewall rule-sets** command. 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]
admin@host# show security application-firewall rule-sets all
...
application-firewall {
  rule-sets root-rs1 {
    rule r1 {
      match {
        dynamic-application [junos:telnet];
      }
      then {
        permit;
      }
    }
    default-rule {
      deny;
    }
  }
  rule-sets root-rs1 {
    rule r2 {
      match {
        dynamic-application-group [junos:web];
      }
      then {
        permit;
      }
    }
  }
  rule-sets root-rs2 {
    rule r1 {
      match {
        dynamic-application [junos:FACEBOOK];
      }
      then {
        deny;
      }
    }
    default-rule {
      permit;
    }
  }
}
```


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

Verification

Confirm that the configuration is working properly.

- [Verifying Application Firewall Configuration on page 241](#)

Verifying Application Firewall Configuration

Purpose View the application firewall configuration on the master logical system.

Action From operational mode, enter the **show security application-firewall rule-set logical-system root-logical-system rule-set all** command.

```
admin@host> show security application-firewall rule-set logical-system root-logical-system
rule-set all
```

```
Rule-set: root-rs1
  Logical system: root-logical-system
  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: root-rs1
  Logical system: root-logical-system
  Rule: r2
    Dynamic Applications: 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: root-rs2
  Logical system: root-logical-system
  Rule: r1
    Dynamic Applications: junos:FACEBOOK
    Action:deny
    Number of sessions matched: 40
Default rule:permit
  Number of sessions matched: 400
Number of sessions with appid pending: 10
```

- See Also**
- [SRX Series Logical Systems Master Administrator Configuration Tasks Overview on page 41](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Understanding Logical Systems Application Firewall Services on page 236](#)

- [Example: Configuring Security Features for the Master Logical Systems on page 146](#)

Understanding Logical Systems Application Tracking Services

AppTrack is an application tracking tool that 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 can be enabled and configured within any logical system. Configuring AppTrack in a logical system is the same as configuring AppTrack on a device that is not configured for logical systems. An AppTrack configuration only applies to the logical system in which it is configured. The name of the logical system is added to AppTrack logs. The master administrator can configure AppTrack for any logical system while a user logical system administrator can only configure AppTrack for the logical system that they are logged in to.



NOTE: The system log configuration is global on the device and must be configured by the master administrator. The user logical system administrator cannot configure system logging for a logical system.

Counters keep track of the number of log messages sent and logs that have failed. AppTrack counters are global to the device. The master administrator as well as user logical system administrators can view AppTrack counters with the **show security application-tracking counters** command.

- See Also**
- [Understanding AppTrack](#)
 - [Example: Configuring AppTrack](#)
 - [Example: Configuring AppTrack for a User Logical Systems on page 246](#)

Example: Configuring Application Firewall Services for a User Logical System

This example describes how to configure application firewall services on a user logical system by a user logical system administrator. User logical system administrators can manage and monitor their own system application firewall rule sets and rules and manage the dynamic applications allowed or blocked on their respective logical systems.

After configuring application firewall rule sets and rules, user logical system administrators add the application firewall rule set information to the security policy on their individual logical systems.

For information about configuring an application firewall within a security policy, see *Application Firewall Overview*.

- [Requirements on page 243](#)
- [Overview on page 243](#)
- [Configuration on page 243](#)
- [Verification on page 245](#)

Requirements

Before you begin:

- Verify that the security zones are configured for the user logical system.
- Verify that the master administrator has allocated application firewall resources (appfw-rule-set and appfw-rule) in the security profile bound to the user logical system.

For more information, see “[Understanding Logical Systems Security Profiles \(Master Administrators Only\)](#)” on page 73.

- Log in to the logical system as the user logical system administrator.

For information about user logical system administrator role functions, see “[Understanding User Logical Systems and the User Logical System Administrator Role](#)” on page 63.

Overview

In this example you configure application firewall services on the ls-product-design user logical system shown in “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on page 65.

This example creates the following application firewall configuration:

- Rule set, ls-product-design-rs1, with rules r1 and r2. When r1 is matched, telnet traffic is allowed through the firewall. When r2 is matched, web traffic is allowed through the firewall.
- Rule set, ls-product-design-rs2, with rule r1. When r1 is matched, Facebook traffic is blocked by the firewall.

All rule sets require a default rule, which specifies whether to permit or deny traffic that is not specified in any rules of a rule set. The default-rule action (permit or deny) must be the opposite from the action that is specified for the other rule(s) in the rule set.

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 ls-product-design-rs1 rule r1 match
dynamic-application junos:telnet
```

```
set security application-firewall rule-sets ls-product-design-rs1 rule r1 then permit
set security application-firewall rule-sets ls-product-design-rs1 rule r2 match
dynamic-application-group junos:web
set security application-firewall rule-sets ls-product-design-rs1 rule r2 then permit
set security application-firewall rule-sets ls-product-design-rs1 default-rule deny
set security application-firewall rule-sets ls-product-design-rs2 rule r1 match
dynamic-application junos:facebook
set security application-firewall rule-sets ls-product-design-rs2 rule r1 then deny
set security application-firewall rule-sets ls-product-design-rs2 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 *Using the CLI Editor in Configuration Mode* in the Junos OS CLI User Guide.

To configure application firewall for a user logical system:

1. Log in to the user logical system as the user logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure an application firewall rule set for this logical system.

```
[edit]
lsdesignadmin1@host:ls-product-design# set security application-firewall rule-sets
ls-product-design-rs1
```

3. Configure a rule for this rule set and specify which dynamic applications and dynamic application groups the rule should match.

```
[edit]
lsdesignadmin1@host:ls-product-design# set security application-firewall rule-sets
ls-product-design-rs1 rule r1 match dynamic-application telnet then permit
```

4. Configure the default rule for this rule set and specify the action to take when the identified dynamic application is not specified in any rules of the rule set.

```
[edit]
lsdesignadmin1@host:ls-product-design# set security application-firewall rule-sets
ls-product-design-rs1 default-rule deny
```

5. Repeat these steps to configure another rule set, ls-product-design-rs2, if desired.

Results

From configuration mode, confirm your configuration by entering the **show security application-firewall rule-set all** command. 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]
lsdesignadmin1@host:ls-product-design# show security application-firewall rule-set all
...
application-firewall {
  rule-sets ls-product-design-rs1 {
    rule r1 {
      match {
        dynamic-application [junos:telnet];
      }
      then {
        permit;
      }
    }
    default-rule {
      deny;
    }
  }
  rule-sets ls-product-design-rs1 {
    rule r2 {
      match {
        dynamic-application-group [junos:web];
      }
      then {
        permit;
      }
    }
  }
  rule-sets ls-product-design-rs2 {
    rule r1 {
      match {
        dynamic-application [junos:FACEBOOK];
      }
      then {
        deny;
      }
    }
    default-rule {
      permit;
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Application Firewall Configuration on page 245](#)

Verifying Application Firewall Configuration

Purpose View the application firewall configuration on the user logical system.

Action From operational mode, enter the `show security application-firewall rule-set all` command.

```
lsdesignadmin1@host:ls-product-design> 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 Applications: 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
    Action:deny
    Number of sessions matched: 40
  Default rule:permit
    Number of sessions matched: 400
  Number of sessions with appid pending: 10
```

- See Also**
- [User Logical Systems Configuration Overview on page 61](#)
 - [Understanding Logical Systems Application Firewall Services on page 236](#)

Example: Configuring AppTrack for a User Logical Systems

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

- [Requirements on page 246](#)
- [Overview on page 247](#)
- [Configuration on page 247](#)
- [Verification on page 248](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See “[User Logical Systems Configuration Overview](#)” on page 61.

- (Master administrator) Configure system logging in the master logical system. See *Network Management and Monitoring Guide*.

Overview

This example shows how to enable application tracking for the security zone ls-product-design-trust in the ls-product-design user logical system shown in “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on page 65.

The first message is generated at session start and update messages are sent every 5 minutes after that or until the session ends. A final message is sent at session end.

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 ls-product-design-trust application-tracking
set security application-tracking first-update
```

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

To configure AppTrack for a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Enable AppTrack for the security zone.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set zones security-zone
ls-product-design-trust application-tracking
```

3. Generate update messages at session start and at 5-minute intervals.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set application-tracking first-update
```

Results From configuration mode, confirm your configuration by entering the **show security** command. 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]
lsdesignadmin1@host:ls-product-design# show security
...
  application-tracking {
    first-update;
  }
...
  zones {
    security-zone ls-product-design-trust {
      ...
      application-tracking;
    }
  }
}
```

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 AppTrack Operation on page 248](#)
- [Verifying Security Flow Session Statistics on page 248](#)
- [Verifying Application System Cache Statistics on page 248](#)
- [Verifying the Status of Application Identification Counter Values on page 249](#)

Verifying AppTrack Operation

Purpose View the AppTrack counters periodically to monitor tracking.

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

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.

Verifying Application System Cache Statistics

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

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

Verifying the Status of Application Identification Counter Values

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

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

See Also

- [Understanding Logical Systems Application Tracking Services on page 242](#)
- [User Logical Systems Configuration Overview on page 61](#)

IPv6 for Logical Systems

IPv6 builds upon the functionality of IPv4, providing improvements to IP addressing, configuration and maintenance, and security. IPv6 supports extensions for authentication and data integrity, which enhance privacy and security. IPv6 uses 128-bit addresses and supports a virtually unlimited number of devices—2 to the 128th power. For more information, see the following topics:

- [IPv6 Addresses in Logical Systems Overview on page 249](#)
- [Understanding IPv6 Dual-Stack Lite in Logical Systems on page 250](#)
- [Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems \(Master Administrators Only\) on page 251](#)
- [Example: Configuring IPv6 Zones for a User Logical Systems on page 259](#)
- [Example: Configuring IPv6 Security Policies for a User Logical Systems on page 263](#)
- [Example: Configuring IPv6 Dual-Stack Lite for a User Logical Systems on page 266](#)

IPv6 Addresses in Logical Systems Overview

IP version 6 (IPv6) increases the size of an IP address from the 32 bits that compose an IPv4 address to 128 bits. Each extra bit given to an address doubles the size of its address space. IPv6 has a much larger address space than the soon-to-be exhausted IPv4 address space.

IPv6 addresses can be configured in logical systems for the following features:

- Interfaces
- Firewall authentication
- Flows
- Routing (BGP only)
- Zones and security policies

- Screen options
- Network Address Translation (except for interface NAT)
- Administrative operations such as Telnet, SSH, HTTPS, and other utilities
- Chassis clusters



NOTE: An IPv6 session consumes twice the memory of an IPv4 session. Therefore the number of sessions available for IPv6 is half the reserved and maximum quotas configured for the flow session resource in a security profile. Use the vty command `show usp flow resource usage cp-session` to check flow session usage.

- See Also**
- [Understanding IPv6 Address Space, Addressing, Address Format, and Address Types](#)
 - [Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems \(Master Administrators Only\) on page 251](#)
 - [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(IPv6\) \(Master Administrators Only\) on page 308](#)
 - [Understanding IPv6 Dual-Stack Lite in Logical Systems on page 250](#)

Understanding IPv6 Dual-Stack Lite in Logical Systems

IPv6 dual-stack lite (DS-Lite) allows migration to an IPv6 access network without changing end-user software. IPv4 users can continue to access IPv4 internet content using their current hardware, while IPv6 users are able to access IPv6 content. A DS-Lite software initiator at the customer edge encapsulates IPv4 packets into IPv6 packets while a software concentrator decapsulates the IPv4-in-IPv6 packets and also performs IPv4 NAT translations.

A specific software concentrator and the set of software initiators that connect with that software concentrator can belong to only one logical system. The master administrator configures the maximum and reserved numbers of software initiators that can be connected to a software concentrator in a logical system using the `dslite-software-initiator` configuration statement at the `[edit system security-profile resources]` hierarchy level. The default maximum value is the system maximum; the default reserved value is 0.



NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of software initiators that can connect to a software concentrator configured for the master logical system. The number of software initiators configured in the master logical system count toward the maximum number of software initiators available on the device.

The user logical system administrator can configure software concentrators for their user logical system and the master administrator can configure software concentrators for the master logical system at the `[edit security softwires]` hierarchy level. The master administrator can also configure software concentrators for a user logical system at the `[edit logical-systems logical-system security softwires]` hierarchy level.



NOTE: The software concentrator IPv6 address can match an IPv6 address configured on either a physical interface or a loopback interface.

- See Also**
- [Example: Configuring IPv6 Dual-Stack Lite for a User Logical Systems on page 266](#)
 - [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Understanding IPv6 Dual-Stack Lite](#)

Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems (Master Administrators Only)

This topic covers configuration of IPv6 interfaces, static routes, and routing instances for the master and interconnect logical systems. It also covers configuration of IPv6 logical tunnel interfaces for user logical systems.

- [Requirements on page 251](#)
- [Overview on page 251](#)
- [Configuration on page 253](#)
- [Verification on page 259](#)

Requirements

Before you begin:

- See “[SRX Series Logical Systems Master Administrator Configuration Tasks Overview](#)” on [page 41](#) to understand how and where this procedure fits in the overall master administrator configuration process.
- See “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on [page 65](#).
- See “[Understanding the Interconnect Logical System and Logical Tunnel Interfaces](#)” on [page 31](#).

Overview

This scenario shows how to configure interfaces for the logical systems on the device, including an interconnect logical system.

- For the interconnect logical system, the example configures logical tunnel interfaces `lt-0/0/0.0`, `lt-0/0/0.2`, and `lt-0/0/0.4`. The example configures a routing instance called `vr` and assigns the interfaces to it.

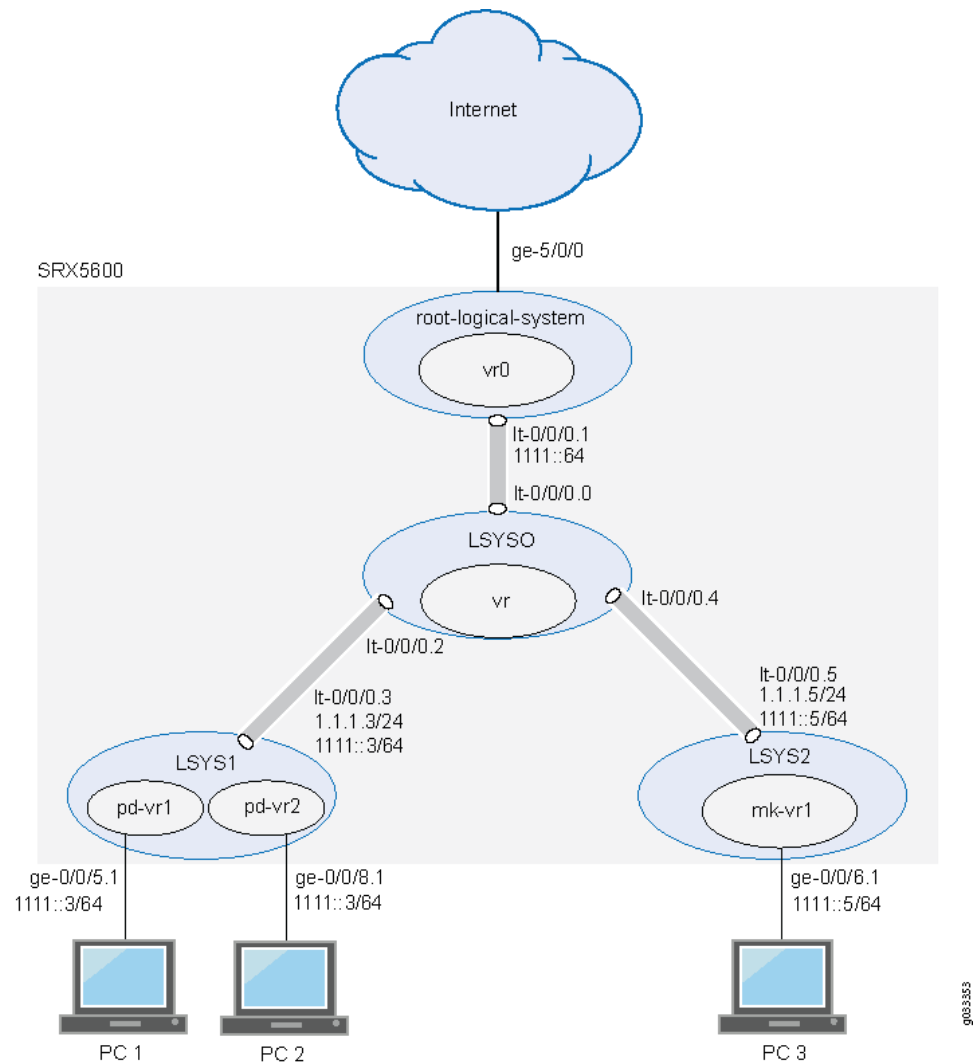
Because the interconnect logical system acts as a virtual switch, it is configured as a VPLS routing instance type. The interconnect logical system's lt-0/0/0 interfaces are configured with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the master and user logical systems are configured with Ethernet as the encapsulation type.

- lt-0/0/0.0 connects to lt-0/0/0.1 on the root logical system.
- lt-0/0/0.2 connects to lt-0/0/0.3 on the LSYS1 logical system.
- lt-0/0/0.4 connects to lt-0/0/0.5 on the LSYS2 logical system.
- For the master logical system, called root-logical-system, the example configures ge-5/0/0 and assigns it to the vr0 routing instance. The example configures lt-0/0/0.1 to connect to lt-0/0/0.0 on the interconnect logical system and assigns it to the vr0 routing instance. The example configures static routes to allow for communication with other logical systems and assigns them to the vr0 routing instance.
- For the LSYS1 logical system, the example configures lt-0/0/0.3 to connect to lt-0/0/0.2 on the interconnect logical system.
- For the LSYS2 logical system, the example configures lt-0/0/0.5 to connect to lt-0/0/0.4 on the interconnect logical system.

[Figure 7 on page 253](#) shows the topology for this deployment including virtual routers and their interfaces for all IPv6 logical systems.

Topology

Figure 7: Configuring IPv6 Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers



Configuration

This topic explains how to configure interfaces for logical systems.

- [Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System on page 254](#)
- [Configuring Interfaces, a Routing Instance, and Static Routes for the Master Logical System on page 255](#)
- [Configuring Logical Tunnel Interfaces for the User Logical Systems on page 257](#)

Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System

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 forwarding-options family inet6 mode flow-based
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems LSYS0 routing-instances vr instance-type vpls
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.0
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.2
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.4
```

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

To configure the interconnect system lt-0/0/0 interfaces and routing instances:

1. Enable flow-based forwarding for IPv6 traffic.

```
[edit security]
user@host# set forwarding-options family inet6 mode flow-based
```

2. Configure the lt-0/0/0 interfaces.

```
[edit logical-systems LSYS0 interfaces]
user@host# set lt-0/0/0 unit 0 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 0 peer-unit 1
user@host# set lt-0/0/0 unit 2 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 2 peer-unit 3
user@host# set lt-0/0/0 unit 4 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 4 peer-unit 5
```

3. Configure the routing instance for the interconnect logical system and add its lt-0/0/0 interfaces to it.

```
[edit logical-systems LSYS0 routing-instances]
user@host# set vr instance-type vpls
user@host# set vr interface lt-0/0/0.0
user@host# set vr interface lt-0/0/0.2
user@host# set vr interface lt-0/0/0.4
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems interconnect-logical-system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

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

```
user@host# show logical-systems LSYS0
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
    }
    unit 4 {
      encapsulation ethernet-vpls;
      peer-unit 5;
    }
  }
}
routing-instances {
  vr {
    instance-type vpls;
    interface lt-0/0/0.0;
    interface lt-0/0/0.2;
    interface lt-0/0/0.4;
  }
}
```

Configuring Interfaces, a Routing Instance, and Static Routes for the Master Logical System

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 interfaces ge-5/0/0 vlan-tagging
set interfaces ge-5/0/0 unit 0 vlan-id 600
set interfaces lt-0/0/0 unit 1 encapsulation Ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet address 1.1.1.1/24
set interfaces lt-0/0/0 unit 1 family inet6 address 1111::1/64
set interfaces ge-5/0/0 unit 0 family inet address 99.99.99.1/24
set interfaces ge-5/0/0 unit 0 family inet6 address 9999::1/64
set routing-instances vr0 instance-type virtual-router
set routing-instances vr0 interface lt-0/0/0.1
set routing-instances vr0 interface ge-5/0/0.0
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 7777::/64 next-hop
  1111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 8888::/64 next-hop
  1111::3
```

```

set routing-instances vr0 routing-options rib vr0.inet6.0 static route 6666::/64 next-hop
  1111::5
set routing-instances vr0 routing-options static route 77.77.77.0/24 next-hop 1.1.1.3
set routing-instances vr0 routing-options static route 88.88.88.0/24 next-hop 1.1.1.3
set routing-instances vr0 routing-options static route 66.66.66.0/24 next-hop 1.1.1.5

```

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 the master logical system interfaces:

1. Configure the master (root) logical system and lt-0/0/0.1 interfaces.

```

[edit interfaces]
user@host# set ge-5/0/0 vlan-tagging
user@host# set ge-5/0/0 unit 0 vlan-id 600
user@host# set lt-0/0/0 unit 1 encapsulation Ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet address 1.1.1.1/24
user@host# set lt-0/0/0 unit 1 family inet6 address 1111::1/64
user@host# set ge-5/0/0 unit 0 family inet address 99.99.99.1/24
user@host# set ge-5/0/0 unit 0 family inet6 address 9999::1/64

```

2. Configure a routing instance for the master logical system, assign its interfaces to it, and configure static routes for it.

```

[edit interfaces routing-instances]
user@host# set vr0 instance-type virtual-router
user@host# set vr0 interface lt-0/0/0.1
user@host# set vr0 interface ge-5/0/0.0
user@host# set vr0 routing-options rib vr0.inet6.0 static route 7777::/64 next-hop
  1111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 8888::/64 next-hop
  1111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 6666::/64 next-hop
  1111::5
user@host# set vr0 routing-options static route 77.77.77.0/24 next-hop 1.1.1.3
user@host# set vr0 routing-options static route 88.88.88.0/24 next-hop 1.1.1.3
user@host# set vr0 routing-options static route 66.66.66.0/24 next-hop 1.1.1.5

```

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

```

[edit]
user@host# show interfaces
ge-5/0/0 {
  vlan-tagging;
  unit 0 {
    vlan-id 600;
    family inet {
      address 99.99.99.1/24;

```



```

    }
    family inet 6{
        address 9999::1/64;
    }
}
lt-0/0/0 {
    unit 1 {
        encapsulation ethernet;
        peer-unit 0;
        family inet {
            address 1.1.1.1/24;
        }
        family inet 6{
            address 1111::1/64;
        }
    }
}
[edit]
user@host# show routing-instances
vr0 {
    instance-type virtual-router;
    interface ge-5/0/0.0;
    interface lt-0/0/0;
    routing-options {
        rib vr0.inet6.0 {
            static {
                route 8888::/64 next-hop 1111::3;
                route 7777::/64 next-hop 1111::3;
                route 6666::/64 next-hop 1111::5;
            }
        }
        static {
            route 77.77.77.0/24 next-hop 1.1.1.3;
            route 88.88.88.0/24 next-hop 1.1.1.3;
            route 66.66.66.0/24 next-hop 1.1.1.5;
        }
    }
}

```

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

Configuring Logical Tunnel Interfaces for the User Logical Systems

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 logical-systems LSYS1 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet address 1.1.1.3/24
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet6 address 1111::3/64
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 encapsulation ethernet

```

```
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet address 1.1.1.5/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet6 address 1111::5/64
```

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

1. Configure the lt-0/0/0 interface for the first user logical system:

```
[edit logical-systems LSYS1 interfaces lt-0/0/0 unit 3]
user@host# set encapsulation ethernet
user@host# set peer-unit 2
user@host# set family inet address 1.1.1.3/24
user@host# set family inet6 address 1111::3/64
```
2. Configure the lt-0/0/0 interface for the second user logical system.

```
[edit logical-systems LSYS2 interfaces lt-0/0/0 unit 5]
user@host# set encapsulation ethernet
user@host# set peer-unit 4
user@host# set family inet address 1.1.1.5/24
user@host# set family inet6 address 1111::5/64
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems LSYS1 interfaces lt-0/0/0**, and **show logical-systems LSYS2 interfaces lt-0/0/0** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show logical-systems LSYS1 interfaces lt-0/0/0

lt-0/0/0 {
  unit 3 {
    encapsulation ethernet;
    peer-unit 2;
    family inet {
      address 1.1.1.3/24;
    }
    family inet 6 {
      address 1111::3/64;
    }
  }
}

user@host# show logical-systems LSYS2 interfaces lt-0/0/0

lt-0/0/0 {
  unit 5 {
    encapsulation ethernet;
    peer-unit 4;
    family inet {
      address 1.1.1.5/24;
    }
    family inet 6 {
```

```
        address 1111::5/64;
    }
}
```

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

Verification

Verifying That the Static Routes Configured for the Master Administrator Are Correct

Purpose Confirm that the configuration is working properly. Verify if you can send data from the master logical system to the other logical systems.

Action From operational mode, use the **ping** command.

- See Also**
- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)
 - [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)
 - [Example: Configuring IPv6 Zones for a User Logical Systems on page 259](#)
 - [Example: Configuring IPv6 Security Policies for a User Logical Systems on page 263](#)

Example: Configuring IPv6 Zones for a User Logical Systems

This example shows how to configure IPv6 zones for a user logical system.

- [Requirements on page 259](#)
- [Overview on page 260](#)
- [Configuration on page 260](#)

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator.
See [“User Logical Systems Configuration Overview” on page 61](#).
- Ensure that forwarding options for inet6 is flow-based. Otherwise, you must configure it and reset the device.

Use the **show security forwarding-options** command to check the configuration.



NOTE: Only the user logical system administrator can configure the forwarding options.

Overview

This example configures the ls-product-design user logical system described in “[Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System](#)” on page 65

This example creates the IPv6 zones and address books described in [Table 25 on page 260](#).

Table 25: User Logical System Zone and Address Book Configuration

Feature	Name	Configuration Parameters
Zones	ls-product-design-trust	<ul style="list-style-type: none"> Bind to interface ge-0/0/5.1. TCP reset enabled.
	ls-product-design-untrust	<ul style="list-style-type: none"> Bind to interface lt-0/0/0.3.
Address books	product-design-internal	<ul style="list-style-type: none"> Address product-designers: 3002::1/96 Attach to zone ls-product-design-trust
	product-design-external	<ul style="list-style-type: none"> Address marketing: 3003::1/24 Address accounting: 3004::1/24 Address others: 3002::2/24 Address set otherlsys: marketing, accounting Attach to zone ls-product-design-untrust

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 logical-system lsys1 security address-book product-design-internal address
  product-designers 3002::1/96
set logical-system lsys1 security address-book product-design-internal attach zone
  ls-product-design-trust
set logical-system lsys1 security address-book product-design-external address marketing
  3003::1/24
set logical-system lsys1 security address-book product-design-external address accounting
  3004::1/24
set logical-system lsys1 security address-book product-design-external address others
  3002::2/24
set logical-system lsys1 security address-book product-design-external address-set
  otherlsys address marketing
set logical-system lsys1 security address-book product-design-external address-set
  otherlsys address accounting
set logical-system lsys1 security address-book product-design-external attach zone
  ls-product-design-untrust
set logical-system lsys1 security zones security-zone ls-product-design-trust tcp-rst
set logical-system lsys1 security zones security-zone ls-product-design-trust interfaces
  ge-0/0/5.1

```

```
set logical-system lsys1 security zones security-zone ls-product-design-untrust interfaces
lt-0/0/0.3
```

Step-by-Step Procedure

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

To configure IPv6 zones in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security zone and assign it to an interface.

```
[edit logical-system lsys1 security zones]
lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-trust
interfaces ge-0/0/5.1
```

3. Configure the TCP-Reset parameter for the zone.

```
[edit logical-system lsys1 security zones security-zone ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set tcp-rst
```

4. Configure a security zone and assign it to an interface.

```
[edit logical-system lsys1 security zones]
lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-untrust
interfaces lt-0/0/0.3
```

5. Create global address book entries.

```
[edit logical-system lsys1 security]
lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
address product-designers 3002::1/96
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address marketing 3003::1/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address accounting 3004::1/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address others 3002::2/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address-set otherlsys address marketing
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
address-set otherlsys address accounting
```

6. Attach address books to zones.

```
[edit logical-system lsys1 security]
lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
attach zone ls-product-design-trust
```

```
lsdesignadmin1@host:ls-product-design#set address-book product-design-external
attach zone ls-product-design-untrust
```

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

```
lsdesignadmin1@host:ls-product-design# show security zones
address-book {
  product-design-internal {
    address product-designers 3002::1/96;
    attach {
      zone ls-product-design-trust;
    }
  }
  product-design-external {
    address marketing 3003::1/24;
    address accounting 3004::1/24;
    address others 3002::2/24;
    address-set otherlsys {
      address marketing;
      address accounting;
    }
    attach {
      zone ls-product-design-untrust;
    }
  }
}
zones {
  security-zone ls-product-design-trust {
    tcp-rst;
    interfaces {
      ge-0/0/5.1;
    }
  }
  security-zone ls-product-design-untrust {
    interfaces {
      lt-0/0/0.3;
    }
  }
}
```

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

- See Also**
- [Understanding Logical Systems Zones on page 128](#)
 - [User Logical Systems Configuration Overview on page 61](#)
 - [Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems \(Master Administrators Only\) on page 251](#)
 - [Example: Configuring IPv6 Security Policies for a User Logical Systems on page 263](#)

Example: Configuring IPv6 Security Policies for a User Logical Systems

This example shows how to configure IPv6 security policies for a user logical system.

- [Requirements on page 263](#)
- [Overview on page 263](#)
- [Configuration on page 263](#)
- [Verification on page 265](#)

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator.

See [“User Logical Systems Configuration Overview” on page 61](#).

- Use the **show system security-profiles policy** command to see the security policy resources allocated to the logical system.
- Configure zones and address books.

See [“Example: Configuring IPv6 Zones for a User Logical Systems” on page 259](#)

Overview

This example shows how to configure the security policies described in [Table 26 on page 263](#).

Table 26: User Logical System Security Policies Configuration

Policy Name	Configuration Parameters
permit-all-to-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> • From zone: ls-product-design-trust • To zone: ls-product-design-untrust • Source address: product-designers • Destination address: otherlsys • Application: any
permit-all-from-otherlsys	Permit the following traffic: <ul style="list-style-type: none"> • From zone: ls-product-design-untrust • To zone: ls-product-design-trust • Source address: otherlsys • Destination address: product-designers • Application: any

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 logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust policy permit-all-to-otherlsys match source-address
product-designers
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust policy permit-all-to-otherlsys match destination-address
otherlsys
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust policy permit-all-to-otherlsys match application any
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust policy permit-all-to-otherlsys then permit
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust policy permit-all-from-otherlsys match source-address otherlsys
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust policy permit-all-from-otherlsys match destination-address
product-designers
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust policy permit-all-from-otherlsys match application any
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
ls-product-design-trust policy permit-all-from-otherlsys 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 the Junos OS CLI User Guide.

To configure IPv6 security policies for a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security policy that permits traffic from the ls-product-design-trust zone to the ls-product-design-untrust zone.

```
[edit logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
ls-product-design-untrust]
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
source-address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
destination-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
application any
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys then
permit
```

3. Configure a security policy that permits traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone.

```
[edit logical-systems lsys1 security policies from-zone ls-product-design-untrust
to-zone ls-product-design-trust]
```



```

lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
source-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
destination-address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
application any
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys 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.

```

lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
  policy permit-all-to-otherlsys {
    match {
      source-address product-designers;
      destination-address otherlsys;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone ls-product-design-untrust to-zone ls-product-design-trust {
  policy permit-all-from-otherlsys {
    match {
      source-address otherlsys;
      destination-address product-designers;
      application any;
    }
    then {
      permit;
    }
  }
}

```

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

Verification

Verifying Policy Configuration

Purpose Verify information about policies and rules.

Action From operational mode, enter the **show security policies detail** command to display a summary of all policies configured on the logical system.

See Also • [Understanding Logical Systems Security Policies on page 167](#)

- [User Logical Systems Configuration Overview on page 61](#)
- [Troubleshooting Security Policies](#)
- [Example: Configuring IPv6 Zones for a User Logical Systems on page 259](#)
- [Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems \(Master Administrators Only\) on page 251](#)

Example: Configuring IPv6 Dual-Stack Lite for a User Logical Systems

This example shows how to configure a software concentrator for a user logical system.

- [Requirements on page 266](#)
- [Overview on page 266](#)
- [Configuration on page 266](#)
- [Verification on page 267](#)

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See [“User Logical Systems Configuration Overview” on page 61](#).
- Use the **show system security-profile dslite-software-initiator** command to see the number software initiators that can be connected to a software concentrator in the logical system.

Overview

This example shows how to configure a software concentrator to decapsulate IPv4-in-IPv6 packets in the ls-product-design user logical system shown in [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#). The IPv6 address of the software concentrator is 3000::1 and the name of the software configuration is sc_1.

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 softwares software-name sc_1 software-concentrator 3000::1 software-type IPv4-in-IPv6
```

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

To configure an IPv6 DS-Lite software concentrator:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Specify the address of the software concentrator and the software type.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set softwares software-name sc_1
software-concentrator 3000::1 software-type IPv4-in-IPv6
```

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

```
[edit]
lsdesignadmin1@host:ls-product-design# show security softwares
software-name sc_1 {
  software-concentrator 3000::1;
  software-type IPv4-in-IPv6;
}
```

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

Verification

Verifying the DS-Lite Configuration

Purpose Verify that the software initiators can connect to the software concentrator configured in the user logical system.

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

If a software initiator is not connected, the operational output looks like this:

```
lsdesignadmin1@host:ls-product-design> show security softwares
Software Name      SC Address      Status  Number of SI connected
sc_1               3000::1         Active  0
```

If a software initiator is connected, the operational output looks like this:

```
lsdesignadmin1@host:ls-product-design> show security softwares
Software Name      SC Address      Status  Number of SI connected
sc_1               3000::1         Connected  1
```

- See Also**
- [Understanding IPv6 Dual-Stack Lite in Logical Systems on page 250](#)
 - [User Logical Systems Configuration Overview on page 61](#)

- Related Documentation**
- [Understanding Logical Systems Zones on page 128](#)

ICAP Redirects for Logical Systems

ICAP is a lightweight protocol used to extend transparent proxy servers, thereby freeing up resources. For more information, see the following topics:

- [ICAP Redirect Support for Logical Systems on page 268](#)
- [Example: Configuring ICAP Redirect Service on SRX Devices on page 269](#)

ICAP Redirect Support for Logical Systems

Starting in Junos OS Release 18.3R1, SRX Series devices support the Internet Content Adaptation Protocol (ICAP) service redirect when the device is configured for logical systems.

ICAP redirect profile is only allowed to attach on the policy which belongs to the same logical system. This profile is applied to a security policy as application services for the permitted traffic. The ICAP profile defines the settings that allow the ICAP server to process request messages, response messages, fallback options (in case of a timeout), connectivity issues, too many requests, or any other conditions.

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet. SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. SSL, also called Transport Layer Security (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private-public key exchange pairs for this level of security. SSL proxy 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.

ICAP redirect services has the dependency on SSL proxy to build secure connections. Because the SSL proxy is not supported on user logical systems in Junos OS Release 18.3R1, ICAP redirect works with clear text connections or with shared certificates in Junos OS Release 18.3R1.

The following sequences are involved in a typical ICAP redirect scenario:

1. The user opens a connection to a Website on the internet.
2. The request goes through the SRX Series device that is acting as a proxy server.

3. The SRX Series device receives information from the end-host, encapsulates the message and forwards the encapsulated ICAP message to the third-party on-premise ICAP server.
4. The ICAP server receives the ICAP request and analyzes it.
5. If the request does not contain any confidential information, the ICAP server sends it back to the proxy server, and directs the proxy server to send the HTTP to the internet.
6. If the request contains confidential information, you can choose to take action (block, permit and log) as per your requirement.

Limitations of SSL Proxy with Logical Systems

Following are the limitations for using ICAP redirect service for user logical systems:

- SSL Proxy is supported only on master logical system in Junos OS Release 18.3R1.
- SSL profile configured to provide a secure connection to the ICAP server is not supported on user logical systems in Junos OS Release 18.3R1.

See Also • For more information on SSL Proxy and benefits of ICAP Redirect, See: *SSL Proxy*.

Example: Configuring ICAP Redirect Service on SRX Devices

This example shows how to define an ICAP redirect profile for an SRX Series device.

- [Requirements on page 269](#)
- [Overview on page 269](#)
- [Configuration on page 270](#)
- [Verification on page 273](#)

Requirements

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 18.3R1 or later. This configuration example is tested for Junos OS Release 18.3R1.

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

Overview

In this example, you configure an ICAP redirect profile in logical systems and apply these profiles as application services in the security policy for the permitted traffic.

[Table 27 on page 270](#) lists the details of the parameters used in this example.

Table 27: ICAP Redirect Configuration Parameters

Parameters	Names	Description
Profile	icap-pf1	The ICAP server profile allows the ICAP server to process request messages, response messages, fallback options and so on, for the permitted traffic. This profile is applied as an application service in the security policy.
Server name	icap-svr1 icap-svr2	The machine name of the remote ICAP host. Client's request is redirected to this ICAP server.
Server IP address	192.0.2.2/24 192.0.2.179/24	The IP address of the remote ICAP host. Client's request is redirected to this ICAP server.
Logical system name	LSYS1	Displays the logical system name which belongs to the same profile.
Security policy	sp1	In a security policy, apply the SSL proxy profile and ICAP redirect profile. to the permitted 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 logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 host
  192.0.2.2/24
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri
  echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1
  respmod-uri echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 sockets
  64
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 host
  192.0.2.179/24
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2
  reqmod-uri echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2
  respmod-uri echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 sockets
  64
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 tls-profile
  dlp_ssl
set logical-systems LSYS1 services icap-redirect profile icap-pf1 http redirect-request
set logical-systems LSYS1 services icap-redirect profile icap-pf1 http redirect-response
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
  sec_policy match source-address any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
  sec_policy match destination-address any

```

```

set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
  sec_policy match application any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
  sec_policy then permit application-services ssl-proxy profile-name ssl-inspect-profile
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
  sec_policy then permit application-services icap-redirect icap-pf1
set logical-systems LSYS1 security policies default-policy permit-all
set logical-systems LSYS1 security zones security-zone trust host-inbound-traffic
  system-services all
set logical-systems LSYS1 security zones security-zone trust host-inbound-traffic protocols
  all
set logical-systems LSYS1 security zones security-zone trust interfaces xe-5/0/0.0
set logical-systems LSYS1 security zones security-zone untrust host-inbound-traffic
  system-services all
set logical-systems LSYS1 security zones security-zone untrust host-inbound-traffic
  protocols all
set logical-systems LSYS1 security zones security-zone untrust interfaces xe-5/0/1.0
set logical-systems LSYS1 interfaces xe-5/0/0 unit 0 family inet address 192.0.2.1/8
set logical-systems LSYS1 interfaces xe-5/0/0 unit 0 family inet6 address 2001:db8::1/64
set logical-systems LSYS1 interfaces xe-5/0/1 unit 0 family inet address 198.51.100.1/8
set logical-systems LSYS1 interfaces xe-5/0/1 unit 0 family inet6 address 2001:db8::2/64

```

Step-by-Step Procedure

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

To configure the ICAP redirect service:

1. Configure the ICAP redirect profile for the first server (icap-svr1).

```

[edit logical-systems LSYS1 services]
user@host# set icap-redirect profile icap-pf1 server icap-svr1 host 192.0.2.2/24
user@host# set icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr1 respmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr1 sockets 64

```

2. Configure the ICAP redirect profile for the second server (icap-svr2).

```

[edit logical-systems LSYS1 services]
user@host# set icap-redirect profile icap-pf1 server icap-svr2 host 192.0.2.179/24
user@host# set icap-redirect profile icap-pf1 server icap-svr2 reqmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr2 respmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr2 sockets 64
user@host# set icap-redirect profile icap-pf1 server icap-svr2 tls-profile dlp_ssl

```

3. Configure the redirect request and the redirect response for the HTTP traffic.

```

[edit logical-systems LSYS1 services]
user@host# set icap-redirect profile icap-pf1 http redirect-request
user@host# set icap-redirect profile icap-pf1 http redirect-response

```

4. Configure a security policy to apply application services for the ICAP redirect to the permitted traffic.

```
[edit logical-systems LSYS1 security]
user@host# set policies from-zone trust to-zone untrust policy sec_policy match
source-address any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match
destination-address any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match
application any
user@host# set policies from-zone trust to-zone untrust policy sec_policy then
permit application-services ssl-proxy profile-name ssl-inspect-profile
user@host# set policies from-zone trust to-zone untrust policy sec_policy then
permit application-services icap-redirect icap-pfl
user@host# set policies default-policy permit-all
```

5. Configure zones.

```
[edit logical-systems LSYS1 security]
user@host# set zones security-zone trust host-inbound-traffic system-services all
user@host# set zones security-zone trust host-inbound-traffic protocols all
user@host# set zones security-zone trust interfaces xe-5/0/0.0
user@host# set zones security-zone untrust host-inbound-traffic system-services
all
user@host# set zones security-zone untrust host-inbound-traffic protocols all
user@host# set zones security-zone untrust interfaces xe-5/0/1.0
```

6. Configure interfaces.

```
[edit logical-systems LSYS1]
user@host# set interfaces xe-5/0/0 unit 0 family inet address 192.0.2.1/8
user@host# set interfaces xe-5/0/0 unit 0 family inet6 address 2001:db8::1/64
user@host# set interfaces xe-5/0/1 unit 0 family inet address 198.51.100.1/8
user@host# set interfaces xe-5/0/1 unit 0 family inet6 address 2001:db8::2/64
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems LSYS1 services icap-redirect**, **show logical-systems LSYS1 security policies**, **show logical-systems LSYS1 security zones**, and **show logical-systems LSYS1 interfaces** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show logical-systems LSYS1 services icap-redirect
profile icap-pfl {
  server icap-svr1 {
    host 192.0.2.2/24;
    reqmod-uri echo;
    respmod-uri echo;
    sockets 64;
  }
  server icap-svr2 {
    host 192.0.2.179/24;
    reqmod-uri echo;
    respmod-uri echo;
    sockets 64;
    tls-profile dlp_ssl;
  }
}
```



```

http {
    redirect-request;
    redirect-response;
}
}

from-zone trust to-zone untrust {
    policy sec_policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    ssl-proxy {
                        profile-name ssl-inspect-profile;
                    }
                    icap-redirect icap-pf1;
                }
            }
        }
    }
}
}
default-policy {
    permit-all;
}
}

```

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

Verification

Verifying ICAP Redirect Configuration

Purpose Verify that the ICAP redirect service is configured on the device.

Action From operational mode, enter the **show services icap-redirect status logical-system** and **show services icap-redirect statistic logical-system** commands.

```
user@host> show services icap-redirect status logical-system LSYS1
```

```

ICAP Status :
  spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
  spu-2 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
  spu-3 Profile: icap-pf1 Server: icap-svr1 : UP

```

```
user@host> show services icap-redirect statistic logical-system LSYS1
```

```

ICAP Redirect statistic:
  Message Redirected           : 12
    Message REQMOD Redirected  : 6
    Message RESPMOD Redirected : 6
  Message Received             : 12

```

Message REQMOD Received	:	6	
Message RESPMOD Received	:	6	
Fallback:	permit	log-permit	reject
Timeout	0	0	0
Connectivity	0	0	0
Default	0	0	0

Meaning The status **Up** indicates that the ICAP redirect service is enabled. The **Message Redirected** and the **Message Received** fields show the number of HTTP requests that have passed through the ICAP channel.

Related Documentation

- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)

Logical Systems in a Chassis Cluster

A chassis cluster provides high availability on SRX Series devices where two devices operate as a single device. Chassis cluster includes the synchronization of configuration files and the dynamic runtime session states between the SRX Series devices, which are part of chassis cluster setup. For more information, see the following topics:

- [Understanding Logical Systems in the Context of Chassis Cluster on page 274](#)
- [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(Master Administrators Only\) on page 275](#)
- [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(IPv6\) \(Master Administrators Only\) on page 308](#)

Understanding Logical Systems in the Context of Chassis Cluster

The behavior of a chassis cluster whose nodes consist of SRX Series devices running logical systems is the same as that of a cluster whose SRX Series nodes in the cluster are not running logical systems. No difference exists between events that cause a node to fail over. In particular, if a link associated with a single logical system fails, then the device fails over to another node in the cluster.

The master administrator configures the chassis cluster (including both primary and secondary nodes) before he or she creates and configures the logical systems. Each node in the cluster has the same configuration, as is the case for nodes in a cluster not running logical systems. All logical system configurations are synchronized and replicated between both nodes in the cluster.

When you use SRX Series devices running logical systems within a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

Starting with Junos OS Release 12.3X48-D50, when you configure the logical systems within a chassis cluster, if logical systems licenses on backup node are not sufficient

when you **commit** the configuration, a warning message is displayed about the number of licenses required on backup node as well, just as on primary node in all the previous releases.

- See Also**
- [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(Master Administrators Only\)](#) on page 275
 - [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(IPv6\) \(Master Administrators Only\)](#) on page 308
 - [Understanding the Interconnect Logical System and Logical Tunnel Interfaces](#) on page 31
 - [Understanding Logical Systems for SRX Series Services Gateways](#) on page 26
 - [Chassis Cluster Overview](#)

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (Master Administrators Only)

This example shows how to configure logical systems in a basic active/passive chassis cluster.



NOTE: The master administrator configures the chassis cluster and creates logical systems (including an optional interconnect logical system), administrators, and security profiles. Either the master administrator or the user logical system administrator configures a user logical system. The configuration is synchronized between nodes in the cluster.

- [Requirements](#) on page 275
- [Overview](#) on page 276
- [Configuration](#) on page 279
- [Verification](#) on page 303

Requirements

Before you begin:

- Obtain two SRX Series Services Gateways with identical hardware configurations. See *Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices*. This chassis cluster deployment scenario includes the configuration of the SRX Series device for connections to an MX240 edge router and an EX8208 Ethernet Switch.
- Physically connect the two devices (back-to-back for the fabric and control ports) and ensure that they are the same models. You can configure both the fabric and control ports on the SRX5000 line. For the SRX1400 or SRX1500 devices or the SRX3000 line, you can configure the fabric ports only. (Platform support depends on the Junos OS release in your installation.) See *Connecting SRX Series Devices to Create a Chassis Cluster*.

- Set the chassis cluster ID and node ID on each device and reboot the devices to enable clustering. See *Example: Setting the Node ID and Cluster ID for SRX Series Devices in a Chassis Cluster*.



NOTE: For this example, chassis cluster and logical system configuration is performed on the primary (node 0) device at the root level by the master administrator. Log in to the device as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).



NOTE: When you use SRX Series devices running logical systems in a chassis cluster, you must purchase and install the same number of logical system licenses for each node in the chassis cluster. Logical system licenses pertain to a single chassis or node within a chassis cluster and not to the cluster collectively.

Overview

In this example, the basic active/passive chassis cluster consists of two devices:

- One device actively provides logical systems, along with maintaining control of the chassis cluster.
- The other device passively maintains its state for cluster failover capabilities should the active device become inactive.



NOTE: Logical systems in an active/active chassis cluster are configured in a similar manner as for logical systems in an active/passive chassis cluster. For active/active chassis clusters, there can be multiple redundancy groups that can be primary on different nodes.

The master administrator configures the following logical systems on the primary device (node 0):

- Master logical system—The master administrator configures a security profile to provision portions of the system’s security resources to the master logical system and configures the resources of the master logical system.
- User logical systems LSYS1 and LSYS2 and their administrators—The master administrator also configures security profiles to provision portions of the system’s security resources to user logical systems. The user logical system administrator can then configure interfaces, routing, and security resources allocated to his or her logical system.
- Interconnect logical system LSYS0 that connects logical systems on the device—The master administrator configures logical tunnel interfaces between the interconnect

logical system and each logical system. These peer interfaces effectively allow for the establishment of tunnels.



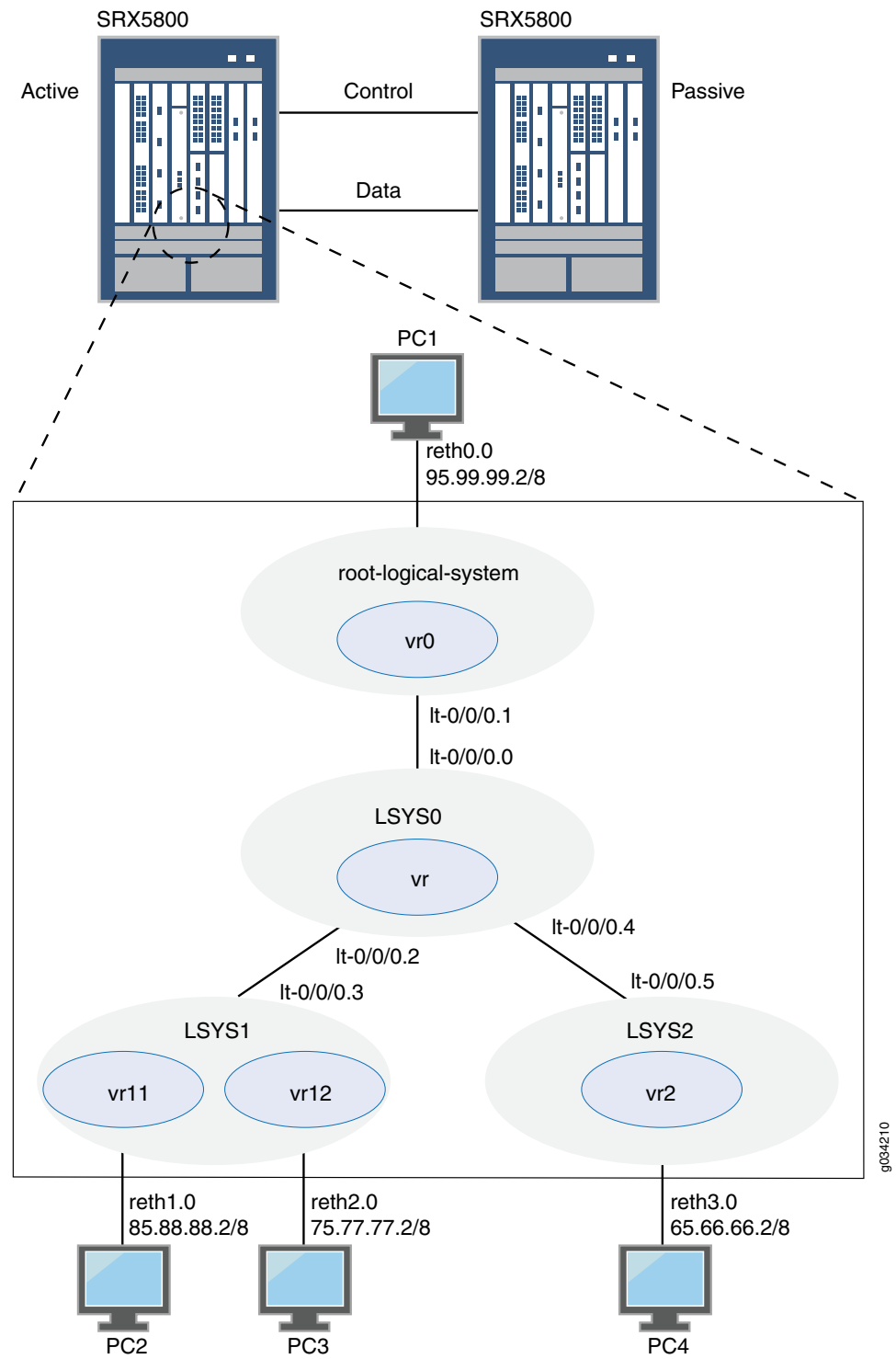
NOTE: This example does not describe configuring features such as NAT, IDP, or VPNs for a logical system. See [“SRX Series Logical Systems Master Administrator Configuration Tasks Overview” on page 41](#) and [“User Logical Systems Configuration Overview” on page 61](#) for more information about features that can be configured for logical systems.

If you are performing proxy ARP in a chassis cluster configuration, you must apply the proxy ARP configuration to the reth interfaces rather than the member interfaces because the reth interfaces contain the logical configurations. See *Configuring Proxy ARP for NAT (CLI Procedure)*.

Topology

[Figure 8 on page 278](#) shows the topology used in this example.

Figure 8: Logical Systems in a Chassis Cluster



Configuration

- [Chassis Cluster Configuration \(Master Administrator\) on page 279](#)
- [Logical System Configuration \(Master Administrator\) on page 283](#)
- [User Logical System Configuration \(User Logical System Administrator\) on page 292](#)

Chassis Cluster Configuration (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

On {primary:node0}

```
set chassis cluster control-ports fpc 0 port 0
set chassis cluster control-ports fpc 6 port 0
set interfaces fab0 fabric-options member-interfaces ge-1/1/0
set interfaces fab1 fabric-options member-interfaces ge-7/1/0
set groups node0 system host-name SRX5800-1
set groups node0 interfaces fxp0 unit 0 family inet address 10.157.90.24/9
set groups node0 system backup-router 10.157.64.1 destination 0.0.0.0/0
set groups node1 system host-name SRX5800-2
set groups node1 interfaces fxp0 unit 0 family inet address 10.157.90.23/19
set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
set apply-groups "${node}"
set chassis cluster reth-count 5
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 100
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 100
set interfaces ge-1/0/0 gigether-options redundant-parent reth0
set interfaces ge-1/0/1 gigether-options redundant-parent reth1
set interfaces ge-1/0/2 gigether-options redundant-parent reth2
set interfaces ge-1/0/3 gigether-options redundant-parent reth3
set interfaces ge-7/0/0 gigether-options redundant-parent reth0
set interfaces ge-7/0/1 gigether-options redundant-parent reth1
set interfaces ge-7/0/2 gigether-options redundant-parent reth2
set interfaces ge-7/0/3 gigether-options redundant-parent reth3
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 95.99.99.1/8
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth3 redundant-ether-options redundancy-group 1
```

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

To configure a chassis cluster:



NOTE: Perform the following steps on the primary device (node 0). They are automatically copied over to the secondary device (node 1) when you execute a **commit** command.

1. Configure control ports for the clusters.

```
[edit chassis cluster]
user@host# set control-ports fpc 0 port 0
user@host# set control-ports fpc 6 port 0
```
2. Configure the fabric (data) ports of the cluster that are used to pass RTOs in active/passive mode.

```
[edit interfaces]
user@host# set fab0 fabric-options member-interfaces ge-1/1/0
user@host# set fab1 fabric-options member-interfaces ge-7/1/0
```
3. Assign some elements of the configuration to a specific member. Configure out-of-band management on the fxp0 interface of the SRX Services Gateway using separate IP addresses for the individual control planes of the cluster.

```
[edit]
user@host# set groups node0 system host-name SRX5800-1
user@host# set groups node0 interfaces fxp0 unit 0 family inet address 10.157.90.24/9
user@host# set groups node0 system backup-router 10.157.64.1 destination 0.0.0.0/0
user@host# set groups node1 system host-name SRX5800-2
user@host# set groups node1 interfaces fxp0 unit 0 family inet address 10.157.90.23/19
user@host# set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
user@host# set apply-groups "${node}"
```
4. Configure redundancy groups for chassis clustering.

```
[edit chassis cluster]
user@host# set reth-count 5
user@host# set redundancy-group 0 node 0 priority 200
user@host# set redundancy-group 0 node 1 priority 100
user@host# set redundancy-group 1 node 0 priority 200
user@host# set redundancy-group 1 node 1 priority 100
```
5. Configure the data interfaces on the platform so that in the event of a data plane failover, the other chassis cluster member can take over the connection seamlessly.


```
[edit interfaces]
user@host# set ge-1/0/0 gigether-options redundant-parent reth0
user@host# set ge-1/0/1 gigether-options redundant-parent reth1
user@host# set ge-1/0/2 gigether-options redundant-parent reth2
user@host# set ge-1/0/3 gigether-options redundant-parent reth3
user@host# set ge-7/0/0 gigether-options redundant-parent reth0
user@host# set ge-7/0/1 gigether-options redundant-parent reth1
user@host# set ge-7/0/2 gigether-options redundant-parent reth2
user@host# set ge-7/0/3 gigether-options redundant-parent reth3
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 95.99.99.1/8
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth2 redundant-ether-options redundancy-group 1
user@host# set reth3 redundant-ether-options redundancy-group 1
```

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

```
user@host> show configuration
version ;
groups {
  node0 {
    system {
      host-name SRX58001;
      backup-router 10.157.64.1 destination 0.0.0.0/0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 10.157.90.24/9;
          }
        }
      }
    }
  }
  node1 {
    system {
      host-name SRX58002;
      backup-router 10.157.64.1 destination 0.0.0.0/0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 10.157.90.23/19;
          }
        }
      }
    }
  }
}
apply-groups "${node}";
chassis {
```

```
cluster {
    control-link-recovery;
    reth-count 5;
    control-ports {
        fpc 0 port 0;
        fpc 6 port 0;
    }
    redundancy-group 0 {
        node 0 priority 200;
        node 1 priority 100;
    }
    redundancy-group 1 {
        node 0 priority 200;
        node 1 priority 100;
    }
}
}
interfaces {
    ge-1/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-1/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-1/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-1/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    ge-7/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-7/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-7/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-7/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
}
fab0 {
    fabric-options {
        member-interfaces {
```

```

        ge-1/1/0;
    }
}
fab1 {
    fabric-options {
        member-interfaces {
            ge-7/1/0;
        }
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 95.99.99.1/8;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
reth2 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
reth3 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
}

```

Logical System Configuration (Master Administrator)

CLI Quick Configuration To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.



NOTE: You are prompted to enter and then reenter plain-text passwords.

On {primary:node0}

```

set logical-systems LSYS1
set logical-systems LSYS2
set logical-systems LSYS0
set system login class lsys1 logical-system LSYS1

```

```
set system login class lsys1 permissions all
set system login user lsys1admin full-name lsys1-admin
set system login user lsys1admin class lsys1
set user lsys1admin authentication plain-text-password
set system login class lsys2 logical-system LSYS2
set system login class lsys2 permissions all
set system login user lsys2admin full-name lsys2-admin
set system login user lsys2admin class lsys2
set system login user lsys2admin authentication plain-text-password
set system security-profile SP-root policy maximum 200
set system security-profile SP-root policy reserved 100
set system security-profile SP-root zone maximum 200
set system security-profile SP-root zone reserved 100
set system security-profile SP-root flow-session maximum 200
set system security-profile SP-root flow-session reserved 100
set system security-profile SP-root root-logical-system
set system security-profile SP0 logical-system LSYS0
set system security-profile SP1 policy maximum 100
set system security-profile SP1 policy reserved 50
set system security-profile SP1 zone maximum 100
set system security-profile SP1 zone reserved 50
set system security-profile SP1 flow-session maximum 100
set system security-profile SP1 flow-session reserved 50
set system security-profile SP1 logical-system LSYS1
set system security-profile SP2 policy maximum 100
set system security-profile SP2 policy reserved 50
set system security-profile SP2 zone maximum 100
set system security-profile SP2 zone reserved 50
set system security-profile SP2 flow-session maximum 100
set system security-profile SP2 flow-session reserved 50
set system security-profile SP2 logical-system LSYS2
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet address 2.1.1.1/24
set routing-instances vr0 instance-type virtual-router
set routing-instances vr0 interface lt-0/0/0.1
set routing-instances vr0 interface reth0.0
set routing-instances vr0 routing-options static route 85.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr0 routing-options static route 75.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr0 routing-options static route 65.0.0.0/8 next-hop 2.1.1.5
set security zones security-zone root-trust host-inbound-traffic system-services all
set security zones security-zone root-trust host-inbound-traffic protocols all
set security zones security-zone root-trust interfaces reth0.0
set security zones security-zone root-untrust host-inbound-traffic system-services all
set security zones security-zone root-untrust host-inbound-traffic protocols all
set security zones security-zone root-untrust interfaces lt-0/0/0.1
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match source-address any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match destination-address any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match application any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust then permit
set security policies from-zone root-untrust to-zone root-trust policy
    root-Untrust_to_root-Trust match source-address any
```

```

set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match destination-address any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match application any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust then permit
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match source-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match destination-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match application any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust then permit
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match source-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match destination-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match application any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  then permit
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems LSYS0 routing-instances vr instance-type vpls
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.0
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.2
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.4
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet address 2.1.1.3/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet address 2.1.1.5/24

```

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 create logical systems and user logical system administrators and configure the master and interconnect logical systems:

1. Create the interconnect and user logical systems.

```

[edit logical-systems]
user@host# set LSYS0
user@host# set LSYS1
user@host# set LSYS2

```

2. Configure user logical system administrators.

a. Configure the user logical system administrator for LSYS1.

```
[edit system login]
user@host# set class lsys1 logical-system LSYS1
user@host# set class lsys1 permissions all
user@host# set user lsys1admin full-name lsys1-admin
user@host# set user lsys1admin class lsys1
user@host# set user lsys1admin authentication plain-text-password
```

b. Configure the user logical system administrator for LSYS2.

```
[edit system login]
user@host# set class lsys2 logical-system LSYS2
user@host# set class lsys2 permissions all
user@host# set user lsys2admin full-name lsys2-admin
user@host# set user lsys2admin class lsys2
user@host# set user lsys2admin authentication plain-text-password
```

3. Configure security profiles and assign them to logical systems.

a. Configure a security profile and assign it to the root logical system.

```
[edit system security-profile]
user@host# set SP-root policy maximum 200
user@host# set SP-root policy reserved 100
user@host# set SP-root zone maximum 200
user@host# set SP-root zone reserved 100
user@host# set SP-root flow-session maximum 200
user@host# set SP-root flow-session reserved 100
user@host# set SP-root root-logical-system
```

b. Assign a dummy security profile containing no resources to the interconnect logical system LSYS0.

```
[edit system security-profile]
user@host# set SP0 logical-system LSYS0
```

c. Configure a security profile and assign it to LSYS1.

```
[edit system security-profile]
user@host# set SP1 policy maximum 100
user@host# set SP1 policy reserved 50
user@host# set SP1 zone maximum 100
user@host# set SP1 zone reserved 50
user@host# set SP1 flow-session maximum 100
user@host# set SP1 flow-session reserved 50
user@host# set SP1 logical-system LSYS1
```

d. Configure a security profile and assign it to LSYS2.

```
[edit system security-profile]
user@host# set SP2 policy maximum 100
user@host# set SP2 policy reserved 50
```

```
user@host# set SP2 zone maximum 100
user@host# set SP2 zone reserved 50
user@host# set SP2 flow-session maximum 100
user@host# set SP2 flow-session reserved 50
user@host# set SP2 logical-system LSYS2
```

4. Configure the master logical system.

a. Configure logical tunnel interfaces.

```
[edit interfaces]
user@host# set lt-0/0/0 unit 1 encapsulation ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet address 2.1.1.1/24
```

b. Configure a routing instance.

```
[edit routing-instances]
user@host# set vr0 instance-type virtual-router
user@host# set vr0 interface lt-0/0/0.1
user@host# set vr0 interface reth0.0
user@host# set vr0 routing-options static route 85.0.0.0/8 next-hop 2.1.1.3
user@host# set vr0 routing-options static route 75.0.0.0/8 next-hop 2.1.1.3
user@host# set vr0 routing-options static route 65.0.0.0/8 next-hop 2.1.1.5
```

c. Configure zones.

```
[edit security zones]
user@host# set security-zone root-trust host-inbound-traffic system-services
all
user@host# set security-zone root-trust host-inbound-traffic protocols all
user@host# set security-zone root-trust interfaces reth0.0
user@host# set security-zone root-untrust host-inbound-traffic system-services
all
user@host# set security-zone root-untrust host-inbound-traffic protocols all
user@host# set security-zone root-untrust interfaces lt-0/0/0.1
```

d. Configure security policies.

```
[edit security policies from-zone root-trust to-zone root-untrust]
user@host# set policy root-Trust_to_root-Untrust match source-address any
user@host# set policy root-Trust_to_root-Untrust match destination-address
any
user@host# set policy root-Trust_to_root-Untrust match application any
user@host# set policy root-Trust_to_root-Untrust then permit
```

```
[edit security policies from-zone root-untrust to-zone root-trust]
user@host# set policy root-Untrust_to_root-Trust match source-address any
user@host# set policy root-Untrust_to_root-Trust match destination-address
any
user@host# set policy root-Untrust_to_root-Trust match application any
user@host# set policy root-Untrust_to_root-Trust then permit
```

```
[edit security policies from-zone root-untrust to-zone root-untrust]
user@host# set policy root-Untrust_to_root-Untrust match source-address any
```

```
user@host# set policy root-Untrust_to_root-Untrust match destination-address
any
user@host# set policy root-Untrust_to_root-Untrust match application any
user@host# set policy root-Untrust_to_root-Untrust then permit

[edit security policies from-zone root-trust to-zone root-trust]
user@host# set policy root-Trust_to_root-Trust match source-address any
user@host# set policy root-Trust_to_root-Trust match destination-address any
user@host# set policy root-Trust_to_root-Trust match application any
user@host# set policy root-Trust_to_root-Trust then permit
```

5. Configure the interconnect logical system.

a. Configure logical tunnel interfaces.

```
[edit logical-systems LSYS0 interfaces]
user@host# set lt-0/0/0 unit 0 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 0 peer-unit 1
user@host# set lt-0/0/0 unit 2 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 2 peer-unit 3
user@host# set lt-0/0/0 unit 4 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 4 peer-unit 5
```

b. Configure the VPLS routing instance.

```
[edit logical-systems LSYS0 routing-instances]
user@host# set vr instance-type vpls
user@host# set vr interface lt-0/0/0.0
user@host# set vr interface lt-0/0/0.2
user@host# set vr interface lt-0/0/0.4
```

6. Configure logical tunnel interfaces for the user logical systems.

a. Configure logical tunnel interfaces for LSYS1.

```
[edit logical-systems LSYS1 interfaces ]
user@host# set lt-0/0/0 unit 3 encapsulation ethernet
user@host# set lt-0/0/0 unit 3 peer-unit 2
user@host# set lt-0/0/0 unit 3 family inet address 2.1.1.3/24
```

b. Configure logical tunnel interfaces for LSYS2.

```
[edit logical-systems LSYS2 interfaces ]
user@host# set lt-0/0/0 unit 5 encapsulation ethernet
user@host# set lt-0/0/0 unit 5 peer-unit 4
user@host# set lt-0/0/0 unit 5 family inet address 2.1.1.5/24
```

Results From configuration mode, confirm the configuration for LSYS0 by entering the **show logical-systems LSYS0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS0
interfaces {
```



```
lt-0/0/0 {  
  unit 0 {  
    encapsulation ethernet-vpls;  
    peer-unit 1;  
  }  
  unit 2 {  
    encapsulation ethernet-vpls;  
    peer-unit 3;  
  }  
  unit 4 {  
    encapsulation ethernet-vpls;  
    peer-unit 5;  
  }  
}  
}  
routing-instances {  
  vr {  
    instance-type vpls;  
    interface lt-0/0/0.0;  
    interface lt-0/0/0.2;  
    interface lt-0/0/0.4;  
  }  
}
```

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

```
[edit]  
user@host# show interfaces  
lt-0/0/0 {  
  unit 1 {  
    encapsulation ethernet;  
    peer-unit 0;  
    family inet {  
      address 2.1.1.1/24;  
    }  
  }  
}  
ge-1/0/0 {  
  gigether-options {  
    redundant-parent reth0;  
  }  
}  
ge-1/0/1 {  
  gigether-options {  
    redundant-parent reth1;  
  }  
}  
ge-1/0/2 {  
  gigether-options {  
    redundant-parent reth2;  
  }  
}  
ge-1/0/3 {
```

```
    gigether-options {
        redundant-parent reth3;
    }
}
ge-7/0/0 {
    gigether-options {
        redundant-parent reth0;
    }
}
ge-7/0/1 {
    gigether-options {
        redundant-parent reth1;
    }
}
ge-7/0/2 {
    gigether-options {
        redundant-parent reth2;
    }
}
ge-7/0/3 {
    gigether-options {
        redundant-parent reth3;
    }
}
fab0 {
    fabric-options {
        member-interfaces {
            ge-1/1/0;
        }
    }
}
fab1 {
    fabric-options {
        member-interfaces {
            ge-7/1/0;
        }
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 95.99.99.1/8;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
reth2 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
```

```
    }
  }
  reth3 {
    redundant-ether-options {
      redundancy-group 1;
    }
  }
[edit]
user@host# show routing-instances
vr0 {
  instance-type virtual-router;
  interface lt-0/0/0.1;
  interface reth0.0;
  routing-options {
    static {
      route 85.0.0.0/8 next-hop 2.1.1.3;
      route 75.0.0.0/8 next-hop 2.1.1.3;
      route 65.0.0.0/8 next-hop 2.1.1.5;
    }
  }
}
[edit]
user@host# show security
policies {
  from-zone root-trust to-zone root-untrust {
    policy root-Trust_to_root-Untrust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
      }
    }
  }
  from-zone root-untrust to-zone root-trust {
    policy root-Untrust_to_root-Trust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
      }
    }
  }
  from-zone root-untrust to-zone root-untrust {
    policy root-Untrust_to_root-Untrust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
```

```

        permit;
    }
}
}
from-zone root-trust to-zone root-trust {
    policy root-Trust_to_root-Trust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
}
zones {
    security-zone root-trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            reth0.0;
        }
    }
    security-zone root-untrust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            lt-0/0/0.1;
        }
    }
}
}

```

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

User Logical System Configuration (User Logical System Administrator)

CLI Quick Configuration

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

Enter the following commands while logged in as the user logical system administrator for LSYS1:

```

set interfaces reth1 unit 0 family inet address 85.88.88.1/8
set interfaces reth2 unit 0 family inet address 75.77.77.1/8
set routing-instances vr11 instance-type virtual-router
set routing-instances vr11 interface lt-0/0/0.3
set routing-instances vr11 interface reth1.0
set routing-instances vr11 routing-options static route 65.0.0.0/8 next-hop 2.1.1.5
set routing-instances vr11 routing-options static route 95.0.0.0/8 next-hop 2.1.1.1
set routing-instances vr12 instance-type virtual-router
set routing-instances vr12 interface reth2.0
set routing-instances vr12 routing-options interface-routes rib-group inet vr11vr12v4
set routing-instances vr12 routing-options static route 85.0.0.0/8 next-table vr11.inet.0
set routing-instances vr12 routing-options static route 95.0.0.0/8 next-table vr11.inet.0
set routing-instances vr12 routing-options static route 65.0.0.0/8 next-table vr11.inet.0
set routing-instances vr12 routing-options static route 2.1.1.0/24 next-table vr11.inet.0
set routing-options rib-groups vr11vr12v4 import-rib vr11.inet.0
set routing-options rib-groups vr11vr12v4 import-rib vr12.inet.0
set security zones security-zone lsys1-trust host-inbound-traffic system-services all
set security zones security-zone lsys1-trust host-inbound-traffic protocols all
set security zones security-zone lsys1-trust interfaces reth1.0
set security zones security-zone lsys1-trust interfaces lt-0/0/0.3
set security zones security-zone lsys1-untrust host-inbound-traffic system-services all
set security zones security-zone lsys1-untrust host-inbound-traffic protocols all
set security zones security-zone lsys1-untrust interfaces reth2.0
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
    lsys1trust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
    lsys1trust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
    lsys1trust-to-lsys1untrust match application any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
    lsys1trust-to-lsys1untrust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
    lsys1untrust-to-lsys1trust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
    lsys1untrust-to-lsys1trust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
    lsys1untrust-to-lsys1trust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
    lsys1untrust-to-lsys1trust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
    lsys1untrust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
    lsys1untrust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
    lsys1untrust-to-lsys1untrust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
    lsys1untrust-to-lsys1untrust then permit
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
    match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
    match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
    match application any

```

```
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
then permit
```

Enter the following commands while logged in as the user logical system administrator for LSYS2:

```
set interfaces reth3 unit 0 family inet address 65.66.66.1/8
set routing-instances vr2 instance-type virtual-router
set routing-instances vr2 interface lt-0/0/0.5
set routing-instances vr2 interface reth3.0
set routing-instances vr2 routing-options static route 75.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr2 routing-options static route 85.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr2 routing-options static route 95.0.0.0/8 next-hop 2.1.1.1
set security zones security-zone lsys2-trust host-inbound-traffic system-services all
set security zones security-zone lsys2-trust host-inbound-traffic protocols all
set security zones security-zone lsys2-trust interfaces reth3.0
set security zones security-zone lsys2-untrust host-inbound-traffic system-services all
set security zones security-zone lsys2-untrust host-inbound-traffic protocols all
set security zones security-zone lsys2-untrust interfaces lt-0/0/0.5
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match application any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust then permit
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match application any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust then permit
```

Step-by-Step Procedure



NOTE: The user logical system administrator performs the following configuration while logged in to his or her user logical system. The master administrator can also configure a user logical system at the [edit logical-systems *logical-system*] hierarchy level.

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 the LSYS1 user logical system:

1. Configure interfaces.

```
[edit interfaces]
lsys1-admin@host:LSYS1# set reth1 unit 0 family inet address 85.88.88.1/8
lsys1-admin@host:LSYS1# set reth2 unit 0 family inet address 75.77.77.1/8
```

2. Configure routing.

```
[edit routing-instances]
lsys1-admin@host:LSYS1# set vr11 instance-type virtual-router
lsys1-admin@host:LSYS1# set vr11 interface lt-0/0/0.3
lsys1-admin@host:LSYS1# set vr11 interface reth1.0
lsys1-admin@host:LSYS1# set vr11 routing-options static route 65.0.0.0/8 next-hop
2.1.1.5
lsys1-admin@host:LSYS1# set vr11 routing-options static route 95.0.0.0/8 next-hop
2.1.1.1
lsys1-admin@host:LSYS1# set vr12 instance-type virtual-router
lsys1-admin@host:LSYS1# set vr12 interface reth2.0
lsys1-admin@host:LSYS1# set vr12 routing-options interface-routes rib-group inet
vr11vr12v4
lsys1-admin@host:LSYS1# set vr12 routing-options static route 85.0.0.0/8 next-table
vr11.inet.0
lsys1-admin@host:LSYS1# set vr12 routing-options static route 95.0.0.0/8 next-table
vr11.inet.0
lsys1-admin@host:LSYS1# set vr12 routing-options static route 65.0.0.0/8 next-table
vr11.inet.0
lsys1-admin@host:LSYS1# set vr12 routing-options static route 2.1.1.0/24 next-table
vr11.inet.0

[edit routing-options]
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v4 import-rib vr11.inet.0
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v4 import-rib vr12.inet.0
```

3. Configure zones and security policies.

```
[edit security zones]
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces reth1.0
```

```

lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces lt-0/0/0.3
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust interfaces reth2.0

[edit security policies from-zone lsys1-trust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match source-address
any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match application
any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match source-address
any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match application
any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
source-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match application
any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-trust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match source-address
any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match application any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust then permit

```

Step-by-Step Procedure To configure the LSYS2 user logical system:

1. Configure interfaces.

```

[edit interfaces]
lsys2-admin@host:LSYS2# set reth3 unit 0 family inet address 65.66.66.1/8

```
2. Configure routing.

```

[edit routing-instances]
lsys2-admin@host:LSYS2# set vr2 instance-type virtual-router
lsys2-admin@host:LSYS2# set vr2 interface lt-0/0/0.5
lsys2-admin@host:LSYS2# set vr2 interface reth3.0

```



```

lsys2-admin@host:LSYS2# set vr2 routing-options static route 75.0.0.0/8 next-hop
2.1.1.3
lsys2-admin@host:LSYS2# set vr2 routing-options static route 85.0.0.0/8 next-hop
2.1.1.3
lsys2-admin@host:LSYS2# set vr2 routing-options static route 95.0.0.0/8 next-hop
2.1.1.1

```

3. Configure zones and security policies.

```

[edit security zones]
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust interfaces reth3.0
lsys2-admin@host:LSYS2# set security zones security-zone lsys2-untrust
host-inbound-traffic system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust host-inbound-traffic
protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust interfaces lt-0/0/0.5

[edit security policies from-zone lsys2-trust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
source-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match application
any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust then permit

[edit security policies from-zone from-zone lsys2-untrust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match application
any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust then permit

[edit security policies from-zone lsys2-untrust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match application
any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust then permit

[edit security policies from-zone lsys2-trust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match source-address
any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match application
any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust then permit

```

Results From configuration mode, confirm the configuration for LSYS1 by entering the **show interfaces**, **show routing-instances**, **show routing-options**, and **show security** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]

lsys1-admin@host:LSYS1# show interfaces

```
interfaces {
  lt-0/0/0 {
    unit 3 {
      encapsulation ethernet;
      peer-unit 2;
      family inet {
        address 2.1.1.3/24;
      }
    }
  }
  reth1 {
    unit 0 {
      family inet {
        address 85.88.88.1/8;
      }
    }
  }
  reth2 {
    unit 0 {
      family inet {
        address 75.77.77.1/8;
      }
    }
  }
}
```

[edit]

lsys1-admin@host:LSYS1# show routing-instances

```
routing-instances {
  vr11 {
    instance-type virtual-router;
    interface lt-0/0/0.3;
    interface reth1.0;
    routing-options {
      static {
        route 65.0.0.0/8 next-hop 2.1.1.5;
        route 95.0.0.0/8 next-hop 2.1.1.1;
      }
    }
  }
  vr12 {
    instance-type virtual-router;
    interface reth2.0;
    routing-options {
      interface-routes {
        rib-group inet vr11vr12v4;
      }
      static {
        route 85.0.0.0/8 next-table vr11.inet.0;
      }
    }
  }
}
```

```

        route 95.0.0.0/8 next-table vr11.inet.0;
        route 65.0.0.0/8 next-table vr11.inet.0;
        route 2.1.1.0/24 next-table vr11.inet.0;
    }
}
}
[edit]
lsys1-admin@host:LSYS1# show routing-options
rib-groups {
    vr11vr12v4 {
        import-rib [ vr11.inet.0 vr12.inet.0 ];
    }
}
[edit]
lsys1-admin@host:LSYS1# show security
security {
    policies {
        from-zone lsys1-trust to-zone lsys1-untrust {
            policy lsys1trust-to-lsys1untrust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone lsys1-untrust to-zone lsys1-trust {
            policy lsys1untrust-to-lsys1trust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone lsys1-untrust to-zone lsys1-untrust {
            policy lsys1untrust-to-lsys1untrust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone lsys1-trust to-zone lsys1-trust {
            policy lsys1trust-to-lsys1trust {

```

```

        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
}
zones {
    security-zone lsys1-trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            reth1.0;
            lt-0/0/0.3;
        }
    }
    security-zone lsys1-untrust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            reth2.0;
        }
    }
}
}

```

From configuration mode, confirm the configuration for LSYS2 by entering the **show interfaces**, **show routing-instances**, and **show security** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

lsys2-admin@host:LSYS2# show interfaces
[edit]
interfaces {
    lt-0/0/0 {
        unit 5 {
            encapsulation ethernet;
            peer-unit 4;
            family inet {
                address 2.1.1.5/24;
            }
        }
    }
}

```

```

    }
  }
}
reth3 {
  unit 0 {
    family inet {
      address 65.66.66.1/8;
    }
  }
}
}
[edit]
lsys2-admin@host:LSYS2# show routing-instances
routing-instances {
  vr2 {
    instance-type virtual-router;
    interface lt-0/0/0.5;
    interface reth3.0;
    routing-options {
      static {
        route 75.0.0.0/8 next-hop 2.1.1.3;
        route 85.0.0.0/8 next-hop 2.1.1.3;
        route 95.0.0.0/8 next-hop 2.1.1.1;
      }
    }
  }
}
[edit]
lsys2-admin@host:LSYS2# show security
security {
  policies {
    from-zone lsys2-trust to-zone lsys2-untrust {
      policy lsys2trust-to-lsys2untrust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys2-untrust to-zone lsys2-trust {
      policy lsys2untrust-to-lsys2trust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
  }
  from-zone lsys2-untrust to-zone lsys2-untrust {

```

```
policy lsys2untrust-to-lsys2untrust {
  match {
    source-address any;
    destination-address any;
    application any;
  }
  then {
    permit;
  }
}
}
from-zone lsys2-trust to-zone lsys2-trust {
  policy lsys2trust-to-lsys2trust {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
}
zones {
  security-zone lsys2-trust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      reth3.0;
    }
  }
  security-zone lsys2-untrust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      lt-0/0/0.5;
    }
  }
}
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Chassis Cluster Status on page 303](#)
- [Troubleshooting Chassis Cluster with Logs on page 303](#)
- [Verifying Logical System Licenses on page 303](#)
- [Verifying Logical System License Usage on page 304](#)
- [Verifying Intra-Logical System Traffic on a Logical System on page 304](#)
- [Verifying Intra-Logical System Traffic Within All Logical Systems on page 305](#)
- [Verifying Traffic Between User Logical Systems on page 306](#)

Verifying Chassis Cluster Status

Purpose Verify the chassis cluster status, failover status, and redundancy group information.

Action From operational mode, enter the **show chassis cluster status** command.

```
{primary:node0}
show chassis cluster status
Cluster ID: 1
```

Node	Priority	Status	Preempt	Manual failover
Redundancy group: 0 , Failover count: 1				
node0	200	primary	no	no
node1	100	secondary	no	no
Redundancy group: 1 , Failover count: 1				
node0	200	primary	no	no
node1	100	secondary	no	no

Troubleshooting Chassis Cluster with Logs

Purpose Identify any chassis cluster issues by looking at the logs on both nodes.

Action From operational mode, enter these **show log** commands.

```
user@host> show log jsrpd
user@host> show log chassisd
user@host> show log messages
user@host> show log dcd
user@host> show traceoptions
```

Verifying Logical System Licenses

Purpose Verify information about logical system licenses.

Action From operational mode, enter the **show system license status logical-system all** command.

```
{primary:node0}
user@host> show system license status logical-system all
node0:
-----
Logical system license status:

logical system name          license status
root-logical-system         enabled
LSYS0                        enabled
LSYS1                        enabled
LSYS2                        enabled
```

Verifying Logical System License Usage

Purpose Verify information about logical system license usage.



NOTE: The actual number of licenses used is only displayed on the primary node.

Action From operational mode, enter the **show system license** command.

```
{primary:node0}
user@host> show system license
License usage:

Feature name          Licenses used  Licenses installed  Licenses needed  Expiry
logical-system         4              25                  0                permanent

Licenses installed:
License identifier: JUNOS305013
License version: 2
Valid for device: JN110B54BAGB
Features:
  logical-system-25 - Logical System Capacity
  permanent
```

Verifying Intra-Logical System Traffic on a Logical System

Purpose Verify information about currently active security sessions within a logical system.

Action From operational mode, enter the **show security flow session logical-system LSYS1** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1
node0:
-----
```



```

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000114, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1782, Valid
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 33, Bytes: 1881

  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 28, Bytes: 2329
Total sessions: 1

node1:
-----

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000001, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14388, Valid
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1

```

Verifying Intra-Logical System Traffic Within All Logical Systems

Purpose Verify information about currently active security sessions on all logical systems.

Action From operational mode, enter the **show security flow session logical-system all** command.

```

{primary:node0}
user@host> show security flow session logical-system all
node0:
-----

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000114, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1776, Valid
Logical system: LSYS1
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 33, Bytes: 1881

  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 28, Bytes: 2329
Total sessions: 1

```

```
node1:
-----

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000001, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14382, Valid
Logical system: LSYS1
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

Verifying Traffic Between User Logical Systems

Purpose Verify information about currently active security sessions between logical systems.

Action From operational mode, enter the **show security flow session logical-system *logical-system-name*** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1

node0:
-----

Flow Sessions on FPC0 PIC1:

Session ID: 10000094, Policy name: root-Untrust_to_root-Trust/5, State: Active,
Timeout: 1768, Valid
  In: 75.77.77.2/34590 --> 95.99.99.2/23;tcp, If: lt-0/0/0.1, Pkts: 23, Bytes:
1351
  Out: 95.99.99.2/23 --> 75.77.77.2/34590;tcp, If: reth0.0, Pkts: 22, Bytes: 1880
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
-----

Flow Sessions on FPC0 PIC1:

Session ID: 10000002, Policy name: root-Untrust_to_root-Trust/5, State: Backup,
Timeout: 14384, Valid
  In: 75.77.77.2/34590 --> 95.99.99.2/23;tcp, If: lt-0/0/0.1, Pkts: 0, Bytes: 0
  Out: 95.99.99.2/23 --> 75.77.77.2/34590;tcp, If: reth0.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC0:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
{primary:node0}
user@host> show security flow session logical-system LSYS2
```

```
node0:
```

```
-----
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000089, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
Timeout: 1790, Valid
In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 40, Bytes:
2252
Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 32, Bytes: 2114
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
node1:
```

```
-----
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000002, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
Timeout: 14398, Valid
In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
{primary:node0}
user@host> show security flow session logical-system all
```

```
node0:
```

```
-----
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000088, Policy name: lsys1trust-to-lsys1trust/11, State: Active,
Timeout: 1782, Valid
Logical system: LSYS1
In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: reth1.0, Pkts: 40, Bytes: 2252
```

```
Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: lt-0/0/0.3, Pkts: 32, Bytes:
2114

Session ID: 80000089, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
Timeout: 1782, Valid
Logical system: LSYS2
In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 40, Bytes:
2252
Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 32, Bytes: 2114
Total sessions: 2

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
-----

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000001, Policy name: lsys1trust-to-lsys1trust/11, State: Backup,
Timeout: 14382, Valid
Logical system: LSYS1
In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: lt-0/0/0.3, Pkts: 0, Bytes: 0

Session ID: 80000002, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
Timeout: 14390, Valid
Logical system: LSYS2
In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

- See Also**
- [Understanding Logical Systems in the Context of Chassis Cluster on page 274](#)
 - [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(IPv6\) \(Master Administrators Only\) on page 308](#)
 - [Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices](#)
 - [Chassis Cluster Overview](#)

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) (Master Administrators Only)

This example shows how to configure logical systems in a basic active/passive chassis cluster with IPv6 addresses.



NOTE: The master administrator configures the chassis cluster and creates logical systems (including an optional interconnect logical system), administrators, and security profiles. Either the master administrator or the user logical system administrator configures a user logical system. The configuration is synchronized between nodes in the cluster.

- [Requirements on page 309](#)
- [Overview on page 309](#)
- [Configuration on page 312](#)
- [Verification on page 336](#)

Requirements

Before you begin:

- Obtain two SRX Series Services Gateways with identical hardware configurations. See *Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices*. This chassis cluster deployment scenario includes the configuration of the SRX Series device for connections to an MX240 edge router and an EX8208 Ethernet Switch.
- Physically connect the two devices (back-to-back for the fabric and control ports) and ensure that they are the same models. You can configure both the fabric and control ports on the SRX5000 line. For the SRX1400 or SRX1500 devices or the SRX3000 line, you can configure the fabric ports only. (Platform support depends on the Junos OS release in your installation.)
- Set the chassis cluster ID and node ID on each device and reboot the devices to enable clustering. See *Example: Setting the Node ID and Cluster ID for SRX Series Devices in a Chassis Cluster*.



NOTE: For this example, chassis cluster and logical system configuration is performed on the primary (node 0) device at the root level by the master administrator. Log in to the device as the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).



NOTE: When you use SRX Series devices running logical systems in a chassis cluster, you must purchase and install the same number of logical system licenses for each node in the chassis cluster. Logical system licenses pertain to a single chassis or node within a chassis cluster and not to the cluster collectively.

Overview

In this example, the basic active/passive chassis cluster consists of two devices:

- One device actively provides logical systems, along with maintaining control of the chassis cluster.
- The other device passively maintains its state for cluster failover capabilities should the active device become inactive.



NOTE: Logical systems in an active/active chassis cluster are configured in a similar manner as for logical systems in an active/passive chassis cluster. For active/active chassis clusters, there can be multiple redundancy groups that can be primary on different nodes.

The master administrator configures the following logical systems on the primary device (node 0):

- Master logical system—The master administrator configures a security profile to provision portions of the system's security resources to the master logical system and configures the resources of the master logical system.
- User logical systems LSYS1 and LSYS2 and their administrators—The master administrator also configures security profiles to provision portions of the system's security resources to user logical systems. The user logical system administrator can then configure interfaces, routing, and security resources allocated to his or her logical system.
- Interconnect logical system LSYS0 that connects logical systems on the device—The master administrator configures logical tunnel interfaces between the interconnect logical system and each logical system. These peer interfaces effectively allow for the establishment of tunnels.



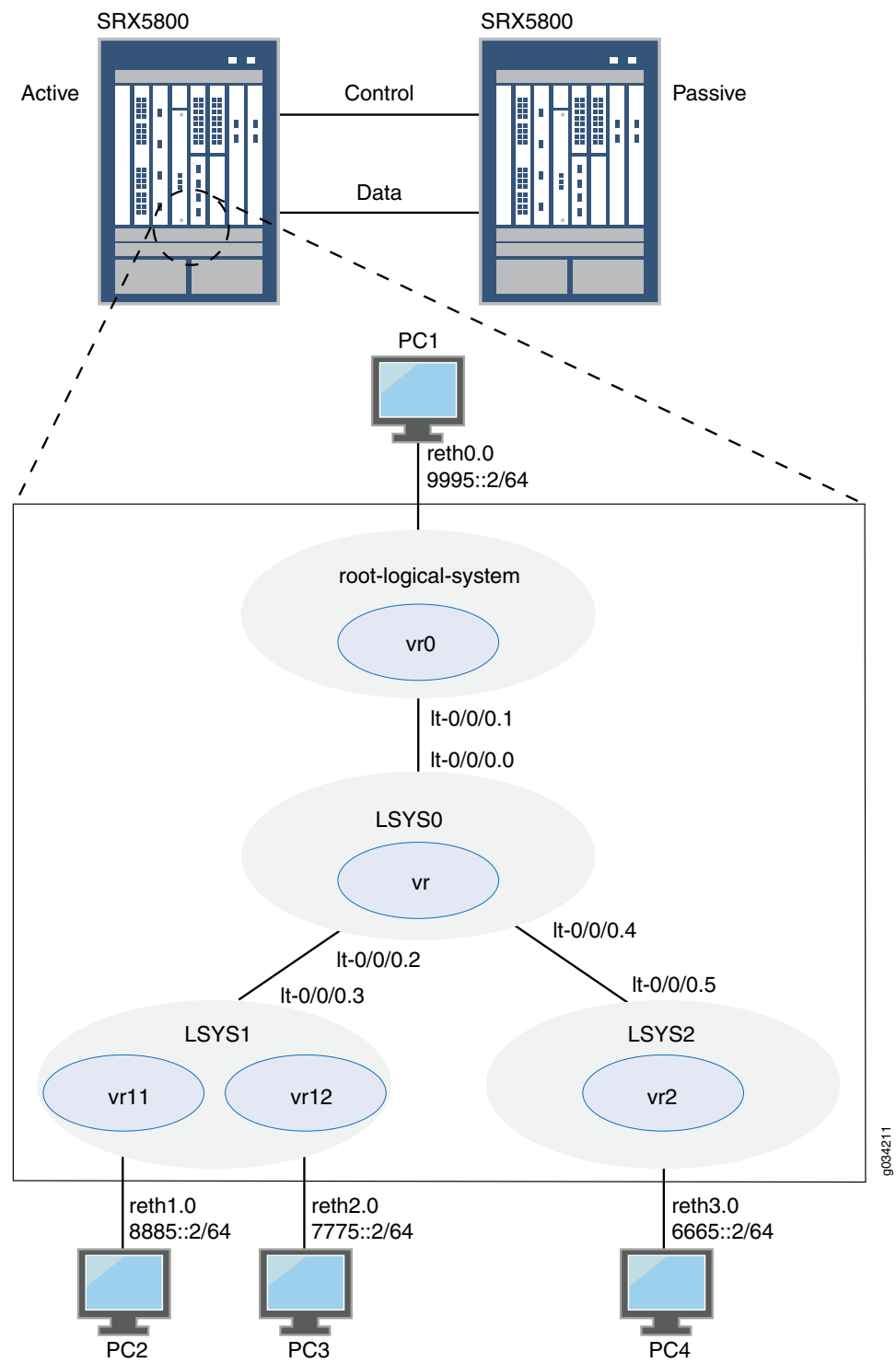
NOTE: This example does not describe configuring features such as NAT, IDP, or VPNs for a logical system. See [“SRX Series Logical Systems Master Administrator Configuration Tasks Overview” on page 41](#) and [“User Logical Systems Configuration Overview” on page 61](#) for more information about features that can be configured for logical systems.

If you are performing proxy ARP in a chassis cluster configuration, you must apply the proxy ARP configuration to the reth interfaces rather than the member interfaces because the reth interfaces contain the logical configurations. See *Configuring Proxy ARP for NAT (CLI Procedure)*.

Topology

[Figure 9 on page 311](#) shows the topology used in this example.

Figure 9: Logical Systems in a Chassis Cluster (IPv6)



Configuration

- [Chassis Cluster Configuration with IPv6 Addresses \(Master Administrator\) on page 312](#)
- [Logical System Configuration with IPv6 Addresses \(Master Administrator\) on page 316](#)
- [User Logical System Configuration with IPv6 \(User Logical System Administrator\) on page 326](#)

Chassis Cluster Configuration with IPv6 Addresses (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

On {primary:node0}

```
set chassis cluster control-ports fpc 0 port 0
set chassis cluster control-ports fpc 6 port 0
set interfaces fab0 fabric-options member-interfaces ge-1/1/0
set interfaces fab1 fabric-options member-interfaces ge-7/1/0
set groups node0 system host-name SRX5800-1
set groups node0 interfaces fxp0 unit 0 family inet address 10.157.90.24/9
set groups node0 system backup-router 10.157.64.1 destination 0.0.0.0/0
set groups node1 system host-name SRX5800-2
set groups node1 interfaces fxp0 unit 0 family inet address 10.157.90.23/19
set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
set apply-groups "${node}"
set chassis cluster reth-count 5
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 100
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 100
set interfaces ge-1/0/0 gigether-options redundant-parent reth0
set interfaces ge-1/0/1 gigether-options redundant-parent reth1
set interfaces ge-1/0/2 gigether-options redundant-parent reth2
set interfaces ge-1/0/3 gigether-options redundant-parent reth3
set interfaces ge-7/0/0 gigether-options redundant-parent reth0
set interfaces ge-7/0/1 gigether-options redundant-parent reth1
set interfaces ge-7/0/2 gigether-options redundant-parent reth2
set interfaces ge-7/0/3 gigether-options redundant-parent reth3
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet6 address 9995::1/64
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth3 redundant-ether-options redundancy-group 1
```


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

To configure a chassis cluster:



NOTE: Perform the following steps on the primary device (node 0). They are automatically copied over to the secondary device (node 1) when you execute a **commit** command.

1. Configure control ports for the clusters.

```
[edit chassis cluster]
user@host# set control-ports fpc 0 port 0
user@host# set control-ports fpc 6 port 0
```
2. Configure the fabric (data) ports of the cluster that are used to pass RTOs in active/passive mode.

```
[edit interfaces]
user@host# set fab0 fabric-options member-interfaces ge-1/1/0
user@host# set fab1 fabric-options member-interfaces ge-7/1/0
```
3. Assign some elements of the configuration to a specific member. Configure out-of-band management on the fxp0 interface of the SRX Services Gateway using separate IP addresses for the individual control planes of the cluster.

```
[edit]
user@host# set groups node0 system host-name SRX5800-1
user@host# set groups node0 interfaces fxp0 unit 0 family inet address 10.157.90.24/9
user@host# set groups node0 system backup-router 10.157.64.1 destination 0.0.0.0/0
user@host# set groups node1 system host-name SRX5800-2
user@host# set groups node1 interfaces fxp0 unit 0 family inet address 10.157.90.23/19
user@host# set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
user@host# set apply-groups "${node}"
```
4. Configure redundancy groups for chassis clustering.

```
[edit chassis cluster]
user@host# set reth-count 5
user@host# set redundancy-group 0 node 0 priority 200
user@host# set redundancy-group 0 node 1 priority 100
user@host# set redundancy-group 1 node 0 priority 200
user@host# set redundancy-group 1 node 1 priority 100
```
5. Configure the data interfaces on the platform so that in the event of a data plane failover, the other chassis cluster member can take over the connection seamlessly.

```
[edit interfaces]
user@host# set ge-1/0/0 gigether-options redundant-parent reth0
user@host# set ge-1/0/1 gigether-options redundant-parent reth1
user@host# set ge-1/0/2 gigether-options redundant-parent reth2
user@host# set ge-1/0/3 gigether-options redundant-parent reth3
user@host# set ge-7/0/0 gigether-options redundant-parent reth0
user@host# set ge-7/0/1 gigether-options redundant-parent reth1
user@host# set ge-7/0/2 gigether-options redundant-parent reth2
user@host# set ge-7/0/3 gigether-options redundant-parent reth3
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet6 address 9995::1/64
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth2 redundant-ether-options redundancy-group 1
user@host# set reth3 redundant-ether-options redundancy-group 1
```

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

```
user@host> show configuration
version ;
groups {
  node0 {
    system {
      host-name SRX58001;
      backup-router 10.157.64.1 destination 0.0.0.0/0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 10.157.90.24/9;
          }
        }
      }
    }
  }
  node1 {
    system {
      host-name SRX58002;
      backup-router 10.157.64.1 destination 0.0.0.0/0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 10.157.90.23/19;
          }
        }
      }
    }
  }
}
apply-groups "${node}";
chassis {
```

```

cluster {
    control-link-recovery;
    reth-count 5;
    control-ports {
        fpc 0 port 0;
        fpc 6 port 0;
    }
    redundancy-group 0 {
        node 0 priority 200;
        node 1 priority 100;
    }
    redundancy-group 1 {
        node 0 priority 200;
        node 1 priority 100;
    }
}
}
interfaces {
    ge-1/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-1/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-1/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-1/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    ge-7/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-7/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-7/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-7/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    fab0 {
        fabric-options {
            member-interfaces {

```

```

        ge-1/1/0;
    }
}
fab1 {
    fabric-options {
        member-interfaces {
            ge-7/1/0;
        }
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet6 {
            address 9995::1/64;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
reth2 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
reth3 {
    redundant-ether-options {
        redundancy-group 1;
    }
}
}

```

Logical System Configuration with IPv6 Addresses (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.



NOTE: You are prompted to enter and then reenter plain-text passwords.

On {primary:node0}

```

set logical-systems LSYS1
set logical-systems LSYS2
set logical-systems LSYS0
set system login class lsyl logical-system LSYS1

```

```
set system login class lsys1 permissions all
set system login user lsys1admin full-name lsys1-admin
set system login user lsys1admin class lsys1
set user lsys1admin authentication plain-text-password
set system login class lsys2 logical-system LSYS2
set system login class lsys2 permissions all
set system login user lsys2admin full-name lsys2-admin
set system login user lsys2admin class lsys2
set system login user lsys2admin authentication plain-text-password
set system security-profile SP-root policy maximum 200
set system security-profile SP-root policy reserved 100
set system security-profile SP-root zone maximum 200
set system security-profile SP-root zone reserved 100
set system security-profile SP-root flow-session maximum 200
set system security-profile SP-root flow-session reserved 100
set system security-profile SP-root root-logical-system
set system security-profile SP0 logical-system LSYS0
set system security-profile SP1 policy maximum 100
set system security-profile SP1 policy reserved 50
set system security-profile SP1 zone maximum 100
set system security-profile SP1 zone reserved 50
set system security-profile SP1 flow-session maximum 100
set system security-profile SP1 flow-session reserved 50
set system security-profile SP1 logical-system LSYS1
set system security-profile SP2 policy maximum 100
set system security-profile SP2 policy reserved 50
set system security-profile SP2 zone maximum 100
set system security-profile SP2 zone reserved 50
set system security-profile SP2 flow-session maximum 100
set system security-profile SP2 flow-session reserved 50
set system security-profile SP2 logical-system LSYS2
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet6 address 2111::1/64
set routing-instances vr0 instance-type virtual-router
set routing-instances vr0 interface lt-0/0/0.1
set routing-instances vr0 interface reth0.0
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 8885::/64 next-hop
    2111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 7775::/64 next-hop
    2111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 6665::/64 next-hop
    2111::5
set security zones security-zone root-trust host-inbound-traffic system-services all
set security zones security-zone root-trust host-inbound-traffic protocols all
set security zones security-zone root-trust interfaces reth0.0
set security zones security-zone root-untrust host-inbound-traffic system-services all
set security zones security-zone root-untrust host-inbound-traffic protocols all
set security zones security-zone root-untrust interfaces lt-0/0/0.1
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match source-address any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match destination-address any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match application any
```

```

set security policies from-zone root-trust to-zone root-untrust policy
  root-Trust_to_root-Untrust then permit
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match source-address any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match destination-address any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match application any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust then permit
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match source-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match destination-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match application any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust then permit
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match source-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match destination-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match application any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  then permit
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems LSYS0 routing-instances vr instance-type vpls
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.0
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.2
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.4
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet6 address 2111::3/64
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet6 address 2111::5/64

```

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

To create logical systems and user logical system administrators and configure the master and interconnect logical systems:

1. Create the interconnect and user logical systems.

```

[edit logical-systems]
user@host# set LSYS0
user@host# set LSYS1

```

```
user@host# set LSYS2
```

2. Configure user logical system administrators.

- a. Configure the user logical system administrator for LSYS1.

```
[edit system login]
user@host# set class lsys1 logical-system LSYS1
user@host# set class lsys1 permissions all
user@host# set user lsys1admin full-name lsys1-admin
user@host# set user lsys1admin class lsys1
user@host# set user lsys1admin authentication plain-text-password
```

- b. Configure the user logical system administrator for LSYS2.

```
[edit system login]
user@host# set class lsys2 logical-system LSYS2
user@host# set class lsys2 permissions all
user@host# set user lsys2admin full-name lsys2-admin
user@host# set user lsys2admin class lsys2
user@host# set user lsys2admin authentication plain-text-password
```

3. Configure security profiles and assign them to logical systems.

- a. Configure a security profile and assign it to the root logical system.

```
[edit system security-profile]
user@host# set SP-root policy maximum 200
user@host# set SP-root policy reserved 100
user@host# set SP-root zone maximum 200
user@host# set SP-root zone reserved 100
user@host# set SP-root flow-session maximum 200
user@host# set SP-root flow-session reserved 100
user@host# set SP-root root-logical-system
```

- b. Assign a dummy security profile containing no resources to the interconnect logical system LSYS0.

```
[edit system security-profile]
user@host# set SP0 logical-system LSYS0
```

- c. Configure a security profile and assign it to LSYS1.

```
[edit system security-profile]
user@host# set SP1 policy maximum 100
user@host# set SP1 policy reserved 50
user@host# set SP1 zone maximum 100
user@host# set SP1 zone reserved 50
user@host# set SP1 flow-session maximum 100
user@host# set SP1 flow-session reserved 50
user@host# set SP1 logical-system LSYS1
```

- d. Configure a security profile and assign it to LSYS2.

```
[edit system security-profile]
```

```
user@host# set SP2 policy maximum 100
user@host# set SP2 policy reserved 50
user@host# set SP2 zone maximum 100
user@host# set SP2 zone reserved 50
user@host# set SP2 flow-session maximum 100
user@host# set SP2 flow-session reserved 50
user@host# set SP2 logical-system LSYS2
```

4. Configure the master logical system.

a. Configure logical tunnel interfaces.

```
[edit interfaces]
user@host# set lt-0/0/0 unit 1 encapsulation ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet6 address 2111::1/64
```

b. Configure a routing instance.

```
[edit routing-instances]
user@host# set vr0 instance-type virtual-router
user@host# set vr0 interface lt-0/0/0.1
user@host# set vr0 interface reth0.0
user@host# set vr0 routing-options rib vr0.inet6.0 static route 8885::/64
    next-hop 2111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 7775::/64 next-hop
    2111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 6665::/64
    next-hop 2111::5
```

c. Configure zones.

```
[edit security zones]
user@host# set security-zone root-trust host-inbound-traffic system-services
    all
user@host# set security-zone root-trust host-inbound-traffic protocols all
user@host# set security-zone root-trust interfaces reth0.0
user@host# set security-zone root-untrust host-inbound-traffic system-services
    all
user@host# set security-zone root-untrust host-inbound-traffic protocols all
user@host# set security-zone root-untrust interfaces lt-0/0/0.1
```

d. Configure security policies.

```
[edit security policies from-zone root-trust to-zone root-untrust]
user@host# set policy root-Trust_to_root-Untrust match source-address any
user@host# set policy root-Trust_to_root-Untrust match destination-address
    any
user@host# set policy root-Trust_to_root-Untrust match application any
user@host# set policy root-Trust_to_root-Untrust then permit

[edit security policies from-zone root-untrust to-zone root-trust]
user@host# set policy root-Untrust_to_root-Trust match source-address any
user@host# set policy root-Untrust_to_root-Trust match destination-address
    any
```



```
user@host# set policy root-Untrust_to_root-Trust match application any
user@host# set policy root-Untrust_to_root-Trust then permit

[edit security policies from-zone root-untrust to-zone root-untrust]
user@host# set policy root-Untrust_to_root-Untrust match source-address any
user@host# set policy root-Untrust_to_root-Untrust match destination-address
any
user@host# set policy root-Untrust_to_root-Untrust match application any
user@host# set policy root-Untrust_to_root-Untrust then permit

[edit security policies from-zone root-trust to-zone root-trust]
user@host# set policy root-Trust_to_root-Trust match source-address any
user@host# set policy root-Trust_to_root-Trust match destination-address any
user@host# set policy root-Trust_to_root-Trust match application any
user@host# set policy root-Trust_to_root-Trust then permit
```

5. Configure the interconnect logical system.

a. Configure logical tunnel interfaces.

```
[edit logical-systems LSYS0 interfaces]
user@host# set lt-0/0/0 unit 0 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 0 peer-unit 1
user@host# set lt-0/0/0 unit 2 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 2 peer-unit 3
user@host# set lt-0/0/0 unit 4 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 4 peer-unit 5
```

b. Configure the VPLS routing instance.

```
[edit logical-systems LSYS0 routing-instances]
user@host# set vr instance-type vpls
user@host# set vr interface lt-0/0/0.0
user@host# set vr interface lt-0/0/0.2
user@host# set vr interface lt-0/0/0.4
```

6. Configure logical tunnel interfaces for the user logical systems.

a. Configure logical tunnel interfaces for LSYS1.

```
[edit logical-systems LSYS1 interfaces ]
user@host# set lt-0/0/0 unit 3 encapsulation ethernet
user@host# set lt-0/0/0 unit 3 peer-unit 2
user@host# set lt-0/0/0 unit 3 family inet6 address 2111::3/64
```

b. Configure logical tunnel interfaces for LSYS2.

```
[edit logical-systems LSYS2 interfaces ]
user@host# set lt-0/0/0 unit 5 encapsulation ethernet
user@host# set lt-0/0/0 unit 5 peer-unit 4
user@host# set lt-0/0/0 unit 5 family inet6 address 2111::5/64
```

Results From configuration mode, confirm the configuration for LSYS0 by entering the **show logical-systems LSYS0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS0
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
    }
    unit 4 {
      encapsulation ethernet-vpls;
      peer-unit 5;
    }
  }
}
routing-instances {
  vr {
    instance-type vpls;
    interface lt-0/0/0.0;
    interface lt-0/0/0.2;
    interface lt-0/0/0.4;
  }
}
```

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

```
[edit]
user@host# show interfaces
lt-0/0/0 {
  unit 1 {
    encapsulation ethernet;
    peer-unit 0;
    family inet6 {
      address 2111::1/64;
    }
  }
}
ge-1/0/0 {
  gigether-options {
    redundant-parent reth0;
  }
}
ge-1/0/1 {
  gigether-options {
    redundant-parent reth1;
  }
}
```

```
    }  
  }  
  ge-1/0/2 {  
    gigeother-options {  
      redundant-parent reth2;  
    }  
  }  
  ge-1/0/3 {  
    gigeother-options {  
      redundant-parent reth3;  
    }  
  }  
  ge-7/0/0 {  
    gigeother-options {  
      redundant-parent reth0;  
    }  
  }  
  ge-7/0/1 {  
    gigeother-options {  
      redundant-parent reth1;  
    }  
  }  
  ge-7/0/2 {  
    gigeother-options {  
      redundant-parent reth2;  
    }  
  }  
  ge-7/0/3 {  
    gigeother-options {  
      redundant-parent reth3;  
    }  
  }  
  fab0 {  
    fabric-options {  
      member-interfaces {  
        ge-1/1/0;  
      }  
    }  
  }  
  fab1 {  
    fabric-options {  
      member-interfaces {  
        ge-7/1/0;  
      }  
    }  
  }  
  reth0 {  
    redundant-ether-options {  
      redundancy-group 1;  
    }  
    unit 0 {  
      family inet6 {  
        address 9995::1/64;  
      }  
    }  
  }  
}
```

```
    reth1 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
    reth2 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
    reth3 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
[edit]
user@host# show routing-instances
vr0 {
    instance-type virtual-router;
    interface lt-0/0/0.1;
    interface reth0.0;
    routing-options {
        rib vr0.inet6.0 {
            static {
                route 8885::/64 next-hop 2111::3;
                route 7775::/64 next-hop 2111::3;
                route 6665::/64 next-hop 2111::5;
            }
        }
    }
}
[edit]
user@host# show security
policies {
    from-zone root-trust to-zone root-untrust {
        policy root-Trust_to_root-Untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-untrust to-zone root-trust {
        policy root-Untrust_to_root-Trust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
```

```
    }  
  }  
  from-zone root-untrust to-zone root-untrust {  
    policy root-Untrust_to_root-Untrust {  
      match {  
        source-address any;  
        destination-address any;  
        application any;  
      }  
      then {  
        permit;  
      }  
    }  
  }  
  from-zone root-trust to-zone root-trust {  
    policy root-Trust_to_root-Trust {  
      match {  
        source-address any;  
        destination-address any;  
        application any;  
      }  
      then {  
        permit;  
      }  
    }  
  }  
}  
zones {  
  security-zone root-trust {  
    host-inbound-traffic {  
      system-services {  
        all;  
      }  
      protocols {  
        all;  
      }  
    }  
    interfaces {  
      reth0.0;  
    }  
  }  
  security-zone root-untrust {  
    host-inbound-traffic {  
      system-services {  
        all;  
      }  
      protocols {  
        all;  
      }  
    }  
    interfaces {  
      lt-0/0/0.1;  
    }  
  }  
}
```

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

User Logical System Configuration with IPv6 (User Logical System Administrator)

CLI Quick Configuration

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

Enter the following commands while logged in as the user logical system administrator for LSYS1:

```
set interfaces reth1 unit 0 family inet6 address 8885::1/64
set interfaces reth2 unit 0 family inet6 address 7775::1/64
set routing-instances vr11 instance-type virtual-router
set routing-instances vr11 interface lt-0/0/0.3
set routing-instances vr11 interface reth1.0
set routing-instances vr11 routing-options rib vr11.inet6.0 static route 6665::/64 next-hop 2111::5
set routing-instances vr11 routing-options rib vr11.inet6.0 static route 9995::/64 next-hop 2111::1
set routing-instances vr12 instance-type virtual-router
set routing-instances vr12 interface reth2.0
set routing-instances vr12 routing-options interface-routes rib-group inet6 vr11vr12v6
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 8885::/64 next-table vr11.inet6.0
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 9995::/64 next-table vr11.inet6.0
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 6665::/64 next-table vr11.inet6.0
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 2111::/64 next-table vr11.inet6.0
set routing-options rib-groups vr11vr12v6 import-rib vr11.inet6.0
set routing-options rib-groups vr11vr12v6 import-rib vr12.inet6.0
set security zones security-zone lsys1-trust host-inbound-traffic system-services all
set security zones security-zone lsys1-trust host-inbound-traffic protocols all
set security zones security-zone lsys1-trust interfaces reth1.0
set security zones security-zone lsys1-trust interfaces lt-0/0/0.3
set security zones security-zone lsys1-untrust host-inbound-traffic system-services all
set security zones security-zone lsys1-untrust host-inbound-traffic protocols all
set security zones security-zone lsys1-untrust interfaces reth2.0
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy lsys1trust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy lsys1trust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy lsys1trust-to-lsys1untrust match application any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy lsys1untrust-to-lsys1trust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy lsys1untrust-to-lsys1trust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy lsys1untrust-to-lsys1trust match destination-address any
```

```
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust then permit
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match application any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  then permit
```

Enter the following commands while logged in as the user logical system administrator for LSYS2:

```
set interfaces reth3 unit 0 family inet6 address 6665::1/64
set routing-instances vr2 instance-type virtual-router
set routing-instances vr2 interface lt-0/0/0.5
set routing-instances vr2 interface reth3.0
set routing-instances vr2 routing-options rib vr2.inet6.0 static route 7775::/64 next-hop
  2111::3
set routing-instances vr2 routing-options rib vr2.inet6.0 static route 8885::/64 next-hop
  2111::3
set routing-instances vr2 routing-options rib vr2.inet6.0 static route 9995::/64 next-hop
  2111::1
set security zones security-zone lsys2-trust host-inbound-traffic system-services all
set security zones security-zone lsys2-trust host-inbound-traffic protocols all
set security zones security-zone lsys2-trust interfaces reth3.0
set security zones security-zone lsys2-untrust host-inbound-traffic system-services all
set security zones security-zone lsys2-untrust host-inbound-traffic protocols all
set security zones security-zone lsys2-untrust interfaces lt-0/0/0.5
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match application any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust then permit
```

```

set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust then permit
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match application any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust then permit

```

Step-by-Step Procedure



NOTE: The user logical system administrator performs the following configuration while logged in to his or her user logical system. The master administrator can also configure a user logical system at the [edit logical-systems *logical-system*] hierarchy level.

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 the LSYS1 user logical system:

1. Configure interfaces.

[edit interfaces]

```
lsys1-admin@host:LSYS1# set reth1 unit 0 family inet6 address 8885::1/64
```

```
lsys1-admin@host:LSYS1# set reth2 unit 0 family inet6 address 7775::1/64
```

2. Configure routing.

[edit routing-instances]

```
lsys1-admin@host:LSYS1# set vr11 instance-type virtual-router
```

```
lsys1-admin@host:LSYS1# set vr11 interface lt-0/0/0.3
```

```
lsys1-admin@host:LSYS1# set vr11 interface reth1.0
```

```
lsys1-admin@host:LSYS1# set vr11 routing-options rib vr11.inet6.0 static route
  6665::/64 next-hop 2111::5
```

```
lsys1-admin@host:LSYS1# set vr11 routing-options rib vr11.inet6.0 static route
  9995::/64 next-hop 2111::1
```

```
lsys1-admin@host:LSYS1# set vr12 instance-type virtual-router
```

```
lsys1-admin@host:LSYS1# set vr12 interface reth2.0
```

```
lsys1-admin@host:LSYS1# set vr12 routing-options interface-routes rib-group inet6
  vr11vr12v6
```

```
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
  8885::/64 next-table vr11.inet6.0
```



```

lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
9995::/64 next-table vr11.inet6.0
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
6665::/64 next-table vr11.inet6.0
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
2111::/64 next-table vr11.inet6.0

[edit routing-options]
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v6 import-rib vr11.inet6.0
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v6 import-rib vr12.inet6.0

```

3. Configure zones and security policies.

```

[edit security zones]
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces reth1.0
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces lt-0/0/0.3
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust interfaces reth2.0

[edit security policies from-zone lsys1-trust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match source-address
any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match application
any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match source-address
any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match application
any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
source-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match application
any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-trust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match source-address
any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match
destination-address any

```

```
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match application any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust then permit
```

Step-by-Step Procedure To configure the LSYS2 user logical system:

1. Configure interfaces.

```
[edit interfaces]
lsys2-admin@host:LSYS2# set reth3 unit 0 family inet6 address 6665::1/64
```

2. Configure routing.

```
[edit routing-instances]
lsys2-admin@host:LSYS2# set vr2 instance-type virtual-router
lsys2-admin@host:LSYS2# set vr2 interface lt-0/0/0.5
lsys2-admin@host:LSYS2# set vr2 interface reth3.0
lsys2-admin@host:LSYS2# set vr2 routing-options rib vr2.inet6.0 static route
7775::/64 next-hop 2111::3
lsys2-admin@host:LSYS2# set vr2 routing-options rib vr2.inet6.0 static route
8885::/64 next-hop 2111::3
lsys2-admin@host:LSYS2# set vr2 routing-options rib vr2.inet6.0 static route
9995::/64 next-hop 2111::1
```

3. Configure zones and security policies.

```
[edit security zones]
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust interfaces reth3.0
lsys2-admin@host:LSYS2# set security zones security-zone lsys2-untrust
host-inbound-traffic system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust host-inbound-traffic
protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust interfaces lt-0/0/0.5

[edit security policies from-zone lsys2-trust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
source-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match application
any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust then permit

[edit security policies from-zone from-zone lsys2-untrust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match application
any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust then permit
```

```
[edit security policies from-zone lsys2-untrust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match application
any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust then permit

[edit security policies from-zone lsys2-trust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match source-address
any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match
destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match application
any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust then permit
```

Results From configuration mode, confirm the configuration for LSYS1 by entering the **show interfaces**, **show routing-instances**, **show routing-options**, and **show security** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
lsys1-admin@host:LSYS1# show interfaces
interfaces {
  lt-0/0/0 {
    unit 3 {
      encapsulation ethernet;
      peer-unit 2;
      family inet6 {
        address 2111::3/64;
      }
    }
  }
  reth1 {
    unit 0 {
      family inet6 {
        address 8885::1/64;
      }
    }
  }
  reth2 {
    unit 0 {
      family inet6 {
        address 7775::1/64;
      }
    }
  }
}
[edit]
lsys1-admin@host:LSYS1# show routing-instances
routing-instances {
  vr11 {
```

```

instance-type virtual-router;
interface lt-0/0/0.3;
interface reth1.0;
routing-options {
  rib vr11.inet6.0 {
    static {
      route 6665::/64 next-hop 2111::5;
      route 9995::/64 next-hop 2111::1;
    }
  }
}
vr12 {
  instance-type virtual-router;
  interface reth2.0;
  routing-options {
    interface-routes {
      rib-group inet6 vr11vr12v6;
    }
    rib vr12.inet6.0 {
      static {
        route 8885::/64 next-table vr11.inet6.0;
        route 9995::/64 next-table vr11.inet6.0;
        route 6665::/64 next-table vr11.inet6.0;
        route 2111::/64 next-table vr11.inet6.0;
      }
    }
  }
}
[edit]
lsys1-admin@host:LSYS1# show routing-options
rib-groups {
  vr11vr12v6 {
    import-rib [ vr11.inet6.0 vr12.inet6.0 ];
  }
}
[edit]
lsys1-admin@host:LSYS1# show security
security {
  policies {
    from-zone lsys1-trust to-zone lsys1-untrust {
      policy lsys1trust-to-lsys1untrust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys1-untrust to-zone lsys1-trust {
      policy lsys1untrust-to-lsys1trust {
        match {

```

```
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
}
from-zone lsys1-untrust to-zone lsys1-untrust {
    policy lsys1untrust-to-lsys1untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone lsys1-trust to-zone lsys1-trust {
    policy lsys1trust-to-lsys1trust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
}
zones {
    security-zone lsys1-trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            reth1.0;
            lt-0/0/0.3;
        }
    }
    security-zone lsys1-untrust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
    }
}
```

```

    }
  }
  interfaces {
    reth2.0;
  }
}
}

```

From configuration mode, confirm the configuration for LSYS2 by entering the **show interfaces**, **show routing-instances**, and **show security** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
lsys2-admin@host:LSYS2# show interfaces
interfaces {
  lt-0/0/0 {
    unit 5 {
      encapsulation ethernet;
      peer-unit 4;
      family inet6 {
        address 2111::5/64;
      }
    }
  }
  reth3 {
    unit 0 {
      family inet6 {
        address 6665::1/64;
      }
    }
  }
}
[edit]
lsys2-admin@host:LSYS2# show routing-instances
routing-instances {
  vr2 {
    instance-type virtual-router;
    interface lt-0/0/0.5;
    interface reth3.0;
    routing-options {
      rib vr2.inet6.0 {
        static {
          route 7775::/64 next-hop 2111::3;
          route 8885::/64 next-hop 2111::3;
          route 9995::/64 next-hop 2111::1;
        }
      }
    }
  }
}
[edit]
lsys2-admin@host:LSYS2# show security
security {
  policies {

```

```
from-zone lsys2-trust to-zone lsys2-untrust {
  policy lsys2trust-to-lsys2untrust {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone lsys2-untrust to-zone lsys2-trust {
  policy lsys2untrust-to-lsys2trust {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone lsys2-untrust to-zone lsys2-untrust {
  policy lsys2untrust-to-lsys2untrust {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone lsys2-trust to-zone lsys2-trust {
  policy lsys2trust-to-lsys2trust {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
}
zones {
  security-zone lsys2-trust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
```

```

        all;
    }
}
interfaces {
    reth3.0;
}
}
security-zone lsys2-untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        lt-0/0/0.5;
    }
}
}
}

```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Chassis Cluster Status \(IPv6\) on page 336](#)
- [Troubleshooting Chassis Cluster with Logs \(IPv6\) on page 337](#)
- [Verifying Logical System Licenses \(IPv6\) on page 337](#)
- [Verifying Logical System License Usage \(IPv6\) on page 337](#)
- [Verifying Intra-Logical System Traffic on a Logical System \(IPv6\) on page 338](#)
- [Verifying Intra-Logical System Traffic Within All Logical Systems \(IPv6\) on page 338](#)
- [Verifying Traffic Between User Logical Systems \(IPv6\) on page 339](#)

Verifying Chassis Cluster Status (IPv6)

Purpose Verify the chassis cluster status, failover status, and redundancy group information.

Action From operational mode, enter the **show chassis cluster status** command.

```

{primary:node0}
show chassis cluster status
Cluster ID: 1
Node          Priority      Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
  node0          200        primary    no       no
  node1          100        secondary  no       no

Redundancy group: 1 , Failover count: 1

```


node0	200	primary	no	no
node1	100	secondary	no	no

Troubleshooting Chassis Cluster with Logs (IPv6)

Purpose Use these logs to identify any chassis cluster issues. You should run these logs on both nodes.

Action From operational mode, enter these **show log** commands.

```
user@host> show log jsrpd
user@host> show log chassisd
user@host> show log messages
user@host> show log dcd
user@host> show traceoptions
```

Verifying Logical System Licenses (IPv6)

Purpose Verify information about logical system licenses.

Action From operational mode, enter the **show system license status logical-system all** command.

```
{primary:node0}
user@host> show system license status logical-system all
node0:
-----
Logical system license status:

logical system name      license status
root-logical-system     enabled
LSYS0                    enabled
LSYS1                    enabled
LSYS2                    enabled
```

Verifying Logical System License Usage (IPv6)

Purpose Verify information about logical system license usage.



NOTE: The actual number of licenses used is only displayed on the primary node.

Action From operational mode, enter the **show system license** command.

```
{primary:node0}
user@host> show system license
License usage:

Feature name              Licenses used  Licenses installed  Licenses needed  Expiry
```

```

logical-system          4          25          0    permanent

Licenses installed:
  License identifier: JUNOS305013
  License version: 2
  Valid for device: JN110B54BAGB
Features:
  logical-system-25 - Logical System Capacity
                    permanent

```

Verifying Intra-Logical System Traffic on a Logical System (IPv6)

Purpose Verify information about currently active security sessions within a logical system.

Action From operational mode, enter the **show security flow session logical-system LSYS1** command.

```

{primary:node0}
user@host> show security flow session logical-system LSYS1
node0:
-----

Flow Sessions on FPC0 PIC1:

Session ID: 10000115, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1784, Valid
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 22, Bytes: 1745
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 19, Bytes: 2108
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
-----

Flow Sessions on FPC0 PIC1:

Session ID: 10000006, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14392, Valid
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

```

Verifying Intra-Logical System Traffic Within All Logical Systems (IPv6)

Purpose Verify information about currently active security sessions on all logical systems.

Action From operational mode, enter the **show security flow session logical-system all** command.

```
{primary:node0}
user@host> show security flow session logical-system all
node0:
-----

Flow Sessions on FPC0 PIC1:

Session ID: 10000115, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1776, Valid
Logical system: LSYS1
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 22, Bytes: 1745
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 19, Bytes: 2108
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
-----

Flow Sessions on FPC0 PIC1:

Session ID: 10000006, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14384, Valid
Logical system: LSYS1
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

Verifying Traffic Between User Logical Systems (IPv6)

Purpose Verify information about currently active security sessions between logical systems.

Action From operational mode, enter the **show security flow session logical-system *logical-system-name*** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1
node0:
-----

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000118, Policy name: lsys1trust-to-lsys1trust/11, State: Active,
Timeout: 1792, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 91, Bytes: 6802
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 65, Bytes: 6701
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
node1:
-----
```

```
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000010, Policy name: lsys1trust-to-lsys1trust/11, State: Backup,
Timeout: 14388, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 0, Bytes: 0
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
{primary:node0}
user@host> show security flow session logical-system LSYS2
```

```
node0:
-----
```

```
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000119, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
Timeout: 1788, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 91, Bytes: 6802
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 65, Bytes: 6701
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
node1:
-----
```

```
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000011, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
Timeout: 14380, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
{primary:node0}
user@host> show security flow session logical-system all
```

```
node0:
```

```
-----
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000118, Policy name: lsys1trust-to-lsys1trust/11, State: Active,
Timeout: 1784, Valid
Logical system: LSYS1
```

```
In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 91, Bytes: 6802
```

```
Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 65, Bytes: 6701
```

```
Session ID: 80000119, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
Timeout: 1784, Valid
Logical system: LSYS2
```

```
In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 91, Bytes: 6802
```

```
Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 65, Bytes: 6701
```

```
Total sessions: 2
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

```
node1:
```

```
-----
Flow Sessions on FPC0 PIC1:
Total sessions: 0
```

```
Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000010, Policy name: lsys1trust-to-lsys1trust/11, State: Backup,
Timeout: 14378, Valid
Logical system: LSYS1
```

```
In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
```

```
Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 0, Bytes: 0
```

```
Session ID: 80000011, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
Timeout: 14376, Valid
Logical system: LSYS2
```

```
In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
```

```
Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 0, Bytes: 0
```

```
Total sessions: 2
```

```
Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

See Also • [Understanding Logical Systems in the Context of Chassis Cluster on page 274](#)

- [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(Master Administrators Only\) on page 275](#)
- *Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices*
- *Chassis Cluster Overview*

Example: Deleting a Logical System

This example shows how to delete a logical system configured for an SRX Series Services Gateway device running logical systems. Only the master administrator can delete a logical system.

- [Requirements on page 342](#)
- [Overview on page 342](#)
- [Configuration on page 342](#)
- [Verification on page 344](#)

Requirements

The example uses an SRX5600 device running Junos OS with Logical Systems.

Alternatively, follow those instructions substituting your own configuration values.

Overview

This example shows how to delete a logical system, which you can do at any time. However, if you have configured the device to include the maximum number of logical systems that are supported you must first delete an existing logical system before you can add another one.

Deletion of a logical system is a simple procedure that includes these tasks:

- Remove from the logical system the security profile that is bound to it.

Note that in this step you are not deleting the security profile—it might be used for other logical systems—but simply detaching it from the logical system that you intend to delete.
- Detach from the logical system any login classes that are associated with it.

Removing them from the logical system does not delete the login classes.
- Delete the logical system.

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.

```
delete system security-profile ls-design-profile logical-system ls-product-design
```

```
delete system login class ls-design-admin logical-system ls-product-design
delete system login class ls-design-user logical-system ls-product-design
delete logical-system ls-product-design
```

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

To delete a logical system:

1. Determine that the logical system that you want to delete exists.

```
[edit]
user@host# show logical-systems ?
interconnect-logical-system Logical system name
ls-accounting-dept Logical system name
ls-marketing-dept Logical system name
ls-product-design Logical system name
```

2. Delete the security profile.
 - a. Verify that security profile that you intend to detach from the logical system is bound to it.

```
[edit]
user@host# show system security-profile ls-design-profile
logical-system [ ls-product-design ];
```

- b. Detach the security profile from the logical system.

```
[edit]
user@host# delete system security-profile ls-design-profile logical-system
ls-product-design
```

3. Delete the login classes.
 - a. Display the login class and login user configurations for the user logical system administrator.

```
user@host> show configuration system login class ls-design-admin
logical-system ls-product-design;
permissions all;
user@host> show configuration system login user lsdesignadmin1
full-name lsdesignadmin1;
uid 2006;
class ls-design-admin;
authentication {
  encrypted-password "$ABC123"; ## SECRET-DATA
}
```

- b. Detach the login class for the administrator from the logical system.

```
[edit]
```

```
user@host# delete system login class ls-design-admin logical-system
ls-product-design
```

- c. Display the login class and login user configurations for the user.

```
user@host> show configuration system login class ls-design-user
logical-system ls-product-design;
permissions view;
user@host> show configuration system login user lsdesignuser1
full-name lsdesignuser1
uid 2007;
class ls-design-user;
authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
}
```

- d. Detach the login class for the user from the logical system.

```
user@host# delete system login class ls-design-user logical-system
ls-product-design
```

4. Delete the logical system.

```
[edit]
user@host# delete logical-system ls-product-design
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems** command. In this case, the logical system that you deleted should not be included in displayed list of logical systems configured for the device. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show logical-systems
interconnect-logical-system Logical system name
ls-accounting-dept Logical system name
interconnect-logical-system Logical system name
ls-marketing-dept Logical system name
```

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 That the Correct Logical System and Its Profile and Attached Class Were Deleted on page 344](#)

Verifying That the Correct Logical System and Its Profile and Attached Class Were Deleted

Purpose Verify if the logical system has been deleted using the show command described previously.

- Related Documentation**
- [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)
 - [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

Troubleshooting Logical Systems

Use the following features to monitor logical systems and troubleshoot the software issues. For more information, see the following topics:

- [Understanding Security Logs and Logical Systems on page 345](#)
- [Understanding Data Path Debugging for Logical Systems on page 346](#)
- [Performing Tracing for Logical Systems \(Master Administrators Only\) on page 347](#)
- [Troubleshooting DNS Name Resolution in Logical System Security Policies \(Master Administrators Only\) on page 352](#)

Understanding Security Logs and Logical Systems

Security logs are system log messages that include security events. If a device is configured for logical systems, security logs generated within the context of a logical system use the name **logname_LS** (for example, **IDP_ATTACK_LOG_EVENT_LS**). The logical system version of a log has the same set of attributes as the log for devices that are not configured for logical systems. The logical system log includes logical-system-name as the first attribute.

The following security log shows the attributes for the IDP_ATTACK_LOG_EVENT log for a device that is *not* configured for logical systems:

```
IDP_ATTACK_LOG_EVENT {
  help "IDP attack log";
  description "IDP Attack log generated for attack";
  type event;
  args timestamp message-type source-address source-port destination-address
  destination-port protocol-name service-name application-name rule-name
  rulebase-name policy-name repeat-count action threat-severity attack-name
  nat-source-address nat-source-port nat-destination-address nat-destination-port
  elapsed-time inbound-bytes outbound-bytes inbound-packets outbound-packets
  source-zone-name source-interface-name destination-zone-name
  destination-interface-name packet-log-id message;
  severity LOG_INFO;
  flag auditable;
  edit "2010/10/01 mvr created";
}
```

The following security log shows the attributes for the IDP_ATTACK_LOG_EVENT_LS log for a device that is configured for logical systems (note that logical-system-name is the first attribute):

```
IDP_ATTACK_LOG_EVENT_LS {
  help "IDP attack log";
  description "IDP Attack log generated for attack";
  type event;
  args logical-system-name timestamp message-type source-address source-port
```

```

destination-address destination-port protocol-name service-name application-name
rule-name rulebase-name policy-name repeat-count action threat-severity
attack-name nat-source-address nat-source-port nat-destination-address
nat-destination-port elapsed-time inbound-bytes outbound-bytes inbound-packets
outbound-packets source-zone-name source-interface-name destination-zone-name
destination-interface-name packet-log-id message;
severity LOG_INFO;
flag auditable;
edit "2010/10/01 mvr created";
}

```

If a device is configured for logical systems, log parsing scripts might need to be modified because the log name includes the **_LS** suffix and the **logical-system-name** attribute can be used to segregate logs by logical system.

If a device is not configured for logical systems, the security logs remain unchanged and scripts built to parse logs do not need any modification.



NOTE: Only the master administrator can configure logging at the [edit security log] hierarchy level. User logical system administrators cannot configure logging for their logical systems.

Stream mode is a set of logging services that includes:

- Off-box logging (SRX Series)
- On-box logging and reporting (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, and SRX4600 Series)

Per logical system configuration is supported for the off-box logging and logs are handled based on these configurations. Previously the user logical system logs were generated from root logical system. For off-box logging, the logical system logs can only be generated from logical system interface.

Limitations

Each SPU can only support a maximum of 1000 connections for standalone and 500 connections for cluster on the SRX5400, SRX5600, and SRX5800 devices in the Junos OS 18.2R1 release. If all the connections are used up, some connections for user logical systems might not be established.



NOTE: The error message will be captured in the [System Log Explorer](#).

Understanding Data Path Debugging for Logical Systems

Data path debugging provides tracing and debugging at multiple processing units along the packet-processing path. Data path debugging can also be performed on traffic between logical systems.



NOTE: Only the master administrator can configure data path debugging for logical systems at the [edit security datapath-debug] level. User logical system administrators cannot configure data path debugging for their logical systems.

End-to-end event tracing traces the path of a packet from when it enters the device to when it leaves the device. When the master administrator configures end-to-end event tracing, the trace output contains logical system information.

The master administrator can also configure tracing for traffic between logical systems. The trace output shows traffic entering and leaving the logical tunnel between logical systems. When the **preserve-trace-order** option is configured, the trace message is sorted chronologically. In addition to the trace action, other actions such as packet-dump and packet-summary may be configured for traffic between logical systems.

Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

See Also • [Performing Tracing for Logical Systems \(Master Administrators Only\) on page 347](#)

Performing Tracing for Logical Systems (Master Administrators Only)



NOTE: Only the master administrator can configure data path debugging for logical systems at the root level.

To configure an action profile for a trace or packet capture:

1. Specify event types and trace actions. You can specify any combination of event types and trace actions. For example, the following statements configure multiple trace actions for each event type:

```
[edit security datapath-debug]
user@host# set action-profile p1 event lbt trace
user@host# set action-profile p1 event lbt count
user@host# set action-profile p1 event lbt packet-summary
user@host# set action-profile p1 event lbt packet-dump
user@host# set action-profile p1 event pot trace
user@host# set action-profile p1 event pot count
user@host# set action-profile p1 event pot packet-summary
user@host# set action-profile p1 event pot packet-dump
user@host# set action-profile p1 event np-ingress trace
user@host# set action-profile p1 event np-ingress count
user@host# set action-profile p1 event np-ingress packet-summary
user@host# set action-profile p1 event np-ingress packet-dump
user@host# set action-profile p1 event np-egress trace
user@host# set action-profile p1 event np-egress count
user@host# set action-profile p1 event np-egress packet-summary
user@host# set action-profile p1 event np-egress packet-dump
user@host# set action-profile p1 event jexec trace
user@host# set action-profile p1 event jexec count
```

```
user@host# set action-profile p1 event jexec packet-summary
user@host# set action-profile p1 event jexec packet-dump
user@host# set action-profile p1 event lt-enter trace
user@host# set action-profile p1 event lt-enter count
user@host# set action-profile p1 event lt-enter packet-summary
user@host# set action-profile p1 event lt-enter packet-dump
user@host# set action-profile p1 event lt-leave trace
user@host# set action-profile p1 event lt-leave count
user@host# set action-profile p1 event lt-leave packet-summary
user@host# set action-profile p1 event lt-leave packet-dump
```

2. Specify action profile options.

```
[edit security datapath-debug]
user@host# set action-profile p1 record-pic-history
user@host# set action-profile p1 preserve-trace-order
```

3. Configure packet filter options.

```
[edit security datapath-debug]
user@host# set packet-filter 1 action-profile p1
user@host# set packet-filter 1 protocol udp
```

To capture trace messages for logical systems:

1. Configure the trace capture file.

```
[edit security datapath-debug]
user@host# set traceoptions file e2e.trace
user@host# set traceoptions file size 10m
```

2. Display the captured trace in operational mode.

```
user@host> show log e2e.trace
Jul  7 09:49:56
09:49:56.417578:CID-00:FPC-01:PIC-00:THREAD_ID-00:FINDEX:0:IIF:75:SEQ:0:TC:0
PIC History: ->C0/F1/P0
NP ingress channel 0 packet
Meta: Src: F1/P0 Dst: F0/P0
IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500

Jul  7 09:49:56
09:49:55.1414031:CID-00:FPC-00:PIC-00:THREAD_ID-04:FINDEX:0:IIF:75:SEQ:0:TC:1
PIC History: ->C0/F1/P0->C0/F0/P0
LBT pkt, payload: DATA
Meta: Src: F1/P0 Dst: F0/P0
IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500

...
(Some trace information omitted)
...

.Jul  7 09:49:56
09:49:55.1415649:CID-00:FPC-00:PIC-00:THREAD_ID-05:FINDEX:0:IIF:75:SEQ:0:TC:16
PIC History: ->C0/F1/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0
POT pkt, action: POT_SEND payload: DATA
Meta: Src: F0/P0 Dst: F1/P0
```

```
IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500
```

```
Jul 7 09:49:56
```

```
09:49:56.419274:CID-00:FPC-01:PIC-00:THREAD_ID-00:FINDEX:0:IIF:75:SEQ:0:TC:17
```

```
PIC History: ->C0/F1/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0->C0/F1/P0
```

```
NP egress channel 0 packet
```

```
Meta: Src: F0/P0 Dst: F1/P0
```

```
IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500
```

3. Clear the log.

```
user@host> clear log e2e.trace
```

To perform packet capture for logical systems:

1. Configure the packet capture file.

```
[edit security datapath-debug]
user@host# set capture-file e2e.pcap
user@host# set capture-file format pcap
user@host# set capture-file size 10m
user@host# set capture-file world-readable
user@host# set capture-file maximum-capture-size 1500
```

2. Enter operational mode to start and then stop the packet capture.

```
user@host> request security datapath-debug capture start
user@host> request security datapath-debug capture stop
```



NOTE: Packet capture files can be opened and analyzed offline with tcpdump or any packet analyzer that recognizes the libpcap format. You can also use FTP or the Session Control Protocol (SCP) to transfer the packet capture files to an external device.

3. Disable packet capture from configuration mode.



NOTE: Disable packet capture before opening the file for analysis or transferring the file to an external device with FTP or SCP. Disabling packet capture ensures that the internal file buffer is flushed and all the captured packets are written to the file.

```
[edit forwarding-options]
user@host# set packet-capture disable
```

4. Display the packet capture.

- To display the packet capture with the tcpdump utility:

```
user@host# tcpdump -nr /var/log/e2e.pcap
09:49:55.1413990 C0/F0/P0 event:11(1bt) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
```

```

09:49:55.1414154 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415062 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415184 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414093 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414638 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415011 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415129 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415511 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415649 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415249 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1415558 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414226 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414696 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414828 C0/F0/P0 event:16(lt-enter) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414919 C0/F0/P0 event:15(lt-leave) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:56.417560 C0/F1/P0 event:1(np-ingress) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:56.419263 C0/F1/P0 event:2(np-egress) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0

```

- To display the packet capture from CLI operational mode:

```

user@host> show security datapath-debug capture
Packet 1, len 568: (C0/F0/P0/SEQ:0:lbt)
00 00 00 00 00 00 50 c5 8d 0c 99 4a 00 00 0a 01
01 02 08 00 45 60 01 f4 00 00 00 00 40 06 4e 9f
0a 01 01 02 1e 01 01 02 5b 9b 30 39 00 00 00 00
00 00 00 00 50 02 00 00 f8 3c 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 ac 7a 00 04
00 00 00 00 b3 e3 15 4e 66 93 15 00 04 22 38 02
38 02 00 00 00 01 00 03 0b 00 00 00 50 d0 1a 08
30 de be bf e4 f3 19 08
Packet 2, len 624: (C0/F0/P0/SEQ:0:lbt)
aa 35 00 00 00 00 00 00 00 00 00 00 03 00 00
00 0a 00 00 00 00 00 00 05 bd 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 c5
8d 0c 99 4a 00 00 0a 01 01 02 08 00 45 60 01 f4
00 00 00 00 40 06 4e 9f 0a 01 01 02 ac 7a 00 04
00 00 00 00 b3 e3 15 4e 0a 94 15 00 04 5a 70 02
70 02 00 00 00 03 00 03 0b 00 00 00 50 d0 1a 08
30 de be bf e4 f3 19 08

...
(Packets 3 through 17 omitted)
...

```

```

Packet 18, len 568: (C0/F1/P0/SEQ:0:np-egress)
00 00 00 04 00 00 00 00 1e 01 01 02 50 c5 8d 0c
99 4b 08 00 45 60 01 f4 00 00 00 00 3e 06 50 9f
0a 01 01 02 1e 01 01 02 5b 9b 30 39 00 00 00 00
00 00 00 00 50 02 00 00 f8 3c 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac 7a 04 00
00 00 00 00 b4 e3 15 4e bf 65 06 00 04 22 38 02
38 02 00 00 00 11 00 03 02 00 00 00 50 d0 1a 08
30 de be bf e4 f3 19 08

```

```
user@host> show security datapath-debug counters
```

```

Datapath debug counters
Packet Filter 1:
lt-enter
Chassis 0 FPC 0 PIC 1: 0
lt-enter
Chassis 0 FPC 0 PIC 0: 1
lt-leave
Chassis 0 FPC 0 PIC 1: 0
lt-leave
Chassis 0 FPC 0 PIC 0: 1
np-egress
Chassis 0 FPC 1 PIC 3: 0
np-egress
Chassis 0 FPC 1 PIC 1: 0
np-egress
Chassis 0 FPC 1 PIC 2: 0
np-egress
Chassis 0 FPC 1 PIC 0: 1
pot
Chassis 0 FPC 0 PIC 1: 0
pot
Chassis 0 FPC 0 PIC 0: 6
np-ingress
Chassis 0 FPC 1 PIC 3: 0
np-ingress
Chassis 0 FPC 1 PIC 1: 0
np-ingress
Chassis 0 FPC 1 PIC 2: 0
np-ingress
Chassis 0 FPC 1 PIC 0: 1
lbt
Chassis 0 FPC 0 PIC 1: 0
lbt
Chassis 0 FPC 0 PIC 0: 4
jexec
Chassis 0 FPC 0 PIC 1: 0
jexec
Chassis 0 FPC 0 PIC 0: 4

```

See Also • [Understanding Data Path Debugging for Logical Systems on page 346](#)

Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only)

Problem **Description:** The address of a hostname in an address book entry that is used in a security policy might fail to resolve correctly.

Cause Normally, address book entries that contain dynamic hostnames refresh automatically for SRX Series devices. The TTL field associated with a DNS entry indicates the time after which the entry should be refreshed in the policy cache. Once the TTL value expires, the SRX Series device automatically refreshes the DNS entry for an address book entry.

However, if the SRX Series device is unable to obtain a response from the DNS server (for example, the DNS request or response packet is lost in the network or the DNS server cannot send a response), the address of a hostname in an address book entry might fail to resolve correctly. This can cause traffic to drop as no security policy or session match is found.

Solution The master administrator can use the **show security dns-cache** command to display DNS cache information on the SRX Series device. If the DNS cache information needs to be refreshed, the master administrator can use the **clear security dns-cache** command.



NOTE: These commands are only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

See Also • [Understanding Logical Systems Security Policies on page 167](#)

Related Documentation • [Security Profiles for Logical Systems on page 73](#)

CHAPTER 3

Tenant Systems

- [Tenant Systems Overview on page 353](#)
- [Security Zones for Tenant Systems on page 377](#)
- [Flow for Tenant Systems on page 381](#)
- [Firewall Authentication for Tenant Systems on page 406](#)
- [Security Policies for Tenant Systems on page 419](#)
- [Screen Options for Tenant Systems on page 424](#)
- [NAT for Tenant Systems on page 429](#)
- [ALG for Tenant Systems on page 436](#)
- [Security Log for Tenant Systems on page 445](#)

Tenant Systems Overview

A tenant system supports routing, services and security features.

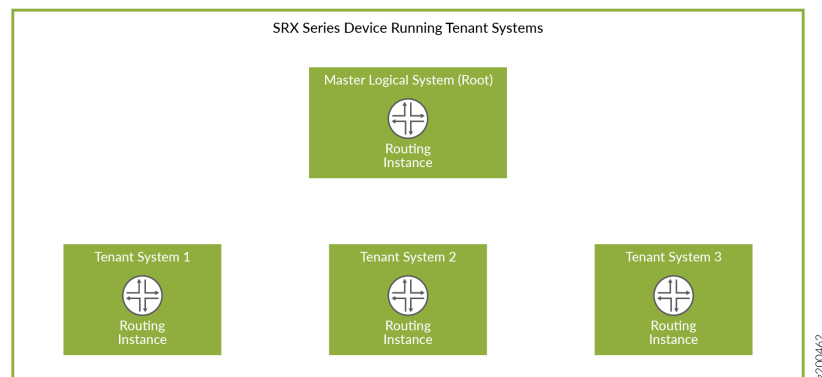
- [Understanding Tenant Systems on page 354](#)
- [Tenant System Configuration Overview on page 358](#)
- [Configuring a Routing Instance for a Tenant System on page 359](#)
- [Example: Configuring Tenant Systems on page 360](#)
- [Understanding Tenant System Security Profiles \(Master Administrators Only\) on page 364](#)
- [Example: Configuring Tenant Systems Security Profiles \(Master Administrators Only\) on page 369](#)

Understanding Tenant Systems

A tenant system is a logical partitioning of the device into multiple security domains with high scalability, similar to logical systems with greater scalability and less routing capabilities. Each tenant system on a device allows you to control a discrete administrative domain for security services. By transforming your device into a multitenant system, you can provide various departments, organizations, customers, and partners—depending on your environment—private use of system security resources and a per-tenant view of the device. A master administrator creates and manages all the tenant systems.

[“Tenant Systems” on page 353](#) shows a single device with a master logical system and discrete tenant systems.

Figure 10: Tenant Systems



Differences Between Logical Systems and Tenant Systems

[Table 28 on page 354](#) describes the key differences between logical systems and tenant systems.

Table 28: Differences Between Logical Systems and Tenant Systems

Functionality	Logical Systems	Tenant Systems
Feature support	Supports all the routing features to provide optimal data routing paths.	Supports routing features and high-scale security virtualization to isolate customer environments.
Scalability	A maximum of 32 logical systems can be configured on a physical SRX Series device.	A maximum of 200 tenant systems can be configured on a physical SRX Series device to provide high scalability.
Routing protocol process	Every logical system needs an individual copy of the routing protocol process to logically separate the resources on a device.	The master logical system has a single routing protocol process which is shared by the tenant systems to achieve the security resource separation on the device.
Routing instance	A default routing instance is automatically created for every logical system.	A tenant system user has to explicitly create a routing instance.

Table 28: Differences Between Logical Systems and Tenant Systems (continued)

Functionality	Logical Systems	Tenant Systems
Logical interface configuration	A logical system administrator can configure the logical interfaces and the interface attributes.	A tenant system administrator cannot configure the logical interfaces. The master administrator assigns the logical interfaces to a tenant system.

Use Cases for Logical Systems and Tenant Systems

A logical system is used when more than one virtual router is required. For example, you have multiple connections to the external network and they cannot co-exist in the same virtual router. Tenant systems are used when you need to separate departments, organization, or customers and each of them can be limited to one virtual router. The main difference between a logical system and a tenant system is that a logical system supports advanced routing functionality using multiple routing instances. In comparison, a tenant system supports only one routing instance, but supports the deployment of significantly more tenants per system.

Deployment Scenarios for Multitenant Systems

You can deploy an SRX Series device running a multitenant system in many environments such as a managed security service provider (MSSP), an enterprise network, or a branch office segment. [Table 29 on page 355](#) describes the various deployment scenarios and the roles played by the tenant systems in such scenarios.

Table 29: Deployment Scenarios with Respect to Tenant Systems

Deployment Scenarios	Roles of a Tenant System
Managed security service provider (MSSP)	<ul style="list-style-type: none"> In a managed security service provider (MSSP), based on the defined service-level agreements (SLAs), each customer can be allocated memory and resources and be isolated from each other to protect data privacy. The MSSP administrator can configure distinct security policies for compliance and control per tenant system. Each customer can discretely manage logs and trace files per tenant systems.
Enterprise network	<ul style="list-style-type: none"> A tenant system can be assigned a unique enterprise function. A tenant system can define discrete security policies to align with the enterprise functional applications. A tenant system can support logging capabilities on these applications and per tenant system.
Branch office segment	<ul style="list-style-type: none"> In a branch office, a tenant system can individually manage and segregate corporate and guest traffic. Advanced security policies can be configured per tenant system; this approach allows granular control of the security policies. A tenant system provides ease of management and troubleshooting.

Benefits of Tenant Systems

- Curtail cost by reducing the number of physical devices required for your organization. You can consolidate services for various groups of users on a single device and reduce the hardware costs, power expenditure, and rack space.
- Provide isolation and logical separation at the tenant system level. Provides the ability to separate tenant systems with administrative separation at large scale in which each tenant system can define its own security controls and restrictions without impacting other tenant systems.

Roles and Responsibilities of Master Administrator, Tenant System Administrator, and Tenant System User

A master administrator creates and manages all the tenant systems. The master administrator can assign the resources to each tenant system and restrict the resources that the tenant system can utilize from the resources of the system. All the system resources are assigned to the master logical system.



NOTE: In Junos OS command-line reference, master logical system is referred as root logical system.

A tenant system is created entirely within the master logical system. Each tenant system supports creation of a single routing instance and allows you to manage the tenant-specific logging capabilities of the device. A tenant system has a tenant system administrator and a tenant system user. [Table 30 on page 356](#) describes the roles and responsibilities of the master administrator, tenant system administrator, and the tenant user for the tenant system.

Table 30: Roles and Responsibilities With Respect to Tenant Systems

Roles	Definition	Responsibilities
Master administrator	A user account with superuser configuration and verification privileges for all logical systems and tenant systems.	<ul style="list-style-type: none"> • View and access all logical systems and tenant systems. • Create login accounts for all the tenant systems and assign the login accounts to the appropriate tenant system. • Create and allocate the resources to the tenant systems. • Create one custom routing instance under the tenant system which acts as the default routing instance for the tenant system. • Create a virtual router under the tenant system and assign it to the tenant system. • Create logical interfaces to assign to the tenant systems. • Manage the tenant systems in the master logical system. • Ensure duplicate names for tenant system, logs, and trace file do not exist.

Table 30: Roles and Responsibilities With Respect to Tenant Systems (continued)

Roles	Definition	Responsibilities
Tenant system administrator	A user account with configuration and verification privileges for the tenant systems.	<ul style="list-style-type: none"> Access and view the resources of the tenant system. <p>The following privileges are not supported by the tenant system administrator:</p> <ul style="list-style-type: none"> Access and view the resources of the tenant system. Define access restrictions and the default routing instance for the tenant system. Access and view the resources of other tenant systems. Modify the number of allocated resources for a tenant system. Configure logical interfaces, virtual router, and policy options.
Tenant system user	A user account with configuration privileges for only the tenant systems to which the user is assigned	<ul style="list-style-type: none"> Configure the resources allocated and routing protocols. Configure schedulers, security profiles, and security features. Configure the assigned routing instance and the interfaces belonging to the routing tables. <p>The following privileges are not supported by the tenant system administrator:</p> <ul style="list-style-type: none"> Access and view the resources of other tenant systems. Modify the number of allocated resources for a tenant system. Configure logical interfaces, virtual router, and policy options.

Tenant System Capacity

The maximum number of tenant systems that can be created on the device are listed in [Table 31 on page 357](#).

Table 31: Tenant Systems Capacity

Platform	Logical Systems Capacity	Tenant Systems Capacity
SRX1500	32	18
SRX4100 and SRX4200	32	168
SRX4600	32	268
SRX5400, SRX5600, and SRX5800 devices with SPC2 cards	32	32
SRX5400, SRX5600, and SRX5800 devices with SPC3 cards	32	0
SRX5400, SRX5600, and SRX5800 devices with SPC2 and SPC3 cards	NA	NA

See Also • Understanding Master Logical Systems

Tenant System Configuration Overview

The master administrator creates a tenant system and assigns an administrator for managing the tenant system. A tenant system can have multiple administrators.

The roles and responsibilities of a tenant system administrator are explained in [“Understanding Tenant Systems” on page 354](#).

The following steps explain the tasks that the tenant system administrator performs to configure the security features in a tenant system:

1. Use the Telnet or SSH services to access the device, and then log in to the tenant system with the login ID and password provided by the master administrator.

```
login: <tenant_name>
password: <password>
```

After you are authenticated, you can access the UNIX shell or CLI shell as per the tenant system configuration.

- The presence of the % prompt indicates the you accessed to the UNIX shell. Access the CLI shell by entering the **CLI** command.

```
% CLI
```

- The presence of the > prompt indicates the CLI has started. The prompt is preceded by a string that contains the username, the hostname of the device, and the name of the tenant system. When the CLI starts, you are at the top level in operational mode.

```
TSYS1_admin1@host:TSYS1>
```

2. Access the configuration mode by entering the **configure** operational mode command.

```
TSYS1_admin1@host:TSYS1> configure
TSYS1_admin1@host:TSYS1#
```

3. Enter the **quit** command to exit the configuration mode and return to the CLI shell.

```
TSYS1_admin1@host:TSYS1# quit
TSYS1_admin1@host:TSYS1>
```

4. The master administrator configures the logical interfaces and assigns those interfaces to the tenant system. Configure one routing instance and the routing protocols, and add options for the routing instance. See [“Configuring a Routing Instance for a Tenant System” on page 359](#).

5. Configure the following security features in the tenant system as necessary:

- Create zones for the tenant system and bind the logical interfaces to the zones. Create address books and use them in the security policies. See [“Example: Configuring Zones in the Tenant System” on page 378](#).
- Configure screen options at the zone level. See [“Example: Configuring Screen Options for a Tenant System” on page 424](#).

- Configure security policies between zones in the tenant system. See [“Example: Configuring Security Policies in a Tenant System” on page 144.](#)

Custom applications or application sets can be created for specific types of traffic. To create a custom application, use the **application** configuration statement at the **[edit applications]** hierarchy level. To create an application set, use the **application-set** configuration statement at the **[edit applications]** hierarchy level.

- Configure firewall authentication to the tenant system. The master administrator creates access profiles in the master logical system. The tenant system administrator then configures a security policy that specifies firewall authentication for matching traffic and configures the type of authentication (pass-through or Web authentication), default access profile, and success banner. See [“Configuring Firewall Authentication for a Tenant System” on page 408.](#)
- Configure Network Address Translation (NAT) for the tenant system. See [“Example: Configuring Network Address Translation for the Tenant Systems” on page 430.](#)
- Configure Application Layer Gateway (ALG) for the tenant system. See [“Example: Configuring ALG in Tenant System” on page 440.](#)

Configuring a Routing Instance for a Tenant System

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. A set of interfaces that belong to the routing instance and the routing protocol parameters control the information in the routing instance. A tenant system can configure the assigned routing instance and the interfaces that belong to the routing instance within a tenant system.



NOTE: Only one routing instance can be created for a tenant system.

The following procedure describes the steps to configure a routing instance and interfaces in a routing table for a tenant system:

1. Create a tenant system named **TSYS1**.

```
[edit]
user@host# set tenants TSYS1
```

2. Create a routing instance **r1** and assign the routing instance type for the tenant system.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 instance-type virtual-router
```

3. Specify the interface name for the routing instance.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 interface ge-0/0/0.0
```

4. Commit the configuration.

```
[edit]
```

```
user@host# commit
```

To view the configuration for the tenant system **TSYS1**, run the **show tenants TSYS1** command.

```
show tenants TSYS1
routing-instances {
  r1 {
    instance-type virtual-router;
    interface ge-0/0/0.0;
  }
}
```

The **show tenants TSYS1** command displays all the routing instance parameters configured for the tenant system **TSYS1**.

Example: Configuring Tenant Systems

This example shows how to configure the logical interfaces, routing instance, zones, and the default security policies for a tenant system.

- [Requirements on page 360](#)
- [Overview on page 360](#)
- [Configuration on page 361](#)
- [Verification on page 363](#)

Requirements

This example uses the following hardware and software components:

- SRX Series device configured with the tenant system.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Log in to the tenant system as the tenant system administrator. See [“Tenant System Configuration Overview” on page 358](#).
- Be sure you know which logical interfaces, logical tunnel interfaces, and corresponding IP addresses are assigned to the tenant system by the master administrator. See [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).
- Understand how to create a tenant system. See [“Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System” on page 65](#)

Overview

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. Logical interfaces on a device are allocated among the tenant systems by the master administrator. The master administrator can configure the interface and its

attributes for the tenant system interfaces. This example shows how the TSYS1 tenant system administrator configures the routing instance, security policies, and security zones for the TSYS1 tenant system.

Table 32 on page 361 provides the parameters used in this example.

Table 32: Tenant System Configuration

Feature	Name	Configuration Parameters
Routing instance	VR1	<ul style="list-style-type: none"> Instance type: virtual router Includes interfaces ge-0/0/2.0 and ge-0/0/4.0 Static routes: <ul style="list-style-type: none"> 192.0.2.1/24 next-hop 198.51.100.0/24
Zones	trust	Bind to interface ge-0/0/2.0
	untrust	Bind to interface ge-0/0/4.0
Policies	default-policy	Permit all 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 routing-instances VR1 instance-type virtual-router
set routing-instances VR1 interface ge-0/0/2.0
set routing-instances VR1 interface ge-0/0/4.0
set routing-instances VR1 routing-options static route 192.0.2.1/24 next-hop
  198.51.100.0/24
set security policies default-policy permit-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/2.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/4.0
```

Step-by-Step Procedure

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

To configure a tenant system:

1. Log in to the tenant system as the administrator for tenant system and enter configuration mode.

```
TSYS1_admin1@host:TSYS1> configure
TSYS1_admin1@host:TSYS1#
```

2. Configure the routing instance and assign interfaces.

```
[edit routing-instances]
TSYS1_admin1@host:TSYS1# set VR1 instance-type virtual-router
TSYS1_admin1@host:TSYS1# set VR1 interface ge-0/0/2.0
TSYS1_admin1@host:TSYS1# set VR1 interface ge-0/0/4.0
```

3. Configure static routes.

```
[edit routing-instances]
TSYS1_admin1@host:TSYS1# set VR1 routing-options static route 192.0.2.1/24
next-hop 198.51.100.0/24
```

4. Configure security policies.

```
[edit security policies]
TSYS1_admin1@host:TSYS1# set default-policy permit-all
```

5. Configure security zones and assign interfaces to each zone.

```
[edit security zones]
TSYS1_admin1@host:TSYS1# set security-zone trust host-inbound-traffic
system-services all
TSYS1_admin1@host:TSYS1# set security-zone trust host-inbound-traffic protocols
all
TSYS1_admin1@host:TSYS1# set security-zone trust interfaces ge-0/0/2.0
TSYS1_admin1@host:TSYS1# set security-zone untrust host-inbound-traffic
system-services all
TSYS1_admin1@host:TSYS1# set security-zone untrust host-inbound-traffic protocols
all
TSYS1_admin1@host:TSYS1# set security-zone untrust interfaces ge-0/0/4.0
```

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

```
TSYS1_admin1@host:TSYS1# show routing-instances
VR1 {
  instance-type virtual-router;
  interface ge-0/0/2.0;
  interface ge-0/0/4.0;
  routing-options {
    static {
      route 192.0.2.1/24 next-hop 198.51.100.0/24;
    }
  }
}
TSYS1_admin1@host:TSYS1# show security
policies {
  default-policy {
    permit-all;
  }
}
```

```

zones {
  security-zone trust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-0/0/2.0;
    }
  }
  security-zone untrust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-0/0/4.0;
    }
  }
}

```

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

Verification

Verifying Policy Configuration

Purpose Verify the security policy details of the TSYS1 tenant system.

Action From operational mode, enter the **show security policies detail** command to view the details of all the security policies configured for the TSYS1 tenant system.

```

TSYS1_admin1@host:TSYS1> show security policies detail
Default policy: permit-all
Pre ID default policy: permit-all

```

Meaning The output displays the security policy details of the TSYS1 tenant system.

See Also • [Understanding Tenant Systems on page 354](#)

Understanding Tenant System Security Profiles (Master Administrators Only)

Tenant systems allow you to virtually divide a supported SRX Series device into multiple devices, securing them from intrusion and attacks, and protecting them from faulty conditions outside their own contexts. To protect tenant systems, security resources are configured in a manner similar to how they are configured for a discrete device. However, the master administrator assigns resources to the tenant systems.

An SRX Series device running tenant systems can be partitioned into tenant systems, an interconnected tenant system, if necessary, and the default master logical system. When the system is initialized, the master logical system is created at the root. All system resources are assigned to it, effectively creating a default master logical system security profile. To distribute security resources across the tenant systems, the master administrator creates security profiles that specify the resources to be allocated to a tenant system. Only the master administrator can configure security profiles and bind them to the tenant systems. The tenant system administrator uses these resources for the respective tenant system.

The tenant systems are defined by the resources allocated to them, including security components, interfaces, routing instance, static routes, and dynamic routing protocols. The master administrator configures the security profiles and assigns them to the tenant systems. You cannot commit a tenant system configuration without a security profile assigned to it.

This topic includes the following sections:

- [Tenant Systems Security Profiles on page 364](#)
- [Understanding How the System Assesses Resources Assignment and Use Across the Tenant Systems on page 365](#)
- [Cases: Assessments of Reserved Resources Assigned Through Security Profiles on page 366](#)

Tenant Systems Security Profiles

The master administrator can configure and assign a security profile to a specific tenant system or multiple tenant systems. The maximum number of security profiles that can be configured depends on the capacity of an SRX Series device. When the maximum number of security profiles have been created, you need to delete a security profile and commit the configuration change before you can create and commit another security profile. In many cases, fewer security profiles are needed because you can bind a single security profile to more than one tenant system.

Security profiles allow you to:

- Share the device's resources, including policies, zones, addresses and address books, flow sessions, and various forms of NAT, among all tenant systems appropriately. You can assign various amounts of a resource to the tenant systems and allow the tenant systems to utilize the resources effectively.

Security profiles protect against one tenant system exhausting a resource that is required at the same time by other tenant systems. Security profiles protect critical

system resources and maintain a better performance among tenant systems when the device is experiencing a heavy traffic flow. Security profiles defend against one tenant system dominating the use of resources and allow the other tenant systems to use the resources effectively.

- Configure the device in a scalable way to allow for creation of additional tenant systems.

You need to delete the security profile of a tenant system before you can delete the tenant system.

Understanding How the System Assesses Resources Assignment and Use Across the Tenant Systems

To provision a tenant system with security features, the master administrator configures a security profile that specifies the resource for each security feature:

- A reserved quota that guarantees that the specified resource amount is always available to the tenant system.
- A maximum allowed quota. If a tenant system requires additional resources that exceed the reserved quota, then it can utilize the resources configured for the global maximum amount if the global resources are not allocated to the other tenant systems. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. The tenant systems need to utilize the global resources effectively based on the available resources.

If a reserved quota is not configured for a resource, the default value is 0. If a maximum allowed quota is not configured for a resource, the default value is the global system quota for the resource (global system quotas are platform-dependent). The master administrator must configure the appropriate maximum allowed quota values in the security profiles so that the maximum resource usage of a specific tenant system does not negatively impact other tenant systems configured on the device.

The system maintains a count of all allocated resources that are reserved, used, and made available again when a tenant system is deleted. This count determines whether resources are available to use for tenant systems or to increase the amount of the resources allocated to existing tenant systems through their security profiles.

Resources configured in security profiles are characterized as static modular resources or dynamic resources. For static resources, we recommend setting a maximum quota for a resource equal or close to the amount specified as its reserved quota, to allow for scalable configuration of tenant systems. A maximum quota for a resource gives a tenant system greater flexibility through access to a larger amount of that resource, but it constrains the amount of resources available to allocate to other tenant systems.

The following security features resources can be specified in a security profile:

- Security zones
- Addresses and address books for security policies
- Application firewall rule sets
- Application firewall rules

- Firewall authentication
- Flow sessions and gates
- NAT, including:
 - Cone NAT bindings
 - NAT destination rule
 - NAT destination pool
 - NAT IP address in source pool without Port Address Translation (PAT)



NOTE: IPv6 addresses in IPv6 source pools without PAT are not included in security profiles.

- NAT IP address in source pool with PAT
- NAT port overloading
- NAT source pool
- NAT source rule
- NAT static rule



NOTE: All resources except flow sessions are static.

You can modify a tenant system security profile dynamically while the security profile is assigned to other tenant systems. However, to ensure that the system resource quota is not exceeded, the system takes the following actions:

- If a static quota is changed, the system process that maintains the tenant system counts for resources specified in security profiles subsequently reevaluates the security profiles assigned to the profile associated with the static quota. This check identifies the number of resources assigned across all tenant systems to determine whether the allocated resources, including their increased amounts are available.

These quota checks are the same quota checks that the system performs when you add a tenant system and bind a security profile to it. They are also performed when you bind a different security profile from the security profile that is currently assigned to it to an existing tenant system (or the master logical system).

- If a dynamic quota is revised, no check is performed, but the revised quota is imposed on future resource usage.

Cases: Assessments of Reserved Resources Assigned Through Security Profiles

To understand how the system assesses allocation of reserved resources through security profiles, consider the following three cases explained in [Table 34 on page 368](#) and that address allocation of the resources and zones. To keep the example simple, 10 zones are allocated in security-profile-1: 4 reserved zones and 6 maximum zones. This example

assumes that the maximum amount specified—six zones—is available for the tenant systems. The system maximum number of zones is 10.

The three cases address the configuration across the tenant systems. The three cases verify whether a configuration succeeds or fails when it is committed based on the allocation of zones.

[Table 33 on page 367](#) shows the security profiles and their zone allocations.

Table 33: Security Profiles Used for Reserved Resource Assessments

Two Security Profiles Used in the Configuration Cases

security-profile-1

- zones reserved quota = 4
- zones maximum quota = 6

NOTE: The master administrator dynamically increases the reserved zone count specified in this profile later.

master-logical-system-profile

- zones maximum quota = 10
- no reserved quota

[Table 34 on page 368](#) shows three cases that illustrate how the system assesses reserved resources for zones across the tenant systems based on the security profile configurations.

- The configuration for the first case succeeds because the cumulative reserved resource quota for zones configured in the security profiles bound to all tenant systems is 8, which is less than the system maximum resource quota.
- The configuration for the second case fails because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 12, which is greater than the system maximum resource quota.
- The configuration for the third case fails because the cumulative reserved resource quota for zones configured in the security profiles bound to all tenant systems is 12, which is greater than the system maximum resource quota.

Table 34: Reserved Resource Allocation Assessment Across Tenant Systems**Reserved Resource Quota Checks Across Tenant Systems****Example 1: Succeeds**

This configuration is within bounds: $4+4+0=8$, maximum capacity =10.

Security Profiles Used

- The security profile security-profile-1 is bound to two tenant systems: tenant-system-1 and tenant-system-2.
- The master-logical-system-profile profile is used exclusively for the master logical system.
- tenant-system-1 = 4 reserved zones.
- tenant-system-2 = 4 reserved zones.
- master-logical-system = 0 reserved zones.

Example 2: Fails

This configuration is out of bounds: $4+4+4=12$, maximum capacity =10.

- tenant-system-1 = 4 reserved zones.
- tenant-system-2 = 4 reserved zones.
- master-logical-system = 0 reserved zones.
- new-tenant-system = 4 reserved zones.

Security Profiles

- The security profile security-profile-1 is bound to two tenant systems: tenant-system-1 and tenant-system-2.
- The master-logical-system-profile is bound to the master logical system and used exclusively for it.
- The master administrator configures a new tenant system called new-tenant-system and binds security-profile-1 to it.

Example 3: Fails

This configuration is out of bounds: $6+6=12$, maximum capacity =10.

The master administrator modifies the reserved zones quota in security-profile-1, increasing the count to 6.

- tenant-system-1 = 6 reserved zones.
- tenant-system-2 = 6 reserved zones.
- master-logical-system = 0 reserved zones.

- See Also**
- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)
 - [Understanding User Logical Systems and the User Logical System Administrator Role on page 63](#)

Example: Configuring Tenant Systems Security Profiles (Master Administrators Only)

This example shows how the master administrator configures security profiles for the master logical system and two tenant systems.

- [Requirements on page 369](#)
- [Overview on page 369](#)
- [Configuration on page 369](#)
- [Verification on page 376](#)

Requirements

This example uses the following hardware and software components:

- SRX Series device configured with tenant systems.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Read the “[Understanding Tenant Systems](#)” on [page 354](#) to understand how this task fits into the overall configuration process.
- Read the “[Flow for Tenant Systems](#)” on [page 381](#) to understand how to create a tenant system, a tenant system administrator, and an interconnect tenant system.

Overview

The master administrator creates security profiles that specify the resources to be allocated across the tenant systems. You cannot commit a tenant system configuration without a security profile assigned to it.

This example shows how to configure the security profiles for different tenant systems described in [Table 35 on page 369](#).

Table 35: Security Profiles for Logical Systems

Logical Systems	Security Profile
Master logical system	Master profile
Tenant system TSYS1	SP1
Tenant system TSYS2	SP2
Interconnect tenant system	Null

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 system security-profile master-profile policy maximum 65
set system security-profile master-profile policy reserved 60
set system security-profile master-profile zone maximum 22
set system security-profile master-profile zone reserved 17
set system security-profile master-profile flow-session maximum 3000
set system security-profile master-profile flow-session reserved 2100
set system security-profile master-profile nat-nopat-address maximum 115
set system security-profile master-profile nat-nopat-address reserved 100
set system security-profile master-profile nat-static-rule maximum 125
set system security-profile master-profile nat-static-rule reserved 100
set system security-profile master-profile auth-entry maximum 1000
set system security-profile master-profile auth-entry reserved 400
set system security-profile master-profile logical-system root-logical-system
set system security-profile SP1 policy maximum 100
set system security-profile SP1 policy reserved 50
set system security-profile SP1 zone maximum 100
set system security-profile SP1 zone reserved 50
set system security-profile SP1 flow-session maximum 100
set system security-profile SP1 flow-session reserved 50
set system security-profile SP1 nat-nopat-address maximum 125
set system security-profile SP1 nat-nopat-address reserved 100
set system security-profile SP1 nat-static-rule maximum 125
set system security-profile SP1 nat-static-rule reserved 100
set system security-profile SP1 auth-entry maximum 1000
set system security-profile SP1 auth-entry reserved 600
set system security-profile SP1 tenant TSYS1
set system security-profile SP2 policy maximum 50
set system security-profile SP2 policy reserved 40
set system security-profile SP2 zone maximum 10
set system security-profile SP2 zone reserved 5
set system security-profile SP2 flow-session maximum 100
set system security-profile SP2 flow-session reserved 50
set system security-profile SP2 nat-nopat-address maximum 125
set system security-profile SP2 nat-nopat-address reserved 100
set system security-profile SP2 nat-static-rule maximum 125
set system security-profile SP2 nat-static-rule reserved 100
set system security-profile SP2 auth-entry maximum 1000
set system security-profile SP2 auth-entry reserved 500
set system security-profile SP2 tenant TSYS2
set system security-profile interconnect-profile tenants interconnect-tenant
```

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

1. Create the first security profile for the master logical system.
 - a. Specify the number of maximum and reserved security policies.

```
[edit system security-profile]
user@host# set master-profile policy maximum 65
user@host# set master-profile policy reserved 60
```

- b. Specify the number of maximum and reserved security zones.

```
[edit system security-profile]
user@host# set master-profile zone maximum 22
user@host# set master-profile zone reserved 17
```

- c. Specify the number of maximum and reserved security sessions.

```
[edit system security-profile]
user@host# set master-profile flow-session maximum 3000
user@host# set master-profile flow-session reserved 2100
```

- d. Specify the number of maximum and reserved source NAT, no-PAT addresses, and static NAT rules.

```
[edit system security-profile]
user@host# set master-profile nat-nopat-address maximum 115
user@host# set master-profile nat-nopat-address reserved 100
user@host# set master-profile nat-static-rule maximum 125
user@host# set master-profile nat-static-rule reserved 100
```

- e. Specify the maximum and reserved number of resources for the firewall authentication entries.

```
[edit system security-profile]
user@host# set master-profile auth-entry maximum 1000
user@host# set master-profile auth-entry reserved 400
```

- f. Bind the security profile to the master logical system.

```
[edit system security-profile]
user@host# set master-profile logical-system root-logical-system
```

2. Create the second security profile for the first tenant system.

- a. Specify the number of maximum and reserved security policies.

```
[edit system security-profile]
user@host# set SP1 policy maximum 100
user@host# set SP1 policy reserved 50
```

- b. Specify the number of maximum and reserved security zones.

```
[edit system security-profile]
user@host# set SP1 zone maximum 100
user@host# set SP1 zone reserved 50
```

- c. Specify the number of maximum and reserved security sessions.

```
[edit system security-profile]
user@host# set SP1 flow-session maximum 100
user@host# set SP1 flow-session reserved 50
```

- d. Specify the number of maximum and reserved source NAT, no-PAT addresses, and static NAT rules.

```
[edit system security-profile]
user@host# set SP1 nat-nopat-address maximum 115
user@host# set SP1 nat-nopat-address reserved 100
user@host# set SP1 nat-static-rule maximum 125
user@host# set SP1 nat-static-rule reserved 100
```

- e. Specify the maximum and reserved number of resources for the firewall authentication entries.

```
[edit system security-profile]
user@host# set SP1 auth-entry maximum 1000
user@host# set SP1 auth-entry reserved 600
```

- f. Bind the security profile to the tenant system TSYS1.

```
[edit system security-profile]
user@host# set security-profile SP1 tenants TSYS1
```

3. Create the third security profile for the second tenant system.

- a. Specify the number of maximum and reserved security policies.

```
[edit system security-profile]
user@host# set SP2 policy maximum 50
user@host# set SP2 policy reserved 40
```

- b. Specify the number of maximum and reserved security zones.

```
[edit system security-profile]
user@host# set SP2 zone maximum 10
user@host# set SP2 zone reserved 5
```

- c. Specify the number of maximum and reserved security sessions.

```
[edit system security-profile]
user@host# set SP2 flow-session maximum 100
user@host# set SP2 flow-session reserved 50
```

- d. Specify the number of maximum and reserved source NAT, no-PAT addresses, and static NAT rules.

```
[edit system security-profile]
user@host# set SP2 nat-nopat-address maximum 115
user@host# set SP2 nat-nopat-address reserved 100
user@host# set SP2 nat-static-rule maximum 125
user@host# set SP2 nat-static-rule reserved 100
```

- e. Specify the maximum and reserved number of resources for the firewall authentication entries.

```
[edit system security-profile]
```

```
user@host# set SP2 auth-entry maximum 1000
user@host# set SP2 auth-entry reserved 600
```

- f. Bind the security profile to the tenant system **TSYS2**.

```
[edit system security-profile]
user@host# set security-profile SP2 tenants TSYS2
```

4. Bind a null security profile to the interconnect tenant system.

```
[edit system security-profile]
user@host# set security-profile interconnect-profile tenants interconnect-tenant
```

Results From configuration mode, confirm your configuration by entering the **show system security-profile** command to view all the configured security profiles.

```
user@host# show system security-profile
SP1 {
  auth-entry {
    maximum 1000;
    reserved 600;
  }
  policy {
    maximum 100;
    reserved 50;
  }
  zone {
    maximum 100;
    reserved 50;
  }
  flow-session {
    maximum 100;
    reserved 50;
  }
  nat-nopat-address {
    maximum 115;
    reserved 100;
  }
  nat-static-rule {
    maximum 125;
    reserved 100;
  }
}
SP2 {
  auth-entry {
    maximum 1000;
    reserved 500;
  }
  policy {
    maximum 50;
    reserved 40;
  }
  zone {
```

```
        maximum 10;
        reserved 5;
    }
    flow-session {
        maximum 100;
        reserved 50;
    }
    nat-nopat-address {
        maximum 115;
        reserved 100;
    }
    nat-static-rule {
        maximum 125;
        reserved 100;
    }
}
master-profile {
    auth-entry {
        maximum 1000;
        reserved 400;
    }
    policy {
        maximum 65;
        reserved 60;
    }
    zone {
        maximum 22;
        reserved 17;
    }
    flow-session {
        maximum 3000;
        reserved 2100;
    }
    nat-nopat-address {
        maximum 115;
        reserved 100;
    }
    nat-static-rule {
        maximum 125;
        reserved 100;
    }
}
```

To view the security profile configured for the tenant systems and the master logical system, enter the **show tenants** and **show logical-systems root-logical-system** commands respectively.

```
user@host# show tenants
interconnect-tenant {
    security-profile {
        interconnect-profile;
    }
}
TSYS1 {
    security-profile {
        SPI;
```

```

    }
  }
  TSYS2 {
    security-profile {
      SP2;
    }
  }
}

user@host# show logical-systems root-logical-system
root-logical-system {
  security-profile {
    master-profile;
  }
}

```

To view the individual security profiles, enter the **show system security-profile master-profile**, the **show system security-profile SP1**, and the **show system security-profile SP2** commands.

```

user@host# show system security-profile master-profile
auth-entry {
  maximum 1000;
  reserved 400;
}
policy {
  maximum 65;
  reserved 60;
}
zone {
  maximum 22;
  reserved 17;
}
flow-session {
  maximum 3000;
  reserved 2100;
}
nat-nopat-address {
  maximum 115;
  reserved 100;
}
nat-static-rule {
  maximum 125;
  reserved 100;
}

user@host# show system security-profile SP1
auth-entry {
  maximum 1000;
  reserved 600;
}
policy {
  maximum 100;
  reserved 50;
}
zone {
  maximum 100;
  reserved 50;
}

```

```
}
flow-session {
    maximum 100;
    reserved 50;
}
nat-nopat-address {
    maximum 115;
    reserved 100;
}
nat-static-rule {
    maximum 125;
    reserved 100;
}

user@host# show system security-profile SP2
auth-entry {
    maximum 1000;
    reserved 500;
}
policy {
    maximum 50;
    reserved 40;
}
zone {
    maximum 10;
    reserved 5;
}
flow-session {
    maximum 100;
    reserved 50;
}
nat-nopat-address {
    maximum 115;
    reserved 100;
}
nat-static-rule {
    maximum 125;
    reserved 100;
}
```

If the output does not display the intended configuration, repeat the configuration instructions in these examples to correct it. If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the security resources that you allocated for tenant systems have been assigned to them, follow this procedure for each tenant system and for all its resources.

- [Verify the Security Profiles Assigned to the Tenant Systems on page 376](#)

Verify the Security Profiles Assigned to the Tenant Systems

Purpose Verify the security resources for each tenant system. Follow this process for all the configured tenant systems.

- Action**
1. Use the Telnet or SSH services to access the device, and then log in to each tenant system as its administrator with the login ID and password provided by the master administrator.

```
login: <tenant_name>
password: <password>
TSYS1_admin1@host:TSYS1>
```

2. Enter the following statement to identify the resources that are configured for the security profile.

```
TSYS1_admin1@host:TSYS1> show system security-profile ?
```

3. Enter the following command at the resulting prompt. Repeat the following step for all the security features configured in the security profiles.

```
TSYS1_admin1@host:TSYS1> show system security-profile zone detail
tenant system name : TSYS1
security profile name : SP1
used amount : 0
reserved amount : 50
maximum quota : 100
```

Meaning The sample output shows the security resources that are configured for each tenant system.

- See Also**
- [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
 - [Understanding Tenant Systems on page 354](#)

Security Zones for Tenant Systems

Security zones can be configured with tenant systems. For more information see the following topics:

- [Understanding Zones for Tenant Systems on page 377](#)
- [Example: Configuring Zones in the Tenant System on page 378](#)

Understanding Zones for Tenant Systems

Security zones are logical entities to which one or more interfaces are bound. Security zones can be configured on the tenant systems by the administrator. On a tenant system, the administrator can configure multiple security zones, dividing the network into network segments to which various security options can be applied.

The master administrator configures the maximum and reserved numbers of security zones for the tenant system. Then the administrator for the tenant system can create the security zones in the tenant system and assign interfaces to each security zone. The

number of zones configured in the tenant system count toward the maximum number of zones available on the device. The **show system security-profile zones** command is used to view the number of security zones allocated to the tenant system and the **show interfaces** command to view the interfaces assigned to the tenant system.

You can configure the following features in a tenant system security zone:

- Interfaces that are part of a security zone.
- Screen options—For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful.
- TCP-Reset—When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the synchronize flag set.
- Host inbound traffic—This feature specifies the kinds of traffic that can reach the device from systems that are directly connected to its interfaces. You can configure these parameters at the zone level, in which case they affect all interfaces of the zone, or at the interface level. Interface configuration overrides that of the zone.

There are no preconfigured security zones in the tenant system.

The management functional zone (MGT) can be configured for the tenant system. There is the management interface per device that is allocated to the tenant system.

The administrator for the tenant system can configure and view all attributes for a security zone in a tenant system. All security zone attributes in a tenant system are also visible to the master administrator.

Example: Configuring Zones in the Tenant System

This example shows how to configure the zones for the tenant system.

- [Requirements on page 378](#)
- [Overview on page 378](#)
- [Configuration on page 379](#)
- [Verification on page 380](#)

Requirements

Before you begin the configuration:

- Configure the interfaces created by the master administrator. See *Example: Configuring Interfaces and Routing Instances for a Tenant System*.

Overview

In this example, you can configure zones for the tenant systems. Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. The **[edit tenants tenant-name security zones]** hierarchy level is used to configure

the security zones. This example configures the security policies and zones described in [Table 36 on page 379](#).

Table 36: Security Zones Parameters

Feature	Configuration Parameters
Zones 1	<ul style="list-style-type: none"> Security zone: trust System services: any-service Bind to interfaces xe-0/0/1.0 (trust), xe-0/0/3.0 (untrust)
Zone 2	<ul style="list-style-type: none"> Security zone: untrust System services: any-service Bind to interfaces xe-0/0/1.0 (trust), xe-0/0/3.0 (untrust)

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 tenants TN1 security zones security-zone trust host-inbound-traffic system-services
any-service
set tenants TN1 security zones security-zone trust interfaces xe-0/0/1.0
set tenants TN1 security zones security-zone untrust host-inbound-traffic system-services
any-service
set tenants TN1 security zones security-zone untrust interfaces xe-0/0/3.0
```

Step-by-Step Procedure

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

To configure security zones in the tenant system:

- Define the tenant system name as TN1.

```
[edit]
user@host# set tenants TN1
```
- Configure a security zone as trust that permits traffic from zone trust and assign it to an interface.

```
[edit tenants TN1 security zones security-zone trust]
user@host# set host-inbound-traffic system-services any-service
user@host# set interfaces xe-0/0/1.0
```
- Configure a security zone as untrust that permits traffic from zone untrust and assign it to an interface.

```
[edit tenants TN1 security zones security-zone untrust]
user@host# set host-inbound-traffic system-services any-service
```

```
user@host# set interfaces xe-0/0/3.0
```

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

```
user@host# show tenants TN1 security zones
security-zone trust {
  host-inbound-traffic {
    system-services {
      any-service;
    }
  }
  interfaces {
    xe-0/0/1.0;
  }
}
security-zone untrust {
  host-inbound-traffic {
    system-services {
      any-service;
    }
  }
  interfaces {
    xe-0/0/3.0;
  }
}
```

Verification

To confirm that the configuration is working properly, perform the following task:

- [Verifying Zone Configuration on page 380](#)

Verifying Zone Configuration

Purpose Verify the information about security zones.

Action To verify the configuration is working properly, enter the **show security zones tenant all** command from operational mode.

```
user@host> show security zones tenant all
```

```
Tenant: TN1
```

```
Security zone: Host
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:
```

```
Security zone: abc
```

```
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:xe-0/0/1.0
```

```
Security zone: def
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:xe-0/0/3.0
```

Meaning The output displays the information of security zones configured on the tenant system.

Related Documentation

- [Security Policies for Tenant Systems on page 419](#)

Flow for Tenant Systems

This topic explains how packets are processed in flow sessions on devices that are configured with tenant systems. It describes how the device running tenant systems handles pass-through traffic between tenant systems. This topic also covers self-traffic as self-initiated traffic within a tenant system and self-traffic terminated on another tenant system. Before addressing tenant systems, the topic provides basic information about the SRX Series architecture with respect to packet processing and sessions. Finally, addresses the sessions and how to change session characteristics.

- [Session Creation for Devices Running Tenant Systems on page 381](#)
- [Configuring Logical Systems and Tenant Systems Interconnect with Multiple VPLS Switches on page 386](#)
- [Configuring tenant systems Interconnect with Logical Tunnel Interface point-to-point connection on page 394](#)
- [Configuring Logical System and Tenant System Interconnect with a Logical Tunnel Interface point-to-point connection on page 400](#)

Session Creation for Devices Running Tenant Systems

A session is created, based on routing and other classification information, to store information and allocate resources for a flow. Basically, a session is established when a traffic enters a tenant system interface, route lookup is performed to identify the next hop interface, and policy lookup is performed.

Optionally, the tenant systems enable you to configure an internal software switch. A virtual private LAN switch (VPLS) is implemented as an interconnect in tenant system. The VPLS enables both transit traffic and traffic terminated at a tenant system to pass between tenant systems. To allow traffic to pass between tenant systems or between tenant system and logical system, logical tunnel (lt-0/0/0) interfaces across the interconnect tenant system are used.



NOTE: Packet sequence occurs at the ingress and the egress interfaces. Packets traversing between tenant systems might not be processed in the order in which they were received on the physical interface.

Understanding Packet Classification

The Packet classification for a flow-based processing is based on both the physical interface and the logical interface and depends on the incoming interface. The packet classification is performed at the ingress point and within a flow, the packet-based processing also takes place on an SPU sometimes.

Packet classification is assessed the same way for devices that are configured with or without tenant systems. The traffic for a dedicated interface is classified to the tenant system that contains that interface. The filters and class-of-service features are typically associated with an interface to influence which packets are allowed to transit the device and to apply special actions to packets as needed.

Understanding the VPLS Switch and Logical Tunnel Interfaces

This topic covers the interconnect tenant system that serves as an internal virtual private LAN service (VPLS) switch connecting one tenant system on the device to another. The topic also explains how logical tunnel (lt-0/0/0) interfaces are used to connect tenant systems through the interconnect tenant system.

A device running tenant systems can use an internal VPLS switch to pass traffic without it leaving the device. For communication between tenant systems on the device to occur, you must configure an lt-0/0/0 interface on each tenant system that will use the internal switch, and you must associate it with its peer lt-0/0/0 interface on the interconnect tenant system, effectively creating a logical tunnel between them. You define a peer relationship at each end of the tunnel when you configure the tenant system's lt-0/0/0 interfaces.

You might want all tenant systems on the device to be able to communicate with one another without using an external switch. Alternatively, you might want some tenant systems to connect across the internal switch but not all of them.



WARNING: If you configure an lt-0/0/0 interface in any tenant system and you do not configure a VPLS switch containing a peer lt-0/0/0 interface for it, the commit will fail.

An SRX Series device running tenant systems can be used in a chassis cluster and each node has the same configuration.

When you use SRX Series devices configured with tenant systems within a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. tenant systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

Handling Pass-Through Traffic for Tenant Systems

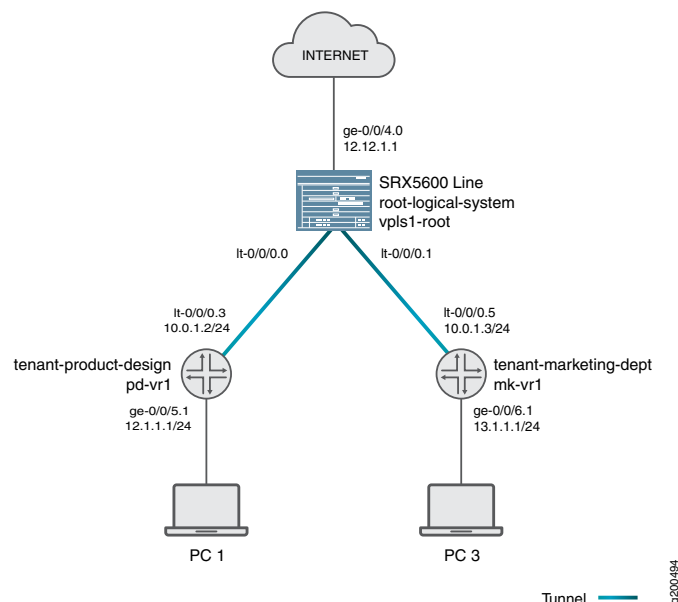
For SRX Series devices running tenant systems, pass-through traffic can exist within a tenant system or between tenant systems.

- [Pass-Through Traffic Between Tenant Systems on page 383](#)

Pass-Through Traffic Between Tenant Systems

Pass-through traffic between tenant systems is complicated by fact that each tenant system has an ingress and an egress interface that the traffic must transit. It is as if traffic were coming into and going out from two devices. Consider how pass-through traffic is handled between tenant systems given in the topology shown in [Figure 11 on page 383](#).

Figure 11: Tenant Systems, Their Virtual Routers, and Their Interfaces



Two sessions must be established for pass-through traffic between tenant systems. (Note that policy lookup is performed in both tenant systems).

- On the incoming tenant system, one session is set up between the ingress interface (a physical interface) and its egress interface (an lt-0/0/0 interface).
- On the egress tenant system, another session is set up between the ingress interface (the lt-0/0/0 interface of the second tenant system) and its egress interface (a physical interface).

Consider how pass-through traffic is handled across tenant systems in the topology shown in [Figure 11 on page 383](#).

- A session is established in the incoming tenant system.

- When a packet arrives on interface ge-0/0/5, it is identified as belonging to the tenant-product-design tenant system.
- Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1.
- As a result of the lookup, the egress interface for the packet is identified as lt-0/0/0.3 with the next hop identified as lt-0/0/0.5, which is the ingress interface in the tenant-marketing-dept.
- A session is established between ge-0/0/5 and lt-0/0/0.3.
- A session is established in the outgoing tenant system.
 - The packet is injected into the flow again from lt-0/0/0.5, and the tenant system context identified as tenant-marketing-dept is derived from the interface.
 - Packet processing continues in the tenant-marketing-dept tenant system.
 - To identify the egress interface, route lookup for the packet is performed in the mk-vr1 routing instances.
 - The outgoing interface is identified as ge-0/0/6, and the packet is transmitted from the interface to the network.

Handling Self-Traffic

Self-traffic is traffic that originates in a tenant system on a device and is either sent out to the network from that tenant system or is terminated on another tenant system on the device.

Self-Initiated Traffic

Self-initiated traffic is generated from a source tenant system context and forwarded directly to the network from the tenant system interface.

The following process occurs:

- When a packet is generated in a tenant system, a process for handling the traffic is started in the tenant system.
- Route lookup is performed to identify the egress interface, and a session is established.
- The tenant system performs a policy lookup and processes the traffic accordingly.

Consider how self-initiated traffic is handled across tenant systems given the topology shown in [Figure 11 on page 383](#).

- A packet is generated in the tenant-product-design tenant system, and a process for handling the traffic is started in the tenant system.
- Route lookup is performed in pd-vr2, and the egress interface is identified as ge-0/0/8.
- A session is established.
- The packet is transmitted to the network from ge-0/0/8.

Traffic Terminated on a Tenant System

When a packet enters the device on an interface belonging to a tenant system and the packet is destined for another tenant system on the device, the packet is forwarded between the tenant systems in the same manner as is pass-through traffic. However, route lookup in the second tenant system identifies the local egress interface as the packet destination. Consequently the packet is terminated on the second tenant system as self-traffic.

- For terminated self-traffic, two policy lookups are performed, and two sessions are established.
 - On the incoming tenant system, one session is set up between the ingress interface (a physical interface) and its egress interface (an lt-0/0/0 interface).
 - On the destination tenant system, another session is set up between the ingress interface (the lt-0/0/0 interface of the second tenant system) and the local interface.

Consider how terminated self-traffic is handled across tenant systems in the topology shown in [Figure 11 on page 383](#).

- A session is established in the incoming tenant system.
 - When a packet arrives on interface ge-0/0/5, it is identified as belonging to the tenant-product-design tenant system.
 - Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1.
 - As a result of the lookup, the egress interface for the packet is identified as lt-0/0/0.3 with the next hop identified as lt-0/0/0.5, the ingress interface in the ls-marketing-dept.
- A session is established between ge-0/0/5 and lt-0/0/0.3.
- A management session is established in the destination tenant system.
 - The packet is injected into the flow again from lt-0/0/0.5, and the tenant system context identified as tenant-marketing-dept is derived from the interface.
 - Packet processing continues in the tenant-marketing-dept tenant system.
 - Route lookup for the packet is performed in the mk-vr1 routing instance. The packet is terminated in the destination tenant system as self-traffic.

Understanding Session and Gate Limitation Control

Sessions are created based on routing and other classification information to store information and allocate resources for a flow. The tenant systems flow module provides session and gate limitation to ensure that these resources are shared among the tenant systems. Resources allocation and limitations for each tenant system are specified in the security profile bound to the tenant system.

- For session limiting, the system checks the first packet of a session against the maximum number of sessions configured for the tenant system. When the maximum limit of session is reached, the device drops the packet and logs the event.
- For gate limiting, the device checks the first packet of a session against the maximum number of gates configured for the tenant system. If the maximum number of gates for a tenant system is reached, the device rejects the gate open request and logs the event.

About Configuring Sessions

Depending on the protocol and service, a session is programmed with a timeout value. For example, the default timeout for TCP is 1800 seconds. The default timeout for UDP is 60 seconds. When a flow is terminated, it is marked as invalid, and its timeout is reduced to 10 seconds. If no traffic uses the session before the service timeout, the session is aged out and freed to a common resource pool for reuse.

You can affect the life of a session in the following ways:

- Age out sessions, based on how full the session table is.
- Set an explicit timeout for aging out TCP sessions.
- Configure a TCP session to be invalidated when it receives a TCP RST (reset) message.
- You can configure sessions to accommodate other systems as follows:
 - Disable TCP packet security checks.
 - Change the maximum segment size.

Configuring Logical Systems and Tenant Systems Interconnect with Multiple VPLS Switches

This example shows how to interconnect logical systems and tenant systems with multiple VPLS switches. This is achieved by configuring multiple logical systems and tenant systems with more than one logical tunnel (LT) interface under a tenant system and multiple VPLS switches that are configured to pass the traffic without leaving an SRX Series device.

- [Requirements on page 386](#)
- [Overview on page 386](#)
- [Configuration on page 387](#)
- [Verification on page 393](#)

Requirements

This example uses an SRX Series device running Junos OS with logical systems and tenant systems.

Overview

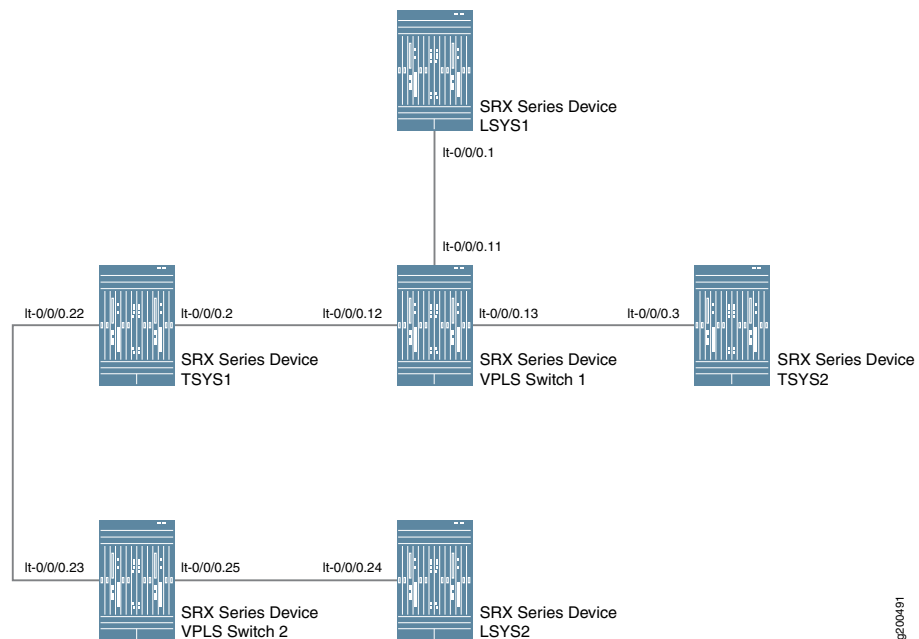
In this example, we configure multiple LT interfaces and multiple VPLS switches under one tenant system.

In this example, we also configure interconnection between multiple logical systems and tenant systems with LT interface point-to-point connections (Encapsulation Ethernet and Encapsulation Frame-Relay).

For interconnected logical systems and tenant systems with multiple VPLS switches, this example configures logical tunnel interfaces lt-0/0/0 with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces and security-profiles are assigned to the logical systems and tenant systems. The routing instance for the VPLS switch-1 and VPLS switch-2 are also assigned to the logical systems and tenant systems.

Figure 12 on page 387 shows the topology for interconnected logical systems and tenant systems with multiple VPLS switches.

Figure 12: Configuring the interconnected logical systems and tenant systems with multiple VPLS switches.



g200491

Configuration

To configure interfaces for the logical system and tenant system, perform these tasks:

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 interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 11 peer-unit 1
set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 12 peer-unit 2
set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
```

```

set interfaces lt-0/0/0 unit 13 peer-unit 3
set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 23 peer-unit 22
set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 25 peer-unit 24
set routing-instances vpls-switch-1 instance-type vpls
set routing-instances vpls-switch-1 interface lt-0/0/0.11
set routing-instances vpls-switch-1 interface lt-0/0/0.12
set routing-instances vpls-switch-1 interface lt-0/0/0.13
set routing-instances vpls-switch-2 instance-type vpls
set routing-instances vpls-switch-2 interface lt-0/0/0.23
set routing-instances vpls-switch-2 interface lt-0/0/0.25
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address 192.168.0.1/24
set interfaces lt-0/0/0 unit 2 encapsulation ethernet
set interfaces lt-0/0/0 unit 2 peer-unit 12
set interfaces lt-0/0/0 unit 2 family inet address 192.168.0.2/24
set interfaces lt-0/0/0 unit 22 encapsulation ethernet
set interfaces lt-0/0/0 unit 22 peer-unit 23
set interfaces lt-0/0/0 unit 22 family inet address 192.168.4.1/30
set tenants TSYS1 routing-instances vr11 instance-type virtual-router
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.2
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.22
set interfaces lt-0/0/0 unit 3 encapsulation ethernet
set interfaces lt-0/0/0 unit 3 peer-unit 13
set interfaces lt-0/0/0 unit 3 family inet address 192.168.0.3/24
set tenants TSYS2 routing-instances vr12 instance-type virtual-router
set tenants TSYS2 routing-instances vr12 interface lt-0/0/0.3
set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 peer-unit 25
set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 family inet address 192.168.4.2/30
set system security-profile SP-user policy maximum 100
set system security-profile SP-user policy reserved 50
set system security-profile SP-user zone maximum 60
set system security-profile SP-user zone reserved 10
set system security-profile SP-user flow-session maximum 100
set system security-profile SP-user flow-session reserved 50
set system security-profile SP-user logical-system LSYS1
set system security-profile SP-user tenant TSYS1
set system security-profile SP-user tenant TSYS2
set system security-profile SP-user logical-system LSYS2

```

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*.

1. Configure the lt-0/0/0 interfaces.

```

[edit]
user@host# set interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 11 peer-unit 1
user@host# set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 12 peer-unit 2
user@host# set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls

```

```

user@host# set interfaces lt-0/0/0 unit 13 peer-unit 3
user@host# set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 23 peer-unit 22
user@host# set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 25 peer-unit 24

```

2. Configure the routing instance for the VPLS switches and add interfaces to it.

```

[edit]
user@host# set routing-instances vpls-switch-1 instance-type vpls
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.11
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.12
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.13
user@host# set routing-instances vpls-switch-2 instance-type vpls
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.23
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.25

```

3. Configure LSYS1 with lt-0/0/0.1 interface and peer lt-0/0/0.11.

```

[edit]
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation
    ethernet
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address
    192.168.0.1/24

```

4. Configure TSYS1 with lt-0/0/0.2 interface and peer lt-0/0/0.12.

```

[edit]
user@host# set interfaces lt-0/0/0 unit 2 encapsulation ethernet
user@host# set interfaces lt-0/0/0 unit 2 peer-unit 12
user@host# set interfaces lt-0/0/0 unit 2 family inet address 192.168.0.2/24
user@host# set interfaces lt-0/0/0 unit 22 encapsulation ethernet
user@host# set interfaces lt-0/0/0 unit 22 peer-unit 23
user@host# set interfaces lt-0/0/0 unit 22 family inet address 192.168.4.1/30
user@host# set tenants TSYS1 routing-instances vr11 instance-type virtual-router
user@host# set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.2
user@host# set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.22

```

5. Configure TSYS2 with lt-0/0/0.3 interface and peer lt-0/0/0.13

```

[edit]
user@host# set interfaces lt-0/0/0 unit 3 encapsulation ethernet
user@host# set interfaces lt-0/0/0 unit 3 peer-unit 13
user@host# set interfaces lt-0/0/0 unit 3 family inet address 192.168.0.3/24
user@host# set tenants TSYS2 routing-instances vr12 instance-type virtual-router
user@host# set tenants TSYS2 routing-instances vr12 interface lt-0/0/0.3

```

6. Configure LSYS2 with lt-0/0/0 interface and peer-unit 24.

```

[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 encapsulation
    ethernet
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 peer-unit 25

```

```
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 family inet
address 192.168.4.2/30
```

7. Assign security-profile for logical-systems.

```
[edit]
user@host# set system security-profile SP-user policy maximum 100
user@host# set system security-profile SP-user policy reserved 50
user@host# set system security-profile SP-user zone maximum 60
user@host# set system security-profile SP-user zone reserved 10
user@host# set system security-profile SP-user flow-session maximum 100
user@host# set system security-profile SP-user flow-session reserved 50
user@host# set system security-profile SP-user logical-system LSYS1
user@host# set system security-profile SP-user tenant TSYS1
user@host# set system security-profile SP-user tenant TSYS2
user@host# set system security-profile SP-user logical-system LSYS2
```

- Results**
- From configuration mode, confirm your configuration by entering the **show interfaces lt-0/0/0**, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it

```
unit 2 {
  encapsulation ethernet;
  peer-unit 12;
  family inet {
    address 192.168.0.2/24;
  }
}
unit 3 {
  encapsulation ethernet;
  peer-unit 13;
  family inet {
    address 192.168.0.3/24;
  }
}
unit 11 {
  encapsulation ethernet-vpls;
  peer-unit 1;
}
unit 12 {
  encapsulation ethernet-vpls;
  peer-unit 2;
}
unit 13 {
  encapsulation ethernet-vpls;
  peer-unit 3;
}
unit 22 {
  encapsulation ethernet;
  peer-unit 23;
  family inet {
    address 192.168.4.1/30;
  }
}
```

```

unit 23 {
    encapsulation ethernet-vpls;
    peer-unit 22;
}
unit 25 {
    encapsulation ethernet-vpls;
    peer-unit 24;
}

```

- From configuration mode, confirm your configuration by entering the **show routing-instances** command. 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
vpls-switch-1 {
    instance-type vpls;
    interface lt-0/0/0.11;
    interface lt-0/0/0.12;
    interface lt-0/0/0.13;
}
vpls-switch-2 {
    instance-type vpls;
    interface lt-0/0/0.23;
    interface lt-0/0/0.25;
}

```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS1** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show logical-systems LSYS1
interfaces {
    lt-0/0/0 {
        unit 1 {
            encapsulation ethernet;
            peer-unit 11;
            family inet {
                address 192.168.0.1/24;
            }
        }
    }
}

```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS2** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show tenants TSYS1
routing-instances {
    vr11 {
        instance-type virtual-router;
        interface lt-0/0/0.2;
        interface lt-0/0/0.22;
    }
}

```

```
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS3**, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS2
routing-instances {
  vr12 {
    instance-type virtual-router;
    interface lt-0/0/0.3;
  }
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS2**, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS2
interfaces {
  lt-0/0/0 {
    unit 24 {
      encapsulation ethernet;
      peer-unit 25;
      family inet {
        address 192.168.4.2/30;
      }
    }
  }
}
```

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

```
[edit]
user@host# show system security-profile
SP-user {
  policy {
    maximum 100;
    reserved 50;
  }
  zone {
    maximum 60;
    reserved 10;
  }
  flow-session {
    maximum 100;
    reserved 50;
  }
  logical-system [ LSYS1 LSYS2 ];
  tenant [ TSYS1 TSYS2 ];
}
```

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 the Security-Profile for all Logical-systems on page 393](#)
- [Verifying the LT Interfaces for all Logical systems on page 393](#)

Verifying the Security-Profile for all Logical-systems

Purpose Verify security profile for each logical systems.

Action From operational mode, enter the **show system security-profile security-log-stream-number logical-system all** command.

```
user@host> show system security-profile assignment summary
```

	Total	Maximum
security-profiles	1	65
logical-systems	1	32
tenants	0	32
logical-systems and tenants	1	64

Meaning The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Verifying the LT Interfaces for all Logical systems

Purpose Verify interfaces for logical systems.

Action From operational mode, enter the **show interfaces lt-0/0/0 terse** command.

```
user@host> show interfaces lt-0/0/0 terse
```

Interface	Admin	Link	Proto	Local	Remote
lt-0/0/0	up	up			
lt-0/0/0.1	up	up	inet	192.168.0.1/24	
lt-0/0/0.2	up	up	inet	192.168.0.2/24	
lt-0/0/0.3	up	up	inet	192.168.0.3/24	
lt-0/0/0.11	up	up	vpls		
lt-0/0/0.12	up	up	vpls		
lt-0/0/0.13	up	up	vpls		
lt-0/0/0.22	up	up	inet	192.168.4.1/30	
lt-0/0/0.23	up	up	vpls		
lt-0/0/0.24	up	up	inet	192.168.4.2/30	
lt-0/0/0.25	up	up	vpls		
lt-0/0/0.32767	up	up			

Meaning The output provides the status of LT interfaces. All the LT interfaces are up.

Configuring tenant systems Interconnect with Logical Tunnel Interface point-to-point connection

This example shows how to interconnect tenant systems with logical tunnel (LT) interfaces in a point-to-point connection.

- [Requirements on page 394](#)
- [Overview on page 394](#)
- [Configuration on page 395](#)
- [Verification on page 400](#)

Requirements

This example uses an SRX Series device running Junos OS with logical systems and tenant systems.

Overview

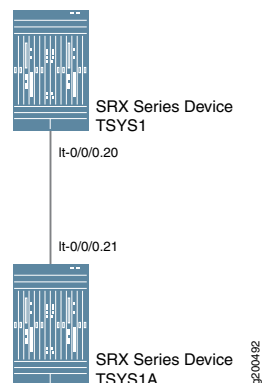
In this example we show how to interconnect tenant systems with logical tunnel (LT) interface in a point-to-point connection.

For the interconnected tenant systems with a point-to-point connection (encapsulation frame-relay) LT interface, this example configures the logical tunnel interface lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems.

The interconnected logical system lt-0/0/0 interface is configured with frame-relay as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the tenant systems are configured with frame-relay as the encapsulation type. A security profile is assigned to the tenant systems.

[Figure 13 on page 394](#) shows the topology for interconnected tenant systems with a point-to-point connection LT interface.

Figure 13: Configuring the interconnect tenant systems with a point-to-point connection LT interface



Configuration

To configure security-zone and assigns interfaces to tenant systems, perform these tasks:

- [Configuring \[item\] on page 396](#)
- [Results on page 398](#)

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 system security-profile sp1 tenant TSYS1
set system security-profile sp2 tenant TSYS1A
set interfaces xe-0/0/5 gigether-options redundant-parent reth0
set interfaces xe-0/0/6 gigether-options redundant-parent reth1
set interfaces xe-1/0/5 gigether-options redundant-parent reth0
set interfaces xe-1/0/6 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 2
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces lt-0/0/0 unit 20 encapsulation ethernet
set interfaces lt-0/0/0 unit 20 peer-unit 21
set interfaces lt-0/0/0 unit 20 family inet address 198.51.1.20/24
set interfaces reth0 unit 0 family inet address 198.51.100.1/24
set interfaces lt-0/0/0 unit 21 encapsulation ethernet
set interfaces lt-0/0/0 unit 21 peer-unit 20
set interfaces lt-0/0/0 unit 21 family inet address 198.51.1.21/24
set interfaces reth1 unit 0 family inet address 192.0.2.1/24
set tenants TSYS1 routing-instances vr11 instance-type virtual-router
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.20
set tenants TSYS1 routing-instances vr11 interface reth0.0
set tenants TSYS1 routing-instances vr11 routing-options static route 192.0.2.0/24 next-hop
  198.51.1.21
set tenants TSYS1 security policies default-policy permit-all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic system-services
  all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic protocols all
set tenants TSYS1 security zones security-zone trust interfaces reth0.0
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic
  system-services all
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic protocols
  all
set tenants TSYS1 security zones security-zone untrust interfaces lt-0/0/0.20
set tenants TSYS1A routing-instances vr12 instance-type virtual-router
set tenants TSYS1A routing-instances vr12 interface lt-0/0/0.21
set tenants TSYS1A routing-instances vr12 interface reth1.0
set tenants TSYS1A routing-instances vr12 routing-options static route 198.51.100.0/24
  next-hop 198.51.1.20
set tenants TSYS1A security policies default-policy permit-all
set tenants TSYS1A security zones security-zone trust host-inbound-traffic
  system-services all
set tenants TSYS1A security zones security-zone trust host-inbound-traffic protocols all
set tenants TSYS1A security zones security-zone trust interfaces reth1.0
```

```
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic
system-services all
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic protocols
all
set tenants TSYS1A security zones security-zone untrust interfaces lt-0/0/0.21
```

Configuring [item]

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*.

1. Define a security profile sp1 and assign to a tenant system TNI. Define another security profile sp1 and assign to a tenant system TSYS1A

```
[edit]
user@host# set system security-profile sp1 tenant TSYS1
user@host# set system security-profile sp2 tenant TSYS1A
```

2. Set the interface for reth0 and reth1 and assign it to the redundancy group 1 and redundancy group 2.

```
[edit]
set interfaces xe-0/0/5 gigether-options redundant-parent reth0
set interfaces xe-0/0/6 gigether-options redundant-parent reth1
set interfaces xe-1/0/5 gigether-options redundant-parent reth0
set interfaces xe-1/0/6 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 2
set interfaces reth1 redundant-ether-options redundancy-group 1
```

3. Set the LT interface as encapsulation ethernet in the tenant system TSYS1.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 encapsulation ethernet
```

4. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 peer-unit 21
```

5. Specify the IP address for the LT interface.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 family inet address 198.51.1.20/24
```

6. Specify the IP address for the reth0.

```
[edit]
user@host# set interfaces reth0 unit 0 family inet address 198.51.100.1/24
```

7. Set the LT interface as encapsulation ethernet in the tenant system TSYS1A.

```
[edit]
```

```
user@host# set interfaces lt-0/0/0 unit 21 encapsulation ethernet
```

8. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 21 peer-unit 20
```

9. Specify the IP address for the LT interface.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 21 family inet address 198.51.1.21/24
```

10. Specify the IP address for the reth1.

```
[edit]
user@host# set interfaces reth1 unit 0 family inet address 192.0.2.1/24
```

11. Define the routing-instances for TSYS1.

```
[edit]
set tenants TSYS1 routing-instances vr11 instance-type virtual-router
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.20
set tenants TSYS1 routing-instances vr11 interface reth0.0
set tenants TSYS1 routing-instances vr11 routing-options static route 192.0.2.0/24
next-hop 198.51.1.21
```

12. Configure a security policy that permits all traffics.

```
[edit]
user@host# set tenants TSYS1 security policies default-policy permit-all
```

13. Configure security zones.

```
[edit]
set tenants TSYS1 security zones security-zone trust host-inbound-traffic
system-services all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic protocols
all
set tenants TSYS1 security zones security-zone trust interfaces reth0.0
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic
system-services all
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic protocols
all
set tenants TSYS1 security zones security-zone untrust interfaces lt-0/0/0.20
```

14. Define the routing-instances for TSYS1A.

```
[edit]
set tenants TSYS1A routing-instances vr12 instance-type virtual-router
set tenants TSYS1A routing-instances vr12 interface lt-0/0/0.21
set tenants TSYS1A routing-instances vr12 interface reth1.0
set tenants TSYS1A routing-instances vr12 routing-options static route
198.51.100.0/24 next-hop 198.51.1.20
```

15. Configure a security policy that permits all traffics.

```
[edit]
set tenants TSYS1A security policies default-policy permit-all
```

16. Configure security zones.

```
[edit]
set tenants TSYS1A security zones security-zone trust host-inbound-traffic
system-services all
set tenants TSYS1A security zones security-zone trust host-inbound-traffic protocols
all
set tenants TSYS1A security zones security-zone trust interfaces reth1.0
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic
system-services all
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic
protocols all
set tenants TSYS1A security zones security-zone untrust interfaces lt-0/0/0.21
```

Results

- From configuration mode, confirm your configuration by entering the **show tenants TSYS1** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS1
routing-instances {
  vr11 {
    instance-type virtual-router;
    interface lt-0/0/0.20;
    interface reth0.0;
    routing-options {
      static {
        route 192.0.2.0/24 next-hop 198.51.1.21;
      }
    }
  }
}
security {
  policies {
    default-policy {
      permit-all;
    }
  }
  zones {
    security-zone trust {
      host-inbound-traffic {
        system-services {
          all;
        }
      }
      protocols {
        all;
      }
    }
  }
}
```

```

    }
    interfaces {
        reth0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        lt-0/0/0.20;
    }
}
}
}

```

- From configuration mode, confirm your configuration by entering the **show tenants TSYS1A** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show tenants TSYS1A
routing-instances {
    vr12 {
        instance-type virtual-router;
        interface lt-0/0/0.21;
        interface reth1.0;
        routing-options {
            static {
                route 198.51.100.0/24 next-hop 198.51.1.20;
            }
        }
    }
}
security {
    policies {
        default-policy {
            permit-all;
        }
    }
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
        }
    }
}

```

```

        reth1.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        lt-0/0/0.21;
    }
}
}
}

```

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 the Security-Profile for all tenant systems on page 400](#)

Verifying the Security-Profile for all tenant systems

Purpose Verify security profile for each logical systems.

Action From operational mode, enter the **show system security-profile zone tenant al** command.

```
user@host> show system security-profile zone tenant al
```

logical-system maximum	tenant name	security profile name	usage	reserved
T1 2048		bronze	1	0
T1A 2048		pX	0	0

Meaning The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Configuring Logical System and Tenant System Interconnect with a Logical Tunnel Interface point-to-point connection

This example shows how to interconnect logical systems and tenant systems with logical tunnel (LT) interface in a point-to-point connection.

Requirements

This example uses an SRX Series device running Junos OS with logical systems and tenant systems.

Overview

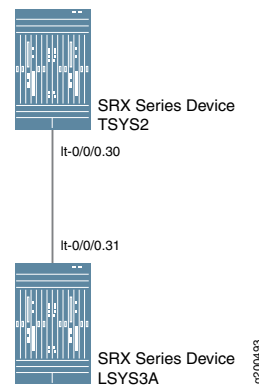
In this example we show how to interconnect logical systems and tenant systems with logical tunnel (LT) interface point-to-point connection.

For the interconnect logical system and tenant system with a point-to-point connection LT interface, the example configures logical tunnel interfaces lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems

To interconnect the logical system and tenant system, lt-0/0/0 interfaces are configured with Ethernet as the encapsulation type. The corresponding peer lt-0/0/0 interfaces are configured with Ethernet as the encapsulation type. A security profile is assigned to the logical system and tenant system

Figure 14 on page 401 shows the topology for interconnected logical systems and tenant systems with LT interface point-to-point connection.

Figure 14: Configuring the interconnect between logical systems and tenant systems with a point-to-point connection LT interface



Configuration

To configure security-zone and assigns interfaces to logical systems, perform these tasks:

- [\[xref target has no title\]](#)
- [Results on page 404](#)

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 system security-profile SP-user tenant TSYS2
set interfaces lt-0/0/0 unit 30 encapsulation ethernet
  
```

```
set interfaces lt-0/0/0 unit 30 peer-unit 31
set interfaces lt-0/0/0 unit 30 family inet address 192.255.2.1/30
set tenants TSYS2 routing-instances vr11 instance-type virtual-router
set tenants TSYS2 routing-instances vr11 interface lt-0/0/0.30
set security zones security-zone LT interfaces lt-0/0/0.30
set system security-profile SP-user logical-system LSYS3A
set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 encapsulation ethernet
set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 peer-unit 20
set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 family inet address 192.255.2.2/30
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match
  source-address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match
  destination-address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match
  application any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT then
  permit
set logical-systems LSYS3A security policies default-policy permit-all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic
  system-services all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic protocols
  all
set logical-systems LSYS3A security zones security-zone LT interfaces lt-0/0/0.31
```

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

1. Define a security profile and assign to a tenant system.
[edit]
user@host# set system security-profile SP-user tenant TSYS2
2. Set the LT interface as encapsulation ethernet in the tenant system.
[edit]
user@host# set interfaces lt-0/0/0 unit 20 encapsulation ethernet
3. Configure a peer relationship for tenant systems TSYS2.
[edit]
user@host# set interfaces lt-0/0/0 unit 20 peer-unit 21
4. Specify the IP address for the LT interface.
[edit]
user@host# set interfaces lt-0/0/0 unit 20 family inet address 192.255.2.1/30
5. Set the security zone for the LT interface.
[edit]
user@host# set logical-systems LSYS2 security zones security-zone LT interfaces lt-0/0/0.30

6. Define a security profile and assign to a logical system.

```
[edit]  
user@host# set system security-profile SP-user logical-system LSYS3A
```
7. Define the routing-instances for TSYS2.

```
[edit]  
set tenants TSYS2 routing-instances vr11 instance-type virtual-router  
set tenants TSYS2 routing-instances vr11 interface lt-0/0/0.30
```
8. Set the LT interface as encapsulation ethernet in the logical system 3A.

```
[edit]  
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 encapsulation  
ethernet
```
9. Configure a peer relationship for logical systems LSYS3A.

```
[edit]  
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 peer-unit 20
```
10. Specify the IP address for the LT interface.

```
[edit]  
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 family inet  
address 192.255.2.2/30
```
11. Configure a security policy that permits traffic from the LT zone to the LT policy LT zone.

```
[edit]  
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT  
policy LT match source-address any  
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT  
policy LT match destination-address any  
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT  
policy LT match application any  
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT  
policy LT then permit
```
12. Configure a security policy that permits traffic from default-policy.

```
[edit]  
user@host# set logical-systems LSYS3A security policies default-policy permit-all
```
13. Configure security zones.

```
[edit]  
user@host# set logical-systems LSYS3A security zones security-zone LT  
host-inbound-traffic system-services all  
user@host# set logical-systems LSYS3A security zones security-zone LT  
host-inbound-traffic protocols all
```

```
user@host# set logical-systems LSYS3A security zones security-zone LT interfaces
lt-0/0/0.31
```

Results

- From configuration mode, confirm your configuration by entering the **show tenants TSYS2** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS2
routing-instances {
  vr11 {
    instance-type virtual-router;
    interface lt-0/0/0.30;
  }
}
```

- From configuration mode, confirm your configuration by entering the **show logical-systems LSYS3A** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS3A
interfaces {
  lt-0/0/0 {
    unit 21 {
      encapsulation ethernet;
      peer-unit 20;
      family inet {
        address 192.255.2.2/30;
      }
    }
  }
}
security {
  policies {
    from-zone LT to-zone LT {
      policy LT {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    default-policy {
      permit-all;
    }
  }
}
zones {
  security-zone LT {
```

```

    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      lt-0/0/0.31;
    }
  }
}

```

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 the LT Interfaces for all Logical and tenant systems on page 405](#)
- [Verifying the Security-Profile for all Logical-systems on page 405](#)

Verifying the LT Interfaces for all Logical and tenant systems

Purpose Verify interfaces for logical systems.

Action From operational mode, enter the **show system security-profile zone all-logical-systems-tenants** command.

```
user@host> show system security-profile zone all-logical-systems-tenants
```

logical-system tenant name	security profile name	usage	reserved
maximum			
root-logical-system	Default-Profile	1	0
2048			
LSYS3A1	gold	1	0
2048			
TSYS23	bronze	1	0
2048			

Meaning The output provides the status of LT interfaces. All the LT interfaces are up.

Verifying the Security-Profile for all Logical-systems

Purpose Verify security profile for each logical systems.

Action From operational mode, enter the **show system security-profile security-log-stream-number logical-system all** command.

```
user@host> show system security-profile security-log-stream-number logical-system all
```

logical system name	security profile name	usage	reserved	maximum
root-logical-system	Default-Profile	2	0	2000
LSYS3A	SP-user	1	10	60

Meaning The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Firewall Authentication for Tenant Systems

The firewall authentication feature is introduced for tenant systems in Junos OS Release 18.3R1 on the Juniper SRX Series devices to enable you to restrict or permit users individually or in groups. The authentication requests are initiated based on destination addresses defined in the policies.

- [Understanding Tenant System Firewall Authentication on page 406](#)
- [Configuring Firewall Authentication for a Tenant System on page 408](#)

Understanding Tenant System Firewall Authentication

A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall.

Firewall authentication is a policy-based authentication method, which requires user to initiate an authentication request through HTTP, FTP or Telnet traffic.

Junos OS enables administrators to restrict and permit firewall users to access protected resources behind a firewall based on their source IP address and other credentials.

The master administrator configures the following:

- maximum and reserved number of firewall authentication sessions in the tenant system.
- access profile using the profile configuration command at the **[edit access]** hierarchy which is available to all the tenant systems.

Access profiles allows to:

- Storing usernames and passwords of users or point to external authentication servers where such information is stored.
- Including the order of authentication methods, LDAP or RADIUS server options, and session options.
- Associating with a security policy in the tenant system.

After defining the firewall users, create a policy that requires the users to authenticate through one of the authentication modes defined in the [Table 37 on page 407](#).

Table 37: Firewall Authentication Options

Authentication Options	Description	Supported Protocols	Supported Backend
Web Authentication	Users use HTTP to connect to an IP address on the device that is enabled for Web authentication and are prompted for the username and password. Subsequent traffic from the user or host to the protected resource is allowed or denied based on the result of this authentication.	HTTP	Local
		HTTPS	LDAP
			RADIUS
			SecurId
Pass-through	Inline authentication with a host or a user from one zone tries to access resources on another zone. The device uses the supported protocols to collect username and password information, and subsequent traffic from the user or host is allowed or denied based on the result of this authentication.	HTTP	Local
		HTTPS	LDAP
		TELNET	RADIUS
		FTP	SecurId
Web Redirect	Automatically redirect client to WebAuth page for authentication (http or https)	HTTP	Local
		HTTPS	LDAP
			RADIUS
			SecurId
Integrated User Firewall	SRX Series devices uses WMI client (WMIC) requests to the AD to get IP address-to-user mapping information in Security event logs.	none	Active Directory
User-Firewall	Same as pass-through but user information is passed to USERID process to go in Auth Table	HTTP	Local
		HTTPS	LDAP
			RADIUS
			SecurId

The tenant system administrator configures the following properties for firewall authentication in the tenant system:

- Security policy that specifies firewall authentication for matching traffic. Firewall authentication is specified with the firewall-authentication configuration statement

at the **[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit]** hierarchy level. In an access profile, users or user groups can be allowed access by the policy can optionally be specified with the client-match configuration statement. If no users or user groups are specified, any user who is successfully authenticated is allowed access.

- The type of authentication (pass-through or Web authentication), default access profile, and success banner for the FTP, Telnet, or HTTP session. These properties are configured with the firewall-authentication configuration statement at the **[edit access]** hierarchy.

Host inbound traffic. Protocols, services, or both are allowed to access the tenant system. The types of traffic are configured with the **host-inbound-traffic** configuration statement at the **[edit security zones security-zone zone-name]** or **[edit security zones security-zone zone-name interfaces interface-name]** hierarchy.

Configuring Firewall Authentication for a Tenant System

This example shows how to send different firewall authentication traffic from the client to server across one tenant system using the three authentication modes pass-through, pass-through with web-redirect, and web authentication.

- [Requirements on page 408](#)
- [Overview on page 408](#)
- [Configuration on page 410](#)
- [Verification on page 418](#)

Requirements

This example uses the following hardware and software components:

- an SRX4100 device
- Junos OS Release 18.3R1 and later
- Telnet or HTTP
- External authentication servers are RADIUS, LDAP, and SecurID

Ensure to have the following configured to send firewall authentication traffic from client to server:

- Configure security zones for a tenant system
- Configure interfaces created by the master administrator

Overview

When a firewall user attempts to initiate a Telnet, HTTP, or HTTPS session to access a resource in another zone, the SRX Series firewall acts a proxy to authenticate the firewall users before allowing the users to access the Telnet, HTTP, or HTTPS servers behind the firewall.

In this example, you can configure a tenant system and bind the security policy to it. When the traffic from is sent from client to server as referred in [Figure 15 on page 410](#), the users are authenticated based on the authentication process defined in the security policy.



NOTE: The master administrator is responsible for creating tenants and assigning the system resources such as routing-instances, interfaces in routing-instances and security-profile to tenant system.

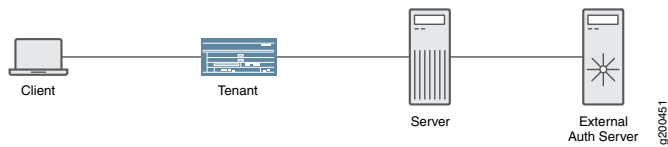
Table 38: Firewall Configuration for the Tenant System

Feature	Name	Description
security-profile	tn1_pf	Name of the security profile. This profile specifies the resources to allocate to a tenant system to which the security profile is bound.
interfaces	xe-0/0/1 xe-0/0/2	Name of the interfaces. The interfaces provide traffic connectivity.
access profile	local_pf radius_pf securid_pf	Name of the access profiles. These profiles are used to define the users and passwords and to obtain authorization information about the user's access right.
SSL termination profile	fwauthhttpspf	Name of the profile. This profile is used for SSL termination services.
routing-instances	vr1	Instance type as virtual routing instance.
security policies	p7	Name of the policy. This policy is used to configure pass-through firewall-authentication using fwauthhttpspf SSL termination profile.
	p1	Name of the policy. This policy is used to configure pass-through firewall-authentication using local_pf access profile.
	p4	Name of the policy. This policy is used to configure pass-through web-redirect firewall-authentication using radius_pf.
	p3	Name of the policy. This policy is used to configure web-authentication firewall-authentication.

Topology

[Figure 15 on page 410](#) shows the topology used in this configuration example. The tenant shown in this topology is an SRX Series device partitioned to multiple tenants. The external servers supported are RADIUS, LDAP, and SecurID. The communication from the client to the tenant happens over xe-0/0/1 interface and from the tenant to the server happens over xe-0/0/2 interface.

Figure 15: Topology for Tenant System



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 system security-profile tn1_pf policy maximum 500
set system security-profile tn1_pf policy reserved 100
set system security-profile tn1_pf zone maximum 50
set system security-profile tn1_pf zone reserved 10
set tenants tn1 security-profile tn1_pf
set services ssl termination profile fwauthhttpspf server-certificate device
set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.0/24
set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.254/16 web-authentication
  http
set interfaces xe-0/0/2 unit 0 family inet address 198.51.100.0/24 web-authentication
  http
set access profile local_pf client test firewall-user password "$ABC123"
set access profile local_pf client test1 client-group local-group1
set access profile local_pf client test1 client-group local-group2
set access profile local_pf client test1 firewall-user password "$BCD678"
set access profile local_pf client test2 client-group local-group2
set access profile local_pf client test2 firewall-user password "$DEF234"
set access profile local_pf client test3 client-group local-group3
set access profile local_pf client test3 firewall-user password "$DBC123"
set access profile local_pf client test4 client-group local-group4
set access profile local_pf client test4 firewall-user password "$FAB123"
set access profile radius_pf authentication-order radius
set access profile radius_pf radius-server 203.0.113.1 secret "$AFD123"
set access profile securid_pf authentication-order securid
set tenants tn1 routing-instances vr1 instance-type virtual-router
set tenants tn1 routing-instances vr1 interface xe-0/0/1.0
set tenants tn1 routing-instances vr1 interface xe-0/0/2.0
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 match
  source-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 match
  destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 match
  application junos-telnet
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 then
  permit firewall-authentication pass-through access-profile local_pf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 match
  source-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 match
  destination-address any

```

```

set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 match
  application any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 then
  permit firewall-authentication pass-through access-profile local_pf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 then
  permit firewall-authentication pass-through ssl-termination-profile fwauthhttpspf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 match
  source-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 match
  destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 match
  application junos-http
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 then
  permit firewall-authentication pass-through access-profile radius_pf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 then
  permit firewall-authentication pass-through web-redirect
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 match
  source-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 match
  destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 match
  application junos-http
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 then
  permit firewall-authentication web-authentication
set tenants tn1 security policies policy-rematch
set tenants tn1 security zones security-zone tn1_trust interfaces xe-0/0/1.0
  host-inbound-traffic system-services all
set tenants tn1 security zones security-zone tn1_trust interfaces xe-0/0/1.0
  host-inbound-traffic protocols all
set tenants tn1 security zones security-zone tn1_untrust interfaces xe-0/0/2.0
  host-inbound-traffic system-services all
set tenants tn1 security zones security-zone tn1_untrust interfaces xe-0/0/2.0
  host-inbound-traffic protocols all
set tenants tn1 access firewall-authentication pass-through default-profile local_pf
set tenants tn1 access firewall-authentication pass-through telnet banner login
  ****tenant1_telnet_login_banner
set tenants tn1 access firewall-authentication pass-through telnet banner success
  ****tenant1_telnet_success_banner
set tenants tn1 access firewall-authentication pass-through telnet banner fail
  ****tenant1_telnet_fail_banner
set tenants tn1 access firewall-authentication web-authentication default-profile
  securid_pf
set tenants tn1 access firewall-authentication web-authentication banner success
  ****tenant1_webauth_success_banner

```

Configuring access profiles and firewall authentication

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*.

1. Configure a security profile tn1_pf and bind it to the tenant system.

```

[edit system security-profile]
user@host# set tn1_pf policy maximum 500

```

```
user@host# set tn1_pf policy reserved 100
user@host# set tn1_pf zone maximum 50
user@host# set tn1_pf zone reserved 10
```

2. Create a tenant system tn1 and bind the security profile tn1_pf to the tenant system.

```
[edit tenants]
user@host# set tn1 security-profile tn1_pf
```

3. Define the access profile used for SSL termination services for HTTPS traffic to trigger pass-through authentication.

```
[edit services]
user@host# set ssl termination profile fwauthhttpspf server-certificate device
```

4. Configure interfaces and assign IP addresses. Enable web authentication at xe-0/0/1 interface.

```
[edit interfaces]
user@host# set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.254/24
web-authentication http
user@host# set interfaces xe-0/0/2 unit 0 family inet address 198.51.100.0/24
web-authentication http
```

5. Configure routing instances and add interfaces to it.

```
[edit tenants tn1 routing-instances]
user@host# set vr1 instance-type virtual-router
user@host# set vr1 interface xe-0/0/1.0
user@host# set vr1 interface xe-0/0/2.0
```

Step-by-Step Procedure

The master administrator is responsible for configuring access profiles in the tenant system. To configure access profiles:

1. Create the access profiles to be used for firewall authentication. Access profiles defines clients as firewall users and the passwords that provide them access for firewall authentication. When unauthenticated traffic is permitted for firewall authentication, the user is authenticated based on the access profile configured in this command.

```
[edit access profile]
user@host# set local_pf client test firewall-user password "$ABC123"
user@host# set local_pf client test1 client-group local-group1
user@host# set local_pf client test1 client-group local-group2
user@host# set local_pf client test1 firewall-user password "$BCD678"
user@host# set local_pf client test2 client-group local-group2
user@host# set local_pf client test2 firewall-user password "$DEF234"
user@host# set local_pf client test3 client-group local-group3
user@host# set local_pf client test3 firewall-user password "$DBC123"
user@host# set local_pf client test4 client-group local-group4
user@host# set local_pf client test4 firewall-user password "$FAB123"
```

2. Create an access profile to configure the RADIUS server.

```
[edit access profile]
user@host# set radius_pf authentication-order radius
user@host# set radius_pf radius-server 203.0.113.1 secret "$AFD123"
```

3. Create an access profile to configure SecurID as the server to be used for external authentication.

```
[edit access profile]
user@host# set securid_pf authentication-order securid
```

Step-by-Step Procedure

Configure different security policies that permit HTTP, HTTPS, and Telnet traffic between zones using pass-through (direct and web-redirect) and web authentication modes in a tenant system.

1. Configure policy p1 for pass-through authentication for Telnet traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 match
source-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 match
destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 match application
junos-telnet
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 then permit
firewall-authentication pass-through access-profile local_pf
```

2. Configure policy p7 for pass-through authentication for HTTPS traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 match
source-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 match
destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 match application
junos-https
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 then permit
firewall-authentication pass-through access-profile local_pf
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 then permit
firewall-authentication pass-through ssl-termination-profile fwauthhttpspf
```

3. Configure policy p4 for pass through authentication using web-redirect for HTTP traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 match
source-address ipv6_addr1
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 match
destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 match application
junos-http
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 then permit
firewall-authentication pass-through access-profile radius_pf
```

```
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 then permit
firewall-authentication pass-through web-redirect
```

4. Configure policy p3 for web authentication for HTTP traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 match
source-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 match
destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 match application
junos-http
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 then permit
firewall-authentication web-authentication
user@host# set policy-rematch
```

5. Configure zones and assign interfaces to each zone in a tenant system.

```
[edit tenants tn1 security zones]
user@host# set security-zone tn1_trust interfaces xe-0/0/1.0 host-inbound-traffic
system-services all
user@host# set security-zone tn1_trust interfaces xe-0/0/1.0 host-inbound-traffic
protocols all
user@host# set security-zone tn1_untrust interfaces xe-0/0/2.0 host-inbound-traffic
system-services all
user@host# set security-zone tn1_untrust interfaces xe-0/0/2.0 host-inbound-traffic
protocols all
```

6. Define a success banner for Telnet sessions. Configure firewall authentication pass-through and web authentication banner for applications in a tenant system.

```
[edit tenants tn1 access firewall-authentication]
user@host# set pass-through default-profile local_pf
user@host# set pass-through telnet banner login *****tenant1_telnet_login_banner
user@host# set pass-through telnet banner success
*****tenant1_telnet_success_banner
user@host# set pass-through telnet banner fail *****tenant1_telnet_fail_banner
user@host# set web-authentication default-profile securid_pf
user@host# set web-authentication banner success
*****tenant1_webauth_success_banner
```

Results

From configuration mode, confirm your configuration by entering the **show system security-profile**, **show interfaces**, **show access**, **show tenants**, and **show services ssl termination** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show interfaces
xe-0/0/1 {
  unit 0 {
    family inet {
      address 192.0.2.0/24;
```

```

        address 192.0.2.254/24 {
            web-authentication {
                http;
                https;
            }
        }
    }
}
xe-0/0/2 {
    unit 0 {
        family inet {
            address 198.51.100.0/24;
        }
    }
}

user@host#show services ssl termination
profile fwauthhttpspf {
    server-certificate device;
}

user@host#show access
profile local_pf {
    client test {
        firewall-user {
            password "$ABC123"; ## SECRET-DATA
        }
    }
    client test1 {
        client-group [ local-group1 local-group2 ];
        firewall-user {
            password "$BCD678"; ## SECRET-DATA
        }
    }
    client test2 {
        client-group local-group2;
        firewall-user {
            password "$DEF234"; ## SECRET-DATA
        }
    }
    client test3 {
        client-group local-group3;
        firewall-user {
            password "$DBC123"; ## SECRET-DATA
        }
    }
    client test4 {
        client-group local-group4;
        firewall-user {
            password "$FAB123"; ## SECRET-DATA
        }
    }
    session-options {
        client-session-timeout 3;
    }
}

```

```
profile radius_pf {
  authentication-order radius;
  session-options {
    client-session-timeout 3;
  }
  radius-server {
    203.0.113.1 secret "$AFD123"; ## SECRET-DATA
  }
}
```

```
user@host# show system security-profile
```

```
tn1_pf {
  policy {
    maximum 500;
    reserved 100;
  }
  zone {
    maximum 50;
    reserved 10;
  }
}
```

```
user@host# show tenants
```

```
tn1 {
  routing-instances {
    vr1 {
      instance-type virtual-router;
      interface xe-0/0/1.0;
      interface xe-0/0/2.0;
    }
  }
  security-profile {
    tn1_pf;
  }
  security {
    policies {
      from-zone tn1_trust to-zone tn1_untrust {
        policy p2 {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit {
              firewall-authentication {
                pass-through {
                  access-profile ldap_pf;
                }
              }
            }
          }
        }
      }
    }
  }
  zones {
    security-zone tn1_trust {
```



```

interfaces {
  xe-0/0/1.0 {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
  }
}
security-zone tn1_untrust {
  interfaces {
    xe-0/0/2.0 {
      host-inbound-traffic {
        system-services {
          all;
        }
        protocols {
          all;
        }
      }
    }
  }
}
access {
  firewall-authentication {
    pass-through {
      default-profile local_pf;
      telnet {
        banner {
          login ****tenant1_telnet_login_banner;
          success ****tenant1_telnet_success_banner;
          fail ****tenant1_telnet_fail_banner;
        }
      }
    }
  }
  web-authentication {
    default-profile radius_pf;
    banner {
      success ****tenant1_webauth_success_banner;
    }
  }
}
}

```

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

Verification

Verifying Firewall User Authentication and Monitoring Users and IP Addresses in the Authentication Table

Purpose The administrator for tenant system can use the **show security firewall-authentication users** or **show security firewall-authentication history** commands to view the information about firewall users and history for the tenant system. The administrator for the tenant system can use the same commands to view information for all tenant systems.

Action From operational mode, enter the following show commands:

```
user@host> show security firewall-authentication history tenant tn1 identifier 10
Username: test
Source IP: 12.12.12.10
Authentication state: Success
Authentication method: Pass-through using HTTP
Access start date: 2018-05-31
Access start time: 17:07:38
Duration of user access: 0:10:01
Lsys: root-logical-system
Tenant: tn1
Source zone: trust-tn1
Destination zone: untrust-tn1
Access profile: test
Bytes sent by this user: 380
Bytes received by this user: 0

user@host> show security firewall-authentication history tenant tn1
History of firewall authentication data:
  Authentications: 2
    Id Source Ip          Date      Time      Duration
Status  User
    1 203.0.112.10        2018-05-27 09:33:05 0:01:44
Success test
    2 203.0.112.10        2018-05-27 10:01:09 0:10:02
Success test

user@host> show security firewall-authentication users tenant tn1
Firewall authentication data:
  Total users in table: 1
    Id Source Ip          Src zone Dst zone Profile  Age
Status  User
    2 203.0.112.10        N/A      N/A      test
1 Success test
```

Meaning The output displays the authenticated firewall users and the firewall authentication history of the users for the tenant system

See Also

- [firewall-authentication on page 479](#)
- [show security firewall-authentication history on page 609](#)

- [show security firewall-authentication users on page 612](#)

Security Policies for Tenant Systems

Security policies can be configured with tenant systems. For more information see the following topics:

- [Understanding Security Policies for Tenant Systems on page 419](#)
- [Example: Configuring Security Policies in the Tenant System on page 420](#)

Understanding Security Policies for Tenant Systems

Security policies enforce rules for what traffic can pass through the firewall and actions that need to take place on the traffic as it passes through the firewall. Through the creation of security policies, the administrator for the tenant system can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from sources to destinations. From the perspective of the security policies, traffic enters one security zone and exits through another security zone. By default, the tenant system denies all traffic in all directions, including intra-zone and inter-zone directions.

Starting in Junos OS Release 18.3R1, the security policies feature supported on logical systems is now extended on tenant systems.

Security policies can be configured in the tenant systems. Tenant security policies are configured the same way as logical system security policies and firewall-wide security policies. Any security policies, policy rules, address books, applications and application sets, and schedulers created within a tenant system are only applicable to that tenant system. Only predefined applications and application sets, such as **junos-ftp**, are shared between the tenant systems.

The administrator for the tenant system can configure and view all attributes for security policies in a tenant system.

Application Timeouts

The application timeout value set for an application determines the session timeout. Application timeout behavior is the same for a tenant system as it is at the root level. However, the administrators of the tenant system can use predefined applications in security policies but cannot modify the timeout value of predefined applications. Application timeout values are stored in the application entry database and in the corresponding tenant system TCP and UDP port-based timeout tables.

Security Policy Allocation

The master administrator creates a security profile to allocate the maximum number of policies that can be configured for each tenant system. The administrator of the tenant system is then restricted by the security profile to create no more than the number of policies described in the security profile. The administrator of the tenant system use the **show system security-profile policy** command to view the number of security policies allocated to the tenant system.

```
user@host> show system security-profile policy
```

logical-system maximum	tenant name	security profile name	usage	reserved
root-logical-system 16000		Default-Profile	1	0

Example: Configuring Security Policies in the Tenant System

This example shows how to configure the security policies for the tenant system.

- [Requirements on page 420](#)
- [Overview on page 420](#)
- [Configuration on page 421](#)
- [Verification on page 422](#)

Requirements

Before you begin the configuration:

- Configure zones. See *Example: Configuring Security Zones in the Tenant System*.
- Use the **show system security-profiles policy** command to see the security policy resources allocated to the tenant system.

Overview

In this example, you can configure a security policy for the tenant system. The administrator for the tenant system user can use **[edit tenants tenant-name security policies]** hierarchy level to configure the security policies. This example configures the security policies described in [Table 39 on page 420](#).

Table 39: Security Policies Parameters

Feature	Configuration Parameters
Policy 1	Permit the following traffic: <ul style="list-style-type: none"> • Policy name: p1 • Tenant name: TN1 • From zone: trust • To zone: untrust • Source address: any • Destination address: any • Application: any

Table 39: Security Policies Parameters (continued)

Feature	Configuration Parameters
Policy 2	Permit the following traffic: <ul style="list-style-type: none"> • Policy name: p1 • Tenant name: TN1 • From zone: untrust • To zone: trust • Source address: any • Destination address: any • Application: any

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 tenants TN1 security policies from-zone trust to-zone untrust policy p1 match
source-address any
set tenants TN1 security policies from-zone trust to-zone untrust policy p1 match
destination-address any
set tenants TN1 security policies from-zone trust to-zone untrust policy p1 match
application any
set tenants TN1 security policies from-zone trust to-zone untrust policy p1 then permit
set tenants TN1 security policies from-zone untrust to-zone trust policy p2 match
source-address any
set tenants TN1 security policies from-zone untrust to-zone trust policy p2 match
destination-address any
set tenants TN1 security policies from-zone untrust to-zone trust policy p2 match
application any
set tenants TN1 security policies from-zone untrust to-zone trust policy p2 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 the Junos OS CLI User Guide.

To configure the security policies in the tenant system:

1. Log in to the tenant system and define the tenant system name as TN1.

```

[edit]
user@host# set tenants TN1

```
2. Create a security policy as p1 that permits traffic from zone trust to zone untrust and configure the match condition.

```

[edit tenants TN1 security policies from-zone trust to-zone untrust]
user@host# set policy p1 match source-address any
user@host# set policy p1 match destination-address any

```

```
user@host# set policy p1 match application any
user@host# set policy p1 then permit
```

3. Create a security policy as p2 that permits traffic from zone untrust to zone trust and configure the match condition.

```
[edit tenants TN1 security policies from-zone untrust to-zone trust]
user@host# set policy p2 match source-address any
user@host# set policy p2 match destination-address any
user@host# set policy p2 match application any
user@host# set policy p2 then permit
```

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

```
user@host# show tenants TN1 security policies
from-zone trust to-zone untrust {
  policy p1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone untrust to-zone trust {
  policy p2 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
```

Verification

Verifying Policy Configuration

Purpose Verify the information about security policies.

Action To verify the configuration is working properly, enter the **show security policies detail tenant TN1** command from operational mode.

```
user@host> show security policies detail tenant TN1
```

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses: any
Destination addresses: any
Application: any
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input bytes      :                0                0 bps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Output bytes     :                0                0 bps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Input packets    :                0                0 pps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Output packets   :                0                0 pps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Session rate     :                0                0 sps
Active sessions  :                0
Session deletions:                0
Policy lookups   :                0
```

Meaning The output displays the information about the security policies configured on the tenant system.

Release History Table

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the security policies feature supported on logical systems is now extended on tenant systems.

Related Documentation

- [Tenant Systems Overview on page 353](#)

Screen Options for Tenant Systems

Screen options for Tenant Systems on SRX Series devices prevent attacks as , such as IP address sweeps, port scans, denial of service (DOS) attacks, ICMP, UDP, and SYN floods as same as Logical Systems. For more information, see the following topics:

- [Understanding Tenant System Screen Options on page 424](#)
- [Example: Configuring Screen Options for a Tenant System on page 424](#)

Understanding Tenant System Screen Options

Using screen options, the device secures a zone by inspecting, and then allowing or denying all connection attempts that require crossing an interface bound to that zone. Junos OS applies the firewall policies, which can contain the content filtering and the IDP components to the traffic that passes the screen filters. All screen options that are available on the device are also available in each tenant system.

Starting in Junos OS Release 18.3R1, the screen options that are supported for logical systems are extended to tenant systems.

See Also

- [Understanding Screens Options on SRX Series Devices](#)

Example: Configuring Screen Options for a Tenant System

This example shows how to configure screen options for a tenant system.

- [Requirements on page 424](#)
- [Overview on page 425](#)
- [Configuration on page 425](#)
- [Verification on page 428](#)

Requirements

Before you begin:

- Understand the tenant system configuration process. See “[Tenant System Configuration Overview](#)” on [page 358](#) to understand how this task fits into the overall configuration process.
- Configure the zones for the tenant system. See “[Security Zones for Tenant Systems](#)” on [page 377](#) to understand how to configure the zones for the tenant systems.

Overview

Using screen options, the security device can protect against the different internal and external attacks for security zones. You can limit the number of concurrent sessions to the same destination IP address in a tenant system. Setting a destination based session limit can ensure that Junos OS allows only an acceptable number of concurrent connection requests—no matter what the source—to reach any one host. When the number of concurrent connection requests to an IP address surpasses the limit, Junos OS blocks further connection attempts to that IP address.

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 tenants TN1 security screen ids-option jscreen limit-session destination-ip-based 80
set tenants TN1 security screen ids-option jscreen icmp ip-sweep threshold 1000
set tenants TN1 security screen ids-option jscreen icmp fragment
set tenants TN1 security screen ids-option jscreen icmp large
set tenants TN1 security screen ids-option jscreen icmp flood threshold 200
set tenants TN1 security screen ids-option jscreen icmp ping-death
set tenants TN1 security screen ids-option jscreen ip bad-option
set tenants TN1 security screen ids-option jscreen ip stream-option
set tenants TN1 security screen ids-option jscreen ip spoofing
set tenants TN1 security screen ids-option jscreen ip strict-source-route-option
set tenants TN1 security screen ids-option jscreen ip unknown-protocol
set tenants TN1 security screen ids-option jscreen ip tear-drop
set tenants TN1 security screen ids-option jscreen tcp syn-fin
set tenants TN1 security screen ids-option jscreen tcp tcp-no-flag
set tenants TN1 security screen ids-option jscreen tcp syn-frag
set tenants TN1 security screen ids-option jscreen tcp port-scan threshold 1000
set tenants TN1 security screen ids-option jscreen tcp syn-ack-ack-proxy threshold 500
set tenants TN1 security screen ids-option jscreen tcp syn-flood alarm-threshold 500
set tenants TN1 security screen ids-option jscreen tcp syn-flood attack-threshold 500
set tenants TN1 security screen ids-option jscreen tcp syn-flood source-threshold 50
set tenants TN1 security screen ids-option jscreen tcp syn-flood destination-threshold
  1000
set tenants TN1 security screen ids-option jscreen tcp syn-flood timeout 10
set tenants TN1 security screen ids-option jscreen tcp land
set tenants TN1 security screen ids-option jscreen tcp winnuke
set tenants TN1 security screen ids-option jscreen tcp tcp-sweep threshold 1000
set tenants TN1 security screen ids-option jscreen udp flood threshold 500
set tenants TN1 security screen ids-option jscreen udp udp-sweep threshold 1000
set tenants TN1 security zones security-zone untrust screen jscreen
```

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

To configure destination-based session limits in a tenant system:

1. Log in to the tenant system as the administrator and enter configuration mode.

```
user@host:TN1#> configure
user@host:TN1#
```

2. Define the tenant system name as TN1 and configure a screen option for a destination-based session limit.

```
[edit tenants TN1]
user@host:TN1# set security screen ids-option jscreen limit-session
destination-ip-based 80
```

3. Configure the ICMP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set icmp ip-sweep threshold 1000
user@host:TN1# set icmp fragment
user@host:TN1# set icmp large
user@host:TN1# set icmp flood threshold 200
user@host:TN1# set icmp ping-death
```

4. Configure the IP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set ip bad-option
user@host:TN1# set ip stream-option
user@host:TN1# set ip spoofing
user@host:TN1# set ip strict-source-route-option
user@host:TN1# set ip unknown-protocol
user@host:TN1# set ip tear-drop
```

5. Configure the TCP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set tcp syn-fin
user@host:TN1# set tcp tcp-no-flag
user@host:TN1# set tcp syn-frag
user@host:TN1# set tcp port-scan threshold 1000
user@host:TN1# set tcp syn-ack-ack-proxy threshold 500
user@host:TN1# set tcp syn-flood alarm-threshold 500
user@host:TN1# set tcp syn-flood attack-threshold 500
user@host:TN1# set tcp syn-flood source-threshold 50
user@host:TN1# set tcp syn-flood destination-threshold 1000
user@host:TN1# set tcp syn-flood timeout 10
user@host:TN1# set tcp land
user@host:TN1# set tcp winnuke
user@host:TN1# set tcp tcp-sweep threshold 1000
```

6. Configure the UDP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set udp flood threshold 500
user@host:TN1# set udp udp-sweep threshold 1000
```

7. Attach the IDS profile to the zone.

```
[edit tenants TN1]
user@host:TN1# set security zones security-zone untrust screen jscreen
```

Results From configuration mode, confirm your configuration by entering the **show tenants TN1 security screen** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TN1 security screen
ids-option jscreen {
  limit-session {
    destination-ip-based 80;
  }
}
ids-option jscreen {
  icmp {
    ip-sweep threshold 1000;
    fragment;
    large;
    flood threshold 200;
    ping-death;
  }
  ip {
    bad-option;
    stream-option;
    spoofing;
    strict-source-route-option;
    unknown-protocol;
    tear-drop;
  }
  tcp {
    syn-fin;
    tcp-no-flag;
    syn-frag;
    port-scan threshold 1000;
    syn-ack-ack-proxy threshold 500;
    syn-flood {
      alarm-threshold 500;
      destination-threshold 1000;
      timeout 10;
    }
    land;
    winnuke;
    tcp-sweep threshold 1000;
  }
  udp {
    flood {
```

```
        threshold 500;
    }
    udp-sweep threshold 1000;
}
}
```

Verification

To confirm that the configuration is working properly, perform the below task:

- [Verifying security screen status on page 428](#)

Verifying security screen status

Purpose Verify that the IDS profile for multiple screening options is configured properly:

Action To verify the configuration is working properly, enter the **show security screen ids-option jscreen tenant TN1** and **show security zone tenant TN1** command from operational mode.

```
user@host> show security screen ids-option jscreen tenant TN1
```

Screen object status:

Name	Value
ICMP flood threshold	200
UDP flood threshold	500
TCP winnuke	enabled
TCP port scan threshold	1000
ICMP address sweep threshold	1000
TCP sweep threshold	1000
UDP sweep threshold	1000
IP tear drop	enabled
TCP SYN flood attack threshold	500
TCP SYN flood alarm threshold	500
TCP SYN flood source threshold	50
TCP SYN flood destination threshold	1000
TCP SYN flood timeout	10
IP spoofing	enabled
ICMP ping of death	enabled
TCP land attack	enabled
TCP SYN fragment	enabled
TCP no flag	enabled
IP unknown protocol	enabled
IP bad options	enabled
IP strict source route option	enabled
IP stream option	enabled
ICMP fragmentation	enabled
ICMP large packet	enabled
TCP SYN FIN	enabled
TCP SYN-ACK-ACK proxy threshold	500

```
user@host> show security zone tenant TN1
```

```
Security zone: untrust
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Screen: jscreen
```

```
Interfaces bound: 0
Interfaces:
```

Meaning The output displays the screen status in the tenant system.

See Also • [Understanding Tenant System Screen Options on page 424](#)

Release History Table

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the screen options that are supported for logical systems are extended to tenant systems.

Related Documentation • [Example: Configuring Tenant Systems on page 360](#)

NAT for Tenant Systems

NAT is a method for modifying or translating network address information in packet headers. Either or both source and destination addresses in a packet may be translated. For more information, see the following topics:

- [Understanding Network Address Translation for Tenant systems on page 429](#)
- [Example: Configuring Network Address Translation for the Tenant Systems on page 430](#)

Understanding Network Address Translation for Tenant systems

Starting in Junos OS Release 18.3R1, the network address translation including source NAT, destination NAT, and static NAT supported on logical systems is supported on tenant systems.

A tenant system has an administrator (tenant administrator) who can configure source NAT, destination NAT, and static NAT for the tenant systems. The tenant administrator can view the details of the source NAT, destination NAT, and static NAT of the tenant system. The master administrator can view the statistics or information of the source NAT, destination NAT, and static NAT for any tenant systems.

For the tenant system, the master administrator can configure the maximum and reserved numbers for the following NAT resources:

- Source NAT pools and destination NAT pools
- IP addresses in the source NAT pools with and without port address translation
- Rules for source, destination, and static NAT
- Prefix list for rule matching

- NAT cone binding
- IP addresses that support port overloading

The reserved numbers allocated guarantees that the specified resource amount is constantly available to the tenant systems. The administrator for tenant systems can use the **show system security-profile** command with a NAT option to view the NAT resources allocated to the tenant system.

- See Also**
- [Understanding Network Address Translation for Tenant systems on page 429](#)
 - [Introduction to NAT](#)

Example: Configuring Network Address Translation for the Tenant Systems

This example shows how to configure source NAT, destination NAT and static NAT for a given tenant systems.

- [Requirements on page 430](#)
- [Overview on page 430](#)
- [Configuration on page 431](#)
- [Verification on page 434](#)

Requirements

This example uses the following hardware and software components:

- SRX Series device with Junos OS Release 18.3R1 or later. This configuration example is tested for Junos OS Release 18.3R1.
- Create tenant system. See : [“Example: Configuring Tenant Systems” on page 360](#).
- Configure network interfaces. See : [“Configuring a Routing Instance for a Tenant System” on page 359](#).

Overview

In this example, first you configure the trust security zone for the private address space and then you configure the untrust security zone for the public address space.

Devices in the untrust zone access a specific host in the trust zone, with the destination IP address 203.0.113.200/24. This example configures the NAT described in Table 1: Tenant System NAT Configuration.

Table 40: Tenant System NAT Configuration

Feature	Name	Configuration Parameters
Static, source and destination NAT rule set	r1	<ul style="list-style-type: none"> • Rule r1 to match packets from untrust zone with destination address. • Destination IP address in matching packets is translated.
Source pool	pat	Address 192.0.2.1 to 192.0.2.24.

Table 40: Tenant System NAT Configuration (continued)

Feature	Name	Configuration Parameters
Destination pool	h1	Address 192.168.1.200.
Proxy ARP	arp	Address 192.0.2.1 to 192.0.2.24.
NAT interfaces for traffic direction.		ge-0/0/0 and ge-0/0/1.

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 tenants tn1 security nat source pool pat address 192.0.2.1 to 192.0.2.24
set tenants tn1 security nat source rule-set from_intf from interface ge-0/0/0.0
set tenants tn1 security nat source rule-set from_intf to interface ge-0/0/1.0
set tenants tn1 security nat source rule-set from_intf rule r1 match source-address
  192.0.2.0/24
set tenants tn1 security nat source rule-set from_intf rule r1 match destination-address
  203.0.113.200/24
set tenants tn1 security nat source rule-set from_intf rule r1 then source-nat pool pat
set tenants tn1 security nat static rule-set from_zone from zone trust
set tenants tn1 security nat static rule-set from_zone rule r1 match source-address
  192.0.2.0/24
set tenants tn1 security nat static rule-set from_zone rule r1 match destination-address
  203.0.113.203/24
set tenants tn1 security nat static rule-set from_zone rule r1 then static-nat prefix
  192.168.1.203/24
set tenants tn1 security nat destination pool h1 address 192.168.1.200
set tenants tn1 security nat destination rule-set from_zone from zone trust
set tenants tn1 security nat destination rule-set from_zone rule r1 match source-address
  192.0.2.0/24
set tenants tn1 security nat destination rule-set from_zone rule r1 match
  destination-address 203.0.113.202/24
set tenants tn1 security nat destination rule-set from_zone rule r1 then destination-nat
  pool h1
set tenants tn1 security nat proxy-arp interface ge-0/0/1.0 address 192.0.2.1 to 192.0.2.24
```

Step-by-Step Procedure

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

To configure NAT in the tenant system:

1. Create a security NAT source pool and rule set for the tenant system.

```
[edit tenant tn1 security nat source]
user@host# set tenants tn1 security nat source pool pat address 192.0.2.1 to
192.0.2.24
```

```

user@host# set tenants tn1 security nat source rule-set from_intf from interface
ge-0/0/0.0
user@host# set tenants tn1 security nat source rule-set from_intf to interface
ge-0/0/1.0
user@host# set tenants tn1 security nat source rule-set from_intf rule r1 match
source-address 192.0.2.0/24
user@host# set tenants tn1 security nat source rule-set from_intf rule r1 match
destination-address 203.0.113.200/24
user@host# set tenants tn1 security nat source rule-set from_intf rule r1 then
source-nat pool pat

```

2. Create a security NAT static rule set for the tenant system.

```

[edit tenants tn1 security nat static]
user@host# set tenants tn1 security nat static rule-set from_zone from zone trust
user@host# set tenants tn1 security nat static rule-set from_zone rule r1 match
source-address 192.0.2.0/24
user@host# set tenants tn1 security nat static rule-set from_zone rule r1 match
destination-address 203.0.113.203/24
user@host# set tenants tn1 security nat static rule-set from_zone rule r1 then
static-nat prefix 192.168.1.203/24

```

3. Create a security NAT destination pool and rule set for the tenant system.

```

[edit tenants tn1 security nat destination]
user@host# set tenants tn1 security nat destination pool h1 address 192.168.1.200
user@host# set tenants tn1 security nat destination rule-set from_zone from zone
trust
user@host# set tenants tn1 security nat destination rule-set from_zone rule r1 match
source-address 192.0.2.0/24
user@host# set tenants tn1 security nat destination rule-set from_zone rule r1 match
destination-address 203.0.113.202/24
user@host# set tenants tn1 security nat destination rule-set from_zone rule r1 then
destination-nat pool h1

```

4. Configure proxy Address Resolution Protocol (ARP).

```

[edit tenant tn1 security nat]
user@host# set tenants tn1 security nat proxy-arp interface ge-0/0/1.0 address
192.0.2.1 to 192.0.2.24

```

Results From configuration mode, confirm your configuration by entering the **show tenants tn1 security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

source {
  pool pat {
    address {
      192.0.2.1 to 192.0.2.24;
    }
  }
  rule-set from_intf {
    from interface ge-0/0/0.0;
  }
}

```



```

to interface ge-0/0/1.0;
rule r1 {
  match {
    source-address 192.168.1.0/24;
    destination-address [203.0.113.200/24 ];
  }
  then {
    source-nat {
      pool {
        pat;
      }
    }
  }
}
}
}
destination {
  pool h1 {
    address 192.168.1.200;
  }
  rule-set from_zone {
    from zone untrust;
    rule r1 {
      match {
        source-address 192.0.2.0/24;
        destination-address 203.0.113.202/24;
      }
      then {
        destination-nat {
          pool {
            h1;
          }
        }
      }
    }
  }
}
}
static {
  rule-set from_zone {
    from zone untrust;
    rule r1 {
      match {
        source-address 192.0.2.0/24;
        destination-address 203.0.113.203/24;
      }
      then {
        static-nat {
          prefix {
            192.168.1.203/24;
          }
        }
      }
    }
  }
}
}
proxy-arp {

```

```
interface ge-0/0/1.0 {  
  address {  
    192.0.2.1 to 192.0.2.24;  
  }  
}
```

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 Static NAT Configuration on page 434](#)
- [Verifying Destination NAT Configuration on page 434](#)
- [Verifying Source NAT Configuration on page 435](#)

Verifying Static NAT Configuration

Purpose To verify that there is traffic matching the static NAT rule set.

Action From operational mode, enter the **show security nat static rule all tenant tn1** command.
View the **Translation hits** field to check for traffic that matches the rule.

```
user@host> show security nat static rule all tenant tn1
```

Sample Output

```
Total static-nat rules: 1  
Total referenced IPv4/IPv6 ip-prefixes: 2/0  
Static NAT rule: r1                               Rule-set: from_zone  
Rule-Id                                           : 1  
Rule position                                     : 1  
From zone                                         : untrust  
Source addresses                                 : 192.0.2.0      - 192.0.2.255  
Destination addresses                             : 203.0.113.203  
Host addresses                                   : 192.168.1.203  
Netmask                                           : 32  
Host routing-instance                             : N/A  
Translation hits                                  : 0  
  Successful sessions                             : 0  
  Failed sessions                                : 0  
Number of sessions                               : 0
```

Meaning The command output displays the static NAT rule. View the **Translation hits** field to check for traffic that matches the static rule.

Verifying Destination NAT Configuration

Purpose To verify that there is traffic matching the destination NAT rule set.

Action From operational mode, enter the **show security nat destination rule all tenant tn1** command. View the **Translation hits** field to check for traffic that matches the rule.

```
user@host> show security nat destination rule all tenant tn1
```

Sample Output

```
Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Destination NAT rule: r1          Rule-set: from_zone
Rule-Id                          : 1
Rule position                    : 1
From zone                       : untrust
Match
  Source addresses               : 192.0.2.0      - 192.0.2.255
  Destination addresses          : 203.0.113.202  - 203.0.113.202
Action                          : h1
Translation hits                 : 0
  Successful sessions           : 0
  Failed sessions               : 0
Number of sessions               : 0
```

Meaning The command output displays the destination NAT rule. View the **Translation hits** field to check for traffic that matches the destination rule.

Verifying Source NAT Configuration

Purpose To verify that there is traffic matching the source NAT rule set.

Action From operational mode, enter the **show security nat source rule all tenant tn1** command. View the **Translation hits** field to check for traffic that matches the rule.

```
user@host> show security nat source rule all tenant tn1
```

Sample Output

```
Total rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
source NAT rule: r1          Rule-set: from_intf
Rule-Id                      : 1
Rule position                 : 1
From interface                : ge-0/0/0.0
To interface                  : ge-0/0/1.0
Match
  Source addresses            : 192.168.1.0      - 192.168.1.255
  Destination addresses       : 203.0.113.200  - 203.0.113.200
Action                       : pat
Persistent NAT type           : N/A
Persistent NAT mapping type   : address-port-mapping
Inactivity timeout            : 0
Max session number            : 0
Translation hits              : 0
  Successful sessions         : 0
  Failed sessions             : 0
Number of sessions            : 0
```

Meaning The command output displays the source NAT rule. View the **Translation hits** field to check for traffic that matches the source rule.

Related Documentation • [Tenant System Configuration Overview on page 358](#)

ALG for Tenant Systems

An Application Layer Gateway (ALG) in tenant systems enables the gateway to parse application layer payloads and take decisions whether to allow or deny traffic to the application server. ALGs supports the applications such as Transfer Protocol (FTP) and various IP protocols that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections. For more information, see the following topics:

- [Understanding ALG Support for Tenant System on page 436](#)
- [Enabling and Disabling ALG for Tenant System on page 437](#)
- [Example: Configuring ALG in Tenant System on page 440](#)

Understanding ALG Support for Tenant System

An Application Layer Gateway (ALG) enables the gateway to parse application layer payloads and take decisions whether to allow or deny traffic to the application server.

Starting in Junos OS Release 18.3R1, the ALG feature supported on logical systems is now extended on tenants systems.

The tenant systems administrator can configure the ALG features for the tenant systems. The master administrator can configure the ALG features and display the ALG information for all tenants. The tenant systems administrator can only apply configurations and display information in its own tenant.

Each tenant system displays the ALG counters to monitor the traffic. For example, use commands **show security alg sip counters tenants TN1** to get SIP counters in tenant systems and **show security alg sip counters tenants all** to get SIP counters in all existing tenant systems.

Enabling the security log for the tenant generates the ALG logs per tenant.



NOTE: When you upgrade to Junos OS Release 18.3R1, the ALG status for each tenant system might be different depending on the default configuration or configuration in a release prior to Junos OS Release 18.3R1. We recommend you to change the ALG configurations for tenant systems as per your requirements after an upgrade to latest Junos OS version.

Enabling and Disabling ALG for Tenant System

This topic shows how to enable or disable the ALG status for each tenant system.

1. By Default IKE ALG is disabled on the tenant system. To enable this ALG, use the following command.

- Enable IKE and ESP ALG with NAT.

```
[edit]
user@host# set tenants TN1 security alg ike-esp-nat enable
```

2. By default, the DNS, FTP, PPTP, SIP, SUNRPC and TWAMP ALGs are enabled on the tenant system. To disable these ALGs, use the following commands.

- Disable DNS ALG.

```
[edit]
user@host# set tenants TN1 security alg dns disable
```

- Disable FTP ALG.

```
[edit]
user@host# set tenants TN1 security alg ftp disable
```

- Disable H323 ALG.

```
[edit]
user@host# set tenants TN1 security alg h323 disable
```

- Disable MGCP ALG.

```
[edit]
user@host# set tenants TN1 security alg mgcp disable
```

- Disable MSRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg msrpc disable
```

- Disable PPTP ALG.

```
[edit]
user@host# set tenants TN1 security alg pptp disable
```

- Disable RSH ALG.

```
[edit]
user@host# set tenants TN1 security alg rsh disable
```

- Disable RTSP ALG.

```
[edit]
user@host# set tenants TN1 security alg rtsp disable
```

- Disable SCCP ALG.

```
[edit]
user@host# set tenants TN1 security alg sccp disable
```

- Disable SIP ALG.

```
[edit]
```

```
user@host# set tenants TN1 security alg sip disable
```

- Disable SQL ALG.

```
[edit]
user@host# set tenants TN1 security alg sql disable
```

- Disable SUNRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg sunrpc disable
```

- Disable TALK ALG.

```
[edit]
user@host# set tenants TN1 security alg talk disable
```

- Disable TFTP ALG.

```
[edit]
user@host# set tenants TN1 security alg tftp disable
```

3. Configuring ALG functions in tenant systems.

- Configure DNS ALG.

```
[edit]
user@host# set tenants TN1 security alg dns
```

- Configure FTP ALG.

```
[edit]
user@host# set tenants TN1 security alg ftp
```

- Configure H323 ALG.

```
[edit]
user@host# set tenants TN1 security alg h323
```

- Configure IKE and ESP ALG with NAT.

```
[edit]
user@host# set tenants TN1 security alg ike-esp-nat
```

- Configure MGCP ALG.

```
[edit]
user@host# set tenants TN1 security alg mgcp
```

- Configure MSRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg msrpc
```

- Configure PPTP ALG.

```
[edit]
user@host# set tenants TN1 security alg pptp
```

- Configure RSH ALG.

```
[edit]
user@host# set tenants TN1 security alg rsh
```

- Configure RTSP ALG.

```
[edit]
user@host# set tenants TN1 security alg rtsp
```

- Configure SCCP ALG.

```
[edit]
user@host# set tenants TN1 security alg sccp
```

- Configure SIP ALG.

```
[edit]
user@host# set tenants TN1 security alg sip
```

- Configure SQL ALG.

```
[edit]
user@host# set tenants TN1 security alg sql
```

- Configure SUNRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg sunrpc
```

- Configure TALK ALG.

```
[edit]
user@host# set tenants TN1 security alg talk
```

- Configure TFTP ALG.

```
[edit]
user@host# set tenants TN1 security alg tftp
```

- Configure TWAMP ALG.

```
[edit]
user@host# set tenants TN1 security alg twamp
```

- Configure extended function for FTP ALG.

```
[edit]
user@host# set tenants TN1 security alg ftp allow-mismatch-ip-address
```

- Configure extended function for MSRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg msrpc map-entry-timeout 10
```

- Configure extended function for SUNRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg sunrpc map-entry-timeout 10
```

- Configure extended function for SIP ALG.

```
[edit]
user@host# set tenants TN1 security alg sip retain-hold-resource
```

Example: Configuring ALG in Tenant System

This example shows how to configure ALGs in tenant system and send traffic based on FTP ALG configuration of the tenant system individually.

- [Requirements on page 440](#)
- [Overview on page 440](#)
- [Configuration on page 440](#)
- [Verification on page 443](#)

Requirements

This example uses the following hardware and software components:

- An SRX device
- Junos OS Release 18.3R1

Before you begin:

- Read the ALG Support for Tenant System to understand how and where this procedure fits in the overall tenant support for ALGs.

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

Overview

In this example, the ALG for FTP is configured to monitor and allow FTP traffic to be exchanged between the clients and the server on a tenant system.

By default, the FTP ALG is enabled on the tenant system.

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 system security-profile p1 policy maximum 100
set system security-profile p1 policy reserved 50
set system security-profile p1 zone maximum 100
set system security-profile p1 zone reserved 50
set system security-profile p1 flow-session maximum 6291456
set system security-profile p1 flow-session reserved 50
set system security-profile p1 flow-gate maximum 524288
set system security-profile p1 flow-gate reserved 50
set tenants TN1 routing-instances VR_TN1 instance-type vpls
set tenants TN1 routing-instances VR_TN1 interface lt-0/0/0.0
set system security-profile p1 tenant TN1
set tenants TN1 security zones security-zone TN1_Czone host-inbound-traffic
system-services all
```



```

set tenants TN1 security zones security-zone TN1_Czone host-inbound-traffic protocols
all
set tenants TN1 security zones security-zone TN1_Czone interfaces ge-0/0/0
set tenants TN1 security zones security-zone TN1_Szone host-inbound-traffic
system-services all
set tenants TN1 security zones security-zone TN1_Szone host-inbound-traffic protocols
all
set tenants TN1 security zones security-zone TN1_Szone interfaces ge-0/0/1
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match source-address any
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match destination-address any
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match application junos-ftp
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match application junos-ping
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11 then
permit
set tenants TN1 security policies default-policy deny-all

```

Configuring FTP ALG in a Tenant System

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

To configure an ALG on a tenant system:

1. Configure a security profile p1 for tenant.


```

[edit]
set system security-profile p1 policy maximum 100
set system security-profile p1 policy reserved 50
set system security-profile p1 zone maximum 100
set system security-profile p1 zone reserved 50
set system security-profile p1 flow-session maximum 6291456
set system security-profile p1 flow-session reserved 50
set system security-profile p1 flow-gate maximum 524288
set system security-profile p1 flow-gate reserved 50

```
2. Configure interfaces and routing instances to the TN1.


```

[edit]
user@host# set tenants TN1 routing-instances VR_TN1 instance-type vpls
user@host# set tenants TN1 routing-instances VR_TN1 interface lt-0/0/0.0

```
3. Configure a security profile p1 and assign it to the tenant system TN1.


```

[edit]
user@host# set system security-profile p1 tenant TN1

```
4. Configure security zones and assign interfaces to each zone.


```

[edit]

```

```
user@host# set tenants TN1 security zones security-zone TN1_Czone
host-inbound-traffic system-services all
user@host# set tenants TN1 security zones security-zone TN1_Czone
host-inbound-traffic protocols all
user@host# set tenants TN1 security zones security-zone TN1_Czone interfaces
ge-0/0/0
user@host# set tenants TN1 security zones security-zone TN1_Szone
host-inbound-traffic system-services all
user@host# set tenants TN1 security zones security-zone TN1_Szone
host-inbound-traffic protocols all
user@host# set tenants TN1 security zones security-zone TN1_Szone interfaces
ge-0/0/1
```

5. Configure a security policy that permits FTP traffic from the TN1_Czone to-zone TN1_Szone.

```
[edit]
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone
TN1_Szone policy p11 match source-address any
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone
TN1_Szone policy p11 match destination-address any
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone
TN1_Szone policy p11 match application junos-ftp
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone
TN1_Szone policy p11 match application junos-ping
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone
TN1_Szone policy p11 then permit
user@host# set tenants TN1 security policies default-policy deny-all
```

Results

From configuration mode, confirm your configuration by entering the **show tenants TN1** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TN1
routing-instances {
  VR_TN1 {
    instance-type vpls;
    interface lt-0/0/0.0;
  }
}
security {
  policies {
    from-zone TN1_Czone to-zone TN1_Szone {
      policy p11 {
        match {
          source-address any;
          destination-address any;
          application [ junos-ftp junos-ping ];
        }
        then {
          permit;
        }
      }
    }
  }
}
```

```

    }
  }
  default-policy {
    deny-all;
  }
}
zones {
  security-zone TN1_Czone {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-0/0/0.0;
    }
  }
  security-zone TN1_Szone {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-0/0/1.0;
    }
  }
}
}
}

```

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

Verification

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

- [Verifying Intra-Tenant System traffic on ALG on page 443](#)
- [Verify ALG status for Tenant System on page 444](#)

Verifying Intra-Tenant System traffic on ALG

Purpose Verify the information about active resources, clients, groups, and sessions created through the resource manager.

Action From operational mode, enter the **show security resource-manager summary** command.

```
user@host> show security resource-manager summary
Active resource-manager clients   : 0
Active resource-manager groups    : 0
Active resource-manager resources : 0
Active resource-manager sessions  : 0
```

Meaning The output displays summary information about active resources, clients, groups, and sessions created through the resource manager.

Verify ALG status for Tenant System

Purpose Verify the ALG status for tenant on the device.

Action To verify the configuration is working properly, enter the **show security alg status tenant TN1** command.

```
user@host> show security alg status tenant TN1
ALG Status:
DNS       : Enabled
FTP       : Enabled
H323      : Disabled
MGCP      : Disabled
MSRPC     : Enabled
PPTP      : Enabled
RSH       : Disabled
RTSP      : Disabled
SCCP      : Disabled
SIP       : Disabled
SQL       : Disabled
SUNRPC    : Enabled
TALK      : Enabled
TFTP      : Enabled
IKE-ESP   : Disabled
TWAMP     : Disabled
```

Meaning The output display the alg status for FTP Enabled for the tenant system TN1.

Related Documentation

- [Tenant Systems Overview on page 353](#)

Security Log for Tenant Systems

Security logs for tenant systems include security events to control system's data planes. Security logs are sent in binary format to an external server from a tenant system interface. Security logs are generated per tenant system.

- [Understanding of Security Log for Tenant Systems on page 445](#)
- [Example: Configure Security Log for Tenant Systems on page 446](#)

Understanding of Security Log for Tenant Systems

Junos OS generates separate log messages to record events that occur on the system's control and data planes. The data plane logs, also called security logs, primarily include security events that are handled inside the data plane. Security logs can be in text or binary format and they can be saved locally (event mode) or sent to an external server (stream mode). The binary format is required for stream mode and recommended to conserve log space in event mode.

If you configure security logs per tenant, then security logs are generated per tenant.

Security logs for a tenant system are sent from a tenant system interface. You can configure the assigned routing instances and the interfaces that belong to the routing tables within a tenant system.

A security profile should be defined with the number of maximum and reserved policies when you configure the stream number for a tenant system. The master administrator can use the security profiles to specify resource allocation.

If a tenant system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available and not allocated to other tenant systems. The maximum allowed quota for stream number specifies the portion of the free global resources that the tenant system can use. The maximum allowed quota does not ensure that the amount specified for the resource in the security profile is available. A reserved quota ensures that the resource amount specified is always available to the tenant system. [Table 41 on page 445](#) shows the comparison of logging stream number capacity.

Table 41: Comparison of Logging Stream Number

Platform	Logging Stream Number Capacity for Tenant System + Logical System	Reserved Logging Stream Number Quota for Tenant System	Maximum Allowed Stream Number Quota for Tenant System	Maximum Allowed Stream Number Quota for Global
SRX5400, SRX5600, and SRX5800	64	0	8	64
SRX4600	300	0	8	600
SRX4100 and 4200	200	0	8	400

Table 41: Comparison of Logging Stream Number (continued)

SRX1500	50	0	8	100
---------	----	---	---	-----

If a device is configured for a tenant system, security logs generated within the context have the **_LS** suffix in the log name, which is the same as the logical system. The following security log shows the attributes of the RT_FLOW_SESSION_CLOSE_LS log for a device that is configured for a tenant system:

```
<14>1 2018-03-12T22:50:09.596Z user RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.137 logical-system-name="TSYS1" reason="Some reason"
source-address="192.0.2.1" source-port="7000" destination-address="198.51.100.2"
destination-port="32768" connection-tag="0" service-name="Fake service"
nat-source-address="192.0.2.1" nat-source-port="7000"
nat-destination-address="198.51.100.2" nat-destination-port="32768"
nat-connection-tag="0" src-nat-rule-type="Fake src nat rule"
src-nat-rule-name="Fake src nat rule" dst-nat-rule-type="Fake dst nat rule"
dst-nat-rule-name="Fake dst nat rule" protocol-id="17" policy-name="Fake policy"
source-zone-name="Fake src zone" destination-zone-name="Fake dst zone"
session-id-32="1" packets-from-client="4294967295" bytes-from-client="4294967293"
packets-from-server="4294967294" bytes-from-server="4294967292"
elapsed-time="4294967291" application="Fake application" nested-application="Fake
nested application" username="Fake username" roles="Fake UAC roles"
packet-incoming-interface="Fake packet incoming if" encrypted="Fake info telling
if the traffic is encrypted" application-category="Fake application category"
application-sub-category="Fake application subcategory" application-risk="-1"]
```

In the above example, security log includes **TSYS1** as the first attribute.

You can view Syslog messages in the [System Log Explorer](#).

Example: Configure Security Log for Tenant Systems

This example shows how to configure security logs for a tenant system.

- [Requirements on page 446](#)
- [Overview on page 447](#)
- [Configuration on page 447](#)
- [Verification on page 449](#)

Requirements

This example uses the following hardware and software components:

- An SRX Series device.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand how to configure a tenant system. See [“Example: Configuring Tenant Systems” on page 360](#)

- Understand how to create security profiles for the master logical system and two tenant systems. See [“Example: Configuring Tenant Systems Security Profiles \(Master Administrators Only\)”](#) on page 369.

Overview

SRX Series devices have two types of log: system logs and security logs. System logs record control plane events, for example, admin login to the device. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy.

The two types of logs can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

For off-box logging, security logs for a tenant system are sent from a tenant system interface. If the tenant system interface is already configured in a routing instance, then configure **routing-instance *routing-instance-name* at edit tenants *tenant-name* security log stream log-stream-name host** hierarchy. If the interface is not configured in routing instance, then no routing instance should be configured at **set tenants *tenant-name* security log stream log-stream-name host** hierarchy.

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 tenants TSYS1 security log mode stream
set tenants TSYS1 security log stream TN1_s format binary host 1.3.54.22
set tenants TSYS1 security log source-address 2.3.45.66
set tenants TSYS1 security log transport protocol tls
set tenants TSYS1 routing-instances TN1_ri instance-type virtual-router
set tenants TSYS1 routing-instances TN1_ri interface ge-0/0/3
set tenants TSYS1 security log stream TN1_s host routing-instance TN1_ri
set system security-profile p1 security-log-stream-number reserved 1
set system security-profile p1 security-log-stream-number maximum 2
set system security-profile p1 tenant TSYS1
```

Step-by-Step Procedure

The following procedure specifies how to configure security logs for a tenant system.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging.


```
[edit ]
user@host# set tenants TSYS1 security log mode stream
user@host# set tenants TSYS1 security log stream TN1_s format binary host 1.3.54.22
```
2. For off-box security logging, specify the source address, which identifies the SRX Series device that generated the log messages. The source address is required.

```
[edit ]
user@host# set tenants TSYS1 security log source-address 2.3.45.66
```

3. Specify the routing instance and define the interface.

```
[edit ]
user@host# set tenants TSYS1 routing-instances TN1_ri instance-type virtual-router
user@host# set tenants TSYS1 routing-instances TN1_ri interface ge-0/0/3
```

4. Define routing instance for a tenant system. If the interface is already configured in routing instance, then configure **routing-instance** *routing-instance-name* at **edit tenants** *tenant-name* **security log stream** *log-stream-name* **host** hierarchy. If the interface is not configured in routing instance, then no routing instance should be configured at **set tenants** *tenant-name* **security log stream** *log-stream-name* **host** hierarchy.

```
[edit ]
user@host# set tenants TSYS1 security log stream TN1_s host routing-instance
TN1_ri
```

5. Specify the security log transport protocol for the device.

```
[edit ]
user@host# set tenants TSYS1 security log transport protocol tls
```

Step-by-Step Procedure

The following procedure specifies how to configure a security profile for a tenant system.

1. Configure a security profile and specify the number of maximum and reserved policies.

```
[edit ]
user@host# set system security-profile p1 security-log-stream-number reserved 1
user@host# set system security-profile p1 security-log-stream-number maximum
2
```

2. Assign the configured security profile to TSYS1.

```
[edit ]
user@host# set system security-profile p1 tenant TSYS1
```

Results

From configuration mode, confirm your configuration by entering the **show system security-profile**, **show tenants TSYS1 security log**, and **show tenants TSYS1 routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS1 security log
mode stream;
source-address 2.3.45.66;
```



```

transport {
  protocol tls;
}
stream TN1_s {
  format binary;
  host {
    1.3.54.22;
    routing-instance TN1_ri;
  }
}

[edit]
user@host# show tenants TSYS1 routing-instances
TN1_ri {
  instance-type virtual-router;
  interface ge-0/0/3.0;
}

[edit]
user@host# show system security-profile
p1 {
  security-log-stream-number {
    maximum 2;
    reserved 1;
  }
  tenant TSYS1;
}

```

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

Verification

Verifying Detailed Output for Security Log

Purpose Verify that the output displays the resource information for all tenant systems.

Action From operational mode, enter the **show system security-profile security-log-stream-number tenant all** command.

logical-system	tenant name	security profile name	usage	reserved	maximum
root-logical-system		Default-Profile	0	0	8
TSYS1		p1	1	1	2

Meaning The output displays the resource information for tenant systems.

CHAPTER 4

Configuration Statements

- [address-book](#) on page 453
- [address-book \(System\)](#) on page 455
- [alg](#) on page 456
- [anti-spam \(Logical System Security Feature Profile\)](#) on page 458
- [anti-virus \(Logical System Security Feature Profile\)](#) on page 460
- [appfw-profile \(System\)](#) on page 462
- [appfw-rule](#) on page 463
- [appfw-rule-set](#) on page 464
- [application-firewall](#) on page 465
- [application-tracking](#) on page 466
- [auth-entry](#) on page 467
- [cluster \(Chassis\)](#) on page 468
- [content-filtering \(Logical System Security Feature Profile\)](#) on page 470
- [cpu](#) on page 472
- [datapath-debug](#) on page 473
- [dslite-software-initiator](#) on page 475
- [file \(System Logging\)](#) on page 476
- [firewall-authentication \(Security\)](#) on page 478
- [firewall-authentication \(tenants\)](#) on page 479
- [web-authentication](#) on page 480
- [pass-through](#) on page 481
- [flow \(Security Flow\)](#) on page 482
- [flow-gate](#) on page 484
- [flow-session](#) on page 485
- [idp \(Security\)](#) on page 487
- [idp \(logical-systems\)](#) on page 496
- [idp-policy](#) on page 496
- [ike \(Security\)](#) on page 497

- [ipsec \(Security\)](#) on page 500
- [log \(Security\)](#) on page 503
- [logical-system \(System Security Profile\)](#) on page 507
- [logical-systems](#) on page 508
- [logical-systems \(All\)](#) on page 510
- [nat](#) on page 511
- [nat-cone-binding](#) on page 515
- [nat-destination-pool](#) on page 516
- [nat-destination-rule](#) on page 517
- [nat-interface-port-ol \(System\)](#) on page 518
- [nat-nopat-address](#) on page 519
- [nat-pat-address](#) on page 520
- [nat-pat-portnum](#) on page 521
- [nat-port-ol-ipnumber](#) on page 522
- [nat-rule-referenced-prefix \(System\)](#) on page 523
- [nat-source-pool](#) on page 524
- [nat-source-rule](#) on page 525
- [nat-static-rule](#) on page 526
- [policies](#) on page 527
- [policy \(System Security Profile\)](#) on page 532
- [policy-with-count](#) on page 533
- [profile \(Access\)](#) on page 534
- [purging](#) on page 535
- [root-authentication](#) on page 536
- [root-logical-system](#) on page 537
- [scheduler \(System Security Profile\)](#) on page 538
- [screen \(Security\)](#) on page 539
- [security-profile](#) on page 543
- [security-profile-resources](#) on page 546
- [stream \(logical-systems security log\)](#) on page 547
- [softwires](#) on page 548
- [web-filtering \(Logical System Security Feature Profile\)](#) on page 549
- [zone \(System Security Profile\)](#) on page 553
- [zones](#) on page 554

address-book

Syntax `address-book (book-name | global) {
 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;
 }
 attach {
 zone zone-name;
 }
 description text;
 }`

Hierarchy Level [edit security]
 [edit tenants *tenant-name* security]

Release Information Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 18.3R1 for tenant systems. Support for wildcard addresses added in Junos OS Release 11.1. Statement moved under the security hierarchy in Junos OS Release 11.2. Support for address range added in Junos OS Release 12.1. The **description** option added in Junos OS Release 12.1.

Description Define entries in the address book. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, wildcard addresses, and address range. You define addresses and address sets in an address book and then use them when configuring different features, such as security policies and NAT.



NOTE: IPv6 wildcard address configuration is not supported in this release.

- Options**
- **address-book *book-name***—Name of the address book.
 - **global**—An address book that is available by default. You can add any combination of IPv4 addresses, IPv6 addresses, wildcard addresses, DNS names, or address range to the global address book. You do not need to attach the global address book to a security

zone; entries in the global address book are available to all security zones that are not attached to address books.

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

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

Related Documentation	<ul style="list-style-type: none"> • <i>Understanding Address Books</i> • <i>Understanding Address Sets</i>
------------------------------	---

address-book (System)

Syntax	<pre>address-book { 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 11.2.
Description	<p>Specify the number of address books that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Understanding Address Books</i>

alg

```

Syntax  alg {
    alg-manager traceoptions name ;
    alg-support-lib traceoptions name ;
    dns <disable> <doctoring (none | sanity-check)> <maximum-message-length bytes>
        <oversize-message-drop> <traceoptions name >;
    ftp (Security ALG) <allow-mismatch-ip-address> <disable> <ftps-extension>
        <line-break-extension> <traceoptions name >;
    h323 <application-screen (Security H323) <message-flood (Security H323) gatekeeper
        threshold messages per second> <unknown-message (Security H323 ALG)
        <permit-nat-applied> <permit-routed>>> <disable> <dscp-rewrite code-point
        code-point> <endpoint-registration-timeout seconds> <media-source-port-any>
        <traceoptions (Security H323 ALG) name >;
    ike-esp-nat {
        enable;
        esp-gate-timeout seconds;
        esp-session-timeout seconds;
        state-timeout seconds;
        traceoptions {
            flag all {
            }
        }
    }
    mgcp <application-screen (Security MGCP) <connection-flood threshold connection
        requests per second per MG> <message-flood (Security MGCP) threshold messages per
        second per MG> <unknown-message (Security MGCP ALG) <permit-nat-applied>
        <permit-routed>>> <disable> <dscp-rewrite code-point code-point>
        <inactive-media-timeout (Security MGCP) seconds> <maximum-call-duration (Security)
        minutes> <traceoptions (Security MGCP ALG) name > <transaction-timeout seconds>;
    msrpc <disable> <group-max-usage group-max-usage> <map-entry-timeout minutes>
        <traceoptions name >;
    pptp <disable> <traceoptions name >;
    rsh <disable> <traceoptions name >;
    rtsp <disable> <traceoptions name >;
    sccp <application-screen (Security SCCP) <call-flood threshold threshold>
        <unknown-message (Security SCCP ALG) <permit-nat-applied> <permit-routed>>>
        <disable> <dscp-rewrite code-point code-point> <inactive-media-timeout (Security
        SCCP) seconds> <traceoptions (Security SCCP ALG) name >;
    sip (Security) <application-screen (Security SIP) <protect deny (Security SIP) (all | name)
        <timeout seconds>>> <unknown-message (Security SIP ALG) <permit-nat-applied>
        <permit-routed>>> <c-timeout minutes> <disable> name distribute-to fpc <pic slot>
        <slot> <dscp-rewrite code-point code-point> <inactive-media-timeout (Security SIP)
        seconds> <maximum-call-duration (Security) minutes> <retain-hold-resource>
        <t1-interval milliseconds> <t4-interval seconds> <traceoptions (Security SIP ALG) name
        >;
    sql <disable> <traceoptions name >;
    sunrpc <disable> <group-max-usage group-max-usage> <map-entry-timeout minutes>
        <traceoptions name >;
    talk <disable> <traceoptions name >;
    tftp (Security ALG) <disable> <traceoptions name >;
    traceoptions (Security ALG) {
        file <filename> <files> <match match> <size size> <(world-readable |
        no-world-readable)>;
    }
}

```



```

        level (brief | detail | extensive | verbose);
        no-remote-trace;
    }
    twamp <traceoptions name >;
}

```

Hierarchy Level [edit logical-systems *name* security],
[edit security],
[edit services]
[edit tenants *tenant-name* security]

Release Information Statement supported in Junos OS Release 18.2R1. Statement supported in Junos OS Release 18.3R1 for tenant systems.

Description Configure an Application Layer Gateway (ALG) for a logical system to process traffic on the device. You can enable or disable related ALGs in a specific logical system by adding logical system name before security keyword.

Options **enable**—Enable ALG in a logical system.
disable—Disable ALG in a logical system.

Required Privilege Level security
tenants

Related Documentation

- [Understanding Application Layer Gateway \(ALG\) in Logical Systems on page 223](#)
- [Example: Enabling FTP ALG in a Logical System on page 227](#)
- [show security alg status logical-system on page 602](#)

anti-spam (Logical System Security Feature Profile)

```
Syntax  anti-spam {
        sbl {
            profile profile-name {
                address-blacklist list-name;
                address-whitelist list-name;
                custom-tag-string [string];
                (sbl-default-server | no-sbl-default-server);
                spam-action (block | tag-header | tag-subject);
            }
        }
    }
```

Hierarchy Level [edit logical-systems *logical-system-name* security utm feature-profile]

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Configures the UTM antispam feature for logical systems. The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects a message deemed to be spam, it blocks the e-mail message or tags the e-mail message header or subject with a preprogrammed string. Antispam filtering uses both a third-party server-based Spam Block List (SBL), and optionally created local whitelists (benign) and blacklists (malicious) for filtering against e-mail messages.

You can also configure the default UTM configuration for antispam feature profile. If you do not configure any option in the antispam feature profile, the values configured in the default UTM configuration are applied. In the default UTM profile, the antispam type is configured as SBL instead of none. This configuration enables the SBL option. However, to use this feature, enable the SBL server using the [edit security utm default-configuration anti-spam sbl sbl-default-server] command.



NOTE: A license check for the antispam configuration is performed at the time of commit and provides a warning if a valid license is not installed on the device. Once a valid license is installed on the device then the custom antispam profile or the default antispam profile is able to process the traffic. If a license is expired or is not installed, the antispam service does not process the traffic.

Options **anti-spam**—Configures the UTM antispam feature for logical system.

address-blacklist—Enter an address blacklist custom object for local list spam filtering.

address-whitelist—Enter an address whitelist custom object for local list spam filtering.

sbl—Antispam filtering allows you to use both a third-party server-based SBL, and optionally created local whitelists and blacklists for filtering against e-mail messages.

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	<ul style="list-style-type: none">• <i>Antispam Filtering Overview</i>• <i>utm default-configuration</i>

anti-virus (Logical System Security Feature Profile)

```
Syntax anti-virus {
    sophos-engine {
        profile name {
            fallback-options {
                content-size (block | log-and-permit | permit);
                default (block | log-and-permit | permit);
                engine-not-ready (block | log-and-permit | permit);
                out-of-resources (block | log-and-permit | permit);
                timeout (block | log-and-permit | permit);
                too-many-requests (block | log-and-permit | permit);
            }
            mime-whitelist {
                exception exception;
                list list;
            }
            notification-options {
                fallback-block {
                    custom-message custom-message;
                    custom-message-subject custom-message-subject;
                    (notify-mail-sender | no-notify-mail-sender);
                    type (message | protocol-only);
                }
                fallback-non-block {
                    custom-message custom-message;
                    custom-message-subject custom-message-subject;
                    (notify-mail-recipient | no-notify-mail-recipient);
                }
                virus-detection {
                    custom-message custom-message;
                    custom-message-subject custom-message-subject;
                    (notify-mail-sender | no-notify-mail-sender);
                    type (message | protocol-only);
                }
            }
            scan-options {
                content-size-limit content-size-limit;
                timeout seconds;
                (uri-check | no-uri-check);
            }
            trickling;
            url-whitelist;
        }
    }
}
```

Hierarchy Level [edit logical-systems *logical-systems-name* security utm feature-profile]

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Configures the UTM Sophos Antivirus feature for logical systems. You can also configure the default UTM configuration for antivirus feature profile. If you do not configure any

option in the antivirus feature profile, the values configured in the default UTM configuration are applied.



NOTE: A license check for the antivirus configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom antivirus profile or the antivirus default profile is able to process traffic. If a license is expired or is not installed, the antivirus service does not process the traffic.

- Options**
- anti-virus**—Configures the UTM antivirus feature for logical systems.
 - mime-whitelist**—This is the comprehensive list for those MIME types that can bypass antivirus scanning.
 - sophos-engine**—The antivirus engine that is used on the device. You can only have one engine type running and you must restart the device if you change engines.
 - fallback-options**—Fallback options helps the system how to handle the errors.
 - notification-options**—There are multiple notification options you can configure to trigger when a virus is detected.
 - fallback-non-block**—Notifications for fallback nonblocking actions.
 - virus-detection**—Notifications to send when a virus is detected.
 - scan-options**—Antivirus sophos-engine scan options.
 - trickling** —HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning.
 - url-whitelist**—Antivirus URL white list is a unique custom list that includes the URLs or IP addresses category to bypass the antivirus scanning.
- 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

- *Unified Threat Management Overview*
- *utm default-configuration*

appfw-profile (System)

Syntax	<pre>appfw-profile { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	<p>Specify the application firewall profile quota of a logical system.</p> <p>As a master administrator, you can create a security profile and specify the kinds and amounts of resources to allocate to a logical system to which the security profile is bound. A security profile is used for share the device's resources, including policies, zones, addresses and address books, flow sessions, and various forms of NAT, among all logical systems appropriately. You can dedicate various amounts of a resource to the logical systems and allow them to compete for use of the free resources.</p>
Options	<ul style="list-style-type: none">• maximum <i>amount</i>—Specify the maximum allowed quota value. Range: 0 through 1024• reserved <i>amount</i>—Specify a reserved quota value that guarantees that the resource amount specified is always available to the logical system.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Application Firewall Overview</i>

appfw-rule

Syntax	<pre>appfw-rule { 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 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>

appfw-rule-set

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	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">• <i>Application Firewall Overview</i>

application-firewall

```

Syntax  application-firewall {
            rule-sets rule-set-name {
                default-rule {
                    (deny | permit);
                }
                rule rule-name {
                    match {
                        dynamic-application [system-application];
                        dynamic-application-group [system-application-group];
                    }
                    then {
                        (deny | permit);
                    }
                }
            }
            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 11.1.

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


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

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

Related Documentation

- *Application Firewall Overview*

application-tracking

Syntax	<pre>application-tracking { disable; (first-update first-update-interval <i>first-update-interval</i>); session-update-interval <i>session-update-interval</i>; }</pre>
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	<p>Enable application tracking (AppTrack).</p> <p>After application identification identifies the application, AppTrack collects statistics for the application usage on the device, and when the session closes, AppTrack generates a message that provides the byte and packet counts and duration of the session, and sends details to the host device such as Security Threat Response Manager (STRM). STRM retrieves the data and provides flow-based application visibility details.</p>
Options	<p>first-update—Generate application tracking initial message when a session is created. This option overrides the first-update-interval option if both are specified.</p> <p>first-update-interval—Interval when the first update message is sent (minutes).</p> <div><div></div><div><p>NOTE: The first-update-interval setting is disregarded if the first-update option is set to log the first message at session start.</p></div></div> <ul style="list-style-type: none">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. <p>Default: 1</p> <p>disable—Disable application tracking.</p> <p>session-update-interval—Frequency in which application tracking update messages are generated (minutes).</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"><i>Example: Configuring AppTrack</i>

auth-entry

Syntax	<pre>auth-entry { 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 11.2.
Description	<p>Specify the number of firewall authentication entries that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Logical Systems Security Profiles (Master Administrators Only) on page 73

cluster (Chassis)

```
Syntax cluster {
    configuration-synchronize {
        no-secondary-bootup-auto no-secondary-bootup-auto;
    }
    control-link-recovery control-link-recovery;
    control-ports fpc {
        port;
    }
    heartbeat-interval milliseconds;
    heartbeat-threshold heartbeat-threshold;
    network-management {
        cluster-master cluster-master;
    }
    redundancy-group name {
        gratuitous-arp-count gratuitous-arp-count;
        hold-down-interval seconds;
        interface-monitor name {
            weight weight;
        }
        ip-monitoring {
            family {
                inet name logical-interface-name secondary-ip-address weight weight;
            }
            global-threshold number;
            global-weight number;
            retry-count number;
            retry-interval seconds;
        }
        node (0 | 1 ) {
            priority number;
        }
        preempt {
            delay seconds;
            limit limit;
            period seconds;
        }
    }
    reth-count number;
    traceoptions {
        file <filename> <files files> <match match> <size size> <(world-readable |
            no-world-readable)>;
        flag name;
        level (alert | all | critical | debug | emergency | error | info | notice | warning);
        no-remote-trace no-remote-trace;
    }
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 9.0.

Description	Configure a chassis cluster. You can perform the configuration under the [edit chassis cluster] configuration stanza to define chassis cluster configuration, operations, and monitoring. The configuration includes specifying configuration synchronization, control link recovery, heartbeat interval and threshold, network management, redundancy group, and traceoptions.
Options	<p>configuration-synchronize—Disable automatic chassis cluster synchronization. See <i>configuration-synchronize (Chassis Cluster)</i>.</p> <p>control-link-recovery—Enable automatic control link recovery option.</p> <p>control-ports—Enable specific chassis cluster control ports.</p> <p>Values:</p> <ul style="list-style-type: none"> fpc—FPC slot number port—Port number <p>heartbeat-interval—Interval between successive heartbeats (milliseconds) Default: 1000 Range: 1000-2000</p> <p>heartbeat-threshold—Number of consecutive missed heartbeats to indicate device failure Default: 3 Range: 3-8</p> <p>network-management—Define parameters for network management. See <i>network-management</i>.</p> <p>redundancy-group <i>name</i>—Define a redundancy group. See <i>redundancy-group (Chassis Cluster)</i>.</p> <p>reth-count—Number of redundant ethernet interfaces Range: 1-128</p> <p>traceoptions—Define chassis cluster redundancy process tracing operations. See <i>traceoptions (Chassis Cluster)</i>.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>ip-monitoring</i>

content-filtering (Logical System Security Feature Profile)

Syntax

```

content-filtering {
    block-command;
    block-content-type {
        activex;
        exe;
        http-cookie;
        java-applet;
        zip;
    }
    block-extension;
    block-mime {
        exception;
        list;
    }
    notification-options {
        custom-message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    permit-command;
}

```

Hierarchy Level [edit logical-systems *logical-systems-name* security utm feature-profile]

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Configures the UTM content-filtering feature for logical systems. The content filtering feature controls file transfers across the gateway by checking traffic against configured filter lists. It evaluates the traffic before all other UTM features, except Web filtering. You can also configure the default UTM configuration for content filtering feature profile. If you do not configure any option in the content filtering feature profile, the values configured in the default UTM configuration are applied.



NOTE: A license check for the content filtering configuration is performed at the time of commit and provides a warning if a valid license is not installed on the device. Once a valid license is installed on the device then the custom content filtering profile or the default content filtering profile is able to process the traffic. If a license is expired or license is not installed, the content filtering service does not process the traffic.

Options **block-command**—Protocol block command custom-objects to the content-filtering profile.

block-content-type—Blocks other available content such as exe, http-cookie, java-applet. This is for HTTP only.

block-extension—Block extensions to the content-filtering profile.

block-mime—MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

notification-options—A message notification to trigger when a content filter is matched.

permit-command—Protocol permit command custom-objects to the content-filtering profile.

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	<ul style="list-style-type: none">• <i>Content Filtering Overview</i>• <i>utm default-configuration</i>
------------------------------	--

cpu

Syntax `cpu {
 reserved percent;
 }`

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

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the percentage of CPU utilization that is always available to a logical system. This value is configured in a security profile that is bound to a logical system.

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



NOTE: The `cpu-control` option at the `[edit system security-profile resources]` hierarchy level must be specified for the reserved value to take effect.

Options **reserved *percent***—A reserved quota that guarantees that the percentage of CPU specified is always available to the logical system.

Range: 0 through 100 percent (decimal point allowed).

Default: 1 percent for the master logical system and 0 percent for user logical systems.



CAUTION: The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota as traffic loss could occur.

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

Related Documentation

- [Understanding Logical Systems Security Profiles \(Master Administrators Only\)](#) on page 73

datapath-debug

```

Syntax  datapath-debug {
            action-profile profile-name {
                event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress | np-ingress
                    | pot) {
                    count;
                    packet-dump;
                    packet-summary;
                    trace;
                }
            }
            module {
                flow {
                    flag {
                        all;
                    }
                }
            }
            preserve-trace-order;
            record-pic-history;
        }
        capture-file {
            filename;
            files number;
            format pacp-format;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        maximum-capture-size value;
        packet-filter packet-filter-name {
            action-profile (profile-name | default);
            destination-port (port-range | protocol-name);
            destination-prefix destination-prefix;
            interface logical-interface-name;
            protocol (protocol-number | protocol-name);
            source-port (port-range | protocol-name);
            source-prefix source-prefix;
        }
        traceoptions {
            file {
                filename;
                files number;
                match regular-expression;
                size maximum-file-size;
                (world-readable | no-world-readable);
            }
            no-remote-trace;
        }
    }

```

Hierarchy Level [edit security]

Release Information Command introduced in Junos OS Release 10.0.

Description Configure the data path debugging options.



NOTE: Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

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 Data Path Debugging for Logical Systems on page 346](#)

dslite-software-initiator

Syntax	<pre>dslite-software-initiator { 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 12.1.
Description	<p>Specify the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user logical system or the master logical system. This statement is configured in the security profile that is bound to the logical system.</p> <p>Only the master administrator can create security profiles and bind them to logical systems. The master administrator:</p> <ul style="list-style-type: none"> • Uses security profiles to provision logical systems with resources • Binds security profiles to user logical systems and the master logical system • Configures more than one security profile, specifying different amounts of resource allocations in various profiles
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 utilize 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. The default is the system maximum. • reserved <i>amount</i>—A reserved quota that guarantees that the resource amount specified is always available to the logical system. The default is 0.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding IPv6 Dual-Stack Lite in Logical Systems on page 250

file (System Logging)

Syntax `file filename {`
 `allow-duplicates;`
 `any (alert | any | critical | emergency | error | info | none | notice | warning);`
 `archive {`
 `archive-sites {`
 `url password;`
 `}`
 `(binary-data | no-binary-data);`
 `files number;`
 `size size;`
 `start-time start-time;`
 `transfer-interval transfer-interval;`
 `(world-readable | no-world-readable);`
 `}`
 `authorization (alert | any | critical | emergency | error | info | none | notice | warning);`
 `change-log (alert | any | critical | emergency | error | info | none | notice | warning);`
 `conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);`
 `daemon (alert | any | critical | emergency | error | info | none | notice | warning);`
 `dfc (alert | any | critical | emergency | error | info | none | notice | warning);`
 `explicit-priority;`
 `external (alert | any | critical | emergency | error | info | none | notice | warning);`
 `firewall (alert | any | critical | emergency | error | info | none | notice | warning);`
 `ftp (alert | any | critical | emergency | error | info | none | notice | warning);`
 `interactive-commands (alert | any | critical | emergency | error | info | none | notice | warning);`
 `kernel (alert | any | critical | emergency | error | info | none | notice | warning);`
 `match "regular-expression";`
 `ntp (alert | any | critical | emergency | error | info | none | notice | warning);`
 `pfe (alert | any | critical | emergency | error | info | none | notice | warning);`
 `security (alert | any | critical | emergency | error | info | none | notice | warning);`
 `structured-data {`
 `brief;`
 `}`
 `user (alert | any | critical | emergency | error | info | none | notice | warning);`
 `}`

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description Specify the file in which to log data.

- Options**
- *filename*—Specify the name of the file in which to log data.
 - *allow-duplicates*—Do not suppress the repeated messages.
 - *any*—Specify all facilities information.
 - *alert*—Specify the conditions that should be corrected immediately.
 - *critical*—Specify the critical conditions.

- *emergency*—Specify the conditions that cause security functions to stop.
- *error*—Specify the general error conditions.
- *info*—Specify the information about normal security operations.
- *none*—Do not specify any messages.
- *notice*—Specify the conditions that should be handled specifically.
- *warning*—Specify the general warning conditions.
- *archive*—Specify the archive file information.
 - *archive-sites*—Specify a list of destination URLs for the archived log files.
 - *url*—Specify the primary and failover URLs to receive archive files.
 - *binary-data*—Mark file such that it contains binary data.
 - *no-binary-data*—Do not mark the file such that it contains binary data.
 - *files*—Specify the number of files to be archived. Range: 1 through 1000 files.
 - *size*—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
 - *world-readable*—Allow any user to read the log file.
 - *no-world-readable*—Do not allow any user to read the log file.
 - *start-time*—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
 - *transfer-interval*—Specify the frequency at which to transfer the files to archive sites.
- *authorization*—Specify the authorization system.
- *change-log*—Specify the configuration change log.
- *conflict-log*—Specify the configuration conflict log.
- *daemon*—Specify the various system processes.
- *dfc*—Specify the dynamic flow capture.
- *explicit-priority*—Include the priority and facility in messages.
- *external*—Specify the local external applications.
- *firewall*—Specify the firewall filtering system.
- *ftp*—Specify the FTP process.
- *interactive-commands*—Specify the commands executed by the UI.
- *kernel*—Specify the kernel information.
- *match*—Specify the regular expression for lines to be logged.
- *ntp*—Specify the NTP process.
- *pfe*—Specify the Packet Forwarding Engine.

- *security*—Specify the security-related information.
- *structured-data*—Log the messages in structured log format.
 - *brief*—Omit English language text from the end of the logged message.
- *user*—Specify the user processes.
 - *info*—Specify the informational messages.

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

firewall-authentication (Security)

Syntax firewall-authentication {
 traceoptions {
 flag *flag*;
 }
}

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5.

Description Define data-plane firewall authentication tracing options.

- Options**
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.
 - **all**—Enable all tracing operations.
 - **authentication**—Trace data-plane firewall authentication events.
 - **proxy**—Trace data-plane firewall authentication proxy events.
 - **detail**—Display moderate amount of data.
 - **extensive**—Display extensive amount of data.
 - **terse**—Display minimum amount of data.

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

- Related Documentation**
- [Firewall User Authentication Overview](#)
 - [Understanding Logical System Firewall Authentication on page 152](#)

firewall-authentication (tenants)

```

Syntax  firewall-authentication {
            pass-through {
                default-profile default-profile;
                ftp {
                    banner (Access FTP HTTP Telnet Authentication) {
                        fail fail;
                        login login;
                        success success;
                    }
                }
                ftp {
                    banner (Access FTP HTTP Telnet Authentication) {
                        fail fail;
                        login login;
                        success success;
                    }
                }
                ftp {
                    banner (Access FTP HTTP Telnet Authentication) {
                        fail fail;
                        login login;
                        success success;
                    }
                }
            }
            traceoptions {
                file <filename> <files files> <match match> <size size> <(world-readable |
                    no-world-readable)>;
                flag name;
                no-remote-trace;
            }
            web-authentication {
                banner {
                    success success;
                }
                default-profile default-profile;
                timeout timeout;
            }
        }

```

Hierarchy Level [edit logical-systems *name* tenants *name* access],
[edit tenants *name* access]

Release Information Statement introduced in Junos OS Release 18.3R1

Description Define the type of firewall authentication on tenant system.

Required Privilege Level access

- Related Documentation**
- [Firewall Authentication for Tenant Systems on page 406](#)
 - [show security firewall-authentication history on page 609](#)
 - [show security firewall-authentication users on page 612](#)
 - [firewall-authentication on page 479](#)

web-authentication

Syntax	<pre>web-authentication { banner { success <i>success</i>; } default-profile <i>default-profile</i>; timeout <i>timeout</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>name</i> tenants <i>name</i> access firewall-authentication], [edit tenants <i>name</i> access firewall-authentication]
Release Information	Statement introduced in Junos OS Release 18.3R1.
Description	Define Web-authentication settings for tenant systems.
Options	<p>default-profile—Name of profile to use for web-authentication</p> <p>timeout—Web-authentication timeout value in seconds</p> <p>Range: 5 through 60</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	flow-tap
Related Documentation	pass-through on page 481

pass-through

Syntax	<pre> pass-through { default-profile <i>default-profile</i>; ftp { banner (Access FTP HTTP Telnet Authentication) { fail <i>fail</i>; login <i>login</i>; success <i>success</i>; } } ftp { banner (Access FTP HTTP Telnet Authentication) { fail <i>fail</i>; login <i>login</i>; success <i>success</i>; } } ftp { banner (Access FTP HTTP Telnet Authentication) { fail <i>fail</i>; login <i>login</i>; success <i>success</i>; } } } </pre>
Hierarchy Level	[edit logical-systems <i>name</i> tenants <i>name</i> access firewall-authentication], [edit tenants <i>name</i> access firewall-authentication]
Release Information	Statement introduced in Junos OS Release 18.3R1.
Description	Pass-through firewall authentication settings
Options	<p>default-profile—Name of profile to use if not specified in policy</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	flow-tap
Related Documentation	firewall-authentication on page 479

flow (Security Flow)

```
Syntax  flow {
        aging {
            early-ageout seconds;
            high-watermark percent;
            low-watermark percent;
        }
        allow-dns-reply;
        ethernet-switching {
            block-non-ip-all;
            bpdu-vlan-flooding;
            bypass-non-ip-unicast;
            no-packet-flooding {
                no-trace-route;
            }
        }
        force-ip-reassembly;
        ipsec-performance-acceleration;
        load distribution {
            session-affinity ipsec;
        }
        packet-log {
            enable;
            throttle-interval;
            packet-filter <filter-name>;
        }
        pending-sess-queue-length (high | moderate | normal);
        route-change-timeout seconds;
        syn-flood-protection-mode (syn-cookie | syn-proxy);
        tcp-mss {
            all-tcp mss value;
            gre-in {
                mss value;
            }
            gre-out {
                mss value;
            }
            ipsec-vpn {
                mss value;
            }
        }
        tcp-session {
            fin-invalidate-session;
            no-sequence-check;
            no-syn-check;
            no-syn-check-in-tunnel;
            rst-invalidate-session;
            rst-sequence-check;
            strict-syn-check;
            tcp-initial-timeout seconds;
            time-wait-state {
                (session-ageout | session-timeout seconds);
            }
        }
    }
```

```

}
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
  packet-filter filter-name {
    destination-port port-identifier;
    destination-prefix address;
    interface interface-name;
    protocol protocol-identifier;
    source-port port-identifier;
    source-prefix address;
  }
  rate-limit messages-per-second;
}
}


```

Hierarchy Level	[edit security]
Release Information	Statement modified in Junos OS Release 9.5.
Description	Determine how the device manages packet flow. The device can regulate packet flow in the following ways:
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	<ul style="list-style-type: none"> • <i>Understanding Traffic Processing on Security Devices</i> • <i>Understanding Session Characteristics for SRX Series Services Gateways</i> • Understanding Packet Flow in Logical Systems for SRX Series Devices on page 32

flow-gate

Syntax	<pre>flow-gate { 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 11.2.
Description	<p>Specify the number of flow gates, also known as pinholes, that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems Security Profiles (Master Administrators Only) on page 73

flow-session

Syntax	<pre>flow-session { 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 11.2.
Description	<p>Specify the number of flow sessions that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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.
	<p> NOTE: An IPv6 session consumes twice the memory of an IPv4 session. Therefore the number of sessions available for IPv6 is half the reserved and maximum quotas configured for the flow session resource in a security profile. Use the vty command <code>show usp flow resource usage cp-session</code> to check flow session usage.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

**Related
Documentation**

- [Understanding Logical Systems Security Profiles \(Master Administrators Only\) on page 73](#)
- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\) on page 79](#)

idp (Security)

```
Syntax idp {
    active-policy policy-name;
    custom-attack attack-name {
        attack-type {
            anomaly {
                direction (any | client-to-server | server-to-client);
                service service-name;
                shellcode (all | intel | no-shellcode | sparc);
                test test-condition;
            }
            chain {
                expression boolean-expression;
                member member-name {
                    attack-type {
                        (anomaly ...same statements as in [edit security idp custom-attack attack-name
                        attack-type anomaly] hierarchy level | signature ...same statements as in [edit
                        security idp custom-attack attack-name attack-type signature] hierarchy
                        level);
                    }
                }
            }
            order;
            protocol-binding {
                application application-name;
                icmp;
                icmpv6;
                ip {
                    protocol-number transport-layer-protocol-number;
                }
                ipv6 {
                    protocol-number transport-layer-protocol-number;
                }
                rpc {
                    program-number rpc-program-number;
                }
                tcp {
                    minimum-port port-number <maximum-port port-number>;
                }
                udp {
                    minimum-port port-number <maximum-port port-number>;
                }
            }
            reset;
            scope (session | transaction);
        }
        signature {
            context context-name;
            direction (any | client-to-server | server-to-client);
            negate;
            pattern signature-pattern;
            protocol {
                icmp {
                    code {
```

```

        match (equal | greater-than | less-than | not-equal);
        value code-value;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    type {
        match (equal | greater-than | less-than | not-equal);
        value type-value;
    }
}
ipv4 {
    destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
    }
    protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
    }
    total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
    }
    ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
    }
}
ipv6 {

```



```
destination {
    match (equal | greater-than | less-than | not-equal);
    value ip-address-or-hostname;
}
flow-label {
    match (equal | greater-than | less-than | not-equal);
    value flow-label-value;
}
hop-limit {
    match (equal | greater-than | less-than | not-equal);
    value hop-limit-value;
}
next-header {
    match (equal | greater-than | less-than | not-equal);
    value next-header-value;
}
payload-length {
    match (equal | greater-than | less-than | not-equal);
    value payload-length-value;
}
source {
    match (equal | greater-than | less-than | not-equal);
    value ip-address-or-hostname;
}
traffic-class {
    match (equal | greater-than | less-than | not-equal);
    value traffic-class-value;
}
tcp {
    ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
    }
    mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size;
    }
    option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
}
```

```
}
source-port {
    match (equal | greater-than | less-than | not-equal);
    value source-port;
}
tcp-flags {
    (ack | no-ack);
    (fin | no-fin);
    (psh | no-psh);
    (r1 | no-r1);
    (r2 | no-r2);
    (rst | no-rst);
    (syn | no-syn);
    (urg | no-urg);
}
urgent-pointer {
    match (equal | greater-than | less-than | not-equal);
    value urgent-pointer;
}
window-scale {
    match (equal | greater-than | less-than | not-equal);
    value window-scale-factor;
}
window-size {
    match (equal | greater-than | less-than | not-equal);
    value window-size;
}
}
udp {
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
    }
}
}
protocol-binding {
    application application-name;
    icmp;
    icmpv6;
    ip {
        protocol-number transport-layer-protocol-number;
    }
    ipv6 {
        protocol-number transport-layer-protocol-number;
    }
    rpc {
        program-number rpc-program-number;
    }
}
```

```

        tcp {
            minimum-port port-number <maximum-port port-number>;
        }
        udp {
            minimum-port port-number <maximum-port port-number>;
        }
    }
    regexp regular-expression;
    shellcode (all | intel | no-shellcode | sparc);
}
recommended-action (close | close-client | close-server | drop | drop-packet | ignore |
    none);
severity (critical | info | major | minor | warning);
time-binding {
    count count-value;
    scope (destination | peer | source);
}
}
custom-attack-group custom-attack-group-name {
    group-members [attack-or-attack-group-name];
}
default-policy default-policy;
dynamic-attack-group dynamic-attack-group-name {
    filters {
        category {
            values [category-value];
        }
        direction {
            expression (and | or);
            values [any client-to-server exclude-any exclude-client-to-server
                exclude-server-to-client server-to-client];
        }
        false-positives {
            values [frequently occasionally rarely unknown];
        }
        performance {
            values [fast normal slow unknown];
        }
        products {
            values [product-value];
        }
        recommended;
        service {
            values [service-value];
        }
        severity {
            values [critical info major minor warning];
        }
        type {
            values [anomaly signature];
        }
    }
}
}
idp-policy policy-name {
    rulebase-exempt {

```

```

rule rule-name {
  description text;
  match {
    attacks {
      custom-attack-groups [attack-group-name];
      custom-attacks [attack-name];
      dynamic-attack-groups [attack-group-name];
      predefined-attack-groups [attack-group-name];
      predefined-attacks [attack-name];
    }
    destination-address ([address-name] | any | any-ipv4 | any-ipv6);
    destination-except [address-name];
    from-zone (zone-name | any );
    source-address ([address-name] | any | any-ipv4 | any-ipv6);
    source-except [address-name];
    to-zone (zone-name | any);
  }
}

rulebase-ips {
  rule rule-name {
    description text;
    match {
      application (application-name | any | default);
      attacks {
        custom-attack-groups [attack-group-name];
        custom-attacks [attack-name];
        dynamic-attack-groups [attack-group-name];
        predefined-attack-groups [attack-group-name];
        predefined-attacks [attack-name];
      }
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any );
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
    terminal;
    then {
      action {
        class-of-service {
          dscp-code-point number;
          forwarding-class forwarding-class;
        }
        (close-client | close-client-and-server | close-server | drop-connection |
         drop-packet | ignore-connection | mark-diffserv value | no-action |
         recommended);
      }
      ip-action {
        (ip-block | ip-close | ip-notify);
        log;
        log-create;
        refresh-timeout;
        target (destination-address | service | source-address | source-zone |
         source-zone-address | zone-service);
      }
    }
  }
}

```

```

        timeout seconds;
    }
    notification {
        log-attacks {
            alert;
        }
        packet-log {
            post-attack number;
            post-attack-timeout seconds;
            pre-attack number;
        }
    }
    severity (critical | info | major | minor | warning);
}
}
}
security-package {
    automatic {
        download-timeout minutes;
        enable;
        interval hours;
        start-time start-time;
    }
    install {
        ignore-version-check;
        ignore-appid-failure;
    }
    proxy-profile proxy-profile;
    source-address address;
    url url-name;
}
sensor-configuration {
    application-identification {
        max-packet-memory value;
        max-tcp-session-packet-memory value;
        max-udp-session-packet-memory value;
    }
    detector {
        protocol-name protocol-name {
            tunable-name tunable-name {
                tunable-value protocol-value;
            }
        }
    }
}
flow {
    (allow-icmp-without-flow | no-allow-icmp-without-flow);
    fifo-max-size value;
    hash-table-size value;
    (log-errors | no-log-errors);
    max-session-offset value;
    max-timers-poll-ticks value;
    reject-timeout value;
    (reset-on-policy | no-reset-on-policy);
    udp-anticipated-timeout value;
}

```

```

global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    gtp (decapsulation | no-decapsulation);
    memory-limit-percent value;
    (policy-lookup-cache | no-policy-lookup-cache);
}
high-availability {
    no-policy-cold-synchronization;
}
ips {
    content-decompression-max-memory-kb value;
    content-decompression-max-ratio value;
    (detect-shellcode | no-detect-shellcode);
    fifo-max-size value;
    (ignore-regular-expression | no-ignore-regular-expression);
    log-supercede-min minimum-value;
    pre-filter-shellcode;
    (process-ignore-s2c | no-process-ignore-s2c);
    (process-override | no-process-override);
    process-port port-number;
}
log {
    cache-size size;
    suppression {
        disable;
        (include-destination-address | no-include-destination-address);
        max-logs-operate value;
        max-time-report value;
        start-log value;
    }
}
packet-log {
    host ip-address <port number>;
    max-sessions percentage;
    source-address ip-address;
    total-memory percentage;
}
re-assembler {
    action-on-reassembly-failure (drop | drop-session | ignore);
    (force-tcp-window-checks | no-force-tcp-window-checks);
    (ignore-memory-overflow | no-ignore-memory-overflow);
    (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);
    ignore-reassembly-overflow;
    max-flow-mem value;
    max-packet-mem value;
    (tcp-error-logging | no-tcp-error-logging);
}
ssl-inspection {
    cache-prune-chunk-size number;
    key-protection;
    maximum-cache-size number;
    session-id-cache-timeout seconds;
    sessions number;
}
}

```

```

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 security]

Release Information Statement modified in Junos OS Release 9.3. The **expression** option added in Junos OS Release 11.4.
Starting in Junos OS Release 18.3R1, when an SRX Series device is configured with unified policies, you can configure multiple IDP policies and set one of those policies as the default IDP policy. If multiple IDP policies are configured for a session and when policy conflict occurs, the device applies the default IDP policy for that session and thus resolves any policy conflicts.



NOTE: If you have configured two or more IDP policies in a unified security policy, then you must configure the default IDP policy.

Description Configure Intrusion Detection and Prevention (IDP) to selectively enforce various IDP attack detection and prevention techniques on 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

- *Understanding Intrusion Detection and Prevention for SRX Series*

idp (logical-systems)

Syntax	idp (default off on);
Hierarchy Level	[edit logical-systems <i>name</i> security]
Release Information	Statement introduced in Junos OS Release 11.4
Description	Configure IDP on master and user logical systems.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	security
Related Documentation	<ul style="list-style-type: none">• show security idp logical system on page 624• Understanding IDP Features in Logical Systems on page 204• IDP in Logical Systems Overview on page 202•

idp-policy

Syntax	idp-policy <i>idp-policy-name</i> ;
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the IDP policy for the security profile.
Options	<i>idp-policy-name</i> —Name of the IDP policy.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Intrusion Detection and Prevention for SRX Series

ike (Security)

```

Syntax  ike {
    gateway gateway-name {
        aaa {
            access-profile profile-name;
        }
        address [ip-address-or-hostname];
        advpn {
            suggester {
                disable;
            }
            partner {
                connection-limit <number>;
                idle-threshold <packets/sec>;
                idle-time <seconds>;
                disable;
            }
        }
        dead-peer-detection {
            (always-send | optimized | probe-idle-tunnel);
            interval seconds;
            threshold number;
        }
        dynamic {
            connections-limit number;
            (distinguished-name <container container-string> <wildcard wildcard-string> |
             hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname
             e-mail-address);
            ike-user-type (group-ike-id | shared-ike-id);
        }
        external-interface external-interface-name;
        fragmentation {
            enable;
            size bytes;
        }
        general-ikeid;
        ike-policy policy-name;
        local-address (ipv4-address | ipv6-address);
        local-identity {
            (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address |
             user-at-hostname e-mail-address);
        }
        nat-keepalive seconds;
        no-nat-traversal;
        remote-identity {
            (distinguished-name <container container-string> <wildcard wildcard-string> |
             hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname
             e-mail-address);
        }
        tcp-encap-profile profile-name;
        version (v1-only | v2-only);
    }
    policy policy-name {

```

```

certificate {
  local-certificate certificate-id;
  peer-certificate-type (pkcs7 | x509-signature);
  policy-oids [ oid ];
  trusted-ca {
    ca-profile ca-profile-name;
    trusted-ca-group trusted-ca-group-name;
  }
}
description description;
mode (aggressive | main);
pre-shared-key (ascii-text key | hexadecimal key);
proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
proposals [proposal-name];
reauth-frequency number;
}
proposal proposal-name {
  authentication-algorithm (md5 | sha-256 | sha-384 | sha1);
  authentication-method (dsa-signatures | ecdsa-signatures-256 | ecdsa-signatures-384
    | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  lifetime-seconds seconds;
}
respond-bad-spi <max-responses>;
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}
}

```

Hierarchy Level	[edit security]
Release Information	Statement modified in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 11.1. The inet6 option added in Junos OS Release 11.1.
Description	Define Internet Key Exchange (IKE) configuration.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

- Related Documentation**
- *IPsec VPN Overview*
 - *ALG Overview*
 - [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

ipsec (Security)

```
Syntax  ipsec {
        policy policy-name {
            description description;
            perfect-forward-secrecy keys (group1 | group14 | group19 | group2 | group20 | group24 |
            group5);
            proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
            proposals [proposal-name];
        }
        proposal proposal-name {
            authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
            description description;
            encryption-algorithm (3des-cbc | aes-128-cbc | aes-128-gcm | aes-192-cbc | aes-192-gcm
            | aes-256-cbc | aes-256-gcm | des-cbc);
            lifetime-kilobytes kilobytes;
            lifetime-seconds seconds;
            protocol (ah | esp);
        }
        security-association sa-name {
            manual {
                direction bidirectional {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key {
                            ascii-text key;
                            hexadecimal key;
                        }
                    }
                    auxiliary-spi auxiliary-spi-value;
                    encryption {
                        algorithm (3des-cbc | des-cbc | null);
                        key {
                            ascii-text key;
                            hexadecimal key;
                        }
                    }
                    protocol (ah | esp);
                    spi spi-value;
                }
            }
            mode transport;
        }
        traceoptions {
            flag flag;
        }
        vpn vpn-name {
            bind-interface interface-name;
            copy-outer-dscp;
            establish-tunnels (immediately | on-traffic);
            ike {
                gateway gateway-name;
                idle-time seconds;
                install-interval seconds;
            }
        }
    }
```

```

    ipsec-policy ipsec-policy-name;
    no-anti-replay;
    proxy-identity {
        local ip-prefix;
        remote ip-prefix;
        service (any | service-name);
    }
}
manual {
    authentication {
        algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    encryption {
        algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        key (ascii-text key | hexadecimal key);
    }
    external-interface external-interface-name;
    gateway ip-address;
    protocol (ah | esp);
    spi spi-value;
}
traffic-selector traffic-selector-name {
    local-ip ip-address/netmask;
    remote-ip ip-address/netmask;
}
}
vpn-monitor {
    destination-ip ip-address;
    optimized;
    source-interface interface-name;
    verify-path {
        destination-ip ip-address;
        packet-size bytes;
    }
}
}
vpn-monitor-options {
    interval seconds;
    threshold number;
}
}

```

Hierarchy Level [edit security]

Release Information Statement modified in Junos OS Release 8.5.

Description Define IPsec configuration.

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

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

Related Documentation

- *IPsec VPN Overview*

log (Security)

```

Syntax  log {
        cache {
            exclude exclude-name {
                destination-address destination-address;
                destination-port destination-port;
                event-id event-id;
                failure;
                interface-name interface-name;
                policy-name policy-name;
                process process-name;
                protocol protocol;
                source-address source-address;
                source-port source-port;
                success;
                user-name user-name;
            }
            limit value;
        }
        disable;
        event-rate rate;
        facility-override (authorization | daemon | ftp | kernel | local | user);
        file {
            files max-file-number;
            name file-name;
            path binary-log-file-path;
            size maximum-file-size;
        }
        format (binary | sd-syslog | syslog);
        max-database-record <max-database-record>;
        mode (event | stream);
        rate-cap <rate-cap-value>;
        report;
        (source-address source-address | source-interface interface-name);
        stream stream-name {
            category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp
                | rtlog | pst-ds-lite | appqos | secintel);
            file {
                name file-name;
                size file-size;
                rotation max-rotation-number;
            }
            filter {
                threat-attack;
            }
            format (binary | sd-syslog | syslog | welf);
            host {
                ip-address;
                port port-number;
            }
            rate-limit {
                log-rate;
            }
        }
    }

```

```
    severity (alert | critical | debug | emergency | error | info | notice | warning);
}
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag (all | configuration | hpl | report | source);
  no-remote-trace;
}
transport {
  protocol (udp | tcp | tls);
  tcp-connections tcp-connections;
  tls-profile tls-profile-name;
}
utc-timestamp;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

- Options**
- cache**—Cache security log events in the audit log buffer.
 - disable**—Disable the security logging for the device.
 - event-rate** *rate*—Limit the rate at which logs are streamed per second.
 - Range:** 0 through 1500
 - Default:** 1500
 - facility-override**—Alternate facility for logging to remote host.
 - file**—Specify the security log file options for logs in binary format.
 - Values:**
 - **max-file-number**—Maximum number of binary log files.
 - The range is 2 through 10 and the default value is 10.
 - **file-name**—Name of binary log file.
 - **binary-log-file-path**—Path to binary log files.
 - **maximum-file-size**—Maximum size of binary log file in megabytes.
 - The range is 1 through 10 and the default value is 10.
 - format**—Set the security log format for the device.
 - max-database-record**—The following are the disk usage range limits for the database:
 - Range:**
 - SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
 - vSRX: 0 through 1,000,000
 - Default:**
 - SRX1500, SRX4100, and SRX4200: 15,000,000
 - vSRX: 1,000,000



NOTE: Be sure there is enough free space in `/var/log/hostlogs/`, otherwise logs might be dropped when written into the database.

- mode**—Control how security logs are processed and exported.
- rate-cap** *rate-cap-value*—Work with event mode only. This option limits the rate at which data plane logs are generated per second.
 - Range:** 0 through 5000 logs per second
 - Default:** 5000 logs per second
- source-address** *source-address*—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface *interface-name*—Specify a source interface name, which is mandatory to configure *stream host*.



NOTE: The **source-address** and **source-interface** are alternate values. Using one of the options is mandatory.

stream—Every stream can configure file or host.

- **category**— Type of events that might be logged.
- **file name**—Specify the filename.
- **file size**—Specify the file size.
 - SRX1500, SRX4100, and SRX4200—The default value is 25 MB and the range is 10 MB through 50 MB.
 - vSRX - The default value is 2 MB and the range is 1 MB through 3 MB.
- **rotation**—Configure the maximum file number for rotation.
 - The default value is 10 and the range is 2 through 19.
- **rate-limit**—Rate-limit for security logs.
 - The range is 1 through 65,535 logs per second and the default value is 65,535 .
- **filter**—Selects the filter to filter the logs to be logged.
- **format**—Specify the log stream format.
- **host**—Destination to send security logs.
- **severity**—Severity threshold for security logs.

traceoptions—Specify security log daemon trace options.

transport—Set security log transport settings.

utc-timestamp—Specify to use UTC time for security log timestamps.

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

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

logical-system (System Security Profile)

Syntax	<code>logical-system <i>logical-system-name</i>;</code>
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>Specify the user logical system to bind the security profile to.</p> <p>The master administrator uses security profiles to provision logical systems with resources. You can bind security profiles to user logical systems and the master logical system. The master administrator can configure more than one security profile allocating different amounts of a resource in various ones.</p> <p>Only the master administrator can create security profiles and bind them to logical systems.</p>
Options	<i>logical-system-name</i> —Name of the logical system.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

logical-systems

```
Syntax  logical-systems logical-system-name {
        security {
            log {
                cache {
                    exclude;
                    limit;
                }
                disable;
                facility-override {
                    authorization;
                    daemon;
                    ftp;
                    kernel;
                    local;
                    user;
                }
                mode {
                    event;
                    stream;
                }
                format {
                    binary;
                    sd-syslog;
                    syslog;
                }
                source-address;
                source-interface;
                stream stream-name;
                transport {
                    protocol (tcp | tls | udp);
                    tls-profile;
                }
            }
        }
    }
```

Hierarchy Level [edit logical-systems]

Release Information Statement introduced in Junos OS Release 18.2R1.

Description Configure logical-system security log. The **set logical-system logical-system-name security log** command is introduced for logging support on SRX Series devices. The following options are not supported under user logical system:

- **event-rate** and **rate-cap**— Use to limit the log rate between Packet Forwarding Engine (PFE) and Routing Engine (RE).
- **file**— Use to store binary log with event mode.
- **max-database-record** and **report**— Use to enable SQLite Version 3 (sqlite3) database for local log management daemon (llmd).

- **traceoptions**—Specify security log daemon trace options.

Options

cache—Cache security log events in the audit log buffer.

disable—Disable the security logging for the device.

facility-override —Alternate facility for logging to remote host.

format—Set security log format for the device.

mode—Controls how security logs are processed and exported.

source-address —Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface —Specify a source interface name, which is mandatory to configure *stream host*.

stream—Set security log stream settings.

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.

Related Documentation

- [Understanding Security Logs and Logical Systems on page 345](#)

logical-systems (All)

Syntax `logical-systems {
 logical-system-name {
 ...logical-system-configuration...
 }
 }`

Hierarchy Level `[edit]`

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure a logical system. Only the master administrator can configure a logical system at `[edit]` hierarchy level.

You can include several of the hierarchies that can be included at the `[edit]` hierarchy level. For descriptions of the applicable statements, see the appropriate hierarchies.



NOTE: The `logical-systems` configuration statement can be used only by the master administrator.

Options `logical-system-name`—Name of the logical system.

Required Privilege all—To view this statement in the configuration.
Level all—To add this statement to the configuration.

Related Documentation

- [Understanding Logical Systems for SRX Series Services Gateways on page 26](#)

nat

```

Syntax  nat {
        destination {
            pool pool-name {
                address ip-address {
                    (port port-number | to ip-address);
                }
                description text;
                routing-instance routing-instance-name;
            }
            rule-set rule-set-name {
                description text;
                from {
                    interface [interface-name];
                    routing-instance [routing-instance-name];
                    zone [zone-name];
                }
                rule rule-name {
                    description text;
                    match {
                        (destination-address <ip-address> | destination-address-name <address-name>);
                        destination-port port-number;
                        protocol [protocol-name-or-number];
                        source-address [ip-address];
                        source-address-name [address-name];
                    }
                    then {
                        destination-nat (off | pool pool-name);
                    }
                }
            }
        }
    }
    proxy-arp {
        interface interface-name {
            address ip-address {
                to ip-address;
            }
        }
    }
    proxy-ndp {
        interface interface-name {
            address ip-address {
                to ip-address;
            }
        }
    }
    source {
        address-persistent;
        interface {
            port-overloading {
                off;
            }
        }
    }
}

```

```
pool pool-name {
    address ip-address {
        to ip-address;
    }
    description text;
    host-address-base ip-address;
    overflow-pool (interface | pool-name);
    port {
        (no-translation | port-overloading-factor number | range port-low <to port-high>);
    }
    routing-instance routing-instance-name;
}
pool-default-port-range lower-port-range to upper-port-range;
pool-utilization-alarm {
    clear-threshold value;
    raise-threshold value;
}
port-randomization {
    disable;
}
port-round-robin {
    disable;
}
rule-set rule-set-name {
    description text;
    from {
        interface [interface-name];
        routing-instance [routing-instance-name];
        zone [zone-name];
    }
    rule rule-name {
        description text;
        match {
            (destination-address <ip-address> | destination-address-name <address-name>);
            destination-port port-number;
            protocol [protocol-name-or-number];
            source-address [ip-address];
            source-address-name [address-name];
        }
        then {
            source-nat {
                interface {
                    persistent-nat {
                        address-mapping;
                        inactivity-timeout seconds;
                        max-session-number value;
                        permit (any-remote-host | target-host | target-host-port);
                    }
                }
            }
            off;
            pool {
                persistent-nat {
                    address-mapping;
                    inactivity-timeout seconds;
                    max-session-number number;
                    permit (any-remote-host | target-host | target-host-port);
                }
            }
        }
    }
}
```

Copyright © 2018, Juniper Networks, Inc. 513

Hierarchy Level	[edit security] [edit tenant <i>tenant-name</i> security]
Release Information	Statement modified in Junos OS Release 9.6. The description option added in Junos OS Release 12.1. The tenant option is introduced in Junos OS Release 18.3R1.
Description	Configure Network Address Translation (NAT) for SRX Series devices.
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	<ul style="list-style-type: none"> • <i>Introduction to NAT</i> • Understanding Logical Systems Network Address Translation on page 117

nat-cone-binding

Syntax	<pre> nat-cone-binding { 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 11.2.
Description	<p>Specify the number of NAT cone binding configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Introduction to NAT</i>

nat-destination-pool

Syntax	<pre>nat-destination-pool { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>] [edit tenant <i>tenant-name</i> system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. The tenant option is introduced in Junos OS Release 18.3R1.
Description	<p>Specify the number of NAT destination pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Introduction to NAT</i>

nat-destination-rule

Syntax	<pre> nat-destination-rule { maximum <i>amount</i>; reserved <i>amount</i>; } </pre>
Hierarchy Level	<pre> [edit system security-profile <i>security-profile-name</i>] [edit tenant <i>tenant-name</i> system security-profile <i>security-profile-name</i>] </pre>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>The tenant option is introduced in Junos OS Release 18.3R1.</p>
Description	<p>Specify the number of NAT destination rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Introduction to NAT</i>

nat-interface-port-ol (System)

Syntax	<pre>nat-interface-port-ol { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the security NAT interface port overloading the quota of a logical system.
Options	<ul style="list-style-type: none">• maximum <i>amount</i>—Specify the maximum allowed quota value. Range: 0 through 64• reserved <i>amount</i>—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	<ul style="list-style-type: none">• <i>Introduction to NAT</i>

nat-nopat-address

Syntax	<pre> nat-nopat-address { 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 11.2.
Description	<p>Specify the number of NAT without port address translation configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Introduction to NAT</i>

nat-pat-address

Syntax	<pre>nat-pat-address { 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 11.2.
Description	<p>Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems Network Address Translation on page 117• Introduction to NAT

nat-pat-portnum

Syntax	<pre> nat-pat-portnum { maximum <i>amount</i>; reserved <i>amount</i>; } </pre>
Hierarchy Level	[edit system security-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile. The total number of PAT pools must not exceed the configured maximum ports for the logical system.
Options	<p>maximum <i>amount</i>—Specify the maximum number of ports allowed for a logical system. The maximum quantity is not guaranteed and is shared among multiple logical systems.</p> <p>reserved <i>amount</i>—Specify the number of resources guaranteed for a logical system.</p> <p>Range: For SRX5600 and SRX5800 devices, up to 402,653,184 ports are supported. Pool specifications for logical systems can be viewed using the show security nat source summary logical-system all command.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Logical Systems for SRX Series Services Gateways on page 26

nat-port-ol-ipnumber

Syntax	<pre>nat-port-ol-ipnumber { 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 11.2.
Description	<p>Specify the number of NAT port overloading IP number configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

nat-rule-referenced-prefix (System)

Syntax	<pre>nat-rule-referenced-prefix { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the security NAT rule referenced IP prefix quota of a logical system.
Options	<ul style="list-style-type: none">• maximum <i>amount</i> —Specify the maximum allowed quota value. Range: 0 through 1,048,576• reserved <i>amount</i> —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	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

nat-source-pool

Syntax	<pre>nat-source-pool { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>] [edit tenant <i>tenant-name</i> system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. The tenant option is introduced in Junos OS Release 18.3R1.
Description	<p>Specify the NAT source pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

nat-source-rule

Syntax	<pre> nat-source-rule { maximum <i>amount</i>; reserved <i>amount</i>; } </pre>
Hierarchy Level	<pre> [edit system security-profile <i>security-profile-name</i>] [edit tenant <i>tenant-name</i> system security-profile <i>security-profile-name</i>] </pre>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>The tenant option is introduced in Junos OS Release 18.3R1.</p>
Description	<p>Specify the NAT source rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Logical Systems for SRX Series Services Gateways on page 26

nat-static-rule

Syntax	<pre>nat-static-rule { maximum <i>amount</i>; reserved <i>amount</i>; }</pre>
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>] [edit tenant <i>tenant-name</i> system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. The tenant option is introduced in Junos OS Release 18.3R1.
Description	<p>Specify the number of NAT static rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

policies

```

Syntax  policies {
        default-policy (deny-all | permit-all);
        from-zone zone-name to-zone zone-name {
            policy policy-name {
                description description;
                match {
                    application {
                        [application];
                        any;
                    }
                    destination-address {
                        [address];
                        any;
                        any-ipv4;
                        any-ipv6;
                    }
                    source-address {
                        [address];
                        any;
                        any-ipv4;
                        any-ipv6;
                    }
                    source-identity {
                        [role-name];
                        any;
                        authenticated-user;
                        unauthenticated-user;
                        unknown-user;
                    }
                }
            }
            scheduler-name scheduler-name;
            then {
                count {
                    alarm {
                        per-minute-threshold number;
                        per-second-threshold number;
                    }
                }
                deny;
                log {
                    session-close;
                    session-init;
                }
                permit {
                    application-services {
                        application-firewall {
                            rule-set rule-set-name;
                        }
                    }
                    application-traffic-control {
                        rule-set rule-set-name;
                    }
                    gprs-gtp-profile profile-name;
                }
            }
        }
    }

```

```
    gprs-sctp-profile profile-name;  
    idp;  
    idp-policy idp-policy;  
    redirect-wx | reverse-redirect-wx;  
    ssl-proxy {  
        profile-name profile-name;  
    }  
    uac-policy {  
        captive-portal captive-portal;  
    }  
    utm-policy policy-name;  
}  
destination-address {  
    drop-translated;  
    drop-untranslated;  
}  
firewall-authentication {  
    pass-through {  
        access-profile profile-name;  
        client-match user-or-group-name;  
        ssl-termination-profile profile-name;  
        web-redirect;  
        web-redirect-to-https;  
    }  
    user-firewall {  
        access-profile profile-name;  
        domain domain-name  
        ssl-termination-profile profile-name;  
    }  
    web-authentication {  
        client-match user-or-group-name;  
    }  
}  
services-offload;  
tcp-options {  
    sequence-check-required;  
    syn-check-required;  
}  
tunnel {  
    ipsec-group-vpn group-vpn;  
    ipsec-vpn vpn-name;  
    pair-policy pair-policy;  
}  
}  
reject;  
}  
}  
}  
global {  
    policy policy-name {  
        description description;  
        match {  
            application {  
                [application];  
                any;  
            }  
        }  
    }  
}
```



```

destination-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
from-zone {
    [zone-name];
    any;
}
source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
source-identity {
    [role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
}
to-zone {
    [zone-name];
    any;
}
}
scheduler-name scheduler-name;
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        idp-policy idp-policy;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
            profile-name profile-name;
        }
    }
}

```

```

    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    initial-tcp-mss mss-value;
    reverse-tcp-mss mss-value;
    sequence-check-required;
    syn-check-required;
}
}
reject;
}
}
}
policy-rematch;
policy-stats {
    system-wide (disable | enable) ;
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5.

Support for the **services-offload** option added in Junos OS Release 11.4.

Support for the **source-identity** option added in Junos OS Release 12.1.

Support for the **description** option added in Junos OS Release 12.1.

Support for the **ssl-termination-profile** and **web-redirect-to-https** options are added starting from Junos OS Release 12.1X44-D10 and Junos OS Release 15.1X49-D40.

Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.

Support for the **domain** option, and for the **from-zone** and **to-zone** global policy match options, added in Junos OS Release 12.1X47-D10.

Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Support for the **extensive** option for **policy-rematch** added in Junos OS Release 15.1X49-D20.

Starting in Junos OS Release 18.2R1, an IDP policy is available within unified security policy. The IDP policy access is simplified and made available under the unified policy as one of the policy. When an IDP policy is available within a unified security policy, configuring source or destination address, source and destination-except, from and to zone, or application is not required, because the match happens in the security policy itself.

Starting in Junos OS Release 18.3R1, when an SRX Series device is configured with a unified policies, you can configure multiple IDP policies and set one of those policies as the default IDP policy. If multiple IDP policies are configured for a session and when policy conflict occurs, the device applies the default IDP policy for that session and thus resolves any policy conflicts.



NOTE: If you have configured two or more IDP policies in a unified security policy, then you must configure the default IDP policy.

Description Configure network security policies.

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

Related Documentation

- *Security Policies Overview*

policy (System Security Profile)

Syntax	<pre>policy { 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 11.2.
Description	<p>Specify the number of security policies that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

policy-with-count

Syntax	<pre>policy-with-count { 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 11.2.
Description	<p>Specify the number of security policies with a count that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Logical Systems for SRX Series Services Gateways on page 26

profile (Access)

```
Syntax  profile profile-name {
        accounting {
            accounting-stop-on-access-deny;
            accounting-stop-on-failure;
            coa-immediate-update;
            duplication;
            immediate-update;
            order [accounting-method];
            statistics (time | volume-time);
            update-interval minutes;
        }
        accounting-order [accounting-method];
        address-assignment pool pool-name;
        authentication-order [ldap | none | password | securid];
        authorization-order [jsrc];
        client client-name {
            chap-secret chap-secret;
            client-group [ group-names ];
            firewall-user {
                password password;
            }
            no-rfc2486;
            pap-password pap-password;
            x-auth ip-address;
        }
        client-name-filter {
            count number;
            domain-name domain-name;
            separator special-character;
        }
        ldap-options {
            assemble {
                common-name common-name;
            }
            base-distinguished-name base-distinguished-name;
            revert-interval seconds;
            search {
                admin-search {
                    distinguished-name distinguished-name;
                    password password;
                }
                search-filter search-filter-name;
            }
        }
        ldap-server server-address {
            port port-number;
            retry attempts;
            routing-instance routing-instance-name;
            source-address source-address;
            timeout seconds;
        }
        provisioning-order (gx-plus | jsrc);
    }
```

```

service {
  accounting-order {
    activation-protocol;
    radius;
  }
}
session-options {
  client-group [group-name];
  client-idle-timeout minutes;
  client-session-timeout minutes;
}
}

```

Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Create a profile containing a set of attributes that define device management access.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Understanding Interfaces</i> • <i>Understanding User Authentication for Security Devices</i> • <i>Ethernet Switching and Layer 2 Transparent Mode Overview</i>

[purging](#)

Syntax	purging;
Hierarchy Level	[edit system arp]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Purge obsolete ARP entries from the cache when an interface or link goes offline.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

root-authentication

Syntax

```
root-authentication {  
    encrypted-password password;  
    load-key-file URL;  
    plain-text-password;  
    ssh-dsa public-key {  
        <from pattern-list>;  
    }  
    ssh-rsa public-key {  
        <from pattern-list>;  
    }  
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify authentication information for the root login.

- Options**
- **encrypted-password *password***—Specify the encrypted authentication password. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.
 - **plain-text-password**—The CLI prompts you for a password encrypts it, and stores the encrypted version in its user database.
 - **load-key-file *URL***—File URL containing one or more SSH keys.
 - **ssh-dsa *public-key***—SSH DSA public key string.
 - **from *pattern-list***—Pattern list of allowed hosts.
 - **ssh-rsa *public-key***—SSH RSA public key string.
 - **from *pattern-list***—Pattern list of allowed hosts.

Required Privilege Level

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

root-logical-system

Syntax	root-logical-system;
Hierarchy Level	[edit system security-profile <i>security-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>Specify root-logical-system to bind the security profile to the master logical system.</p> <p>The master administrator uses security profiles to provision logical systems with resources. The security profile containing this statement must be bound to root-logical-system only.</p> <p>Only the master administrator can create security profiles and bind them to logical systems.</p>
Options	none
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

scheduler (System Security Profile)

Syntax	<pre>scheduler { 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 11.2.
Description	<p>Specify the number of schedulers that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system.• can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems for SRX Series Services Gateways on page 26

screen (Security)

```
Syntax  screen {
        ids-option screen-name {
            alarm-without-drop;
            description text;
            icmp {
                flood {
                    threshold number;
                }
                fragment;
                icmpv6-malformed;
                ip-sweep {
                    threshold number;
                }
                large;
                ping-death;
            }
            ip {
                bad-option;
                block-frag;
                ipv6-extension-header {
                    AH-header;
                    ESP-header;
                    HIP-header;
                }
                destination-header {
                    ILNP-nonce-option;
                    home-address-option;
                    line-identification-option;
                    tunnel-encapsulation-limit-option;
                    user-defined-option-type <type-low> to <type-high>;
                }
                fragment-header;
                hop-by-hop-header {
                    CALIPSO-option;
                    RPL-option;
                    SFM-DPD-option;
                    jumbo-payload-option;
                    quick-start-option;
                    router-alert-option;
                    user-defined-option-type <type-low> to <type-high>;
                }
                mobility-header;
                no-next-header;
                routing-header;
                shim6-header
                user-defined-option-type <type-low> to <type-high>;
            }
        }
        ipv6-extension-header-limit limit;
        ipv6-malformed-header;
        loose-source-route-option;
        record-route-option;
        security-option;
    }
```

```
source-route-option;
spoofing;
stream-option;
strict-source-route-option;
tear-drop;
timestamp-option;
unknown-protocol;
tunnel {
    gre {
        gre-4in4;
        gre-4in6;
        gre-6in4;
        gre-6in6;
    }
    ip-in-udp {
        teredo;
    }
    ipip {
        ipip-4in4;
        ipip-4in6;
        ipip-6in4;
        ipip-6in6;
        ipip-6over4;
        ipip-6to4relay;
        isatap;
        dslite;
    }
    bad-inner-header;
}
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
}
syn-frag;
```


Options **ids-options screen-name**—Name of the screen configured at the **security screen ids-options** level. Define screens for the intrusion detection service (IDS).

trap—Configure trap interval. Enable or disable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes. Traps are unsolicited messages sent from an SNMP agent to remote network management systems or trap receivers.

white-list—Set of IP addresses for white list. Configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process. A whitelist contains known trusted IP addresses and URLs. Content downloaded from locations on the whitelist does not have to be inspected for malware.

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 • *Attack Detection and Prevention Overview*


security-profile

```
Syntax  security-profile security-profile-name {
    address-book {
        maximum amount;
        reserved amount;
    }
    appfw-profile {
        maximum amount;
        reserved amount;
    }
    appfw-rule {
        maximum amount;
        reserved amount;
    }
    appfw-rule-set {
        maximum amount;
        reserved amount;
    }
    auth-entry {
        maximum amount;
        reserved amount;
    }
    cpu {
        reserved percent;
    }
    dslite-software-initiator {
        maximum amount;
        reserved amount;
    }
    flow-gate {
        maximum amount;
        reserved amount;
    }
    flow-session {
        maximum amount;
        reserved amount;
    }
    icap-redirect-profile {
        maximum amount;
        reserved amount;
    }
    idp-policy idp-policy-name;
    logical-system [logical-system-name];
    nat-cone-binding {
        maximum amount;
        reserved amount;
    }
    nat-destination-pool {
        maximum amount;
        reserved amount;
    }
    nat-destination-rule {
        maximum amount;
    }
}
```

```
    reserved amount;  
  }  
  nat-interface-port-ol {  
    maximum amount;  
    reserved amount;  
  }  
  nat-nopat-address {  
    maximum amount;  
    reserved amount;  
  }  
  nat-pat-address {  
    maximum amount;  
    reserved amount;  
  }  
  nat-pat-portnum {  
    maximum amount  
    reserved amount  
  }  
  nat-port-ol-ipnumber {  
    maximum amount;  
    reserved amount;  
  }  
  nat-rule-referenced-prefix {  
    maximum amount;  
    reserved amount;  
  }  
  nat-source-pool {  
    maximum amount;  
    reserved amount;  
  }  
  nat-source-rule {  
    maximum amount;  
    reserved amount;  
  }  
  nat-static-rule {  
    maximum amount;  
    reserved amount;  
  }  
  policy {  
    maximum amount;  
    reserved amount;  
  }  
  policy-with-count {  
    maximum amount;  
    reserved amount;  
  }  
  root-logical-system;  
  scheduler {  
    maximum amount;  
    reserved amount;  
  }  
  zone {  
    maximum amount;  
    reserved amount;  
  }
```


Hierarchy Level	[edit system] [edit tenants <tenant-name>]
Release Information	Statement introduced in Junos OS Release 11.2. The dslite-softwire-initiator option introduced in Junos OS Release 12.1. The security-profile option added under the tenants hierarchy in Junos OS Release 18.3R1. The icap redirect profile option is introduced in Junos OS Release 18.3R1.
Description	<p>Create a security profile and specify the kinds and amounts of resources to allocate to a logical system to which the security profile is bound.</p> <p>As a master administrator, you can create a security profile and bind it to more than one logical system if you want to allocate the same kinds and amounts of resources to them. For details on how many security profiles you can create, see “Understanding Logical Systems Security Profiles (Master Administrators Only)” on page 73. When you reach the limit, you must delete a security profile and commit the configuration before you can create and commit the configuration for another security profile.</p> <p>Only the master administrator can create security profiles.</p>
Options	<ul style="list-style-type: none">• security-profile-name—Name of the security profile. <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems Security Profiles (Master Administrators Only) on page 73• Example: Configuring Logical Systems Security Profiles (Master Administrators Only) on page 79

security-profile-resources

Syntax	<pre>security-profile-resources { cpu-control; cpu-control-target <i>percent</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure global settings that apply to all logical systems in the device.
Options	<p>cpu-control—Enable CPU utilization control.</p> <p>cpu-control-target <i>percent</i>—Specify the upper limit for CPU utilization on the device under normal operating conditions.</p> <p>Range: 0 through 100 percent (decimal point allowed).</p> <p>Default: 80 percent.</p> <div><div></div><div><p>NOTE: The cpu-control option must be specified for the cpu-control-target value to take effect.</p></div></div>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding Logical Systems Security Profiles (Master Administrators Only) on page 73• Example: Configuring Logical Systems Security Profiles (Master Administrators Only) on page 79

stream (logical-systems security log)

Syntax	<pre> stream <i>name</i> { category <i>name</i>; file { allow-duplicates; name; rotation; size; } filter <i>name</i>; format (binary sd-syslog syslog welf); host <i>port</i>; rate-limit <i>rate</i>; severity (alert critical debug emergency error info notice warning); } </pre>
Hierarchy Level	[edit logical-systems <i>name</i> security log]
Release Information	Statement introduced in Junos OS Release 18.2R1.
Description	Defines the set security log stream settings. When the logging mode is set to stream , security logs generated in the data plane are streamed out a revenue traffic port directly to a remote server. All the categories can be configured for sending specific category logs to different log servers for stream mode log forwarding.
Options	<p>category—Type of logged events.</p> <p>filter—Selects the filter to filter the logs to be logged.</p> <p>format—Specify the log stream format.</p> <p>host—Destination to send security logs.</p> <p>rate-limit—Rate-limit for security logs. Range: 1 through 65535 Default: 65535</p> <p>severity—Severity threshold for security logs.</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"> logical-systems security log

softwires

Syntax

```
softwires {
  softwire-name name {
    softwire-concentrator ipv6-address;
    softwire-type IPv4-in-IPv6;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | flow);
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 12.1.

Description Configure softwires for IPv6 dual-stack lite (DS-Lite). DS-Lite allows migration to an IPv6 access network without changing end-user software. IPv4 users can continue to access IPv4 internet content using their current hardware, while IPv6 users are able to access IPv6 content.

- Options**
- **softwire-name *name***—Name of the softwire configuration.
 - **softwire-concentrator *ipv6-address***—IPv6 address of the concentrator.
 - **softwire-type**—Must be IPv4-in-IPv6.

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.

web-filtering (Logical System Security Feature Profile)

```
Syntax  web-filtering {
        juniper-enhanced {
            profile name {
                base-filter base-filter;
                block-message {
                    type custom-redirect-url;
                    url url;
                }
                category name {
                    action (block | log-and-permit | permit | quarantine);
                    custom-message custom-message;
                }
                custom-block-message custom-block-message;
                default (block | log-and-permit | permit | quarantine);
                fallback-settings {
                    default (block | log-and-permit);
                    server-connectivity (block | log-and-permit);
                    timeout (block | log-and-permit);
                    too-many-requests (block | log-and-permit);
                }
                no-safe-search;
                quarantine-custom-message quarantine-custom-message;
                quarantine-message {
                    type custom-redirect-url;
                    url url;
                }
                site-reputation-action {
                    fairly-safe (block | log-and-permit | permit | quarantine);
                    harmful (block | log-and-permit | permit | quarantine);
                    moderately-safe (block | log-and-permit | permit | quarantine);
                    suspicious (block | log-and-permit | permit | quarantine);
                    very-safe (block | log-and-permit | permit | quarantine);
                }
                timeout seconds;
            }
        }
        juniper-local {
            profile name {
                block-message {
                    type custom-redirect-url;
                    url url;
                }
                category name {
                    action (block | log-and-permit | permit | quarantine);
                    custom-message custom-message;
                }
                custom-block-message custom-block-message;
                default (block | log-and-permit | permit);
                fallback-settings {
                    default (block | log-and-permit);
                    server-connectivity (block | log-and-permit);
                    timeout (block | log-and-permit);
                }
            }
        }
    }
```

```

        too-many-requests (block | log-and-permit);
    }
    quarantine-custom-message quarantine-custom-message;
    quarantine-message {
        type custom-redirect-url;
        url url;
    }
    timeout seconds;
}
}
websense-redirect {
    profile name {
        account account;
        block-message {
            type custom-redirect-url;
            url url;
        }
        category name {
            action (block | log-and-permit | permit | quarantine);
            custom-message custom-message;
        }
        custom-block-message custom-block-message;
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        quarantine-custom-message quarantine-custom-message;
        quarantine-message {
            type custom-redirect-url;
            url url;
        }
        server {
            host host;
            port port;
            routing-instance routing-instance;
        }
        sockets sockets;
        timeout seconds;
    }
}
}

```

Hierarchy Level [edit logical-systems *logical-systems-name* security utm feature-profile]

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Configures the UTM Web filtering feature for logical systems. The Web filtering allows you to manage Internet usage by preventing access to inappropriate Web content. The potential policies conflict check of the Web filtering feature is independent of the content filtering, antivirus, and antispam features. You can also configure the default UTM configuration for Web filtering feature profile. If you do not configure any option in the Web filtering feature profile, the values configured in the default UTM configuration are applied.

- Options**
- juniper-enhanced**—Enables Enhanced Web Filtering (EWF) on the device.
 - base-filter**—A base filter is an object that contains a category-action pair for all categories defined in the category file.
 - block-message**—Juniper enhanced block message settings.
 - category**—Select a custom URL category list you created (custom objects) for filtering against.
 - custom-block-message**—Enter a custom message to be sent when HTTP requests are blocked.
 - default**—Specify an action for the profile, for requests that experience internal errors in the Web filtering module.
 - fallback-settings**—Fallback settings helps the system how to handle errors.
 - no-safe-search**— Do not perform safe-search for Juniper enhanced protocol. Safe-search redirect supports HTTP only. Therefore it is not possible to generate a redirect response for HTTPS search URLs. Safe-search redirects can be disabled by using the CLI option **no-safe-search**.
 - quarantine-custom-message**—Juniper enhanced quarantine custom message.
 - quarantine-message**—Juniper enhanced quarantine message settings.
 - server**—Set server parameters by entering the server name or IP address.
 - site-reputation-action**—Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.
 - timeout**—Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied.
Range: 1 through 1800
 - juniper-local**—Enables Juniper Networks local URL filtering on the device.
 - block-message**—Juniper local block message settings.
 - websense-redirect**—Web filtering websense redirect engine. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.
 - type**—Type of Web filtering solution or URL filtering solution used by the device.

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**
- [Unified Threat Management Overview](#)
 - [utm default-configuration](#)

zone (System Security Profile)

Syntax	<pre>zone { 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 11.2.
Description	<p>Specify the zones that user logical system administrators and master logical system administrators can configure for their logical systems if 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 user logical systems and the master logical system. • can configure more than one security profile, specifying different amounts of resource allocations 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 utilize 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>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Logical Systems Security Profiles (Master Administrators Only) on page 73 • Example: Configuring Logical Systems Security Profiles (Master Administrators Only) on page 79

zones

```

Syntax  zones {
        functional-zone {
            management {
                description text;
                host-inbound-traffic {
                    protocols protocol-name {
                        except;
                    }
                    system-services service-name {
                        except;
                    }
                }
            }
            interfaces interface-name {
                host-inbound-traffic {
                    protocols protocol-name {
                        except;
                    }
                    system-services service-name {
                        except;
                    }
                }
            }
            screen screen-name;
        }
    }
    security-zone zone-name {
        address-book {
            address address-name {
                ip-prefix {
                    description text;
                }
                description text;
                dns-name domain-name {
                    ipv4-only;
                    ipv6-only;
                }
                range-address lower-limit to upper-limit;
                wildcard-address ipv4-address/wildcard-mask;
            }
            address-set address-set-name {
                address address-name;
                address-set address-set-name;
                description text;
            }
        }
        advance-policy-based-routing;
        application-tracking;
        description text;
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
        }
    }

```

```

        system-services service-name {
            except;
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
    tcp-rst;
}

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:

- Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.
- Security zone—Most common type of zone that is used as a building block in policies.

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

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

Related Documentation

- *Security Zones Overview*
- *Supported System Services for Host Inbound Traffic*

CHAPTER 5

Operational Commands

- clear security application-firewall rule-set statistics logical-system
- clear security dns-cache
- clear security firewall-authentication users
- clear security firewall-authentication history
- clear security idp attack table
- clear security idp counters ips
- clear security idp counters pdf-decoder
- clear security idp counters ssl-inspection
- clear security idp counters memory
- clear security idp counters memory
- clear security idp counters tcp-reassembler
- clear security idp counters application-identification
- clear security idp counters action
- clear security idp counters dfa
- clear security idp counters flow
- clear security idp counters log
- clear security idp counters http-decoder
- clear security idp counters packet-log
- clear security idp counters packet
- clear security idp counters policy-manager
- clear security flow session tenant
- request security datapath-debug capture start
- request security datapath-debug capture stop
- set chassis cluster cluster-id node node-number reboot
- show chassis cluster status
- show log
- show route tenant
- show security application-firewall rule-set

- `show security application-firewall rule-set logical-system`
- `show security application-tracking counters`
- `show security alg status logical-system`
- `show security datapath-debug capture`
- `show security datapath-debug counter`
- `show security dns-cache`
- `show security firewall-authentication history`
- `show security firewall-authentication users`
- `show security flow session`
- `show security flow session tenant`
- `show security idp logical system`
- `show security idp attack table`
- `show security idp counters action`
- `show security idp counters application-identification`
- `show security idp counters memory`
- `show security idp counters ssl-inspection`
- `show security idp counters pdf-decoder`
- `show security idp counters log`
- `show security idp counters ips`
- `show security idp counters dfa`
- `show security idp counters flow`
- `show security idp counters http-decoder`
- `show security idp counters packet-log`
- `show security idp counters packet`
- `show security idp counters policy-manager`
- `show security idp counters tcp-reassembler`
- `show security idp logical-system policy-association`
- `show security idp policies`
- `show security idp policy-commit-status`
- `show security idp policy-templates-list`
- `show security idp security-package-version`
- `show security ike security-associations`
- `show security ipsec security-associations`
- `show security match-policies`
- `show security nat destination rule`
- `show security nat destination summary`
- `show security nat source rule`

- `show security nat source summary`
- `show security nat static rule`
- `show security policies`
- `show security screen statistics`
- `show services user-identification authentication-table`
- `show system security-profile`
- `show system security-profile scheduler`
- `show system security-profile security-log-stream-number detail logical-system all`
- `show system security-profile security-log-stream-number logical-system all`
- `show system security-profile security-log-stream-number summary`
- `show security softwires`
- `show security zones`

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

Syntax The master, or root, administrator can issue the following statements:

```
clear security application-firewall rule-set statistics [logical-system logical-system-name |  
all | root-logical-system]
```

The user logical system administrator can issue the following statement:

```
clear security application-firewall rule-set statistics all
```

Release Information Command introduced in Junos OS Release 11.4.

Description Clear all security application firewall rule set statistics.



NOTE: User logical system administrators can clear statistics only for the logical systems they can access. For information about master and user administrator roles in logical systems, see [“Understanding the Master Logical Systems and the Master Administrator Role” on page 40](#).

Starting in Junos OS Release 18.2R1 application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Options *logical-system-name*—Name of a specific logical system.

all—(default) Clear all rule set statistics for a specific logical system or all logical systems.

root-logical-system—Clear application firewall rule set statistics on the root logical system (master administrator only).

Required Privilege Level clear

Related Documentation

- [show security application-firewall rule-set logical-system on page 598](#)

Output Fields This command produces no output.

clear security dns-cache

Syntax clear security dns-cache <dns-name *dns-name*>

Release Information Command introduced in Junos OS Release 12.1X44-D10.

Description Reset DNS cache information.



NOTE: This command is only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

Options

- **dns-name**—Clear DNS cache information for the specified name.

Required Privilege Level clear

Related Documentation

- [show security dns-cache on page 607](#)
- [Understanding the Master Logical Systems and the Master Administrator Role on page 40](#)

clear security firewall-authentication users

Syntax	<pre>clear security firewall-authentication users <node (node-id all local primary)> <address> <identifier> <logical-system (logical-system-name all)> <root-logical-system (address auth-type from-zone identifier tenant to-zone)> <tenant (tenant-name all)></pre>
Release Information	Command introduced in Junos OS Release 8.5. The node options added in Junos OS Release 9.0. The tenant option introduced in Junos OS Release 18.3R1.
Description	Clear firewall authentication tables for all users.
Options	<ul style="list-style-type: none">• node—(Optional) For chassis cluster configurations, clear firewall authentication details for all users on a specific node.<ul style="list-style-type: none">• node-id—Identification number of the node. It can be 0 or 1.• all—Clear all nodes.• local—Clear the local node.• primary—Clear the primary node.• address—Display authentication entries based on ip address.• identifier—Display authentication entries by id.• logical-system—Display firewall authentication tables based on logical system name.• node—(Optional) For chassis cluster configurations, display firewall authentication details for all users on a specific node.<ul style="list-style-type: none">• node-id—Identification number of the node. It can be 0 or 1.• all—Display information about all nodes.• local—Display information about the local node.• primary—Display information about the primary node.• root-logical-system—Display firewall authentication tables for root logical system.• tenant—Display firewall authentication tables based on tenant name.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>Firewall User Authentication Overview</i>• show security firewall-authentication users on page 612

List of Sample Output [clear security firewall-authentication users on page 563](#)
 [clear security firewall-authentication users node 1 on page 563](#)
 [clear security firewall-authentication users tenant all on page 563](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

 This command produces no output.

Sample Output

[clear security firewall-authentication users](#)

```
user@host> clear security firewall-authentication users node 1
node0:
-----
node1:
-----
```

Sample Output

[clear security firewall-authentication users node 1](#)

```
user@host> clear security firewall-authentication users node 1
node1:
-----
```

[clear security firewall-authentication users tenant all](#)

```
user@host> clear security firewall-authentication users tenant all
```

clear security firewall-authentication history

Syntax	<pre>clear security firewall-authentication history <node (node-id all local primary)> <address> <identifier> <logical-system (logical-system-name all)> <root-logical-system (address auth-type from-zone identifier tenant to-zone)> <tenant (tenant-name all)></pre>
Release Information	Command introduced in Junos OS Release 8.5. The node options added in Junos OS Release 9.0. The tenant option introduced in Junos OS Release 18.3R1.
Description	Clear all firewall authentication history information.
Options	<ul style="list-style-type: none">• node—(Optional) For chassis cluster configurations, clear all firewall authentication history on a specific node (device) in the cluster.<ul style="list-style-type: none">• node-id—Identification number of the node. It can be 0 or 1.• all—Clear all nodes.• local—Clear the local node.• primary—Clear the primary node.• address—Display authentication entries based on ip address.• identifier—Display authentication entries by id.• logical-system—Display firewall authentication tables based on logical system name.• node—(Optional) For chassis cluster configurations, display firewall authentication details for all users on a specific node.<ul style="list-style-type: none">• node-id—Identification number of the node. It can be 0 or 1.• all—Display information about all nodes.• local—Display information about the local node.• primary—Display information about the primary node.• root-logical-system—Display firewall authentication tables for root logical system.• tenant—Display firewall authentication tables based on tenant name.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>Firewall User Authentication Overview</i>• show security firewall-authentication history on page 609

List of Sample Output [clear security firewall-authentication history on page 565](#)
 [clear security firewall-authentication history node 1 on page 565](#)
 [clear security firewall-authentication history tenant all on page 565](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

 This command produces no output.

Sample Output

[clear security firewall-authentication history](#)

```
user@host> clear security firewall-authentication history
node0:
-----
node1:
-----
```

Sample Output

[clear security firewall-authentication history node 1](#)

```
user@host> clear security firewall-authentication history node 1
node1:
-----
```

[clear security firewall-authentication history tenant all](#)

```
user@host> clear security firewall-authentication history tenant all
```

clear security idp attack table

Syntax	clear security idp attack table clear security idp attack table logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Clear details of the IDP attack table.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp attack table on page 625
Output Fields	This command produces no output.

clear security idp counters ips

Syntax	clear security idp counters ips clear security idp counters ips logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Reset all the ips counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>ips</i>• show security idp counters ips on page 642
Output Fields	This command produces no output.

clear security idp counters pdf-decoder

Syntax	clear security idp counters pdf-decoder clear security idp counters pdf-decoder logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the PDF-Decode enabled sessions.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters pdf-decoder on page 636
Output Fields	This command produces no output.

clear security idp counters ssl-inspection

Syntax	clear security idp counters ssl-inspection clear security idp counters ssl-inspection logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the session encryption and decryption values for IDP counters.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters ssl-inspection on page 634
Output Fields	This command produces no output.

clear security idp counters memory

Syntax	clear security idp counters memory clear security idp counters memory logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the memory allocation and reallocation counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters memory on page 632
Output Fields	This command produces no output.

clear security idp counters memory

Syntax	clear security idp counters memory clear security idp counters memory logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the memory allocation and reallocation counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters memory on page 632
Output Fields	This command produces no output.

clear security idp counters tcp-reassembler

Syntax	clear security idp counters tcp-reassembler clear security idp counters tcp-reassembler logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Reset all the TCP reassembler counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>re-assembler</i>• show security idp counters tcp-reassembler on page 665
Output Fields	This command produces no output.

clear security idp counters application-identification

Syntax	clear security idp counters application-identification clear security idp counters application-identification logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Reset all the application identification counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>application-identification</i>• show security idp counters application-identification on page 628
Output Fields	This command produces no output.

clear security idp counters action

Syntax	clear security idp counters action clear security idp counters action logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the action counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters action on page 626
Output Fields	This command produces no output.

clear security idp counters dfa

Syntax	clear security idp counters dfa clear security idp counters dfa logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the DFA counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters dfa on page 646
Output Fields	This command produces no output.

clear security idp counters flow

Syntax	clear security idp counters flow clear security idp counters flow logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the IDP flow-related counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>flow (Security IDP)</i>• show security idp counters flow on page 648
Output Fields	This command produces no output.

clear security idp counters log

Syntax	clear security idp counters log clear security idp counters log logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Reset all the IDP log counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• <i>event-rate</i>• show security idp counters log on page 638
Output Fields	This command produces no output.

clear security idp counters http-decoder

Syntax	clear security idp counters http-decoder clear security idp counters http-decoder logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the HTTP decoder counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters http-decoder on page 655
Output Fields	This command produces no output.

clear security idp counters packet-log

Syntax	clear security idp counters packet-log clear security idp counters packet-log logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Reset all the IDP counters value for packet log.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show security idp counters packet-log on page 657
List of Sample Output	command-name (optional-text) on page 579 command-name (optional-text) on page 579 command-name (optional-text) on page 579
Output Fields	

Sample Output

command-name (optional-text)

```
user@host> command-name option1 option2
Paste router command output here
```

command-name (optional-text)

```
user@host> command-name option1 option2
Paste
router command output here
```

command-name (optional-text)

```
user@host> command-name option1 option2
Paste router command
output here
```

clear security idp counters packet

Syntax	clear security idp counters packet clear security idp counters packet logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Reset all the IDP packet counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters packet on page 659
Output Fields	This command produces no output.

clear security idp counters policy-manager

Syntax	clear security idp counters policy-manager clear security idp counters policy-manager logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Reset all the IDP policies counter values.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security idp counters policy-manager on page 663
Output Fields	This command produces no output.

clear security flow session tenant

Syntax	clear security flow session tenant (<i>tenant-name</i> all)
Release Information	Command introduced in Junos OS Release 18.3R1.
Description	Clears the information about the currently active security flow sessions of the tenant systems on the device. You can either clear the currently active security flow sessions for a specific tenant system or for all the tenant systems.
Options	tenant-name —Name of the tenant system. all —Clears the security flow session information for all the tenant systems.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security flow session tenant on page 622
List of Sample Output	clear security flow session tenant T1 on page 582 clear security flow session tenant all on page 582
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security flow session tenant T1

```
user@host> clear security flow session tenant T1
0 active sessions cleared
1 active sessions cleared
0 active sessions cleared
0 active sessions cleared
```

clear security flow session tenant all

```
user@host> clear security flow session tenant all
0 active sessions cleared
2 active sessions cleared
0 active sessions cleared
0 active sessions cleared
```

request security datapath-debug capture start

Syntax request security datapath-debug capture start

Release Information Command introduced in Junos OS Release 10.0.

Description Start the data path debugging capture.



NOTE: Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

Required Privilege Level maintenance

Related Documentation • [Understanding Data Path Debugging for Logical Systems on page 346](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security datapath-debug capture start

```
user@host> request security datapath-debug capture start
datapath-debug capture started on file
```

request security datapath-debug capture stop

Syntax	request security datapath-debug capture stop
Release Information	Command introduced in Junos OS Release 10.0.
Description	Stop the data path debugging capture.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Understanding Data Path Debugging for Logical Systems on page 346
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security datapath-debug capture stop

```
user@host> request security datapath-debug capture stop
datapath-debug capture successfully stopped, use show security datapath-debug
capture to view
```


set chassis cluster cluster-id node node-number reboot

Syntax set chassis cluster cluster-id *cluster-id* node *node-number* reboot

Release Information Support for extended cluster identifiers (more than 15 identifiers) added in Junos OS Release 12.1X45-D10.

Description Sets the chassis cluster identifier (ID) and node ID on each device, and reboots the devices to enable clustering. The system uses the chassis cluster ID and chassis cluster node ID to apply the correct configuration for each node (for example, when you use the **apply-groups** command to configure the chassis cluster management interface). The chassis cluster ID and node ID statements are written to the EPROM, and the statements take effect when the system is rebooted.

Setting a cluster ID to 0 is equivalent to disabling a cluster. A cluster ID greater than 15 can only be set when the fabric and control link interfaces are connected back-to-back.



NOTE: If you have a cluster set up and running with an earlier release of Junos OS, you can upgrade to Junos OS Release 12.1X45-D10 or later and re-create a cluster with cluster IDs greater than 16. If for any reason you decide to revert to the previous version of Junos OS that did not support extended cluster IDs, the system comes up with standalone devices after you reboot. If the cluster ID set is less than 16 and you roll back to a previous release, the system comes back with the previous setup.

Options cluster-id *cluster-id*—Identifies the cluster within the Layer 2 domain.

Range: 0 through 255

node *node*—Identifies a node within a cluster.

Range: 0 through 1

Required Privilege Level maintenance

- Related Documentation**
- [Example: Setting the Chassis Cluster Node ID and Cluster ID](#)
 - [Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 31](#)
 - [Example: Configuring Logical Systems in an Active/Passive Chassis Cluster \(Master Administrators Only\) on page 275](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

show chassis cluster status

Syntax	show chassis cluster status <redundancy-group <i>group-number</i> >
Release Information	Support for monitoring failures added in Junos OS Release 12.1X47-D10.
Description	Display the current status of the Chassis Cluster. You can use this command to check the status of chassis cluster nodes, redundancy groups, and failover status.
Options	<ul style="list-style-type: none"> • none—Display the status of all redundancy groups in the chassis cluster. • redundancy-group <i>group-number</i>—(Optional) Display the status of the specified redundancy group.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>redundancy-group (Chassis Cluster)</i> • <i>clear chassis cluster failover-count</i> • <i>request chassis cluster failover node</i> • <i>request chassis cluster failover reset</i>
List of Sample Output	show chassis cluster status on page 587 show chassis cluster status with preemptive delay on page 588 show chassis cluster status redundancy-group 1 on page 588
Output Fields	Table 42 on page 586 lists the output fields for the show chassis cluster status command. Output fields are listed in the approximate order in which they appear.

Table 42: show chassis cluster status Output Fields

Field Name	Field Description
Cluster ID	ID number (1-15) of a cluster is applicable for releases upto Junos OS Release 12.1X45-D10. ID number (1-255) is applicable for Releases 12.1X45-D10 and later. Setting a cluster ID to 0 is equivalent to disabling a cluster.
Redundancy-Group	You can create up to 128 redundancy groups in the chassis cluster.
Node name	Node (device) in the chassis cluster (node0 or node1).
Priority	Assigned priority for the redundancy group on that node.

Table 42: show chassis cluster status Output Fields (continued)

Field Name	Field Description
Status	<p>State of the redundancy group (Primary, Secondary, Lost, or Unavailable).</p> <ul style="list-style-type: none"> • Primary—Redundancy group is active and passing traffic. • Secondary—Redundancy group is passive and not passing traffic. • Lost—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster and there is a control link failure, one node cannot exchange heartbeats, or when the other node is rebooted. • Unavailable—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node, or if only one node is present in the cluster.
Preempt	<ul style="list-style-type: none"> • Yes: Primary state can be preempted based on priority. • No: Change in priority will not preempt the primary state.
Manual failover	<ul style="list-style-type: none"> • Yes: Primary state is set manually through the CLI with the request chassis cluster failover node or request chassis cluster failover redundancy-group command. This overrides Priority and Preempt. • No: Primary state is not set manually through the CLI.
Monitor-failures	<ul style="list-style-type: none"> • None: Cluster working properly. • Monitor Failure code: Cluster is not working properly and the respective failure code is displayed.

Sample Output

show chassis cluster status

```
user@host> show chassis cluster status
```

```
Monitor Failure codes:
```

```

CS Cold Sync monitoring      FL Fabric Connection monitoring
GR GRES monitoring          HW Hardware monitoring
IF Interface monitoring      IP IP monitoring
LB Loopback monitoring      MB Mbuf monitoring
NH Nexthop monitoring       NP NPC monitoring
SP SPU monitoring           SM Schedule monitoring
CF Config Sync monitoring
```

```
Cluster ID: 1
```

```
Node  Priority Status      Preempt Manual  Monitor-failures
```

```
Redundancy group: 0 , Failover count: 1
```

```
node0 200 primary no no None
node1 1 secondary no no None
```

```
Redundancy group: 1 , Failover count: 1
```

```
node0 101 primary no no None
node1 1 secondary no no None
```

Sample Output

show chassis cluster status with preemptive delay

```
user@host> show chassis cluster status
```

```
Cluster ID: 1
Node  Priority Status          Preempt Manual  Monitor-failures
Redundancy group: 0, Failover count: 1
node0  200      primary      no      no      None
node1  100      secondary   no      no      None
Redundancy group: 1, Failover count: 3
node0  200      primary-preempt-hold yes no  None node1  100      secondary
              yes      no      None
```

Sample Output

show chassis cluster status redundancy-group 1

```
user@host> show chassis cluster status redundancy-group 1
```

```
Monitor Failure codes:
  CS Cold Sync monitoring      FL Fabric Connection monitoring
  GR GRES monitoring           HW Hardware monitoring
  IF Interface monitoring      IP IP monitoring
  LB Loopback monitoring       MB Mbuf monitoring
  NH Nexthop monitoring        NP NPC monitoring
  SP SPU monitoring            SM Schedule monitoring
  CF Config Sync monitoring
```

```
Cluster ID: 1
Node  Priority Status          Preempt Manual  Monitor-failures
Redundancy group: 1 , Failover count: 1
node0  101      primary      no      no      None
node1  1        secondary   no      no      None
```

show log

List of Syntax [Syntax on page 589](#)
 [Syntax \(QFX Series and OCX Series\) on page 589](#)
 [Syntax \(TX Matrix Router\) on page 589](#)

Syntax `show log`
 `<filename | user <username>>`

Syntax (QFX Series and OCX Series) `show log filename`
 `<device-type (device-id | device-alias)>`

Syntax (TX Matrix Router) `show log`
 `<all-lcc | lcc number | scc>`
 `<filename | user <username>>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Option *device-type (device-id | device-alias)* is introduced in Junos OS Release 13.1 for the QFX Series.
 Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description List log files, display log file contents, or display information about users who have logged in to the router or switch.



NOTE: On MX Series routers, modifying a configuration to replace a service interface with another service interface is treated as a catastrophic event. When you modify a configuration, the entire configuration associated with the service interface—including NAT pools, rules, and service sets—is deleted and then re-created for the newly specified service interface. If there are active sessions associated with the service interface that is being replaced, these sessions are deleted and the NAT pools are then released, which leads to the generation of the NAT_POOL_RELEASE system log messages. However, because NAT pools are already deleted as a result of the catastrophic configuration change and no longer exist, the NAT_POOL_RELEASE system log messages are not generated for the changed configuration.

Options `none`—List all log files.

`<all-lcc | lcc number | scc>`—(Routing matrix only) (Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace *number* with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).

device-type—(QFabric system only) (Optional) Display log messages for only one of the following device types:

- **director-device**—Display logs for Director devices.
- **infrastructure-device**—Display logs for the logical components of the QFabric system infrastructure, including the diagnostic Routing Engine, fabric control Routing Engine, fabric manager Routing Engine, and the default network Node group and its backup (NW-NG-0 and NW-NG-0-backup).
- **interconnect-device**—Display logs for Interconnect devices.
- **node-device**—Display logs for Node devices.



NOTE: If you specify the **device-type** optional parameter, you must also specify either the **device-id** or **device-alias** optional parameter.

(device-id | device-alias)—If a device type is specified, display logs for a device of that type. Specify either the device ID or the device alias (if configured).

filename—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.



NOTE: The **filename** parameter is mandatory for the QFabric system. If you did not configure a syslog filename, specify the default filename of messages.

user <username>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include **username**, display logging information about the specified user.

Required Privilege Level

trace

Related Documentation

- [syslog \(System\)](#)

List of Sample Output

[show log on page 591](#)
[show log filename on page 591](#)
[show log filename \(QFabric System\) on page 591](#)
[show log user on page 592](#)

Sample Output

show log

```
user@host> show log
total 57518
-rw-r--r-- 1 root bin      211663 Oct  1 19:44 dcd
-rw-r--r-- 1 root bin      999947 Oct  1 19:41 dcd.0
-rw-r--r-- 1 root bin      999994 Oct  1 17:48 dcd.1
-rw-r--r-- 1 root bin      238815 Oct  1 19:44 rpd
-rw-r--r-- 1 root bin     1049098 Oct  1 18:00 rpd.0
-rw-r--r-- 1 root bin     1061095 Oct  1 12:13 rpd.1
-rw-r--r-- 1 root bin     1052026 Oct  1 06:08 rpd.2
-rw-r--r-- 1 root bin     1056309 Sep 30 18:21 rpd.3
-rw-r--r-- 1 root bin     1056371 Sep 30 14:36 rpd.4
-rw-r--r-- 1 root bin     1056301 Sep 30 10:50 rpd.5
-rw-r--r-- 1 root bin     1056350 Sep 30 07:04 rpd.6
-rw-r--r-- 1 root bin     1048876 Sep 30 03:21 rpd.7
-rw-rw-r-- 1 root bin      19656 Oct  1 19:37 wtmp
```

show log filename

```
user@host> show log rpd
Oct  1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct  1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct  1 18:00:18
Oct  1 18:00:19 KRT recv len 56 V9 seq 148 op add Type route/if af 2 addr
192.0.2.21 nhop type local nhop 192.0.2.21
Oct  1 18:00:19 KRT recv len 56 V9 seq 149 op add Type route/if af 2 addr
192.0.2.22 nhop type unicast nhop 192.0.2.22
Oct  1 18:00:19 KRT recv len 48 V9 seq 150 op add Type ifaddr index 24 devindex
43
Oct  1 18:00:19 KRT recv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct  1 18:00:19 KRT recv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct  1 18:00:19 KRT recv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct  1 18:00:19 KRT recv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...
```

show log filename (QFabric System)

```
user@qfabric> show log messages
Mar 28 18:00:06 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:06 ED1486
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2159)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1486
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC: @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 242726)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
```

```

jnxFruName PIC: @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 242757)
Mar 28 18:00:16 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:16 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:27 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:27 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default__NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default__NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:55 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:55 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:01:10 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:01:10 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:02:37 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:02:37 ED1491
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 33809)

```

show log user

```

user@host> show log user

```

usera	mg2546		Thu Oct 1 19:37	still logged in
usera	mg2529		Thu Oct 1 19:08 - 19:36	(00:28)
usera	mg2518		Thu Oct 1 18:53 - 18:58	(00:04)
root	mg1575		Wed Sep 30 18:39 - 18:41	(00:02)
root	ttyp2	aaa.bbbb.com	Wed Sep 30 18:39 - 18:41	(00:02)
userb	ttyp1	192.0.2.0	Wed Sep 30 01:03 - 01:22	(00:19)

show route tenant

Syntax `show route tenant`
`< (all | tenant-name) >`

Release Information Statement introduced in Junos OS Release 18.3R1.

Description Displays the routing table information for the tenant systems.

A tenant system is a logical partitioning of the device into multiple security domains similar to logical systems, to provide high scalability. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. A set of interfaces that belong to the routing instances and the routing protocol parameters control the information in the routing tables. A tenant system can configure the assigned routing instances and the interfaces within a tenant system.

Options **all**—Displays the summary statistics about the all entries in the routing table.
tenant-name—Specify the tenant system name.

Required Privilege Level view

List of Sample Output [show route tenant tenant1 on page 594](#)

Output Fields [Table 43 on page 593](#) lists the output fields for the **show route tenant** command. Output fields are listed in the approximate order in which they appear.

Table 43: show route summary Output Fields

Field Name	Field Description
routing-table-name	Name of the routing table (for example, inet.0).
destinations	Number of destinations that correspond to the routes in the routing table.
routes	Number of routes in the routing table: <ul style="list-style-type: none"> active—Number of routes that are active. holddown—Number of routes that are in the hold-down state before being declared inactive. hidden—Number of routes that are not used because of routing policy.
Direct	Routes on the directly connected network.
Local	Specify the local routes.
OSPF	Name of the protocol from which the route was learnt.

Sample Output

show route tenant tenant1

```
user@host> show route tenant tenant1
tenant1.inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
12.1.1.0/24      *[Direct/0] 00:33:07
> via ge-0/0/0.0
12.1.1.1/32      *[Local/0] 00:33:07
Local via ge-0/0/0.0
224.0.0.5/32     *[OSPF/10] 00:30:31, metric 1
MultiRecv
tenant1.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
ff02::2/128      *[INET6/0] 00:33:33
MultiRecv
```

show security application-firewall rule-set

Syntax	<code>show security application-firewall rule-set (<<i>rule-set-name</i>> all)</code>
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	<p>Display information about the specified rule set defined in the application firewall.</p> <p>The application firewall is defined by a collection of rule sets. A rule set defines the rules that specify match criteria, including dynamic applications, and the action to be taken for matching traffic.</p> <p>Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the [edit security application-firewall] hierarchy and all the configuration options under this hierarchy are deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.</p>
Options	<p><i>rule-set-name</i>—Name of the rule set.</p> <p>all—Display information about all the application firewall rule sets.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>clear security application-firewall rule-set statistics</i>
List of Sample Output	<p>show security application-firewall rule-set my_ruleset1 on page 596</p> <p>show security application-firewall rule-set all on page 596</p>
Output Fields	Table 44 on page 595 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 44: 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 44: 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

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” on page 26](#).

Starting in Junos OS Release 18.2R1, the application firewall (AppFW) functionality is deprecated. As a part of this change, the **[edit security application-firewall]** hierarchy and all the configuration options under this hierarchy are deprecated—rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Options *rule-set-name*—Name of a specific rule set.

logical-system-name—Name of a specific logical system.

all—(default) Display all rule sets for all logical systems. The user logical system administrator can display all rule sets only for the logical system they can access.

root-logical-system—Display application firewall rule set information for the root logical system (master administrator only).

Required Privilege Level view

Related Documentation

- [clear security application-firewall rule-set statistics logical-system on page 560](#)

List of Sample Output [show security application-firewall rule-set logical-system all on page 599](#)
[show security application-firewall rule-set all on page 600](#)

Output Fields [Table 45 on page 599](#) 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 45: show security application-firewall rule-set logical-system Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.
Logical system	Name of the logical system.
Rule	Name of the rule. <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	The default rule applied when the identified application is not specified in any rules of the rule set. <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

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	<ul style="list-style-type: none"> • <i>Understanding AppTrack</i> • <i>Example: Configuring AppTrack</i>
Output Fields	Table 46 on page 601 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 46: 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 alg status logical-system

Syntax	<code>show security alg status logical-system</code> <code><logical-system-name></code>
Release Information	Statement introduced in Junos OS Release 18.2R1.
Description	Display the ALG status for a specific logical system or for all logical systems on the device.
Options	logical-system-name —Display ALG status for specific logical system. all —Display ALG status for all logical systems.
Additional Information	The show security alg status command is used to view the ALG status in root logical system. The show security alg status logical-system lsys1 command is used to view the ALG status in logical system lsys1. The show security alg status logical-system all command is used to view the ALG status of all existing logical systems.



NOTE: Only users under root logical system can view the ALG status for all logical systems. The keyword `logical-system` is not required in the command `show security alg status logical-system lsys1` when you log in to a particular logical system.

Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Understanding Application Layer Gateway (ALG) in Logical Systems on page 223• alg on page 456• Example: Enabling FTP ALG in a Logical System on page 227
List of Sample Output	show security alg status logical-system all on page 602 show security alg status logical-system LSYS1 on page 604

Output Fields

Sample Output

show security alg status logical-system all

```
user@host> show security alg status logical-system all
Logical system: root-logical-system
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
```

```
H323      : Disabled
MGCP      : Disabled
MSRPC     : Enabled
PPTP      : Enabled
RSH       : Disabled
RTSP      : Disabled
SCCP      : Disabled
SIP       : Disabled
SQL       : Disabled
SUNRPC    : Enabled
TALK      : Enabled
TFTP      : Enabled
IKE-ESP   : Disabled
```

Logical system: LSYS2

ALG Status:

```
DNS       : Enabled
FTP       : Enabled
H323      : Disabled
MGCP      : Disabled
MSRPC     : Enabled
PPTP      : Enabled
RSH       : Disabled
RTSP      : Disabled
SCCP      : Disabled
SIP       : Disabled
SQL       : Disabled
SUNRPC    : Enabled
TALK      : Enabled
TFTP      : Enabled
IKE-ESP   : Disabled
```

Logical system: LSYS0

ALG Status:

```
DNS       : Enabled
FTP       : Enabled
H323      : Disabled
MGCP      : Disabled
MSRPC     : Enabled
PPTP      : Enabled
RSH       : Disabled
RTSP      : Disabled
SCCP      : Disabled
SIP       : Disabled
SQL       : Disabled
SUNRPC    : Enabled
TALK      : Enabled
TFTP      : Enabled
IKE-ESP   : Disabled
```

Logical system: LSYS1

ALG Status:

```
DNS       : Enabled
FTP       : Enabled
H323      : Disabled
MGCP      : Disabled
MSRPC     : Enabled
PPTP      : Enabled
RSH       : Disabled
RTSP      : Disabled
SCCP      : Disabled
```

```

SIP      : Disabled
SQL      : Disabled
SUNRPC   : Enabled
TALK     : Enabled
TFTP     : Enabled
IKE-ESP  : Disabled

```

```
{secondary:node0}
```

show security alg status logical-system LSYS1

```
user@host> show security alg status logical-system LSYS1
```

```
ALG Status:
```

```

DNS      : Enabled
FTP      : Enabled
H323     : Disabled
MGCP     : Disabled
MSRPC    : Enabled
PPTP     : Enabled
RSH      : Disabled
RTSP     : Disabled
SCCP     : Disabled
SIP      : Disabled
SQL      : Disabled
SUNRPC   : Enabled
TALK     : Enabled
TFTP     : Enabled
IKE-ESP  : Disabled

```

```
{secondary:node0}
```

show security datapath-debug capture

Syntax	show security datapath-debug capture
Release Information	Command introduced in Junos OS Release 10.0.
Description	Display details of the data path debugging capture file.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show security datapath-debug counter on page 606 • Understanding Data Path Debugging for Logical Systems on page 346
List of Sample Output	show security datapath—debug capture on page 605
Output Fields	Output fields are listed in the approximate order in which they appear.

Sample Output

show security datapath—debug capture

```

user@host> show security datapath-debug capture
Packet 1, len 120: (C0/F0/P0/SEQ:71:1bt)
91 00 00 47 11 00 10 00 9a 14 00 19 03 00 00 00
00 00 00 00 00 01 00 47 10 00 00 00 00 00 00 00
00 1f 12 f8 dd 29 00 21 59 84 f4 01 81 00 02 1e
08 00 45 60 01 f4 00 00 00 00 3f 06 73 9f 01 01
01 02 03 01 01 02 d4 31 d4 31 00 00 00 00 00 00
00 00 50 02 00 00 ff ad 00 00 00 00
Packet 2, len 120: (C0/F0/P0/SEQ:71:1bt)
90 00 00 47 04 00 00 00 00 00 00 00 02 02 00 47
10 00 00 00 00 00 00 00 50 00 a6 1c 00 00 00 00
00 00 00 0a 00 00 00 00 00 00 09 d9 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 1f 12 f8
dd 29 00 21 59 84 f4 01 81 00 02 1e

```

show security datapath-debug counter

Syntax	show security datapath-debug counter
Release Information	Command introduced in Junos OS Release 10.0.
Description	Display details of the data path debugging counter.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show security datapath-debug capture on page 605• Understanding Data Path Debugging for Logical Systems on page 346
List of Sample Output	show security datapath-debug counter on page 606
Output Fields	Output fields are listed in the approximate order in which they appear.

Sample Output

show security datapath-debug counter

```
user@host> show security datapath-debug counter
Datapath debug counters
Packet Filter 1:
np-ingress
Chassis 0 FPC 4 : 1
np-ingress
Chassis 0 FPC 3 : 0
np-egress
Chassis 0 FPC 4 : 1
np-egress
Chassis 0 FPC 3 : 0
jexec
Chassis 0 FPC 0 PIC 1: 0
jexec
Chassis 0 FPC 0 PIC 0: 1
lbt
Chassis 0 FPC 0 PIC 1: 0
lbt
Chassis 0 FPC 0 PIC 0: 2
pot
Chassis 0 FPC 0 PIC 1: 0
pot
```

show security dns-cache

Syntax `show security dns-cache <dns-name dns-name>`

Release Information Command introduced in Junos OS Release 12.1X44-D10.

Description Display DNS cache information.



NOTE: This command is only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

Options • **dns-name**—Display DNS cache information for the specified name.

Required Privilege Level view

Related Documentation • [clear security dns-cache on page 561](#)

List of Sample Output [show security dns-cache on page 607](#)
[show security dns-cache dns-name dns2.test.com on page 608](#)

Output Fields [Table 47 on page 607](#) lists the output fields for the **show security dns-cache** command. Output fields are listed in the approximate order in which they appear.

Table 47: show security dns-cache Output Fields

Field Name	Field Description
DNS Name	DNS name.
Address Family	IPv4 or IPv6.
TTL	Time-to-live value.
IP Address	IP address for the DNS name.

Sample Output

show security dns-cache

```
user@host> show security dns-cache
DNS Name: dns1.test.com:
Address Family: IPv4, TTL: 10
IP Address: 1.1.1.1
```

```
Address Family: IPv6: TTL = 15
  IP Address: 2001:1.1.1.1
DNS Name: dns2.test.com:
Address Family: IPv4, TTL: 20
  IP Address: 2.2.2.2
  IP Address: 2.2.2.3
```

Sample Output

`show security dns-cache dns-name dns2.test.com`

```
user@host> show security dns-cache dns-name dns2.test.com
DNS Name: dns2.test.com:
Address Family: IPv4, TTL: 20
  IP Address: 2.2.2.2
  IP Address: 2.2.2.3
```


show security firewall-authentication history

Syntax	<pre>show security firewall-authentication history <address (address)> <from-zone (from-zone)> <identifier (identifier)> <logical-system (logical-system-name all)> <node (node-id all local primary)> <root-logical-system (address from-zone identifier tenant to-zone)> <tenant (tenant-name all)> <to-zone (to-zone)></pre>
Release Information	Command introduced in Junos OS Release 8.5. The node option is added in Junos OS Release 9.0. The tenant option is introduced in Junos OS Release 18.3R1.
Description	Displays security firewall authentication user history information and verify the number of firewall users who successfully authenticated and the number of firewall users who failed to log in.
Options	<ul style="list-style-type: none"> • none—Display history of firewall authentication information. • address—Display authentication entries based on IP address. • from-zone—Display authentication entries matching the given source zone, null for web-authentication and userfw-authentication. • identifier—Display authentication entries by user identifier. • logical-system—Display firewall authentication tables based on logical system name. • node—(Optional) For chassis cluster configurations, display all firewall authentication history on a specific node (device) in the cluster. <ul style="list-style-type: none"> • node-id—Identification number of the node. It can be 0 or 1. • all—Display information about all nodes. • local—Display information about the local node. • primary—Display information about the primary node. • root-logical-system—Display firewall authentication tables for root logical system. • tenant—Display firewall authentication tables based on tenant name. • to-zone—Display authentication entry matching the given destination zone, null for web-auth and userfw-auth.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Understanding Logical System Firewall Authentication on page 152 • Firewall User Authentication Overview

List of Sample Output [show security firewall-authentication history on page 610](#)
[show security firewall-authentication history node all on page 610](#)
[show security firewall-authentication history tenant tn1 on page 611](#)

Output Fields [Table 48 on page 610](#) lists the output fields for the **show security firewall-authentication history** command. Output fields are listed in the approximate order in which they appear.

Table 48: show security firewall-authentication history Output Fields

Field Name	Field Description
Authentications	Number of authentications.
Id	Identification number.
Source IP	IP address of the authentication source.
Date	Authentication date.
Time	Authentication time.
Duration	Authentication duration.
Status	Authentication status success or failure.
User	Name of the user.

Sample Output

show security firewall-authentication history

```
user@host> show security firewall-authentication history
History of firewall authentication data:
Authentications: 1
      Id Source Ip      Date      Time      Duration  Status  User
      1 203.0.113.1     2007-04-03 11:43:06 00:00:45  Success hello
```

Sample Output

show security firewall-authentication history node all

```
user@host> show security firewall-authentication history node all
node0:
-----
History of firewall authentication data:
Authentications: 2
Id Source Ip      Date      Time      Duration  Status  User
1 203.0.113.1     2008-01-04 12:00:10 0:05:49  Success local1
2 203.0.113.1     2008-01-04 14:36:52 0:01:03  Success local1
node1:
-----
History of firewall authentication data:
Authentications: 1
```

Id	Source Ip	Date	Time	Duration	Status	User
	203.0.113.1	2008-01-04	14:59:43	1193046:06:	Success	local1

`show security firewall-authentication history tenant tn1`

```
user@host> show security firewall-authentication history tenant tn1
History of firewall authentication data:
Authentications: 0
```

show security firewall-authentication users

Syntax show security firewall-authentication users
 <address (*ip-address*)>
 <auth-type (pass-through | user-firewall | web-authentication)>
 <from-zone (*from-zone*)>
 <identifier (*identifier*)>
 <logical-system (*logical-system-name* | all)>
 <node (*node-id* | all | local | primary)>
 <root-logical-system (address | auth-type | from-zone | identifier | tenant | to-zone)>
 <tenant (*tenant-name* |all)>
 <to-zone (*to-zone*)>

Release Information Command introduced in Junos OS Release 8.5. The **node** options added in Junos OS Release 9.0. The **tenant** option is introduced in Junos OS Release 18.3R1.

Description Display firewall authentication details about all users and verify the number of firewall users who successfully authenticated and firewall users who failed to log in.

- Options**
- none—Display details about all firewall authentication users.
 - address—Display authentication entries based on ip address.
 - auth-type—Display authentication entries matching the given auth-type.
 - from-zone—Display authentication entries matching the given source zone, null for web-auth and userfw-auth.
 - identifier—Display authentication entries by id.
 - logical-system—Display firewall authentication tables based on logical system name.
 - **node**—(Optional) For chassis cluster configurations, display firewall authentication details for all users on a specific node.
 - *node-id*—Identification number of the node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.
 - root-logical-system—Display firewall authentication tables for root logical system.
 - tenant—Display firewall authentication tables based on tenant name.
 - to-zone—Display authentication entry matching the given destination zone, null for web-auth and userfw-auth.

Required Privilege Level view

Related Documentation • [Firewall User Authentication Overview](#)

List of Sample Output [show security firewall-authentication users on page 613](#)
[show security firewall-authentication users node 0 on page 613](#)
[show security firewall-authentication users node all on page 614](#)

Output Fields [Table 49 on page 613](#) lists the output fields for the **show security firewall-authentication users** command. Output fields are listed in the approximate order in which they appear.

Table 49: show security firewall-authentication users Output Fields

Field Name	Field Description
Total users in table	Gives count of how many entries/users the command will display.
Id	Identification number.
Source IP	IP address of the authentication source.
Src zone	User traffic received from the zone.
Dst zone	User traffic destined to the zone.
Profile	Name of profile used for authentication.
Age	Idle timeout for the user.
Status	Authentication status success or failure.
User	Name of the user.

Sample Output

show security firewall-authentication users

```
user@host> show security firewall-authentication users
Firewall authentication data:
Total users in table: 1
      Id Source Ip      Src zone Dst zone Profile   Age Status   User
      1 192.0.2.5/24      z1      z2      p1         0 Success local1
```

Sample Output

show security firewall-authentication users node 0

```
user@host> show security firewall-authentication users node 0
node0:
-----
Firewall authentication data:
Total users in table: 1
      Id Source Ip      Src zone Dst zone Profile   Age Status   User
```

```
3 192.0.2.5/24      z1      z2      p1      1 Success  local1
```

Sample Output

show security firewall-authentication users node all

```
user@host> show security firewall-authentication users node all
node0:
-----
Firewall authentication data:
Total users in table: 1
      Id Source Ip      Src zone Dst zone Profile   Age Status  User
      3 192.0.2.5      z1      z2      p1           1 Success local1
```

```
node1:
-----
Firewall authentication data:
Total users in table: 1
      Id Source Ip      Src zone Dst zone Profile   Age Status  User
      2 192.0.2.5      z1      z2      p1           1 Success local1
```

show security firewall-authentication users tenant all

```
user@host> show security firewall-authentication users tenant all
Firewall authentication data:
Total users in table: 1
      Id Source Ip      Src zone Dst zone Profile   Age
Status  User
      2 192.0.2.10      N/A      N/A      test-rad    1
Success b1
```

show security flow session

Syntax `show security flow session [<filter>] [brief | extensive | summary]
<node (node-id | all | local | primary) >`

Release Information Command introduced in Junos OS Release 8.5. Support for filter and view options added in Junos OS Release 10.2.
Application firewall, dynamic application, and logical system filters added in Junos OS Release 11.2.
Policy ID filter added in Junos OS Release 12.3X48-D10.
Support for connection tag added in Junos OS Release 15.1X49-D40.
The **tenant** option introduced in Junos OS Release 18.3R1.

Description Display information about all currently active security sessions on the device.



NOTE: For the normal flow sessions, the `show security flow session` command displays byte counters based on IP header length. However, for sessions in Express Path mode, the statistics are collected from the IOC2 and IOC3 ASIC hardware engines and include full packet length with L2 headers. Because of this, the output displays slightly larger byte counters for sessions in Express Path mode than for the normal flow session.

Options • *filter*—Filter the display by the specified criteria.

The following filters reduce the display to those sessions that match the criteria specified by the filter. Refer to the specific **show** command for examples of the filtered output.

advanced-anti-malware—Show advanced-anti-malware sessions. For details on the **advanced-anti-malware** option, see the [Sky Advanced Threat Prevention CLI Reference Guide](#).

all-logical-systems-tenants—All multitenancy systems.

application—Predefined application name.

application-firewall—Application firewall enabled.

application-firewall-rule-set—Application firewall enabled with the specified rule set.

application-traffic-control—Application traffic control session.

application-traffic-control-rule-set—Application traffic control rule set name and rule name.

conn-tag—Session connection tag (0..4294967295).

destination-port—Destination port.

destination-prefix—Destination IP prefix or address.

dynamic-application—Dynamic application.

dynamic-application-group—Dynamic application.

encrypted—Encrypted traffic.

family—Display session by family.

idp—IDP-enabled sessions.

interface—Name of incoming or outgoing interface.

logical-system (all | *logical-system-name*)—Name of a specific logical system or **all** to display all logical systems.

nat—Display sessions with network address translation.

node—(Optional) For chassis cluster configurations, display security flow session information on a specific node (device) in the cluster.

- **node-id** —Identification number of the node. It can be 0 or 1.
- **all** —Display information about all nodes.
- **local** —Display information about the local node.
- **primary**—Display information about the primary node.

policy-id—Display session information based on policy ID; the range is 1 through 4,294,967,295.

protocol—IP protocol number.

resource-manager—Resource manager.

root-logical-system—Display root logical system as default.

security-intelligence—Display security intelligence sessions.

services-offload—Display services offload sessions.

session-identifier—Display session with specified session identifier.

source-port—Source port.

source-prefix—Source IP prefix.

tenant—Displays the security flow session information for a tenant system.

tunnel—Tunnel sessions.

- **brief | extensive | summary**—Display the specified level of output.
- **none**—Display information about all active sessions.

Required Privilege Level view

Related Documentation

- *Understanding Traffic Processing on Security Devices*
- *clear security flow session all*

List of Sample Output

[show security flow session on page 619](#)
[show security flow session \(with default policy\) on page 619](#)
[show security flow session brief on page 620](#)
[show security flow session extensive on page 620](#)
[show security flow session summary on page 620](#)

Output Fields Table 50 on page 617 lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 50: 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

Table 50: show security flow session Output Fields (continued)

Field Name	Field Description	Level of Output
Timeout	Idle timeout after which the session expires.	brief
		extensive
		none
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).	brief
		extensive
		none
Bytes	Number of received and transmitted bytes.	brief
		extensive
		none
Pkts	Number of received and transmitted packets.	brief
		extensive
		none
Total sessions	Total number of sessions.	brief
		extensive
		none
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).	brief
		extensive
		none
Status	Session status.	extensive
Flag	Internal flag depicting the state of the session, used for debugging purposes.	extensive
Source NAT pool	The name of the source pool where NAT is used.	extensive
Dynamic application	Name of the application.	extensive
Application traffic control rule-set	AppQoS rule set for this session.	extensive
Rule	AppQoS rule for this session.	extensive
Maximum timeout	Maximum session timeout.	extensive

Table 50: show security flow session Output Fields (continued)

Field Name	Field Description	Level of Output
Current timeout	Remaining time for the session unless traffic exists in the session.	extensive
Session State	Session state.	extensive
Start time	Time when the session was created, offset from the system start time.	extensive
Unicast-sessions	Number of unicast sessions.	Summary
Multicast-sessions	Number of multicast sessions.	Summary
Services-offload-sessions	Number of services-offload sessions.	Summary
Failed-sessions	Number of failed sessions.	Summary
Sessions-in-use	Number of sessions in use. <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 (with default policy)

```

root> show security flow session
Session ID: 36, Policy name: pre-id-default-policy/n, Timeout: 2, Valid
  In: 10.10.10.2/61606 --> 10.10.10.1/179;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
  Pkts: 1, Bytes: 64,
  Out: 10.10.10.1/179 --> 10.10.10.2/61606;tcp, Conn Tag: 0x0, If: .local..0,
  Pkts: 1, Bytes: 40,

```

show security flow session brief

```
root> show security flow session brief
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 62, Valid
  In: 203.0.113.11/1000 --> 203.0.113.1/2000;udp, Conn Tag: 0x0, If: reth1.0,
  Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp, Conn Tag: 0x0, If: reth0.0,
  Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1
```

show security flow session extensive

```
root> show security flow session extensive
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Status: Normal, State: Active
Flags: 0x8000040/0x18000000/0x12000003
Policy name: SG/4
Source NAT pool: Null, Application: junos-gprs-gtp-v0-udp/76
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 90, Current timeout: 54
Session State: Valid
Start time: 6704, Duration: 35
  In: 203.0.113.11/1000 --> 201.11.0.100/2000;udp,
    Conn Tag: 0x0, Interface: reth1.0,
    Session token: 0x6, Flag: 0x40000021
    Route: 0x86053c2, Gateway: 201.10.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 86
    CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp,
    Conn Tag: 0x0, Interface: reth0.0,
    Session token: 0x7, Flag: 0x50000000
    Route: 0x86143c2, Gateway: 203.0.113.11, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
    CP Session ID: 10320276

Total sessions: 1
```

show security flow session summary

```
root> show security flow session summary
Flow Sessions on FPC10 PIC1:
Unicast-sessions: 1
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456
```

```
Flow Sessions on FPC10 PIC2:  
Unicast-sessions: 0  
Multicast-sessions: 0  
Services-offload-sessions: 0  
Failed-sessions: 0  
Sessions-in-use: 0  
  Valid sessions: 0  
  Pending sessions: 0  
  Invalidated sessions: 0  
  Sessions in other states: 0  
Maximum-sessions: 6291456
```

```
Flow Sessions on FPC10 PIC3:  
Unicast-sessions: 0  
Multicast-sessions: 0  
Services-offload-sessions: 0  
Failed-sessions: 0  
Sessions-in-use: 0  
  Valid sessions: 0  
  Pending sessions: 0  
  Invalidated sessions: 0  
  Sessions in other states: 0  
Maximum-sessions: 6291456
```

show security flow session tenant

Syntax	show security flow session tenant (<i>tenant-name</i> all)
Release Information	Command introduced in Junos OS Release 18.3R1.
Description	Displays the information about the currently active security flow sessions of the tenant systems on the device. You can either view the currently active security flow sessions information for a specific tenant system or for all the tenant systems.
Options	<p>tenant-name—Name of the tenant system.</p> <p>all—Displays the security flow session information for all the tenant systems.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear security flow session tenant on page 582
List of Sample Output	<p>show security flow session tenant T1 on page 623</p> <p>show security flow session tenant all on page 623</p>
Output Fields	Table 51 on page 622 lists the output fields for the show security flow session tenant command. Output fields are listed in the approximate order in which they appear.

Table 51: show security flow session tenant

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming security flow session details. The incoming security flow session details include the source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets, and bytes.
Out	Reverse security flow session details. The reverse security flow session details include the 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 security flow sessions.
Policy name	Name and ID of the policy that the first packet of the security flow session matched.

Table 51: show security flow session tenant (continued)

Field Name	Field Description
Tenant	Name of the tenant system.

Sample Output

show security flow session tenant T1

```

root@host> show security flow session tenant T1
Flow Sessions on FPC7 PIC1:

Session ID: 290000224, Policy name: default-policy-logical-system-32/2, Timeout:
1790, Valid
Tenant: T1
  In: 203.0.113.0/39767 --> 203.0.113.1/23;tcp, Conn Tag: 0x0, If: xe-3/0/1.0,
Pkts: 39, Bytes: 2136, CP Session ID: 1225556754
  Out: 203.0.113.1/23 --> 203.0.113.0/39767;tcp, Conn Tag: 0x0, If: lt-0/0/0.101,
Pkts: 31, Bytes: 1872, CP Session ID: 1225556754

```

show security flow session tenant all

```

root@host> show security flow session tenant all
Flow Sessions on FPC7 PIC1:

Session ID: 290000224, Policy name: default-policy-logical-system-32/2, Timeout:
1790, Valid
Tenant: T1
  In: 203.0.113.0/39767 --> 203.0.113.1/23;tcp, Conn Tag: 0x0, If: xe-3/0/1.0,
Pkts: 39, Bytes: 2136, CP Session ID: 1225556754
  Out: 203.0.113.1/23 --> 203.0.113.0/39767;tcp, Conn Tag: 0x0, If: lt-0/0/0.101,
Pkts: 31, Bytes: 1872, CP Session ID: 1225556754

Session ID: 290000225, Policy name: default-policy-logical-system-33/2, Timeout:
1790, Valid
Tenant: T2
  In: 203.0.113.3/39767 --> 203.0.113.4/23;tcp, Conn Tag: 0x0, If: lt-0/0/0.103,
Pkts: 39, Bytes: 2136, CP Session ID: 1225556755
  Out: 203.0.113.4/23 --> 203.0.113.3/39767;tcp, Conn Tag: 0x0, If: xe-9/0/0.0,
Pkts: 31, Bytes: 1872, CP Session ID: 1225556755
Total sessions: 2

Flow Sessions on FPC7 PIC2:
Total sessions: 0

Flow Sessions on FPC7 PIC3:
Total sessions: 0

```

show security idp logical system

Syntax show security idp logical-system

Release Information Command introduced in Junos OS Release 18.3R1.

Description Display information about the logical systems and the IDP policies associated to the logical systems.

Options

- **logical-system**— Show the IDP policy assigned to a logical system. The IDP policy is assigned to a logical system through the security profile.
- **policy-association**

Required Privilege Level view

Related Documentation

- *clear security idp*

List of Sample Output [show security idp logical-system policy-association on page 624](#)

Sample Output

show security idp logical-system policy-association

```
user@host> show security idp logical-system policy-association
Logical system          IDP policy
root-logical-system     policy1
LSYS1                   idpengine
```


show security idp attack table

Syntax	show security idp attack table show security idp attack table logical-system <logical-system>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display detailed information of IDP attack table.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear security idp attack table on page 566
List of Sample Output	show security idp attack table on page 625
Output Fields	Table 52 on page 625 lists the output fields for the show security idp attack table command. Output fields are listed in the approximate order in which they appear.

Table 52: show security idp attack table Output Fields

Field Name	Field Description
Attack name	Name of the attack that you want to match in the monitored network traffic.
Hits	<p>Total number of attack matches.</p> <p>On SRX Series devices, for brute force and time-binding-related attacks, the logging is to be done only when the match count is equal to the threshold. That is, only one log is generated within the 60-second period in which the threshold is measured. This process prevents repetitive logs from being generated and ensures consistency with other IDP platforms, such as IDP-standalone.</p> <p>When no attack is seen within the 60-second period and the BFQ entry is flushed out, the match count starts over the new attack match shows up in the attack table, and the log is generated.</p>

Sample Output

show security idp attack table

```

user@host> show security idp attack table
IDP attack statistics:
  Attack name                               #Hits
HTTP:OVERFLOW:PI3WEB-SLASH-OF              1

```

show security idp counters action

Syntax	show security idp counters action show security idp counters action logical-system <logical-system>
Release Information	Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display detailed information of IDP counter type and value.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear security idp counters action on page 574
List of Sample Output	show security idp counters action on page 626 show security idp counters action on page 627
Output Fields	Table 53 on page 626 lists the output fields for the show security idp counters action command. Output fields are listed in the approximate order in which they appear.

Table 53: show security idp counters action Output Fields

Field Name	Field Description
IDP counter type	Name of the action
Value	Number of packets dropped, recommended, and ignored based on the action in the IDP counters.

Sample Output

show security idp counters action

```

user@host> show security idp counters action
IDP counters:

    IDP counter type      Value
    None                  0
    Recommended           0
    Ignore                 0
    Diffserv               0
    Drop packet            0
    Drop                   0
    Close                  0
    Close server           0
    Close client           0
    IP action rate limit   0
    IP action drop         0
    IP action close        0
    IP action notify       0
    IP action failed       0

```

show security idp counters action

```
user@host> show security idp counters action logical-system LSYSO
```

```
IDP counters:
```

IDP counter type	Value
None	0
Recommended	0
Ignore	0
Diffserv	0
Drop packet	0
Drop	0
Close	0
Close server	0
Close client	0
IP action rate limit	0
IP action drop	0
IP action close	0
IP action notify	0
IP action failed	0

show security idp counters application-identification

Syntax	show security idp counters application-identification show security idp counters application-identification logical-system <logical-system>
Release Information	Command introduced in Junos OS Release 9.2. Modified in Junos OS Release 12.1. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the status of all IDP application identification (AI) counter values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear security idp counters application-identification on page 573
List of Sample Output	show security idp counters application-identification on page 630
Output Fields	Table 54 on page 628 lists the output fields for the show security idp counters application-identification command. Output fields are listed in the approximate order in which they appear.

Table 54: show security idp counters application-identification Output Fields

Field Name	Field Description
AI matches	Number of sessions with an AI signature match.
AI no-matches	Number of sessions with no AI signature match.
AI-enabled sessions	Number of sessions with AI enabled.
AI-disabled sessions	Number of sessions with AI disabled.
AI-disabled sessions due to ssl encapsulated flows	Number of sessions with AI disabled due to SSL encapsulated flows.
AI-disabled sessions due to cache hit	Number of sessions with AI disabled due to a cache match.
AI-disabled sessions due to configuration	Number of sessions with AI disabled because the configured session limit was reached.
AI-disabled sessions due to protocol remapping	Number of sessions with AI disabled due to protocol remapping.
AI-disabled sessions due to RPC match	Number of sessions with AI disabled due to an RPC match.
AI-disabled sessions due to gate match	Number of sessions with AI disabled due to a gate match.

Table 54: show security idp counters application-identification Output Fields (continued)

Field Name	Field Description
AI-disabled sessions due to non-TCP/UDP flows	Number of sessions with AI disabled due to non-TCP or non-UDP flows.
AI-disabled sessions due to session limit	Number of sessions with AI disabled because the maximum session limit was reached.
AI-disabled sessions due to session packet memory limit	Number of sessions with AI disabled because the memory usage limit per session was reached.
AI-disabled sessions due to global packet memory limit	Number of sessions with AI disabled because the global memory usage limit was reached.
AI sessions current global reassembler packet memory usage	Number of AI sessions with current global reassembler packet memory usage limit
AI sessions peak global reassembler packet memory usage	Number of AI sessions with peak global reassembler packet memory usage limit
AI sessions current global packet memory usage	Number of AI sessions with current global packet memory usage limit
AI sessions peak global packet memory usage	Number of AI sessions with peak global packet memory usage limit
AI-sessions dropped due to malloc failure before session create	Number of AI sessions dropped because the malloc failure occurred before session create.
AI-sessions dropped due to malloc failure after create	Number of AI sessions dropped because the malloc failure occurred after session create.
AI-Packets received on sessions marked for drop due to malloc failure	Number of AI packets received on sessions that are marked to be dropped because the malloc failure.
Packets cloned for AI	Number of packets cloned for application identification.
Policy update	Number of times the IDP policy has been updated.
Total PME prematch job ignored	Number of jobs ignored because of pattern matching engine (PME) not matching.
Total packets for which prematch job were ignored	Number of packets for which signature matching was ignored as prematch found.
Prematch busy packet count	Number of packets saved as they are handed off for signature matching during prematch reprocess.
Final match busy packet count	Number of packets saved as they are handed off for signature matching during final match reprocess.
Total AI busy packet count	Number of times AI saved packet handed off for signature matching.

Table 54: show security idp counters application-identification Output Fields (continued)

Field Name	Field Description
Final match processed busy packet count	Number of times a packet processed for final matching before signature matching.
Prematch processed busy packet count	Number of times a packet processed for prematch before signature match.
Prematch ignored busy packet count	Number of packets ignored for signature matching as prematch found.
AI done busy packet count	Number of packets signature matching not completed before AI done.
JPME flow for Ignored jobs destroyed	Number of jobs destroyed because of flow mismatch due to policy relookup.
Set AI done for prematch	Number of sessions set for AI applied.
AI done for prematch	Number of sessions with AI applied.

Sample Output

show security idp counters application-identification

```

user@host> show security idp counters application-identification

IDP counter type                                     Value
AI matches                                           0
AI no-matches                                         0
AI-enabled sessions                                  0
AI-disabled sessions                                  0
AI-disabled sessions due to ssl encapsulated flows    0
AI-disabled sessions due to cache hit                 0
AI-disabled sessions due to configuration             0
AI-disabled sessions due to protocol remapping        0
AI-disabled sessions due to RPC match                 0
AI-disabled sessions due to gate match               0
AI-disabled sessions due to non-TCP/UDP flows         0
AI-disabled sessions due to session limit             0
AI-disabled sessions due to session packet memory limit 0
AI-disabled sessions due to global packet memory limit 0
AI sessions current global reass packet memory usage  0
AI sessions peak global reass packet memory usage     0
AI sessions current global packet memory usage        0
AI sessions peak global packet memory usage           0
AI-sessions dropped due to malloc failure before session create 0
AI-sessions dropped due to malloc failure after create  0
AI-Packets received on sessions marked for drop due to malloc failure 0
Packets cloned for AI                                0
Policy update                                          0
Total PME prematch job ignored                        0
Total packets for which prematch job were ignored     0
Prematch busy packet count                           0
Final match busy packet count                         0
Total AI busy packet count                           0
Final match processed busy packet count               0

```

Prematch processed busy packet count	0
Prematch ignored busy packet count	0
AI done busy packet count	0
JPME flow for Ignored jobs destroyed	0
Set AI done for prematch	0
AI done for prematch	0

show security idp counters memory

Syntax	show security idp counters memory show security idp counters memory logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display detailed information of allocated, reallocated IDP counters memory values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear security idp counters memory on page 570
List of Sample Output	show security idp counters memory on page 632
Output Fields	Table 55 on page 632 lists the output fields for the show security idp counters memory command. Output fields are listed in the approximate order in which they appear.

Table 55: show security idp counters memory Output Fields

Field Name	Field Description
IDP counter type	Name of the counter type
Value	Number of requests made for memory allocation and reallocation,

Sample Output

show security idp counters memory

```

user@host> show security idp counters memory
IDP counters:

    IDP counter type                               Value
Memory allocation requested                       928058
Memory reallocation requested                     0
Memory allocation failed                         0
Memory reallocation failed                       0
Memory free requested                             889749
Memory free failed                               0
IDP Arena requested                              0
IDP Arena failed                                0
IDP Arena freed                                  0
Objcache requested                               132
Objcache failed                                  0
Objcache freed                                    2
Objcache over limit                              0
Objcache invalid record                          0
Detector Objcache requested                       21032
Detector Objcache failed                         0

```


Detector Objcache freed	20324
Detector Objcache invalid record	0
Detector Arena requested	0
Detector Arena failed	0
Detector Arena freed	0
Kzalloc requested	910823
Kzalloc failed	0
Kzalloc freed	885264
Pool alloc called	0
Pool alloc subscribed size	0
Pool alloc done	0
Pool free called	0
Pool free done	0
Malloc over limit	0
Remote free deadbeef	0

show security idp counters ssl-inspection

Syntax	show security idp counters ssl-inspection show security idp counters ssl-inspection logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display the IDP counters value for decrypted and encrypted sessions.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear security idp counters ssl-inspection on page 569
List of Sample Output	show security idp counters ssl-inspection on page 634 show security idp counters ssl-inspection logical-system LSYS1 on page 635
Output Fields	Table 56 on page 634 lists the output fields for the show security idp counters ssl-inspection command. Output fields are listed in the approximate order in which they appear.

Table 56: show security idp counters ssl-inspection Output Fields

Field Name	Field Description
IDP counter type	Name of the action
Value	Number of packets and sessions decrypted, sessions not decrypted.

Sample Output

show security idp counters ssl-inspection

```

user@host> show security idp counters ssl-inspection
IDP counters:

    IDP counter type                Value
Packets Decrypted                  0
Sessions Decrypted                  0
Sessions Not Decrypted              0
Sessions Not Decrypted - Configuration 0
Sessions Not Decrypted - No Key      0
Sessions Not Decrypted - Unsupported Ciphers 0
Sessions Not Decrypted - Unsupported Compression 0
Sessions Not Decrypted - Unsupported Key Exchange 0
Sessions Not Decrypted - Bulk Decryption Failure 0
Sessions Not Decrypted - Key Generation Failure 0
Sessions Not Decrypted - Temporary Certificate 0
Sessions Not Decrypted - Handshake Verification Failure 0
Sessions Not Decrypted - ID Cache Miss 0
Sessions Not Decrypted - Session Limit 0
Sessions Not Decrypted - Message Size 0

```

Sessions Not Decrypted - No Memory	0
Sessions New Key	0
Sessions Used Key	0
Session ID Cache Hits	0
Session ID Cache Misses	0
Sessions Used XLR RSA SAE for Key Decryption	0
Sessions - Error when XLR RSA SAE used	0

show security idp counters ssl-inspection logical-system LSYS1

user@host> show security idp counters ssl-inspection logical-system LSYS1
IDP counters:

IDP counter type	Value
Packets Decrypted	0
Sessions Decrypted	0
Sessions Not Decrypted	0
Sessions Not Decrypted - Configuration	0
Sessions Not Decrypted - No Key	0
Sessions Not Decrypted - Unsupported Ciphers	0
Sessions Not Decrypted - Unsupported Compression	0
Sessions Not Decrypted - Unsupported Key Exchange	0
Sessions Not Decrypted - Bulk Decryption Failure	0
Sessions Not Decrypted - Key Generation Failure	0
Sessions Not Decrypted - Temporary Certificate	0
Sessions Not Decrypted - Handshake Verification Failure	0
Sessions Not Decrypted - ID Cache Miss	0
Sessions Not Decrypted - Session Limit	0
Sessions Not Decrypted - Message Size	0
Sessions Not Decrypted - No Memory	0
Sessions New Key	0
Sessions Used Key	0
Session ID Cache Hits	0
Session ID Cache Misses	0
Sessions Used XLR RSA SAE for Key Decryption	0
Sessions - Error when XLR RSA SAE used	0

show security idp counters pdf-decoder

Syntax	show security idp counters pdf-decoder show security idp counters pdf-decoder logical-system <i>logical-system</i>
Release Information	Command introduced for user logical systems in Junos OS Release 18.3R1
Description	Displays IDP counters value for PDF-Decode enabled sessions, requests, and memory limit IDP counter types.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear security idp counters pdf-decoder on page 568
List of Sample Output	show security idp counters pdf-decoder on page 636 show security idp counters pdf-decoder logical-system LSYS1 on page 637
Output Fields	Table 57 on page 636 lists the output fields for the show security idp counters pdf-decoder command. Output fields are listed in the approximate order in which they appear.

Table 57: show security idp counters pdf-decoder Output Fields

Field Name	Field Description
IDP counter type	Name of the action
Value	Number of PDF-decode enabled sessions and requests for the IDP counters.

Sample Output

show security idp counters pdf-decoder

```

user@host> show security idp counters pdf-decoder
IDP counters:

    IDP counter type                               Value
PDF-Decode enabled sessions                       0
PDF-Decode requests                              0
PDF-decode in pending state                      0
PDF-decode finished successfully                 0
PDF-decode per file memory limit reached         0
PDF-decode memory limit reached                 0
PDF-decode session limit reached                 0
PDF-decode malloc count                         0
PDF-decode free count                          0
PDF-decode bypassed - Global memory limit        0
PDF-decode bypassed - Per file memory limit      0
PDF-decode bypassed - Document encrypted         0
PDF-decode bypassed - Unsupported filter decode  0

```

PDF-decode bypassed	- corrupted PDF file	0
PDF-decode bypassed	- unsupported obj-stream length	0
PDF-decode bypassed	- filter decode failed	0

show security idp counters pdf-decoder logical-system LSYS1

```
user@host> show security idp counters pdf-decoder logical-system LSYS1
IDP counters:
```

IDP counter type	Value
PDF-Decode enabled sessions	0
PDF-Decode requests	0
PDF-decode in pending state	0
PDF-decode finished successfully	0
PDF-decode per file memory limit reached	0
PDF-decode memory limit reached	0
PDF-decode session limit reached	0
PDF-decode malloc count	0
PDF-decode free count	0
PDF-decode bypassed - Global memory limit	0
PDF-decode bypassed - Per file memory limit	0
PDF-decode bypassed - Document encrypted	0
PDF-decode bypassed - Unsupported filter decode	0
PDF-decode bypassed - corrupted PDF file	0
PDF-decode bypassed - unsupported obj-stream length	0
PDF-decode bypassed - filter decode failed	0

show security idp counters log

Syntax	show security idp counters log show security idp counters log logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display the status of all IDP log counter values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>event-rate</i> • <i>clear security idp counters log</i>
List of Sample Output	show security idp counters log on page 640 show security idp counters log logical-system LSYS1 on page 640
Output Fields	Table 58 on page 638 lists the output fields for the show security idp counters log command. Output fields are listed in the approximate order in which they appear.

Table 58: show security idp counters log Output Fields

Field Name	Field Description
Logs dropped	Number of logs that are dropped.
Suppressed log count	Number of logs that are suppressed.
Logs waiting for post-window packets (Unsupported)	Number of logs waiting for post-window packets.
Logs ready to be sent (Unsupported)	Number of logs ready to be sent.
Logs in suppression list (Unsupported)	Number of logs considered for suppression list.
Log timers created	Number of times the log timer is created.
Logs timers expired	Number of times the log timer is expired.
Log timers cancelled	Number of times the log timer is canceled.

Table 58: show security idp counters log Output Fields (continued)

Field Name	Field Description
Logs ready to be sent high watermark (Unsupported)	Number of packets that are ready to be sent with high degree watermark.
Log receive buffer full (Unsupported)	Number of times the buffer is full.
Packet log too big (Unsupported)	Number of packet logs that exceeded allowed packet log size.
Reads per second (Unsupported)	Number of packets that are read per second.
Logs in read buffer high watermark (Unsupported)	Number of high watermark packets that are in read buffer.
Packets logged	Number of packets that are logged,
Packets lost (Unsupported)	Number of packets that are failed to log.
Packets copied (Unsupported)	Number of packets copied during packet log.
Packets held (Unsupported)	Number of packets held for packet log.
Packets released	Number of packets that are released from hold.
IP Action Messages (Unsupported)	Number of IP action messages.
IP Action Drops (Unsupported)	Number of IP action messages dropped.
IP Action Exists (Unsupported)	Number of exits during IP action creation.
NWaits (Unsupported)	Number of logs waiting for post window packets.

Table 58: show security idp counters log Output Fields (continued)

Field Name	Field Description
Match vectors	Number of attacks in IDS match vector.
Supercedes	Number of attacks in supercede vector.

Sample Output

show security idp counters log

```

user@host> show security idp counters log
IDP counters:
IDP counter type                               Value
Logs dropped                                   0
Suppressed log count                           0
Logs waiting for post-window packets           0
Logs ready to be sent                          0
Logs in suppression list                       0
Log timers created                             0
Logs timers expired                           0
Log timers cancelled                           0
Logs ready to be sent high watermark           0
Log receive buffer full                        0
Packet log too big                             0
Reads per second                              1
Logs in read buffer high watermark             0
Log Bytes in read buffer high watermark        0
Packets logged                                0
Packets lost                                  0
Packets copied                                0
Packets held                                  0
Packets released                              0
IP Action Messages                            0
IP Action Drops                               0
IP Action Exists                              0
Nwaits                                         0
Match vectors                                 0
Supercedes                                    0
Kpacket too big                               0

```

show security idp counters log logical-system LSYS1

```

user@host> show security idp counters log logical-system LSYS1
IDP counters:
IDP counter type                               Value
Logs dropped                                   0
Suppressed log count                           0
Logs waiting for post-window packets           0
Logs ready to be sent                          0
Logs in suppression list                       0
Log timers created                             0
Logs timers expired                           0
Log timers cancelled                           0
Logs ready to be sent high watermark           0
Log receive buffer full                        0
Packet log too big                             0

```


Reads per second	0
Logs in read buffer high watermark	0
Log Bytes in read buffer high watermark	0
Packets logged	0
Packets lost	0
Packets copied	0
Packets held	0
Packets released	0
IP Action Messages	0
IP Action Drops	0
IP Action Exists	0
NWaits	0
Match vectors	0
Supercedes	0
send succeed	0
send fail	0
retries on send failures	0
uac send succeed	0
uac send fail	0
idpd to flowd alloc msg fail	0
idpd to flowd enqueue log msg fail	0
idpd to flowd enqueue log msg succeed	0
idpd to flowdlog msg dequeued	0
idpd to flowdlog unknown msg type	0
flowd send succeed	0
flowd send fail	0
objcache alloc failure for sc_pcap_mbuf_info_t	0
pcap mbuf alloc fail counter	0
pcap mbuf reinj failed	0
pcap fragmented packets count	0
idpd to flowd pcap messages count in dedicated mode	0
idpd pcap type1 messages count	0
idpd pcap type2 messages count	0
idpd pcap type3 messages count	0
Kpacket too big	0

show security idp counters ips

Syntax	show security idp counters ips show security idp counters ips logical-system <i>logical-system</i>
Release Information	Command modified in Junos OS Release 11.2. Command modified for user logical systems in Junos OS Release 18.3R1.
Description	Display the status of all IPS counter values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • ips • clear security idp counters ips on page 567
List of Sample Output	show security idp counters ips on page 643 show security idp counters ips logical-system LSYS1 on page 644
Output Fields	Table 59 on page 642 lists the output fields for the show security idp counters ips command. Output fields are listed in the approximate order in which they appear.

Table 59: show security idp counters ips Output Fields

Field Name	Field Description
TCP fast path	Number of TCP packets skipped for IDS processing.
Layer-4 anomalies	Number of Layer-4 protocol error or anomaly.
Anomaly hash misses	Number of times look failed on anomaly hash.
Line context matches	Number of attempts to match line based attacks in traffic stream.
Stream256 context matches	Number of attempts to match stream based attacks in first 256 bytes of traffic stream.
Stream context matches	Number of attempts to match stream based attacks in traffic stream.
Packet context matches	Number of attempts to match packet based attacks in traffic packet.
Packet header matches	Number of attempts to match packet header based attacks in traffic packet.
Context matches	Number of attempts to match protocol context based attacks in traffic stream.
Regular expression matches	Number of attempts to match PCRE expressions in traffic stream.
Tail DFAs	Number of attempts to match an attack on tail DFA group matches.

Table 59: show security idp counters ips Output Fields (continued)

Field Name	Field Description
Exempted attacks	Number of attacks exempted from match as per exempt rulebase.
Out of order chains	Number of times attack is excluded from match due to member attacks in an attack group did not complete chain.
Partial chain matches	Number of attacks in partial chain match with attack scope as transaction.
IDS device FIFO size	Number of IDS contexts in virtual IDS device.
IDS device FIFO overflows	Number of times an IDS context can not be written as the IDS device is full.
Brute force queue size	Number of entries in the brute force queue.
IDS cache hits (Unsupported)	Number of sessions those found attack instance in IDS cache.
IDS cache misses (Unsupported)	Number of sessions those did not find attack instance in IDS cache.
Shellcode detection invocations	Number of times shell code match is attempted.
Wrong offsets	Number of times attack's offset is not within the service offset range.
No peer MAC (Unsupported)	Number of times flow peer MAC address is not available.

Sample Output

show security idp counters ips

```

user@host> show security idp counters ips
IDP counters:
IDP counter type                               Value
TCP fast path                                  15
Layer-4 anomalies                              0
Anomaly hash misses                            3
Line context matches                           5
Stream256 context matches                      5
Stream context matches                         5
Packet context matches                         0
Packet header matches                         0
Context matches                               12
Regular expression matches                     0
Tail DFAs                                      0
Exempted attacks                              0
Out of order chains                           0
Partial chain matches                          0
IDS device FIFO size                           0

```

IDS device FIFO overflows	0
Brute force queue size	0
IDS cache hits	0
IDS cache misses	0
Shellcode detection invocations	0
Wrong offsets	0
No peer MAC	0
Content-decompression memory usage in KB	0
Content-decompression memory over limit	0
Content-decompression gunzip called	0
Content-decompression gunzip failed	0
Content-decompression others called	0
Content-decompression others failed	0
Content-decompression input bytes	0
Content-decompression output bytes	0
Content-decompression ratio over limit	0
Content-decompression type mismatch	0

show security idp counters ips logical-system LSYS1

```
user@host> show security idp counters ips logical-system LSYS1
IDP counters:
```

IDP counter type	Value
TCP fast path	40
Layer-4 anomalies	0
Anomaly hash misses	4
Line context matches	0
Stream256 context matches	0
Stream context matches	0
Packet context matches	0
Packet header matches	0
Context matches	4
Context reset	0
Regular expression matches	0
Tail DFAs	0
Exempted attacks	0
Out of order chains	0
Partial chain matches	0
IDS device FIFO size	0
IDS device FIFO overflows	0
Brute force queue size	2
IDS cache hits	0
IDS cache misses	0
Shellcode detection invocations	0
Wrong offsets	0
No peer MAC	0
Content-decompression memory usage in KB	0
Content-decompression memory over limit	0
Content-decompression gunzip called	0
Content-decompression gunzip failed	0
Content-decompression others called	0
Content-decompression others failed	0
Content-decompression input bytes	0
Content-decompression output bytes	0
Content-decompression ratio over limit	0
Content-decompression type mismatch	0
URL track session bypassed	0
Exceeded max Tail DFA transition limit	0
Number of times HS stream close failed	0
Number of times HS stream open failed	0

Number of times HS scan stream failed	0
Number of times HS scan failed	0

show security idp counters dfa

Syntax	show security idp counters dfa show security idp counters dfa logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display the status of all DFA counter values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear security idp counters dfa on page 575
List of Sample Output	show security idp counters dfa on page 646 show security idp counters dfa logical-system LSYS1 on page 646
Output Fields	Table 60 on page 646 lists the output fields for the show security idp counters dfa command. Output fields are listed in the approximate order in which they appear.

Table 60: show security idp counters dfa Output Fields

Field Name	Field Description
DFA Group Merged Usage	Number of DFA groups merged.
DFA Matches	Number of DFA matches found.

Sample Output

show security idp counters dfa

```

user@host> show security idp counters dfa
IDP counters:

IDP counter type                Value
DFA Group Merged Usage          0
DFA Matches                      0
DFA compressed                  0
DFA group compressed            0
DFA uncompressed                0
DFA group uncompressed          0

```

1

show security idp counters dfa logical-system LSYS1

```

user@host> show security idp counters dfa logical-system LSYS1
IDP counters:

```

IDP counter type	Value
DFA Group Merged Usage	0
DFA Matches	0
DFA compressed	0
DFA group compressed	0
DFA uncompressed	0
DFA group uncompressed	0

show security idp counters flow

Syntax show security idp counters flow
show security idp counters flow logical-system *logical-system*

Release Information Command introduced in Junos OS Release 9.2.
Command introduced for user logical system in Junos OS Release 18.3R1.

Description Display the status of all IDP flow counter values.



NOTE: On SRX Series devices with IDP enabled, if IDP attacks are configured for a single direction (server or client), a flow in the opposite direction does not need IDP processing. For TCP traffic, the TCP optimization feature ensures minimal processing for these flows without running into reassembly errors.

Required Privilege Level view

Related Documentation

- *flow (Security IDP)*
- [clear security idp counters flow on page 576](#)

List of Sample Output [show security idp counters flow on page 652](#)

Output Fields [Table 61 on page 648](#) lists the output fields for the **show security idp counters flow** command. Output fields are listed in the approximate order in which they appear.

Table 61: show security idp counters flow Output Fields

Field Name	Description
Fast-path packets	Number of packets that are set through fast path after completing IDP policy lookup.
Slow-path packets	Number of packets that are sent through slow path during IDP policy lookup.
Session construction failed (Unsupported)	Number of times the packet failed to establish the session.
Session limit reached	Number of sessions that reached IDP sessions limit.
Session inspection depth reached	Number of sessions that reached inspection depth.
Memory limit reached	Number of sessions that reached memory limit.

Table 61: show security idp counters flow Output Fields (continued)

Field Name	Description
Not a new session (Unsupported)	Number of sessions that extended beyond time limit.
Invalid index at age-out (Unsupported)	Invalid session index in session age-out message.
Packet logging	Number of packets saved for packet logging.
Policy cache hits	Number of sessions that matched policy cache.
Policy cache misses	Number of sessions that did not match policy cache.
Policy cache entries	Number of policy cache entries.
Maximum flow hash collisions	Maximum number of packets, of one flow, that share the same hash value.
Flow hash collisions	Number of packets that share the same hash value.
Gates added	Number of gate entries added for dynamic port identification.
Gate matches (Unsupported)	Number of times a gate is matched.
Sessions deleted	Number of sessions deleted.
Sessions aged-out (Unsupported)	Number of sessions that are aged out if no traffic is received within session timeout value.
Sessions in-use while aged-out (Unsupported)	Number of sessions in use during session age-out.
TCP flows marked dead on RST/FIN	Number of sessions marked dead on TCP RST/FIN.
policy init failed	Policy initiation failed.
Number of times Sessions exceed high mark	Number of times sessions exceeded the high mark.
Number of sessions exceeds high mark	Number of sessions that exceed high mark.
Number of sessions drops below low mark	Number of sessions that fall below low mark.

Table 61: show security idp counters flow Output Fields (continued)

Field Name	Description
Memory of sessions exceeds high mark	Session memory exceeds high mark.
Memory of sessions drops below low mark	Session memory drops below low mark.
SM Sessions encountered memory failures	Number of SM sessions that encountered memory failures.
SM Packets on sessions with memory failures	Number of SM packets that encountered memory failures.
Sessions constructed	Number of sessions established.
SM Sessions dropped	Number of SM sessions dropped.
SM sessions ignored	Number of sessions ignored in Security Module (SM).
SM sessions interested	Number of SM sessions interested.
SM sessions not interested	Number of SM sessions not interested.
SM sessions interest error	Number of errors created for SM sessions interested.
Sessions destructed	Number of sessions destructed.
SM Session Create	Number of SM sessions created.
SM Packet Process	Number of packets processed from SM.
SM FTP data session ignored by IDP	Number of SM FTP data sessions that are ignored by IDP.
SM Session close	Number of SM sessions closed.
SM client-to-server packets	Number of SM client-to-server packets.
SM server-to-client packets	Number of SM server-to-client packets.
SM client-to-server L7 bytes	Number of SM client-to-server Layer 7 bytes.
SM server-to-client L7 bytes	Number of SM server-to-client Layer 7 bytes.
Client-to-server flows ignored	Number of client-to-server flow sessions that are ignored.
Server-to-client flows ignored	Number of server-to-client flow sessions that are ignored.
Server-to-client flows tcp optimized	Number of server-to-client flow TCP sessions that are optimized.

Table 61: show security idp counters flow Output Fields (continued)

Field Name	Description
Client-to-server flows tcp optimized	Number of client-to-server flow TCP sessions that are optimized.
Both directions flows ignored	Number of server-to-client and client-to-server flow sessions that are ignored.
Fail-over sessions dropped	Number of failover sessions dropped.
Sessions dropped due to no policy	Number of sessions dropped because there was no active IDP policy.
IDP Stream Sessions dropped due to memory failure	Number of IDP stream sessions that are dropped because of memory failure.
IDP Stream Sessions ignored due to memory failure	Number of IDP stream sessions that are ignored because of memory failure.
IDP Stream Sessions closed due to memory failure	Number of IDP stream sessions that are closed because of memory failure.
IDP Stream Sessions accepted	Number of IDP stream sessions that are accepted.
IDP Stream Sessions constructed	Number of IDP stream sessions that are constructed.
IDP Stream Sessions destructed	Number of IDP stream sessions that are destructed.
IDP Stream Move Data	Number of stream data events handled by IDP.
IDP Stream Sessions ignored on JSF SSL Event	Number of IDP stream sessions that are ignored because of a JSF SSL proxy event.
IDP Stream Sessions not processed for no matching rules	Number of IDP stream sessions that are not processed for no matching rules.
IDP Stream stbuf dropped	Number of IDP stream plug-in buffers dropped.
IDP Stream stbuf reinjected	Number of IDP stream plug-in buffers injected.
Busy packets from stream plugin	Number of packets saved as one or more packets of this session from stream plug-in.
Busy packets from packets plugin	Number of saved packets for IDP stream plug-in sessions.
Bad kpp	Number of internal marked packets logged for IDP processing.
Lsys policy id lookup failed sessions	Number of sessions that failed logical systems policy lookup.
Busy packets	Number of packets saved as one or more packets of this session are handed off for asynchronous processing.
Busy packet errors	Number of packets found with IP checksum error after asynchronous processing is completed.

Table 61: show security idp counters flow Output Fields (continued)

Field Name	Description
Dropped queued packets (async mode)	Number of queued packets dropped based on policy action, reinjection failures, or if the session is marked to destruct.
Dropped queued packets failed (async mode)	Not used currently.
Reinjected packets (async mode)	Number of packets reinjected into the queue.
Reinjected packets failed (async mode)	Number of failed reinjected packets.
AI saved processed packet	Number of AI packets saved for which the asynchronous processing is completed.
Busy packet count incremented	Number of times the busy packet count incremented in asynchronous processing.
busy packet count decremented	Number of times the busy packet count decremented in asynchronous processing.
session destructed in pme	Number of sessions destructed as a part of asynchronous result processing.
session destruct set in pme	Number of sessions set to be destructed as a result of asynchronous processing.
KQ op	Number of sessions with one of the following status: <ul style="list-style-type: none"> KQ op hold—number of times packets held by IDP. KQ op drop—number of times packets dropped by IDP. KQ op route—number of times IDP decided to be route the packet directly. KQ op Continue—number of times IDP decided to continue to process the packet. KQ op error—number of times error occurred while IPD processing packet. KQ op stop—number of times IDP decided to stop processing the packet.
PME wait not set	Number of AI saved packets given for signature matching.
PME wait set	Number of packets given for signature matching without AI save.
PME KQ run not called	Number of times signature matching results processed out of packet receiving order.

Sample Output

show security idp counters flow

```
user@host> show security idp counters flow
IDP counters:
```

IDP counter type	Value
Fast-path packets	40252
Slow-path packets	127
Session construction failed	0

Session limit reached	0
Session inspection depth reached	0
Memory limit reached	0
Not a new session	0
Invalid index at ageout	0
Packet logging	0
Policy cache hits	92
Policy cache misses	67
Policy cache entries	67
Maximum flow hash collisions	0
Flow hash collisions	0
Gates added	0
Gate matches	0
Sessions deleted	127
Sessions aged-out	0
Sessions in-use while aged-out	0
TCP flows marked dead on RST/FIN	13
Policy init failed	0
Number of times Sessions exceed high mark	0
Number of times Sessions drop below low mark	0
Memory of Sessions exceeds high mark	0
Memory of Sessions drops below low mark	0
SM Sessions encountered memory failures	0
SM Packets on sessions with memory failures	0
IDP session gate creation requests	0
IDP session gate creation acknowledgements	0
IDP session gate hits	0
IDP session gate timeouts	0
Number of times Sessions crossed the CPU threshold value that is set	0
Number of times Sessions crossed the CPU upper threshold	0
Sessions constructed	127
SM Sessions ignored	0
SM Sessions dropped	0
SM Sessions interested	168
SM Sessions not interested	4
SM Sessions interest error	0
Sessions destructed	127
SM Session Create	127
SM Packet Process	52257
SM ftp data session ignored by idp	0
SM Session close	127
SM Client-to-server packets	20066
SM Server-to-client packets	32191
SM Client-to-server L7 bytes	167292
SM Server-to-client L7 bytes	28523514
Client-to-server flows ignored	1
Server-to-client flows ignored	1
Server-to-client flows tcp optimized	3
Client-to-server flows tcp optimized	0
Both directions flows ignored	32
Fail-over sessions dropped	0
Sessions dropped due to no policy	0
IDP Stream Sessions dropped due to memory failure	0
IDP Stream Sessions ignored due to memory failure	0
IDP Stream Sessions closed due to memory failure	0
IDP Stream Sessions accepted	0
IDP Stream Sessions constructed	0
IDP Stream Sessions destructed	0
IDP Stream Move Data	0
IDP Stream Sessions ignored on JSF SSL Event	0

IDP Stream Sessions not processed for no matching rules	0
IDP Stream stbuf dropped	0
IDP Stream stbuf reinjected	0
Busy pkts from stream plugin	0
Busy pkts from pkt plugin	0
bad kpp	0
Lsys policy id lookup failed sessions	0
Busy packets	0
Busy packet Errors	0
Dropped queued packets (async mode)	0
Dropped queued packets failed(async mode)	0
Reinjected packets (async mode)	0
Reinjected packets failed(async mode)	0
AI saved processed packet	0
busy packet count incremented	0
busy packet count decremented	0
session destructed in pme	0
session destruct set in pme	0
kq op hold	0
kq op drop	0
kq op route	0
kq op continue	35155
kq op error	0
kq op stop	0
PME wait not set	0
PME wait set	0
PME KQ run not called	0

show security idp counters http-decoder

Syntax	show security idp counters http-decoder show security idp counters http-decoder logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display the status of all HTTP decoders.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear security idp counters http-decoder on page 578
List of Sample Output	show security idp counters http-decoder on page 655 show security idp counters http-decoder logical-system LSYS1 on page 656
Output Fields	Table 62 on page 655 lists the output fields for the show security idp counters http-decoder command. Output fields are listed in the approximate order in which they appear.

Table 62: show security idp counters http-decoder Output Fields

Field Name	Field Description
No of file-decoder requests from MIME over HTTP	Number of active file decoder requests sent over HTTP from MIME.
No of pending file-decoder requests from MIME over HTTP	Number of pending file decoder requests sent over HTTP from MIME.
No of completed file-decoder requests from MIME over HTTP	Number of completed file decoder requests sent over HTTP from MIME.
No of unrecognized file type from MIME over HTTP	Number of unrecognized file types sent over HTTP from MIME.
No of compressed payload transferred over HTTP	Number of compressed files transferred over HTTP from MIME.

Sample Output

show security idp counters http-decoder

```

user@host> show security idp counters http-decoder
IDP counters:
IDP counter type                               Value
No of file-decoder requests from MIME over HTTP      0
No of pending file-decoder requests from MIME over HTTP 0

```

No of completed file-decoder requests from MIME over HTTP	0
No of unrecognized file type from MIME over HTTP	0
No of compressed payload transferred over HTTP	0
No of bypassed files over HTTP	0

`show security idp counters http-decoder logical-system LSYS1`

```
user@host> show security idp counters http-decoder logical-system LSYS1
IDP counters:
```

IDP counter type	Value
No of file-decoder requests from MIME over HTTP	0
No of pending file-decoder requests from MIME over HTTP	0
No of completd file-decoder requests from MIME over HTTP	0
No of unrecognized file type from MIME over HTTP	0
No of compressed payload transferred over HTTP	0
No of bypassed files over HTTP	0

show security idp counters packet-log

Syntax	show security idp counters packet-log show security idp counters packet-log logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 10.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display the values of all IDP packet-log counters.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear security idp counters packet-log on page 579
Output Fields	The following table lists the output fields for the show security idp counters packet-log command. Output fields are listed in the approximate order in which they appear.

Field Name	Field Description
Total packets captured since packet capture was activated	Number of packets captured by the device by the IDP service.
Total sessions enabled since packet capture was activated	Number of sessions that have performed packet capture since the capture facility was activated.
Sessions currently enabled for packet capture	Number of sessions that are actively capturing packets at this time.
Packets currently captured for enabled sessions	Number of packets that have been captured by active sessions.
Packet clone failures	Number of packet capture failures due to cloning error.
Session log object failures	Number of objects containing log messages generated during packet capture that were not successfully transmitted to the host.
Session packet log object failures	Number of objects containing captured packets that were not successfully transmitted to the host.
Sessions skipped because session limit exceeded	Number of sessions that could not initiate packet capture because the maximum number of sessions specified for the device were conducting captures at that time.
Packets skipped because packet limit exceeded	Number of packets not captured because the packet limit specified for this device was reached.
Packets skipped because total memory limit exceeded	Number of packets not captured because the memory allocated for packet capture on this device was exceeded.

Sample Output

show security idp counters packet-log

```
user@host> show security idp counters packet-log
IDP counters:
Total packets captured since packet capture was activated      0
Total sessions enabled since packet capture was activated      0
Sessions currently enabled for packet capture                  0
Packets currently captured for enabled sessions                0
Packet clone failures                                         0
Session log object failures                                    0
Session packet log object failures                             0
Sessions skipped because session limit exceeded               0
Packets skipped because packet limit exceeded                  0
Packets skipped because total memory limit exceeded            0
```

show security idp counters http-decoder logical-system LSYS1

```
user@host> show security idp counters http-decoder logical-system LSYS1
IDP counters:

IDP counter type                                             Value
No of file-decoder requests from MIME over HTTP              0
No of pending file-decoder requests from MIME over HTTP      0
No of completd file-decoder requests from MIME over HTTP     0
No of unrecognized file type from MIME over HTTP              0
No of compressed payload transferred over HTTP                0
No of bypassed files over HTTP                                0
```

show security idp counters packet

Syntax	show security idp counters packet show security idp counters packet logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. The fields Dropped by IDP policy and Dropped by Error added in Junos OS Release 10.1. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the status of all IDP packet counter values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear security idp counters packet on page 580
List of Sample Output	show security idp counters packet on page 661 show security idp counters packet logical-system LSYS1 on page 661
Output Fields	Table 63 on page 659 lists the output fields for the show security idp counters packet command. Output fields are listed in the approximate order in which they appear.

Table 63: show security idp counters packet Output Fields

Field Name	Field Description
Processed packets	Number of packets processed by the IDP service.
Dropped packets	Number of packets dropped by the IDP service. The counter for all dropped packets.
Dropped by IDP policy	Number of packets dropped by the IDP policy. The counter for dropped packets due to the action specified in the IDP policy (starting with the attack detection).
Dropped by Error	Number of packets dropped by error. The difference between Dropped packets and Dropped by IDP policy . IDS drops are primarily due to policy actions. Reassembly errors lead to packet drops. So all drops shown in show security idp counters ips , show security idp counters flow and show security idp counters tcp-reassembler add to Dropped by Error . All drops includes reassembly errors, anomalies similar to bad ip header and TTL errors.
Dropped sessions	Number of sessions dropped.
(Unsupported)	

Table 63: show security idp counters packet Output Fields (continued)

Field Name	Field Description
Bad IP headers	Number of packets that fail IP header length validity check.
Packets with IP options	Number of packets that contain the optional header fields.
Decapsulated packets	Number of packets that are decapsulated.
GRE decapsulations (Unsupported)	Number of packets that are generic routing encapsulation (GRE) decapsulated.
PPP decapsulations (Unsupported)	Number of packets that are Point-to-Point Protocol (PPP) decapsulated.
TCP decompression uncompressed IP (Unsupported)	Number of uncompressed IP headers that are to be TCP decompressed.
TCP decompression compressed IP (Unsupported)	Number of compressed IP headers that are to be TCP decompressed.
Deferred-send packets (Unsupported)	Number of deferred IP packets that are sent out.
IP-in-IP packets (Unsupported)	Number of packets that are IP-in-IP encapsulated.
TTL errors (Unsupported)	Number of packets with TTL error in the header.
Routing loops (Unsupported)	Number of packets that continue to be routed in an endless circle due to an inconsistent routing state.
No-route packets (Unsupported)	Number of packets that could not be routed further.
Flood IP (Unsupported)	Number of packets that are identified as IP flood packets.
Invalid ethernet headers (Unsupported)	Number of packets that are identified with an invalid Ethernet header.
Packets attached	Number of packets attached.

Table 63: show security idp counters packet Output Fields (continued)

Field Name	Field Description
Packets cloned	Number of packets that are cloned.
Packets allocated	Number of packets allocated.
Packets destructed	Number of packets destructed.

Sample Output

show security idp counters packet

```

user@host> show security idp counters packet
IDP counters:
IDP counter type                               Value
Processed packets                             27
Dropped packets                               0
Dropped by IDP policy                         0
Dropped by error                             0
Dropped sessions                             0
Bad IP headers                                0
Packets with IP options                       0
Decapsulated packets                         0
GRE decapsulations                           0
PPP decapsulations                           0
TCP decompression uncompressed IP             0
TCP decompression compressed IP              0
Deferred-send packets                        0
IP-in-IP packets                             0
TTL errors                                    0
Routing loops                                0
STP drops                                    0
No-route packets                             0
Flood IP                                      0
Invalid ethernet headers                     0
Packets attached                             28
Packets cloned                               28
Packets allocated                             0
Packets destructed                           55

```

show security idp counters packet logical-system LSYS1

```

user@host> show security idp counters packet logical-system LSYS1
IDP counters:

IDP counter type                               Value
Processed packets                             64
Dropped packets                               0
Dropped ICMP packets                         0
Dropped TCP packets                         0
Dropped UDP packets                         0
Dropped Other packets                       0
Dropped by IDP Policy                       0
Dropped by Error                           0
Dropped sessions                           0
Bad IP headers                              0

```

Packets with IP options	0
Decapsulated packets	0
GRE decapsulations	0
PPP decapsulations	0
GTP decapsulations	0
GTP flows	0
TCP decompression uncompressed IP	0
TCP decompression compressed IP	0
Deferred-send packets	0
IP-in-IP packets	0
TTL errors	0
Routing loops	0
STP drops	0
No-route packets	0
Flood IP	0
Invalid ethernet headers	0
Packets attached	64
IP Packet attach failed	0
Packets cloned	25
Packets allocated	0
Packets destructed	89
Packet data buffer allocated	24
Packet data buffer released	24
Buffer allocation on clone avoided	0
Late buffer allocation on clone	0
Distinct clone request	0
KPP clone buf cache allocated	0
KPP clone buf cache released	0
KPP clone buf cache used	0
KQMSG constructed	69
KQMSG destructed	69
jbuf copy failed	0
jbuf pullup failed	0
jbuf copy done	0
jbuf copy freed	0
jbuf copy reinjected	0

show security idp counters policy-manager

Syntax	show security idp counters policy-manager show security idp counters policy-manager logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the status of all IDP policies counter values.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear security idp counters policy-manager on page 581
List of Sample Output	show security idp counters policy-manager on page 663 show security idp counters policy-manager logical-system LSYS1 on page 663
Output Fields	Table 64 on page 663 lists the output fields for the show security idp counters policy-manager command. Output fields are listed in the approximate order in which they appear.

Table 64: show security idp counters policy-manager Output Fields

Field Name	Field Description
Number of policies	Number of policies installed.
Number of aged out policies	Number of IDP policies that are expired.

Sample Output

show security idp counters policy-manager

```

user@host> show security idp counters policy-manager
IDP counters:
  IDP counter type          Value
  Number of policies        0
  Number of aged out policies 0

```

show security idp counters policy-manager logical-system LSYS1

```

user@host> show security idp counters policy-manager logical-system LSYS1
IDP counters:
  IDP counter type          Value
  Number of policies        1
  Number of aged out policies 0
  Policy compile failure due to memory 0

```


show security idp counters tcp-reassembler


Syntax	show security idp counters tcp-reassembler show security idp counters tcp-reassembler logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the status of all TCP reassembler counter values.
	<div>  <p>NOTE: On SRX Series devices with IDP enabled, if IDP attacks are configured for a single direction (server or client), a flow in the opposite direction does not need IDP processing. For TCP traffic, the TCP optimization feature ensures minimal processing for these flows without running into reassembly errors.</p> </div>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>re-assembler</i> • clear security idp counters tcp-reassembler on page 572
List of Sample Output	show security idp counters tcp-reassembler on page 667 show security idp counters tcp-reassembler logical-system LSYS1 on page 668
Output Fields	Table 65 on page 665 lists the output fields for the show security idp counters tcp-reassembler command. Output fields are listed in the approximate order in which they appear.

Table 65: show security idp counters tcp-reassembler Output Fields

Field Name	Field Description
Bad TCP checksums (Unsupported)	Number of packets that have incorrect TCP checksums.
Bad TCP headers	Number of bad TCP headers detected.
Slow path segments	Number of segments that are sent through the slow path if the TCP segment does not pass fast-path segment validation.
Fast path segments	Number of segments that are sent through the fast path after passing a predefined TCP validation sequence.
Tcp Optimized s2c segments	Number of TCP segments that are sent through optimized re-assembly process from server to client.

Table 65: show security idp counters tcp-reassembler Output Fields (continued)

Field Name	Field Description
Tcp Optimized c2s segments	Number of TCP segments that are sent through optimized re-assembly process from server to client.
Sequence number wrap around errors	Number of packets that wrap around of the sequence number.
Session reuses	Number of sessions that reused an already established TCP session.
SYN retransmissions	Number of SYN packets that are retransmitted.
Bad three way handshake acknowledgements	Number of packets that have incorrect three-way handshake acknowledgements (ACK packet).
Sequence number out of sync flows	Number of packets that have out-of-sync sequence numbers.
Fast path pattern matches in queued up streams	Number of queued packets that have fast path pattern match.
New segments with no overlaps with old segment	Number of new segments that do not overlap with old segment.
New segment overlaps with beginning of old segment	Number of new segments that overlap with beginning of old segment.
New segment overlaps completely with old segment	Number of new segments that overlap completely with old segment.
New segment is contained in old segment	Number of new segments contained in old segment.
New segment overlaps with end of old segment	Number of new segments that overlap with the end of old segment.
New segment begins after end of old segment	Number of new segments that overlap after the end of old segment.
Memory consumed by new segment	Memory that is consumed by the new segment.
Peak memory consumed by new segments	Peak memory that is consumed by the new segment.
Segments in memory	Number of segments that are stored in memory for processing.
Per-flow memory overflows	Number of segments dropped after reaching per flow memory limit.
Global memory overflows	Number of segments dropped after reaching reassembler global memory limit.
Overflow drops	Number of packets that are dropped due to memory overflow.

Table 65: show security idp counters tcp-reassembler Output Fields (continued)

Field Name	Field Description
Copied packets (Unsupported)	Number of packets copied in reassembler.
Closed Acks	Number of Ack packets seen without having seen SYN on the same session.
Ack Validation failures	Number of Invalid ACKs received from server during 3-way handshake.
Simultaneous syn	Number of simultaneous syn packets seen.
C2S synack	Number of C2S Syn/Ack packets seen.
Segment to left of receiver window	Number of segments falling left of receive window.
Segment to right of receiver window	Number of segments falling right of receive window.
SYN seen in the window	Number of Syn packets seen after connection establishment.
ACK bit is off	Number of packets seen without ACK after connection establishment.
Unexpected FIN	Number of unexpected FIN packets seen.
Duplicate Syn/Ack with different SEQ	Number of Syn/Ack packets with different SEQ numbers.

Sample Output

show security idp counters tcp-reassembler

```
user@host> show security idp counters tcp-reassembler
IDP counters:
```

IDP counter type	Value
Bad TCP checksums	0
Bad TCP headers	0
Slow path segments	90
Fast path segments	7099
Tcp Optimized s2c segments	0
Tcp Optimized c2s segments	0
Sequence number wrap around errors	0
Session reuses	0
SYN retransmissions	0
Bad three way handshake acknowledgements	0
Sequence number out of sync flows	0
Fast path pattern matches in queued up streams	0
New segments with no overlaps with old segment	0
New segment overlaps with beginning of old segment	0
New segment overlaps completely with old segment	0
New segment is contained in old segment	0
New segment overlaps with end of old segment	0
New segment begins after end of old segment	3
Memory consumed by new segment	0

Peak memory consumed by new segments	3821
Segments in memory	0
Per-flow memory overflows	0
Global memory overflows	0
Overflow drops	0
Copied packets	0
Closed Acks	3
Ack Validation failure	0
Simultaneous syn	0
C2S synack	0
segment to left of receiver window	0
segment to right of receiver window	0
SYN seen in the window	0
ACK bit is off	0
Unexpected FIN	0
Duplicate Syn/Ack with different SEQ	0

show security idp counters tcp-reassembler logical-system LSYS1

```
user@host> show security idp counters tcp-reassembler logical-system LSYS1
IDP counters:
```

IDP counter type	Value
Bad TCP checksums	0
Bad TCP headers	0
Slow path segments	37
Fast path segments	27
Tcp Optimized s2c segments	0
Tcp Optimized c2s segments	0
Sequence number wrap around errors	0
Session reuses	0
SYN retransmissions	0
Bad three way handshake acknowledgements	0
Sequence number out of sync flows	0
Fast path pattern matches in queued up streams	0
New segments with no overlaps with old segment	0
New segment overlaps with beginning of old segment	0
New segment overlaps completely with old segment	0
New segment is contained in old segment	0
New segment overlaps with end of old segment	0
New segment begins after end of old segment	0
Memory consumed by new segment	0
Peak memory consumed by new segments	2021
Segments in memory	0
Per-flow memory overflows	0
Global memory overflows	0
Overflow drops	0
Overflow drops - missing packets	0
Copied packets	0
Closed Acks	0
Ack Validation failure	0
Simultaneous syn	0
C2S synack	0
segment to left of receiver window	0
segment to right of receiver window	0
SYN seen in the window	0
ACK bit is off	0
Unexpected FIN	0
Duplicate Syn/Ack with different SEQ	0

show security idp logical-system policy-association

Syntax	show security idp logical-system policy-association
Release Information	Command introduced in Junos OS Release 11.3.
Description	Display the IDP policy assigned to a logical system. The IDP policy is assigned to a logical system through the security profile.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> security-profile on page 543
List of Sample Output	show security idp logical-system policy-association on page 669
Output Fields	Table 66 on page 669 lists the output fields for the show security idp logical-system policy-association command.

Table 66: show security idp logical-system policy-association Output Fields

Field Name	Field Description
Logical system	Name of the logical system to which an IDP policy is assigned.
IDP policy	Name of the IDP policy that is specified in the security profile that is bound to the logical system.

Sample Output

show security idp logical-system policy-association

```

user@host> show security idp logical-system policy-association
Logical system      IDP policy
root-logical-system idp-policy1
lsys1               idp-policy2

```

show security idp policies

Syntax	show security idp policies show security idp policies logical-system <i>logical-system</i>
Release Information	Command introduced in Junos OS Release 10.1. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the list of currently installed policies.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>show security idp active-policy</i>
Output Fields	

Sample Output

show security idp policies

```
user@host>show security idp policies
Subscriber:  s0,          Installed policies:  1

  ID      Name      Sessions      Memory      detector
  0       new1       0            10179       9.2.160090324
```

show security idp policies logical-system LSYS0

```
user@host> show security idp policies logical-system LSYS0
PIC : FPC 0 PIC 0:
ID      Name              Sessions      Memory      Detector
53                                     0           189712      12.6.130180509
```

show security idp policy-commit-status

Syntax	show security idp policy-commit-status show security idp policy-commit-status logical-system <i>logical-system</i>
Release Information	Command introduced in JUNOS OS Release 10.4. Starting with Junos OS Release 12.3X48-D15 and Junos OS Release 17.3R1, a new pattern matching engine is introduced for the SRX Series IDP feature. This scanning mechanism helps improve performance and policy loading. The new engine is 9.223 times faster than the existing DFA engine. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the IDP policy commit status. For example, status of policy compilation or load.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show security idp status • show security idp policy-commit-status clear
List of Sample Output	show security idp policy-commit-status on page 671 show security idp policy-commit-status logical-system LSYS1 on page 671

Sample Output

show security idp policy-commit-status

```
user@host> show security idp policy-commit-status
IDP policy[/var/db/idpd/bins/test.bin.gz.v] and
detector[/var/db/idpd/sec-repository/installed-detector/libidp-detector.so.tgz.v]
loaded successfully.

The loaded policy size is:45583070 Bytes
```

Sample Output

show security idp policy-commit-status logical-system LSYS1

```
user@host> show security idp policy-commit-status logical-system LSYS1
IDP policy[/var/db/idpd/bins//idp-policy-combined.bin.gz.v] and
detector[/var/db/idpd/sec-repository/installed-detector/libidp-detector.so.tgz.v]
loaded successfully.
The loaded policy size is:7416 Bytes
```

show security idp policy-templates-list

Syntax	show security idp policy-templates-list
Release Information	Command introduced in Junos OS Release 10.1. Command introduced for user logical system in Junos OS Release 18.3R1.
Description	Display the list of available policy templates for logical systems.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>show security idp active-policy</i>

Sample Output

show security idp policy-templates-list

```
user@host>show security idp policy-templates-list
  Web_Server
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Server-Protection
Server-Protection-1G
Client-Protection
Client-Protection-1G
Client-And-Server-Protection
Client-And-Server-Protection-1G
Recommended
```


show security idp security-package-version

Syntax	show security idp security-package-version
Release Information	Command introduced in Junos OS Release 9.2. Command introduced for user logical systems in Junos OS Release 18.3R1.
Description	Display information of the currently installed security package version and detector version.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>security-package</i> • <i>request security idp security-package download</i> • <i>request security idp security-package install</i>
List of Sample Output	show security idp security-package-version on page 673 show security idp security-package-version on page 673
Output Fields	Table 67 on page 673 lists the output fields for the show security idp security-package-version command. Output fields are listed in the approximate order in which they appear.

Table 67: show security idp security-package-version Output Fields

Field Name	Field Description
Attack database version	Attack database version number that is currently installed on the system.
Detector version	Detector version number that is currently installed on the system.
Policy template version	Policy template version number that is currently installed on the system.

Sample Output

show security idp security-package-version

```
user@host> show security idp security-package-version
Attack database version:1154(Mon Apr 28 15:08:42 2008)
Detector version :9.1.140080400
Policy template version :7
```

show security idp security-package-version

```
user@host:LSYS1> show security idp security-package-version
```

Attack database version:1154(Mon Apr 28 15:08:42 2008)
Detector version :9.1.140080400
Policy template version :7

show security ike security-associations

Syntax `show security ike security-associations`
`<peer-address>`
`<brief | detail>`
`<family (inet | inet6)>`
`<fpc slot-number>`
`<index SA-index-number>`
`<kmd-instance (all | kmd-instance-name)>`
`<pic slot-number>`
`<sa-type shortcut >`

Release Information Command introduced in Junos OS Release 8.5. Support for the **fpc**, **pic**, and **kmd-instance** options added in Junos OS Release 9.3. Support for the **family** option added in Junos OS Release 11.1. Support for Auto Discovery VPN added in Junos OS Release 12.3X48-D10. Support for IKEv2 reauthentication added in Junos OS Release 15.1X49-D60. Support for IKEv2 fragmentation added in Junos OS Release 15.1X49-D80.

Description Display information about Internet Key Exchange security associations (IKE SAs).

- Options**
- **none**—Display standard information about existing IKE SAs, including index numbers.
 - **peer-address**—(Optional) Display details about a particular SA based on the IPv4 or IPv6 address of the destination peer. This option and **index** provide the same level of output.
 - **brief**—(Optional) Display standard information about all existing IKE SAs. (Default)
 - **detail**—(Optional) Display detailed information about all existing IKE SAs.
 - **family**—(Optional) Display IKE SAs by family. This option is used to filter the output.
 - **inet**—IPv4 address family.
 - **inet6**—IPv6 address family.
 - **fpc slot-number**—(Optional) Display information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.



NOTE: In a chassis cluster, when you execute the CLI command `show security ike security-associations pic <slot-number> fpc <slot-number>` in operational mode, only the primary node information about the existing IPsec SAs in the specified Flexible PIC Concentrator (FPC) slot and PIC slot is displayed.

- **index SA-index-number**—(Optional) Display information for a particular SA based on the index number of the SA. For a particular SA, display the list of existing SAs by using the command with no options. This option and **peer-address** provide the same level of output.

- **kmd-instance** —(Optional) Display information about existing IKE SAs in the key management process (in this case, it is KMD) identified by FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.
 - **all**—All KMD instances running on the Services Processing Unit (SPU).
 - **kmd-instance-name**—Name of the KMD instance running on the SPU.
- **pic slot-number** —(Optional) Display information about existing IKE SAs in this PIC slot. This option is used to filter the output.
- **sa-type**—(Optional for ADVPN) Type of SA. **shortcut** is the only option for this release.

Required Privilege Level view

Related Documentation [• Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems on page 180](#)

List of Sample Output [show security ike security-associations \(IPv4\) on page 679](#)
[show security ike security-associations \(IPv6\) on page 679](#)
[show security ike security-associations detail \(SRX300, SRX320, SRX340, SRX345, and SRX550HM Devices\) on page 679](#)
[show security ike security-associations detail \(SRX5400, SRX5600, and SRX5800 Devices\) on page 680](#)
[show security ike security-associations family inet6 on page 680](#)
[show security ike security-associations index 222075191 detail on page 681](#)
[show security ike security-associations index 788674 detail on page 681](#)
[show security ike security-associations 192.168.1.2 on page 682](#)
[show security ike security-associations fpc 6 pic 1 kmd-instance all \(SRX Series Devices\) on page 682](#)
[show security ike security-associations detail \(ADVPN Suggester, Static Tunnel\) on page 682](#)
[show security ike security-associations detail \(ADVPN Partner, Static Tunnel\) on page 683](#)
[show security ike security-associations detail \(ADVPN Partner, Shortcut\) on page 683](#)
[show security ike security-associations sa-type shortcut \(ADVPN\) on page 683](#)
[show security ike security-associations sa-type shortcut detail \(ADVPN\) on page 683](#)
[show security ike security-associations detail \(IKEv2 Reauthentication\) on page 684](#)
[show security ike security-associations detail \(IKEv2 Fragmentation\) on page 684](#)

Output Fields [Table 68 on page 676](#) lists the output fields for the **show security ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 68: show security ike security-associations Output Fields

Field Name	Field Description
IKE Peer or Remote Address	IP address of the destination peer with which the local peer communicates.

Table 68: show security ike security-associations Output Fields (continued)

Field Name	Field Description
Index	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
Gateway Name	Name of the IKE gateway.
Location	<ul style="list-style-type: none"> • FPC—Flexible PIC Concentrator (FPC) slot number. • PIC—PIC slot number. • KMD-Instance—The name of the KMD instance running on the SPU, identified by <i>FPC slot-number</i> and <i>PIC slot-number</i>. Currently, 4 KMD instances are running on each SPU, and any particular IKE negotiation is carried out by a single KMD instance.
Role	Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder.
State	<p>State of the IKE SAs:</p> <ul style="list-style-type: none"> • DOWN—SA has not been negotiated with the peer. • UP—SA has been negotiated with the peer.
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.
Responder cookie	<p>Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.</p> <p>A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.</p>
Exchange type	<p>Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between one another. Each exchange type or mode determines the number of messages and the payload types that are contained in each message. The modes are:</p> <ul style="list-style-type: none"> • main—The exchange is done with six messages. This mode encrypts the payload, protecting the identity of the neighbor. • aggressive—The exchange is done with three messages. This mode does not encrypt the payload, leaving the identity of the neighbor unprotected. <p>NOTE: IKEv2 protocol does not use the mode configuration for negotiation. Therefore, the mode displays the version number of the security association.</p>
Authentication method	Method used to authenticate the source of IKE messages, which can be either Pre-shared-keys or digital certificates, such as DSA-signatures , ECDSA-signatures-256 , ECDSA-signatures-384 , or RSA-signatures .
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Table 68: show security ike security-associations Output Fields (continued)

Field Name	Field Description
Reauth Lifetime	When enabled, number of seconds remaining until reauthentication triggers a new IKEv2 SA negotiation.
IKE Fragmentation	<p>Enabled means that both the IKEv2 initiator and responder support message fragmentation and have negotiated the support during the IKE_SA_INIT message exchange.</p> <p>Size shows the maximum size of an IKEv2 message before it is fragmented.</p>
Algorithms	<p>IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:</p> <ul style="list-style-type: none"> • Authentication—Type of authentication algorithm used: <ul style="list-style-type: none"> • sha1—Secure Hash Algorithm 1 authentication. • md5—MD5 authentication. • Encryption—Type of encryption algorithm used: <ul style="list-style-type: none"> • aes-256-cbc—Advanced Encryption Standard (AES) 256-bit encryption. • aes-192-cbc—AES 192-bit encryption. • aes-128-cbc—AES 128-bit encryption. • 3des-cbc—3 Data Encryption Standard (DES) encryption. • des-cbc—DES encryption.
Diffie-Hellman group	Specifies the IKE Diffie-Hellman group.
Traffic statistics	<ul style="list-style-type: none"> • Input bytes—Number of bytes received. • Output bytes—Number of bytes transmitted. • Input packets—Number of packets received. • Output packets—Number of packets transmitted. • Input fragmented packets—Number of IKEv2 fragmented packets received. • Output fragmented packets—Number of IKEv2 fragmented packets transmitted.
Flags	<p>Notification to the key management process of the status of the IKE negotiation:</p> <ul style="list-style-type: none"> • caller notification sent—Caller program notified about the completion of the IKE negotiation. • waiting for done—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • waiting for remove—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • waiting for policy manager—Negotiation is waiting for a response from the policy manager.
IPSec security associations	<ul style="list-style-type: none"> • number created: The number of SAs created. • number deleted: The number of SAs deleted.

Table 68: show security ike security-associations Output Fields (continued)

Field Name	Field Description
Phase 2 negotiations in progress	<p>Number of Phase 2 IKE negotiations in progress and status information:</p> <ul style="list-style-type: none"> • Negotiation type—Type of Phase 2 negotiation. Junos OS currently supports quick mode. • Message ID—Unique identifier for a Phase 2 negotiation. • Local identity—Identity of the local Phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)</i>. • Remote identity—Identity of the remote Phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)</i>. • Flags—Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> • caller notification sent—Caller program notified about the completion of the IKE negotiation. • waiting for done—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • waiting for remove—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • waiting for policy manager—Negotiation is waiting for a response from the policy manager.

Sample Output

show security ike security-associations (IPv4)

```

user@host> show security ike security-associations
Index Remote Address State Initiator cookie Responder cookie Mode
8 192.168.1.2 UP 3a895f8a9f620198 9040753e66d700bb Main
Index Remote Address State fInitiator cookie Responder cookie Mode
9 192.168.1.3 UP 5ba96hfa9f65067 70890755b65b80b Main

```

show security ike security-associations (IPv6)

```

user@host> show security ike security-associations
Index State Initiator cookie Responder cookie Mode Remote Address
5 UP e48efd6a444853cf 0d09c59aafb720be Aggressive 2001:db8::1112

```

show security ike security-associations detail (SRX300, SRX320, SRX340, SRX345, and SRX550HM Devices)

```

user@host> show security ike security-associations detail
IKE peer 192.168.134.245, Index 2577565, Gateway Name: tropic
Role: Initiator, State: UP
Initiator cookie: b869b3424513340a, Responder cookie: 4cb3488cb19397c3
Exchange type: Main, Authentication method: Pre-shared-keys Trusted CA group:
xyz_ca_grp
Local: 192.168.134.241:500, Remote: 192.168.134.245:500
Lifetime: Expires in 169 seconds
Peer ike-id: 192.168.134.245
AAA assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : aes128-cbc
Pseudo random function: hmac-sha1

```

```

Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes :          1012
  Output bytes :         1196
  Input packets:          4
  Output packets:         5
Flags: IKE SA is created
IPSec security associations: 1 created, 0 deleted
Phase 2 negotiations in progress: 0

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local: 192.168.134.241:500, Remote: 192.168.134.245:500
Local identity: 192.168.134.241
Remote identity: 192.168.134.245
Flags: IKE SA is created

```

show security ike security-associations detail (SRX5400, SRX5600, and SRX5800 Devices)

```

user@host> show security ike security-associations detail
IKE peer 192.168.2, Index 914039858, Gateway Name: tropic
Location: FPC 3, PIC 1, KMD-Instance 3
Role: Initiator, State: UP
Initiator cookie: 219a697652bdde37, Responder cookie: b49c30b229d36bcd
Exchange type: Aggressive, Authentication method: Pre-shared-keys Trusted CA
group: xyz_ca_grp
Local: 192.168.1.1:500, Remote: 192.168.1.2:500
Lifetime: Expires in 26297 seconds
Peer ike-id: 192.168.1.2
AAA user-name: not available
AAA assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha1-96
  Encryption          : 3des-cbc
  Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes :          0
  Output bytes :          0
  Input packets:          0
  Output packets:         0
IPSec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

```

show security ike security-associations family inet6

```

user@host> show security ike security-associations family inet6
IKE peer 2001:db8:1212::1112, Index 5, Gateway Name: tropic
Role: Initiator, State: UP
Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aafb720be
Exchange type: Aggressive, Authentication method: Pre-shared-keys
Local: 2001:db8:1212::1111:500, Remote: 2001:db8:1212::1112:500
Lifetime: Expires in 19518 seconds
Peer ike-id: not valid
AAA assigned IP: 0.0.0.0
Algorithms:
  Authentication      : sha1
  Encryption          : 3des-cbc
  Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:

```



```

Input bytes :          1568
Output bytes :         2748
Input packets:           6
Output packets:         23
Flags: Caller notification sent
IPSec security associations: 5 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 2900338624
Local: 2001:db8:1212::1111:500, Remote: 2001:db8:1212::1112:500
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Flags: Caller notification sent, Waiting for done

```

show security ike security-associations index 222075191 detail

```

user@host> show security ike security-associations index 222075191 detail
node0:
-
IKE peer 192.168.1.2, Index 222075191, Gateway Name: ZTH_HUB_GW
Location: FPC 0, PIC 3, KMD-Instance 2
Auto Discovery VPN:
Type: Static, Local Capability: Suggester, Peer Capability: Partner
Suggester Shortcut Suggestions Statistics:
  Suggestions sent      :    2
  Suggestions accepted:    4
  Suggestions declined:    1
Role: Responder, State: UP
Initiator cookie: 7b996b4c310d2424, Responder cookie: 5724c5882a212157
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 192.168.1.1:500, Remote: 192.168.1.2:500
Lifetime: Expires in 828 seconds
Peer ike-id: C=US, DC=example, ST=CA, L=Sunnyvale, O=example, OU=engineering,
CN=cssvk36-d
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : aes256-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input bytes :          20474
Output bytes :         21091
Input packets:           237
Output packets:         237
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 192.168.1.1:500, Remote: 192.168.1.2:500
Local identity: C=US, DC=example, ST=CA, L=Sunnyvale, O=example,
OU=engineering, CN=host1
Remote identity: C=US, DC=example, ST=CA, L=Sunnyvale, O=example,
OU=engineering, CN=host2
Flags: IKE SA is created

```

show security ike security-associations index 788674 detail

```

user@host> show security ike security-associations index 788674 detail

```

```

IKE peer 192.168.1.1, Index 788674, Gateway Name: ZTH_SPOKE_GW
Auto Discovery VPN:
  Type: Static, Local Capability: Partner, Peer Capability: Suggester
Partner Shortcut Suggestions Statistics:
  Suggestions received:    2
  Suggestions accepted:    2
  Suggestions declined:    0
Role: Initiator, State: UP
Initiator cookie: 7b996b4c310d2424, Responder cookie: 5724c5882a212157
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 192.168.1.2:500, Remote: 192.168.1.1:500
Lifetime: Expires in 734 seconds
Peer ike-id: C=US, DC=example, ST=CA, L=Sunnyvale, O=example, OU=engineering,
CN=test
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication          : hmac-sha1-96
  Encryption              : aes256-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group    : DH-group-5
Traffic statistics:
  Input bytes  :          22535
  Output bytes :          21918
  Input packets:           256
  Output packets:          256
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local: 192.168.1.2:500, Remote: 192.168.1.1:500
Local identity: C=US, DC=example, ST=CA, L=Sunnyvale, O=example,
OU=engineering, CN=host1
Remote identity: C=US, DC=example, ST=CA, L=Sunnyvale, O=example,
OU=engineering, CN=host2
Flags: IKE SA is created

```

show security ike security-associations 192.168.1.2

```

user@host> show security ike security-associations 192.168.1.2
Index      State Initiator cookie Responder cookie Mode Remote Address
8          UP      3a895f8a9f620198 9040753e66d700bb Main 192.168.1.2

```

show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```

user@host> show security ike security-associations fpc 6 pic 1 kmd-instance all
Index      Remote Address State Initiator cookie Responder cookie Mode
1728053250 192.168.1.2    UP      fc959afd1070d10b bdeb7e8c1ea99483 Main

```

show security ike security-associations detail (ADVPN Suggester, Static Tunnel)

```

user@host> show security ike security-associations detail
IKE peer 192.168.0.105, Index 13563297, Gateway Name: zth_hub_gw
Location: FPC 0, PIC 0, KMD-Instance 1
Auto Discovery VPN:
  Type: Static, Local Capability: Suggester, Peer Capability: Partner
Suggester Shortcut Suggestions Statistics:
  Suggestions sent          : 12
  Suggestion response accepted: 12

```

```

    Suggestion response declined: 0
    Role: Responder, State: UP
    Initiator cookie: 4d3f4e4b2e75d727, Responder cookie: 81ab914e13cecd21
    Exchange type: IKEv2, Authentication method: RSA-signatures
    Local: 192.168.0.154:500, Remote: 192.168.0.105:500
    Lifetime: Expires in 26429 seconds
    Peer ike-id: DC=example, CN=host02, L=Sunnyvale, ST=CA, C=US

```

show security ike security-associations detail (ADVPN Partner, Static Tunnel)

```

user@host> show security ike security-associations detail
IKE peer 192.168.0.154, Index 4980720, Gateway Name: zth_spoke_gw
  Location: FPC 0, PIC 0, KMD-Instance 1
  Auto Discovery VPN:
  Type: Static, Local Capability: Partner, Peer Capability: Suggester
  Partner Shortcut Suggestions Statistics:
    Suggestions received: 12
    Suggestions accepted: 12
    Suggestions declined: 0
  Role: Initiator, State: UP
  Initiator cookie: 4d3f4e4b2e75d727, Responder cookie: 81ab914e13cecd21
  Exchange type: IKEv2, Authentication method: RSA-signatures
  Local: 192.168.0.105:500, Remote: 192.168.0.154:500
  Lifetime: Expires in 26252 seconds
  Peer ike-id: DC=example, CN=host01, OU=SBU, O=example, L=Sunnyvale, ST=CA, C=US

```

show security ike security-associations detail (ADVPN Partner, Shortcut)

```

user@host> show security ike security-associations detail
IKE peer 192.168.0.106, Index 4980737, Gateway Name:
GW-ADVPN-GT-ADVPN-zth_spoke_vpn-268173323
  Location: FPC 0, PIC 0, KMD-Instance 1
  Auto Discovery VPN:
  Type: Shortcut, Local Capability: Partner, Peer Capability: Partner
  Role: Responder, State: UP
  Initiator cookie: e1ed0c655929debc, Responder cookie: 437de6ed784ba63e
  Exchange type: IKEv2, Authentication method: RSA-signatures
  Local: 192.168.0.105:500, Remote: 192.168.0.106:500
  Lifetime: Expires in 28796 seconds
  Peer ike-id: DC=example, CN=paulyd, L=Sunnyvale, ST=CA, C=US

```

show security ike security-associations sa-type shortcut (ADVPN)

```

user@host> show security ike security-associations sa-type shortcut

```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
4980742	UP	vb56fbe694eaae5b6	064dbccbf3b2aab	IKEv2	192.168.0.106

show security ike security-associations sa-type shortcut detail (ADVPN)

```

user@host> show security ike security-associations sa-type shortcut detail
IKE peer 192.168.0.106, Index 4980742, Gateway Name:
GW-ADVPN-GT-ADVPN-zth_spoke_vpn-268173327
  Location: FPC 0, PIC 0, KMD-Instance 1
  Auto Discovery VPN:
  Type: Shortcut, Local Role: Partner, Peer Role: Partner
  Role: Responder, State: UP

```

show security ike security-associations detail (IKEv2 Reauthentication)

```

user@host> show security ike security-associations detail
IKE peer 10.1.2.11, Index 6009224, Gateway Name: GW
Role: Responder, State: UP
Initiator cookie: 2c74d14c798a9d70, Responder cookie: 83cbb49bfbc80cb
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 10.1.1.11:500, Remote: 10.1.2.11:500
Lifetime: Expires in 173 seconds
Reauth Lifetime: Expires in 600 seconds
Peer ike-id: vsrx@example.net
AAA assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : aes128-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-2
Traffic statistics:
Input bytes  :          1782
Output bytes :          1743
Input packets:           2

```

show security ike security-associations detail (IKEv2 Fragmentation)

```

user@host> show security ike security-associations detail
IKE peer 172.24.23.157, Index 11883008, Gateway Name: routebased_s2s_gw-552_1
Role: Responder, State: UP
Initiator cookie: f3255e720f162e3a, Responder cookie: 17555e3ff7451841
Exchange type: Main, Authentication method: Pre-shared-keys Trusted CA group:
xyz_ca_grp
Local: 192.168.254.1:500, Remote: 172.24.23.157:500
Lifetime: Expires in 530 seconds
Reauth Lifetime: Disabled
IKE Fragmentation: Enabled, Size: 576
Peer ike-id: 172.24.23.157
AAA assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : 3des-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input bytes  :          1004
Output bytes :           756
Input packets:           6
Output packets:          4
Input fragmented packets: 3
Output fragmented packets: 3
IPSec security associations: 1 created, 1 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 192.168.254.1:500, Remote: 172.24.23.157:500
Local identity: 192.168.254.1
Remote identity: 172.24.23.157
Flags: IKE SA is created

```

show security ipsec security-associations

Syntax show security ipsec security-associations
 <brief | detail>
 <family (inet | inet6)>
 <fpc *slot-number* pic *slot-number*>
 <index *SA-index-number*>
 <kmd-instance (all | *kmd-instance-name*)>
 <pic *slot-number* fpc *slot-number*>
 <sa-type shortcut>
 <traffic-selector *traffic-selector-name*>
 <vpn-name *vpn-name*>

Release Information Command introduced in Junos OS Release 8.5. Support for the **family** option added in Junos OS Release 11.1. Support for the **vpn-name** option added in Junos OS Release 11.4R3. Support for the **traffic-selector** option and traffic selector field added in Junos OS Release 12.1X46-D10. Support for Auto Discovery VPN (ADVPN) added in Junos OS Release 12.3X48-D10. Support for IPsec datapath verification added in Junos OS Release 15.1X49-D70. Support for thread anchorship added in Junos OS Release 17.4R1.

Description Display information about the IPsec security associations (SAs).

Options **none**—Display information about all SAs.

brief | detail—(Optional) Display the specified level of output. The default is **brief**.

family—(Optional) Display SAs by family. This option is used to filter the output.

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.

fpc *slot-number* pic *slot-number*—(Optional) Display information about existing IPsec SAs in the specified Flexible PIC Concentrator (FPC) slot and PIC slot.



NOTE: In a chassis cluster, when you execute the CLI command `show security ipsec security-associations pic <slot-number> fpc <slot-number>` in operational mode, only the primary node information about the existing IPsec SAs in the specified Flexible PIC Concentrator (FPC) slot and PIC slot is displayed.

index *SA-index-number*—(Optional) Display detailed information about the specified SA identified by this index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.

kmd-instance—(Optional) Display information about existing IPsec SAs in the key management process (in this case, it is KMD) identified by the FPC *slot-number* and PIC *slot-number*.

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- **kmd-instance-name**—Name of the KMD instance running on the SPU.

pic slot-number fpc slot-number—(Optional) Display information about existing IPsec SAs in the specified PIC slot and FPC slot.

sa-type—(Optional for ADVPN) Display information for the specified type of SA. **shortcut** is the only option for this release.

traffic-selector traffic-selector-name—(Optional) Display information about the specified traffic selector.

vpn-name vpn-name—(Optional) Display information about the specified VPN.

Required Privilege Level

view

Related Documentation

- [clear security ipsec security-associations](#)
- [Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems on page 180](#)

List of Sample Output

[show security ipsec security-associations \(IPv4\) on page 690](#)
[show security ipsec security-associations \(IPv6\) on page 690](#)
[show security ipsec security-associations index 131073 detail on page 691](#)
[show security ipsec security-associations brief on page 692](#)
[show security ipsec security-associations detail on page 692](#)
[show security ipsec security-associations family inet6 on page 694](#)
[show security ipsec security-associations fpc 6 pic 1 kmd-instance all \(SRX Series Devices\) on page 694](#)
[show security ipsec security-associations detail \(ADVPN Suggester, Static Tunnel\) on page 694](#)
[show security ipsec security-associations detail \(ADVPN Partner, Static Tunnel\) on page 695](#)
[show security ipsec security-associations sa-type shortcut \(ADVPN\) on page 696](#)
[show security ipsec security-associations sa-type shortcut detail \(ADVPN\) on page 696](#)
[show security ipsec security-associations family inet detail on page 697](#)
[show security ipsec security-associations detail \(SRX4600\) on page 698](#)

Output Fields

[Table 69 on page 687](#) lists the output fields for the **show security ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 69: show security ipsec security-associations

Field Name	Field Description	Level of Output
Total active tunnels	Total number of active IPsec tunnels.	brief
ID	Index number of the SA. You can use this number to get additional information about the SA.	All levels
Algorithm	<p>Cryptography used to secure exchanges between peers during the IKE negotiations includes:</p> <ul style="list-style-type: none"> • An authentication algorithm used to authenticate exchanges between the peers. • An encryption algorithm used to encrypt data traffic. 	brief
SPI	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: IKE and IPsec.	brief
Life: sec/kb	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.	brief
Mon	The Mon field refers to VPN monitoring status. If VPN monitoring is enabled, then this field displays U (up) or D (down). A hyphen (-) means VPN monitoring is not enabled for this SA. A V means that IPsec datapath verification is in progress.	brief
Isys	The root system.	brief
Port	If Network Address Translation (NAT) is used, this value is 4500. Otherwise, it is the standard IKE port, 500.	All levels
Gateway	IP address of the remote gateway.	brief
Virtual-system	Name of the logical system.	detail
VPN name	IPsec name for VPN.	detail
State	<p>State has two options, Installed and Not Installed.</p> <ul style="list-style-type: none"> • Installed—The SA is installed in the SA database. • Not Installed—The SA is not installed in the SA database. <p>For transport mode, the value of State is always Installed.</p>	detail

Table 69: show security ipsec security-associations (continued)

Field Name	Field Description	Level of Output
Local gateway	Gateway address of the local system.	detail
Remote gateway	Gateway address of the remote system.	detail
Traffic selector	Name of the traffic selector.	detail
Local identity	Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN).	detail
Remote identity	IP address of the destination peer gateway.	detail
Version	IKE version, either IKEv1 or IKEv2.	detail
DF-bit	State of the don't fragment bit: set or cleared .	detail
Location	<p>FPC—Flexible PIC Concentrator (FPC) slot number.</p> <p>PIC—PIC slot number.</p> <p>KMD-Instance—The name of the KMD instance running on the SPU, identified by <i>FPC slot-number</i> and <i>PIC slot-number</i>. Currently, 4 KMD instances running on each SPU, and any particular IPsec negotiation is carried out by a single KMD instance.</p>	detail
Tunnel events	Tunnel event and the number of times the event has occurred. See <i>Tunnel Events</i> for descriptions of tunnel events and the action you can take.	detail
Anchorship	Anchor thread ID for the SA (for SRX4600 Series devices with the detail option).	
Direction	Direction of the SA; it can be inbound or outbound.	detail
AUX-SPI	<p>Value of the auxiliary security parameter index(SPI).</p> <ul style="list-style-type: none"> When the value is AH or ESP, AUX-SPI is always 0. When the value is AH+ESP, AUX-SPI is always a positive integer. 	detail
Mode	<p>Mode of the SA:</p> <ul style="list-style-type: none"> transport—Protects host-to-host connections. tunnel—Protects connections between security gateways. 	detail

Table 69: show security ipsec security-associations (continued)

Field Name	Field Description	Level of Output
Type	Type of the SA: <ul style="list-style-type: none"> • manual—Security parameters require no negotiation. They are static and are configured by the user. • dynamic—Security parameters are negotiated by the IKE protocol. Dynamic SAs are not supported in transport mode. 	detail
State	State of the SA: <ul style="list-style-type: none"> • Installed—The SA is installed in the SA database. • Not Installed—The SA is not installed in the SA database. For transport mode, the value of State is always Installed .	detail
Protocol	Protocol supported. <ul style="list-style-type: none"> • Transport mode supports Encapsulation Security Protocol (ESP) and Authentication Header (AH). • Tunnel mode supports ESP and AH. 	detail
Authentication	Type of authentication used.	detail
Encryption	Type of encryption used.	detail
Soft lifetime	The soft lifetime informs the IPsec key management system that the SA is about to expire. Each lifetime of an SA has two display options, hard and soft, one of which must be present for a dynamic SA. This allows the key management system to negotiate a new SA before the hard lifetime expires. <ul style="list-style-type: none"> • Expires in seconds—Number of seconds left until the SA expires. 	detail
Hard lifetime	The hard lifetime specifies the lifetime of the SA. <ul style="list-style-type: none"> • Expires in seconds—Number of seconds left until the SA expires. 	detail
Lifesize Remaining	The lifesize remaining specifies the usage limits in kilobytes. If there is no lifesize specified, it shows unlimited. <ul style="list-style-type: none"> • Expires in kilobytes—Number of kilobytes left until the SA expires. 	detail
Anti-replay service	State of the service that prevents packets from being replayed. It can be Enabled or Disabled .	detail

Table 69: show security ipsec security-associations (continued)

Field Name	Field Description	Level of Output
Replay window size	Size of the antireplay service window, which is 64 bits.	detail
Bind-interface	The tunnel interface to which the route-based VPN is bound.	detail
Copy-Outer-DSCP	Indicates if the system copies the outer DSCP value from the IP header to the inner IP header.	detail

Sample Output

For brevity, the show command outputs does not display all the values of the configuration. Only a subset of the configuration is displayed. Rest of the configuration on the system has been replaced with ellipses (...).

show security ipsec security-associations (IPv4)

```

user@host> show security ipsec security-associations
Total active tunnels: 2      Total Ipsec sas: 18
ID   Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<131073 ESP:aes256/sha256 2d8e710b 1949/ unlim - root 500  5.0.0.1
>131073 ESP:aes256/sha256 5f3a3239 1949/ unlim - root 500  5.0.0.1
<131073 ESP:aes256/sha256 5d227e19 1949/ unlim - root 500  5.0.0.1
>131073 ESP:aes256/sha256 5490da 1949/ unlim - root 500  5.0.0.1
<131073 ESP:aes256/sha256 211fb8bc 1949/ unlim - root 500  5.0.0.1
>131073 ESP:aes256/sha256 dde29cd0 1949/ unlim - root 500  5.0.0.1
<131073 ESP:aes256/sha256 49b64080 1949/ unlim - root 500  5.0.0.1
>131073 ESP:aes256/sha256 314afea0 1949/ unlim - root 500  5.0.0.1
<131073 ESP:aes256/sha256 fec6f6ea 1949/ unlim - root 500  5.0.0.1
>131073 ESP:aes256/sha256 428a3a0d 1949/ unlim - root 500  5.0.0.1
<131073 ESP:aes256/sha256 74daba1f 1949/ unlim - root 500  5.0.0.1
>131073 ESP:aes256/sha256 6b51809c 1949/ unlim - root 500  5.0.0.1
<131073 ESP:aes256/sha256 10051bfe 1949/ unlim - root 500  5.0.0.1
...

```

show security ipsec security-associations (IPv6)

```

user@host> show security ipsec security-associations
Total active tunnels: 1
ID   Algorithm      SPI      Life:sec/kb  Mon vsys Port  Gateway

```

```

131074 ESP:aes256/sha256 14caf1d9 3597/ unlim - root 500 2001:db8::1112
131074 ESP:aes256/sha256 9a4db486 3597/ unlim - root 500 2001:db8::1112

```

show security ipsec security-associations index 131073 detail

```

user@host> show security ipsec security-associations index 131073 detail
ID: 131073 Virtual-system: root, VPN Name: IPSEC_VPN1
Local Gateway: 4.0.0.1, Remote Gateway: 5.0.0.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1
Port: 500, Nego#: 18, Fail#: 0, Def-Del#: 0 Flag: 0x600a39
Multi-sa, Configured SAs# 9, Negotiated SAs#: 9
Tunnel events:
  Mon Apr 23 2018 22:20:54 -0700: IPsec SA negotiation successfully completed
(1 times)
  Mon Apr 23 2018 22:20:54 -0700: IKE SA negotiation successfully completed (2
times)
  Mon Apr 23 2018 22:20:18 -0700: User cleared IKE SA from CLI, corresponding
IPsec SAs cleared (1 times)
  Mon Apr 23 2018 22:19:55 -0700: IPsec SA negotiation successfully completed
(2 times)
  Mon Apr 23 2018 22:19:23 -0700: Tunnel is ready. Waiting for trigger event
or peer to trigger negotiation (1 times)
  Mon Apr 23 2018 22:19:23 -0700: Bind-interface's zone received. Information
updated (1 times)
  Mon Apr 23 2018 22:19:23 -0700: External interface's zone received. Information
updated (1 times)
Direction: inbound, SPI: 2d8e710b, AUX-SPI: 0
, VPN Monitoring: -
  Hard lifetime: Expires in 1930 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 1563 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc
  Anti-replay service: counter-based enabled, Replay window size: 64
  Multi-sa FC Name: default
Direction: outbound, SPI: 5f3a3239, AUX-SPI: 0
, VPN Monitoring: -
  Hard lifetime: Expires in 1930 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 1563 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
  Anti-replay service: counter-based enabled, Replay window size: 64
  Multi-sa FC Name: default
Direction: inbound, SPI: 5d227e19, AUX-SPI: 0
, VPN Monitoring: -
  Hard lifetime: Expires in 1930 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 1551 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
  Anti-replay service: counter-based enabled, Replay window size: 64
  Multi-sa FC Name: best-effort
Direction: outbound, SPI: 5490da, AUX-SPI: 0
, VPN Monitoring: -
  Hard lifetime: Expires in 1930 seconds
  Lifesize Remaining: Unlimited

```

```

Soft lifetime: Expires in 1551 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
...

```

Starting with Junos OS Release 18.2R1, the CLI **show security ipsec security-associations index *index-number* detail** output displays all the child SA details including forwarding class name.

show security ipsec security-associations brief

```

user@host> show security ipsec security-associations brief
Total active tunnels: 2      Total Ipsec sas: 18
  ID   Algorithm      SPI      Life:sec/kb Mon lsys Port Gateway
<131073 ESP:aes256/sha256 89e5098 1569/ unlim - root 500 5.0.0.1

>131073 ESP:aes256/sha256 fcee9d54 1569/ unlim - root 500 5.0.0.1

<131073 ESP:aes256/sha256 f3117676 1609/ unlim - root 500 5.0.0.1

>131073 ESP:aes256/sha256 6050109f 1609/ unlim - root 500 5.0.0.1

<131073 ESP:aes256/sha256 e01f54b1 1613/ unlim - root 500 5.0.0.1

>131073 ESP:aes256/sha256 29a05dd6 1613/ unlim - root 500 5.0.0.1

<131073 ESP:aes256/sha256 606c90f6 1616/ unlim - root 500 5.0.0.1

>131073 ESP:aes256/sha256 9b5b059d 1616/ unlim - root 500 5.0.0.1

<131073 ESP:aes256/sha256 b8116d6d 1619/ unlim - root 500 5.0.0.1

>131073 ESP:aes256/sha256 b7ed6bfd 1619/ unlim - root 500 5.0.0.1

<131073 ESP:aes256/sha256 4f5ce754 1619/ unlim - root 500 5.0.0.1

>131073 ESP:aes256/sha256 af8984b6 1619/ unlim - root 500 5.0.0.1

...

```

show security ipsec security-associations detail

```

user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: IPSEC_VPN1
Local Gateway: 4.0.0.1, Remote Gateway: 5.0.0.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1
Port: 500, Nego#: 99, Fail#: 0, Def-Del#: 0 Flag: 0x600a39
Multi-sa, Configured SAs# 9, Negotiated SAs#: 9
Tunnel events:
  Tue Apr 24 2018 02:22:42 -0700: IKE SA rekey successfully completed (8 times)

  Tue Apr 24 2018 02:17:55 -0700: IPSec SA rekey successfully completed (58
times)
  Mon Apr 23 2018 23:12:27 -0700: IPSec SA negotiation successfully completed
(1 times)
  Mon Apr 23 2018 23:12:27 -0700: IKE SA negotiation successfully completed (1
times)

```

```

times)
Mon Apr 23 2018 23:12:21 -0700: IPSec SAs cleared as corresponding IKE SA
deleted (1 times)
Mon Apr 23 2018 23:12:21 -0700: No response from peer. Negotiation failed (1
times)
Mon Apr 23 2018 22:47:34 -0700: IPSec SA rekey successfully completed (8
times)
Mon Apr 23 2018 22:44:28 -0700: IKE SA rekey successfully completed (1 times)

Mon Apr 23 2018 22:20:54 -0700: IPSec SA negotiation successfully completed
(1 times)
Mon Apr 23 2018 22:20:54 -0700: IKE SA negotiation successfully completed (2
times)
Mon Apr 23 2018 22:20:18 -0700: User cleared IKE SA from CLI, corresponding
IPSec SAs cleared (1 times)
Mon Apr 23 2018 22:19:55 -0700: IPSec SA negotiation successfully completed
(2 times)
Mon Apr 23 2018 22:19:23 -0700: Tunnel is ready. Waiting for trigger event
or peer to trigger negotiation (1 times)
Direction: inbound, SPI: 89e5098, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 1557 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1182 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: default
Direction: outbound, SPI: fcee9d54, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 1557 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1182 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: default
Direction: inbound, SPI: f3117676, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 1597 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1205 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: custom_q1
Direction: outbound, SPI: 6050109f, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 1597 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1205 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: custom_q1
Direction: inbound, SPI: e01f54b1, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 1601 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1210 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed

```

```

Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: best-effort
Direction: outbound, SPI: 29a05dd6, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 1601 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1210 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
...

```

show security ipsec security-associations family inet6

```

user@host> show security ipsec security-associations family inet6
Virtual-system: root
Local Gateway: 2001:db8:1212::1111, Remote Gateway: 2001:db8:1212::1112
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
DF-bit: clear
Direction: inbound, SPI: 14caf1d9, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3440 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2813 seconds
Mode: tunnel, Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: 9a4db486, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3440 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2813 seconds
Mode: tunnel, Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64

```

show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```

user@host> show security ipsec security-associations fpc 6 pic 1 kmd-instance all
Total active tunnels: 1

```

ID	Gateway	Port	Algorithm	SPI	Life:sec/kb	Mon	vsys
<2	192.168.1.2	500	ESP:aes256/sha256	67a7d25d	28280/unlim	-	0
>2	192.168.1.2	500	ESP:aes256/sha256	a23cbcdc	28280/unlim	-	0

show security ipsec security-associations detail (ADVPN Suggester, Static Tunnel)

```

user@host> show security ipsec security-associations detail
ID: 70516737 Virtual-system: root, VPN Name: ZTH_HUB_VPN
Local Gateway: 192.168.1.1, Remote Gateway: 192.168.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear
Bind-interface: st0.1

```

```

Port: 500, Nego#: 5, Fail#: 0, Def-Del#: 0 Flag: 0x608a29
Tunnel events:
Tue Nov 03 2015 01:24:27 -0800: IPsec SA negotiation successfully completed (1
times)
Tue Nov 03 2015 01:24:27 -0800: IKE SA negotiation successfully completed (4
times)
Tue Nov 03 2015 01:23:38 -0800: User cleared IPsec SA from CLI (1 times)
Tue Nov 03 2015 01:21:32 -0800: IPsec SA negotiation successfully completed (1
times)
Tue Nov 03 2015 01:21:31 -0800: IPsec SA delete payload received from peer,
corresponding IPsec SAs cleared (1 times)
Tue Nov 03 2015 01:21:27 -0800: IPsec SA negotiation successfully completed (1
times)
Tue Nov 03 2015 01:21:13 -0800: Tunnel configuration changed. Corresponding
IKE/IPsec SAs are deleted (1 times)
Tue Nov 03 2015 01:19:27 -0800: IPsec SA negotiation successfully completed (1
times)
Tue Nov 03 2015 01:19:27 -0800: Tunnel is ready. Waiting for trigger event or
peer to trigger negotiation (1 times)
Location: FPC 0, PIC 3, KMD-Instance 2
Direction: inbound, SPI: 43de5d65, AUX-SPI: 0
Hard lifetime: Expires in 1335 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 996 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled

, Replay window size: 64
Location: FPC 0, PIC 3, KMD-Instance 2
Direction: outbound, SPI: 5b6e157c, AUX-SPI: 0
Hard lifetime: Expires in 1335 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 996 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled

, Replay window size: 64

```

show security ipsec security-associations detail (ADVPN Partner, Static Tunnel)

```

user@host> show security ipsec security-associations detail
ID: 67108872 Virtual-system: root, VPN Name: ZTH_SPOKE_VPN
Local Gateway: 192.168.1.2, Remote Gateway: 192.168.1.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x8608a29
Tunnel events:
Tue Nov 03 2015 01:24:26 -0800: IPsec SA negotiation successfully completed (1
times)
Tue Nov 03 2015 01:24:26 -0800: IKE SA negotiation successfully completed (4
times)
Tue Nov 03 2015 01:23:37 -0800: IPsec SA delete payload received from peer,
corresponding IPsec SAs cleared (1 times)
Tue Nov 03 2015 01:21:31 -0800: IPsec SA negotiation successfully completed (1
times)

```

```

times)
Tue Nov 03 2015 01:21:31 -0800: Tunnel is ready. Waiting for trigger event or
peer to trigger negotiation (1 times)
Tue Nov 03 2015 01:18:26 -0800: Key pair not found for configured local
certificate. Negotiation failed (1 times)
Tue Nov 03 2015 01:18:13 -0800: CA certificate for configured local certificate
not found. Negotiation not initiated/successful (1 times)
Direction: inbound, SPI: 5b6e157c, AUX-SPI: 0
Hard lifetime: Expires in 941 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 556 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 43de5d65, AUX-SPI: 0
Hard lifetime: Expires in 941 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 556 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

```

show security ipsec security-associations sa-type shortcut (ADVPN)

```

user@host> show security ipsec security-associations sa-type shortcut
Total active tunnels: 1
ID           Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<268173318  ESP:aes256/sha256  6f164ee0  3580/ unlim - root 500 192.168.0.111
>268173318  ESP:aes256/sha256  e6f29cb0  3580/ unlim - root 500 192.168.0.111

```

show security ipsec security-associations sa-type shortcut detail (ADVPN)

```

user@host> show security ipsec security-associations sa-type shortcut detail
node0:
-----
ID: 67108874 Virtual-system: root, VPN Name: ZTH_SPOKE_VPN
Local Gateway: 192.168.1.2, Remote Gateway: 192.168.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Auto Discovery VPN:
  Type: Shortcut, Shortcut Role: Initiator
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 4500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x40608a29
Tunnel events:
  Tue Nov 03 2015 01:47:26 -0800: IPSec SA negotiation successfully completed
(1 times)
  Tue Nov 03 2015 01:47:26 -0800: Tunnel is ready. Waiting for trigger event
or peer to trigger negotiation (1 times)
  Tue Nov 03 2015 01:47:26 -0800: IKE SA negotiation successfully completed (1
times)
Direction: inbound, SPI: b7a5518, AUX-SPI: 0
Hard lifetime: Expires in 1766 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1381 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

```



```

Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: b7e0268, AUX-SPI: 0
Hard lifetime: Expires in 1766 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1381 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

```

show security ipsec security-associations family inet detail

```

user@host> show security ipsec security-associations family inet detail
ID: 131073 Virtual-system: root, VPN Name: ike-vpn
Local Gateway: 192.168.1.1, Remote Gateway: 192.168.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv1
DF-bit: clear
, Copy-Outer-DSCP Enabled
Bind-interface: st0.99

Port: 500, Nego#: 116, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
Tunnel events:
Fri Oct 30 2015 15:47:21 -0700: IPSec SA rekey successfully completed (115
times)
Fri Oct 30 2015 11:38:35 -0700: IKE SA negotiation successfully completed (12
times)
Mon Oct 26 2015 16:41:07 -0700: IPSec SA negotiation successfully completed (1
times)
Mon Oct 26 2015 16:40:56 -0700: Tunnel is ready. Waiting for trigger event or
peer to trigger negotiation (1 times)
Mon Oct 26 2015 16:40:56 -0700: External interface's address received.
Information updated (1 times)
Location: FPC 0, PIC 1, KMD-Instance 1
Direction: inbound, SPI: 81b9fc17, AUX-SPI: 0
Hard lifetime: Expires in 1713 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1090 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled

, Replay window size: 64
Location: FPC 0, PIC 1, KMD-Instance 1
Direction: outbound, SPI: 727f629d, AUX-SPI: 0
Hard lifetime: Expires in 1713 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1090 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

Anti-replay service: counter-based enabled

, Replay window size: 64

```

show security ipsec security-associations detail (SRX4600)

```
user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: ike-vpn
Local Gateway: 62.1.1.3, Remote Gateway: 62.1.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.0
Port: 500, Nego#: 25, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
Tunnel events:
  Fri Jan 12 2007 07:50:10 -0800: IPSec SA rekey successfully completed (23
times)
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 6
Direction: inbound, SPI: 812c9c01, AUX-SPI: 0
  Hard lifetime: Expires in 2224 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 1598 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

  Anti-replay service: counter-based enabled, Replay window size: 64
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 7
Direction: outbound, SPI: c4de0972, AUX-SPI: 0
  Hard lifetime: Expires in 2224 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 1598 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes256-cbc (256 bits)

  Anti-replay service: counter-based enabled, Replay window size: 64
```

show security match-policies

Syntax `show security match-policies`
 `destination-ip <ip-address>`
 `destination-port <port-number>`
 `from-zone <zone-name>`
 `global`
 `logical-system <logical-system-name>`
 `protocol <protocol-name | protocol-number>`
 `result-count <number>`
 `root-logical-system`
 `source-end-user-profile <device-identity-profile-name>`
 `source-identity <role-name>`
 `source-ip <ip-address>`
 `source-port <port-number>`
 `tenant <tenant-name>`
 `to-zone <zone-name>`

Release Information Command introduced in Junos OS Release 10.3.
 Command updated in Junos OS Release 10.4.
 Command updated in Junos OS Release 12.1.
 Command updated to include optional from-zone and to-zone global match options in Junos OS Release 12.1X47-D10.
 The **tenant** option is introduced in Junos OS Release 18.3R1.

Description The **show security match-policies** command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, then the **show security match-policies** command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The **result-count** option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are “shadowed” by the first and are never encountered by matching traffic.



NOTE: The **show security match-policies** command is applicable only to security policies; IDP policies are not supported.

- Options**
- **destination-ip** *destination-ip*—Displays the destination IP address of the traffic.
 - **destination-port** *destination-port*—Displays the destination port number of the traffic. Range is 1 through 65,535.
 - **from-zone** *zone-name*—Displays the name or ID of the source zone of the traffic.
 - **global**—Displays information about global policies.

- **logical-system**—Displays the logical system name.
- **protocol** *protocol-name* | *protocol-number*—Displays the protocol name or numeric value of the traffic.
 - **ah** or 51
 - **egp** or 8
 - **esp** or 50
 - **gre** or 47
 - **icmp** or 1
 - **igmp** or 2
 - **igp** or 9
 - **ipip** or 94
 - **ipv6** or 41
 - **ospf** or 89
 - **pgm** or 113
 - **pim** or 103
 - **rdp** or 27
 - **rsvp** or 46
 - **sctp** or 132
 - **tcp** or 6
 - **udp** or 17
 - **vrrp** or 112
- **result-count** *number*—(Optional) Displays the number of policy matches. Valid range is from 1 through 16. The default value is 1.
- **root-logical-system**—Displays root logical system as default.
- **source-end-user-profile** *device-identity-profile-name*—(Optional) Displays the device identity profile that specifies characteristics that can apply to one or more devices.
- **source-identity** *role-name*—(Optional) Displays the source identity of the traffic determined by the user role.
- **source-ip** *source-ip*—Displays the source IP address of the traffic.
- **source-port** *source-port*—Displays the source port number of the traffic. Range is 1 through 65,535.
- **tenant**—Displays the name of the tenant system.
- **to-zone** *zone-name*—Displays the name or ID of the destination zone of the traffic.

Required Privilege Level view

Related Documentation

- *clear security policies statistics*
- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

List of Sample Output

[Example 1: show security match-policies on page 702](#)
[Example 2: show security match policies ... result-count on page 703](#)
[Example 3: show security match policies ... source-identity on page 703](#)
[Example 4: show security match policies ... global on page 703](#)
[show security match-policies tenant TN1 from-zone trust to-zone untrust source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp on page 704](#)

Output Fields [Table 70 on page 701](#) lists the output fields for the **show security match-policies** command. Output fields are listed in the approximate order in which they appear.

Table 70: show security match-policies Output Fields

Field Name	Field Description
Policy	Name of the applicable policy.
Action or Action-type	<p>The action to be taken for traffic that matches the policy's match criteria. Actions include the following:</p> <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
State	<p>Status of the policy:</p> <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	An internal number associated with the policy.

Table 70: show security match-policies Output Fields (continued)

Field Name	Field Description
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, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.
From zone	Name of the source zone.
To zone	Name of the destination zone.
Source addresses	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	The names and corresponding IP addresses of the destination addresses (or address sets) for a policy as entered in the destination zone's address book. A packet's destination address must match one of these addresses for the policy to apply to it.
Application	Name of a preconfigured or custom application, or any if no application is specified.
IP protocol	Numeric value for the IP protocol used by the application, such as 6 for TCP or 1 for ICMP.
ALG	If an ALG is associated with the session, the name of the ALG. Otherwise, 0.
Inactivity timeout	Elapsed time without activity after which the application is terminated.
Source-port range	Range of matching source ports defined in the policy.
Destination-port range	Range of matching destination ports defined in the policy.
Source identities	One or more user roles defined in the matching policy.
global	Display information about global policies.
device-identity-profile-name	Device identity profile that specifies characteristics that can apply to one or more devices.

Sample Output

Example 1: show security match-policies

```

user@host> show security match-policies from-zone z1 to-zone z2 source-ip 10.10.10.1
destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 198.51.100.0/24
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 203.0.113.0/24
    d3: 192.0.2.1/32

```

```

Application: junos-ftp
IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [21-21]

```

Example 2: show security match policies ... result-count

```

user@host> show security match-policies from-zone zone-A to-zone zone-B source-ip 10.10.10.1
destination-ip 192.0.2.5 source-port 1004 destination-port 80 protocol tcp result-count 5
Policy: p1, action-type: permit, State: enabled, Index: 4
Sequence number: 1
From zone: zone-A, To zone: zone-B
Source addresses:
sa1: 10.10.0.0/16
Destination addresses:
da5: 192.0.2.0/24
Application: any
IP protocol: 1, ALG: 0, Inactivity timeout: 0
Source port range: [1000-1030]
Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
Sequence number: 15
From zone: zone-A, To zone: zone-B
Source addresses:
sa11: 10.10.10.1/32
Destination addresses:
da15: 192.0.2.5/32
Application: any
IP protocol: 1, ALG: 0, Inactivity timeout: 0
Source port range: [1000-1030]
Destination port range: [80-80]

```

Example 3: show security match policies ... source-identity

```

user@host> show security match-policies from-zone untrust to-zone trust source-ip 10.10.10.1
destination-ip 192.0.2.1 destination-port 21 protocol 6 source-port 1234 source-identity role1
Policy: p1, action-type: permit, State: enabled, Index: 40
Policy Type: Configured
Sequence number: 1
From zone: untrust, To zone: trust
Source addresses:
a1: 10.0.0.0/8
Destination addresses:
d1: 192.0.2.0/24
Application: junos-ftp
IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [21-21]
Source identities: role1
Per policy TCP Options: SYN check: No, SEQ check: No

```

Example 4: show security match policies ... global

```

user@host> show security match-policies global source-ip 10.10.10.1 destination-ip 192.0.2.5
source-port 1004 destination-port 80 protocol tcp result-count 5
Policy: gp1, action-type: permit, State: enabled, Index: 6, Scope Policy: 0
Policy Type: Configured, global
Sequence number: 1
From zones:

```

```
Any
To zones:
Any
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security match-policies tenant TN1 from-zone trust to-zone untrust source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp

```
user@host> show security match-policies tenant TN1 from-zone trust to-zone untrust source-ip
10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp
```

```
Policy: p1, action-type: permit, State: enabled, Index: 4
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
a2: 198.51.100.0/24
a3: 10.10.10.1/32
Destination addresses:
d2: 203.0.113.0/24
d3: 192.0.2.1/32
Application: junos-ftp
IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [21-21]
```


show security nat destination rule

Syntax	show security nat destination rule <i>rule-name</i> all logical-system (<i>logical-system-name</i>) root-logical-system tenant (<i>tenant-name</i>)
Release Information	<p>Command introduced in Junos OS Release 9.2. The Description output field added in Junos OS Release 12.1.</p> <p>Support for IPv6 logical systems and the Successful sessions, Failed sessions and Number of sessions output fields added in Junos OS Release 12.1X45-D10.</p> <p>Output for multiple destination ports and the application option field added in Junos OS Release 12.1X47-D10.</p> <p>The tenant option is introduced in Junos OS Release 18.3R1.</p>
Description	Display information about the specified destination Network Address Translation (NAT) rule. Destination NAT rules are processed after static NAT rules but before source NAT rules.
Options	<p>rule-name—Display information about the specified destination NAT rule.</p> <p>all—Display information about all the destination NAT rules.</p> <p>logical-system —Display information about the destination NAT rules for a specified logical system. Specify all to display information for all logical systems.</p> <p>root-logical-system—Display information about the destination NAT rules for the master (root) logical system.</p> <p>tenant—Display information about the destination NAT rules for a specified tenant system. Specify all to display information for all tenant systems.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • rule (Security Destination NAT)
List of Sample Output	show security nat destination rule dst2-rule on page 706 show security nat destination rule all on page 707 show security nat destination rule all tenant on page 707
Output Fields	Table 71 on page 706 lists the output fields for the show security nat destination rule command. Output fields are listed in the approximate order in which they appear.

Table 71: show security nat destination rule Output Fields

Field Name	Field Description
Total destination-nat rules	Number of destination NAT rules.
Total referenced IPv4/IPv6 ip-prefixes	Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly as address names and as address set names in the rule.
Destination NAT rule	Name of the destination NAT rule.
Description	Description of the destination NAT rule.
Rule-Id	Rule identification number.
Rule position	Position of the destination NAT rule.
From routing instance	Name of the routing instance from which the packets flow.
From interface	Name of the interface from which the packets flow.
From zone	Name of the zone from which the packets flow.
Source addresses	Name of the source addresses that match the rule. The default value is any.
Destination addresses	Name of the destination addresses that match the rule. The default value is any.
Action	The action taken when a packet matches the rule's tuples. Actions include the following: <ul style="list-style-type: none"> destination NAT pool—Use user-defined destination NAT pool to perform destination NAT. off—Do not perform destination NAT.
Destination ports	Destination ports number that match the rule. The default value is any.
Application	Indicates whether the application option is configured.
Translation hits	Number of translation hits.
Successful sessions	Number of successful session installations after the NAT rule is matched.
Failed sessions	Number of unsuccessful session installations after the NAT rule is matched.
Number of sessions	Number of sessions that reference the specified rule.

Sample Output

show security nat destination rule dst2-rule

```
user@host>show security nat destination rule dst2-rule
```

```

Destination NAT rule: dst2-rule          Rule-set: dst2
Description                             : The destination rule dst2-rule is for the sales
team
Rule-Id                                 : 1
Rule position                           : 1
From routing instance                   : ri1
                                         : ri2
Match
  Source addresses                      : add1
                                         add2
  Destination addresses                 : add9
Action                                 : off

Destination port                        : 0
Translation hits                       : 68
  Successful sessions                  : 25
  Failed sessions                     : 43
Number of sessions                     : 2

```

Sample Output

show security nat destination rule all

```

user@host> show security nat destination rule all

Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0

Destination NAT rule: r4          Rule-set: rs4
Rule-Id                          : 2
Rule position                     : 2
From zone                        : untrust
Match
  Source addresses                : 192.0.2.0 - 192.0.2.255
  Destination addresses           : 198.51.100.0 - 198.51.100.255
  Application                     : configured
Action                           : off
Translation hits                  : 0
  Successful sessions             : 0
  Failed sessions                 : 0
Number of sessions               : 0

```

show security nat destination rule all tenant

```

user@host> show security nat destination rule all tenant tn1

Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Destination NAT rule: r1          Rule-set: from_zone
Rule-Id                          : 1
Rule position                     : 1
From zone                        : untrust
Match
  Source addresses                : 192.0.2.0 - 192.0.2.255
  Destination addresses           : 203.0.113.202 - 203.0.113.202
Action                           : h1
Translation hits                  : 0

```

```
Successful sessions : 0
Failed sessions    : 0
Number of sessions : 0
```

show security nat destination summary

Syntax	show security nat destination summary logical-system (<i>logical-system-name</i>) root-logical-system tenant (<i>tenant-name</i>)
Release Information	Command introduced in Junos OS Release 9.2. Support for IPv6 logical systems added in Junos OS Release 12.1X45-D10. The tenant option is introduced in Junos OS Release 18.3R1.
Description	Display a summary of Network Address Translation (NAT) destination pool information.
Options	<p>none—Display summary information about the destination NAT pool.</p> <p>logical-system —Display summary information about the destination NAT for a specified logical system. Specify all to display information for all logical systems.</p> <p>root-logical-system—Display summary information about the destination NAT for the master (root) logical system.</p> <p>tenant —Display information about the destination NAT for a specified tenant system. Specify all to display information for all tenant systems.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>pool (Security Destination NAT)</i> • <i>rule (Security Destination NAT)</i>
List of Sample Output	show security nat destination summary on page 710 show security nat destination summary tenant on page 710
Output Fields	Table 72 on page 709 lists the output fields for the show security nat destination summary command. Output fields are listed in the approximate order in which they appear.

Table 72: show security nat destination summary Output Fields

Field Name	Field Description
Total destination nat pool number	Number of destination NAT pools.
Pool name	Name of the destination address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.

Table 72: show security nat destination summary Output Fields (continued)

Field Name	Field Description
Port	Port number.
Total	Number of IP addresses that are in use.
Available	Number of IP addresses that are free for use.
Total destination nat rule number	Number of destination NAT rules.
Total hit times	Number of times a translation in the translation table is used for all the destination NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the destination NAT rules.

Sample Output

show security nat destination summary

```
user@host> show security nat destination summary
```

```

Total pools: 2
Pool name      Address Range      Routing Instance  Port  Total Address
dst-p1         203.0.113.1 -203.0.113.1      default         0     1
dst-p2         2001:db8::1 - 2001:db8::1  default         0     1

Total rules: 171
Rule name      Rule set  From      Action
dst2-rule      dst2      ri1
               ri2
               ri3
               ri4
               ri5
               ri6
               ri7
dst3-rule      dst3      ri9
               ri1
               ri2
               ri3
               ri4
               ri5
...

```

show security nat destination summary tenant

```
user@host> show security nat destination summary tenant tn1
```

```

Total pools: 1
Pool name      Address Range      Routing Instance  Port  Total Address

```

h1	192.168.1.200 - 192.168.1.200	0	1
Total rules: 1			
Rule name	Rule set	From	Action
r1	from_zone	untrust	h1

show security nat source rule

Syntax	<code>show security nat static rule</code> <i>rule-name</i> <code>all</code> <code>logical-system (logical-system-name)</code> <code>root-logical-system</code> <code>tenant (tenant-name)</code>
Release Information	Command introduced in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 11.2. The Description output field added in Junos OS Release 12.1. Support for IPv6 logical systems and the Source port , Successful sessions , Failed sessions , and Number of sessions output fields added in Junos OS Release 12.1X45-D10. Output for multiple destination ports and the application output field added in Junos OS Release 12.1X47-D10. The tenant option is introduced in Junos OS Release 18.3R1.
Description	Display information about the specified source Network Address Translation (NAT) rule.
Options	rule-name —Name of the rule. all —Display information about all the source NAT rules. logical-system —Display information about the source NAT rules for a specified logical system. Specify all to display information for all logical systems. root-logical-system —Display information about the source NAT rules for the master (root) logical system. tenant —Display information about the source NAT rules for a specified tenant system. Specify all to display information for all tenant systems.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• rule (Security Source NAT)
List of Sample Output	show security nat source rule r2 on page 714 show security nat source rule all on page 714 show security nat source rule all tenant on page 715
Output Fields	Table 73 on page 713 lists the output fields for the show security nat source rule command. Output fields are listed in the approximate order in which they appear

Table 73: show security nat source rule Output Fields

Field Name	Field Description
Source NAT rule	Name of the source NAT rule.
Total rules	Number of source NAT rules.
Total referenced IPv4/IPv6 ip-prefixes	Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly, as address names, and as address set names in the rule.
Description	Description of the source NAT rule.
Rule-Id	Rule identification number.
Rule position	Position of the source NAT rule.
From zone	Name of the zone from which the packets flow.
To zone	Name of the zone to which the packets flow.
From routing instance	Name of the routing instance from which the packets flow.
To routing instance	Name of the routing instance to which the packets flow.
From interface	Name of the interface from which the packets flow.
To interface	Name of the interface to which the packets flow.
Source addresses	Name of the source addresses that match the rule.
Source port	Source port numbers that match the rule.
Destination address	Name of the destination addresses that match the rule.
Destination ports	Destination port numbers that match the rule.
Application	Indicates whether the application option is configured.
Action	<p>The action taken in regard to a packet that matches the rule's tuples. Actions include the following:</p> <ul style="list-style-type: none"> • off—Do not perform source NAT. • source NAT pool—Use user-defined source NAT pool to perform source NAT • interface—Use egress interface's IP address to perform source NAT.
Persistent NAT type	Persistent NAT type.
Persistent NAT mapping type	Persistent NAT mapping type.
Inactivity timeout	Inactivity timeout for persistent NAT binding.

Table 73: show security nat source rule Output Fields (continued)

Field Name	Field Description
Max session number	Maximum number of sessions.
Translation hits	Number of translation hits.
Successful sessions	Number of successful session installations after the NAT rule is matched.
Failed sessions	Number of unsuccessful session installations after the NAT rule is matched.
Number of sessions	Number of sessions that reference the specified rule.

Sample Output

show security nat source rule r2

```

user@host> show security nat source rule r2

source NAT rule: r2          Rule-set: src-nat
Description                  : The source rule r2 is for the sales team
Rule-Id                      : 1
Rule position                 : 1
From zone                    : zone1
To zone                       : zone9
Match
  Source addresses           : add1
                             : add2
  Destination addresses      : add9
                             : add10
  Destination port           : 1002          - 1002
Action                       : off
  Persistent NAT type        : N/A
  Persistent NAT mapping type : address-port-mapping
  Inactivity timeout         : 0
  Max session number         : 0
  Translation hits           : 4719
  Successful sessions        : 2000
  Failed sessions            : 2719
  Number of sessions         : 5

```

Sample Output

show security nat source rule all

```

user@host> show security nat source rule all
Logical system: root
Total rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 3/0

source NAT rule: r2          Rule-set: rs2
Rule-Id                     : 2
Rule position                : 1
From zone                    : trust
To zone                       : untrust
Match

```

```

Source addresses      : 192.0.2.0 - 192.0.2.255
Destination addresses : 203.0.113.0 - 203.0.113.255
                     198.51.100.0 - 198.51.100.255
Application          : configured
Action               : off
Persistent NAT type   : N/A
Persistent NAT mapping type : address-port-mapping
Inactivity timeout    : 0
Max session number    : 0
Translation hits      : 0
Successful sessions   : 0
Failed sessions       : 0
Number of sessions    : 0

```

Sample Output

show security nat source rule all tenant

```

user@host> show security nat source rule all tenant tn1
Total rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
source NAT rule: r1                      Rule-set: from_intf
Rule-Id                                : 1
Rule position                           : 1
From interface                          : ge-0/0/0.0
To interface                            : ge-0/0/1.0
Match
  Source addresses                       : 192.168.1.0 - 192.168.1.255
  Destination addresses                   : 203.0.113.200 - 203.0.113.200
Action                                  : pat
Persistent NAT type                      : N/A
Persistent NAT mapping type              : address-port-mapping
Inactivity timeout                       : 0
Max session number                       : 0
Translation hits                         : 0
Successful sessions                      : 0
Failed sessions                          : 0
Number of sessions                      : 0

```

show security nat source summary

Syntax show security nat source summary
 logical-system (*logical-system-name*)
 root-logical-system
 tenant (*tenant-name*)

Release Information Command introduced in Junos OS Release 9.2.
 Support for IPv6 logical systems added in Junos OS Release 12.1X45-D10.
 The tenant option is introduced in Junos OS Release 18.3R1.

Description Display a summary of Network Address Translation (NAT) source information.

Options **none**—Display summary source NAT information.

logical-system—Display summary information about the source NAT for a specified logical system. Specify **all** to display information for all logical systems.

root-logical-system—Display summary information about the source NAT for the master (root) logical system.

tenant—Display summary information about the source NAT for a specified tenant system. Specify **all** to display information for all tenant systems.

Required Privilege Level view

Release History Table

Release	Description
12.3X48-D55	Starting in Junos OS Release 12.3X48-D55, and Junos OS Release 15.1X49-D90, and Junos OS Release 17.3R1, the total number of addresses that are in use for pools with IPv6 prefixes is shown as zero (0).

Related Documentation

- *pool (Security Source NAT)*
- *rule (Security Source NAT)*

List of Sample Output [show security nat source summary on page 717](#)
[show security nat source summary tenant on page 718](#)

Output Fields [Table 74 on page 717](#) lists the output fields for the **show security nat source summary** command. Output fields are listed in the approximate order in which they appear.

Table 74: show security nat source summary Output Fields

Field Name	Field Description
Total source nat pool number	Number of source NAT pools.
Pool name	Name of the source address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.
PAT	Whether Port Address Translation (PAT) is enabled (yes or no).
Total Address	Number of IP addresses that are in use. Starting in Junos OS Release 12.3X48-D55, and Junos OS Release 15.1X49-D90, and Junos OS Release 17.3R1, the total number of addresses that are in use for pools with IPv6 prefixes is shown as zero (0).
Total source nat rule number	Number of source NAT rules.
Total port number usage for port translation pool	Number of ports assigned to the pool.
Maximum port number for port translation pool	Maximum number of NAT or PAT transactions done at any given time.

Sample Output

show security nat source summary

```

user@host> show security nat source summary logical-system all

Logical system: root-logical-system
Total port number usage for port translation pool: 67108864
Maximum port number for port translation pool: 134217728

Logical system: lsys1
Total port number usage for port translation pool: 193536
Maximum port number for port translation pool: 134217728
Total pools: 2

Logical system: root-logical-system
Pool      Address      Routing  PAT  Total
Name      Range        Instance
pool1     10.1.1.0-10.1.4.255-
          10.1.5.0-10.1.8.255  default  yes  2048

Logical system: lsys1
Pool      Address      Routing  PAT  Total
Name      Range        Instance
pool2     203.0.113.1-203.0.113.3  default  yes  3

```

Total rules: 1

Logical system: root-logical-system

Rule name	Rule set	From	To	Action
rule 1	ruleset1	ge-2/2/2.0	ge-2/2/3.0	pool1
rule 1		ge-2/2/4.0	ge-2/2/5.0	

show security nat source summary tenant

user@host> show security nat source summary tenant tn1

Total port number usage for port translation pool: 1548288

Maximum port number for port translation pool: 268435456

Total pools: 1

Pool Name	Address Range	Routing Instance	PAT	Total Address
pat	192.0.2.1-192.0.2.24	default	yes	24

Total rules: 1

Rule name	Rule set	From	To	Action
r1	from_intf	ge-0/0/0.0	ge-0/0/1.0	pat

show security nat static rule

Syntax	<pre>show security nat static rule rule-name all logical-system (logical-system-name) root-logical-system tenant (tenant-name)</pre>
Release Information	<p>Command introduced in Junos OS Release 9.3.</p> <p>The Description output field added in Junos OS Release 12.1.</p> <p>Support for IPv6 logical systems and the Successful sessions, Failed sessions, Number of sessions, Source addresses and Source ports output fields added in Junos OS Release 12.1X45-D10.</p> <p>The Destination NPTv6 addr and Destination NPTv6 Netmask output fields added in Junos OS Release 12.3X48-D25.</p> <p>The tenant option is introduced in Junos OS Release 18.3R1.</p>
Description	<p>Display information about the specified static Network Address Translation (NAT) rule. Traffic directions allows you to specify from interface, from zone, or from routing-instance and packet information can be source addresses and ports, and destination addresses and ports.</p>
Options	<p>rule-name—Name of the rule.</p> <p>all—Display information about all the static NAT rules.</p> <p>logical-system—Display information about the static NAT rules for a specified logical system. Specify all to display information for all logical systems.</p> <p>root-logical-system—Display information about the static NAT rules for the master (root) logical system.</p> <p>tenant—Display information about the static NAT rules for a specified tenant system. Specify all to display information for all tenant systems.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • rule (Security Static NAT)
List of Sample Output	<p>show security nat static rule on page 721</p> <p>show security nat static rule all tenant on page 721</p> <p>show security nat static rule (IPv6) on page 721</p> <p>show security nat static rule all on page 722</p>

Output Fields Table 75 on page 720 lists the output fields for the **show security nat static rule** command. Output fields are listed in the approximate order in which they appear.

Table 75: show security nat static rule Output Fields

Field Name	Field Description
Static NAT rule	Name of the static NAT rule.
Total referenced IPv4/IPv6 ip-prefixes	Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly, as address names, and as address set names in the rule.
Rule-set	Name of the rule set. Currently, you can configure 8 rules within the same rule set.
Description	Description of the static NAT rule.
Rule-Id	Rule identification number.
Rule position	Position of the rule that indicates the order in which it applies to traffic.
From interface	Name of the interface from which the packets flow.
From routing instance	Name of the routing instance from which the packets flow.
From zone	Name of the zone from which the packets flow.
Destination addresses	Name of the destination addresses that match the rule.
Destination NPTv6 addr	Destination address that matches the rule.
Source addresses	Name of the source addresses that match the rule.
Host addresses	Name of the host addresses that match the rule.
Netmask	Subnet IP address.
Destination NPTv6 Netmask	Subnet IPv6 address.
Host routing-instance	Name of the host routing instance.
Destination port	Destination port numbers that match the rule. The default value is any.
Source port	Source port numbers that match the rule.
Total static-nat rules	Number of static NAT rules.
Translation hits	Number of times a translation in the translation table is used for a static NAT rule.
Successful sessions	Number of successful session installations after the NAT rule is matched.

Table 75: show security nat static rule Output Fields (continued)

Field Name	Field Description
Failed sessions	Number of unsuccessful session installations after the NAT rule is matched.
Number of sessions	Number of sessions that reference the specified rule.

Sample Output

show security nat static rule

```

user@host> show security nat static rule sta-r2

Static NAT rule: sta-r2                Rule-set: sta-nat
Description                           : The static rule sta-r2 is for the sales team
Rule-Id                               : 1
Rule position                          : 1
From zone                             : zone9
Destination addresses                  : add3
Host addresses                         : add4
Netmask                               : 24
Host routing-instance                  : N/A
Translation hits                       : 2
  Successful sessions                  : 2
  Failed sessions                      : 0
Number of sessions                     : 2

```

Sample Output

show security nat static rule all tenant

```

user@host> show security nat static rule all tenant tn1

Total static-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Static NAT rule: r1                    Rule-set: from_zone
Rule-Id                               : 1
Rule position                          : 1
From zone                             : untrust
Source addresses                       : 192.0.2.0      - 192.0.2.255
Destination addresses                  : 203.0.113.203
Host addresses                         : 192.168.1.203
Netmask                               : 32
Host routing-instance                  : N/A
Translation hits                       : 0
  Successful sessions                  : 0
  Failed sessions                      : 0
Number of sessions                     : 0

```

Sample Output

show security nat static rule (IPv6)

```

user@host> show security nat static rule r1

Static NAT rule: r1                    Rule-set: rs1

```

```
Rule-Id                : 1
Rule position          : 1
From zone              : trust
Destination NPTv6 addr : 2001:db8::
Destination NPTv6 Netmask : 48
Host addresses         : 2001:db8::3000
Netmask                : 48
Host routing-instance  : N/A
Translation hits       : 0
    Successful sessions : 0
    Failed sessions    : 0
Number of sessions     : 0
```

Sample Output

show security nat static rule all

```
user@host> show security nat static rule all
```

```
Static NAT rule: r1                Rule-set: rs1
Rule-Id                          : 1
Rule position                    : 1
From zone                        : trust
Source addresses                 : 192.0.2.0 -192.0.2.3
                                : addr1
Source ports                     : 200 - 300
Destination addresses           : 198.51.100.0
Host addresses                   : 203.0.113.0
Netmask                         : 24
Host routing-instance           : N/A
Translation hits                 : 4
    Successful sessions          : 4
    Failed sessions             : 0
Number of sessions              : 4
Static NAT rule: r2                Rule-set: rs1
Rule-Id                          : 2
Rule position                    : 2
From zone                        : trust
Source addresses                 : 192.0.2.0 -192.0.2.255
Destination addresses            : 203.0.113.1
Destination ports                : 100 - 200
Host addresses                   : 192.0.2.1
Host ports                      : 300 - 400
Netmask                         : 32
Host routing-instance           : N/A
Translation hits                 : 4
    Successful sessions          : 4
    Failed sessions             : 0
Number of sessions              : 4
```

show security policies

Syntax show security policies
 application-firewall
 count
 detail
 from-zone <zone-name>
 global
 hit-count
 interface
 logical-system <logical-system-name>
 policy <policy-name>
 root-logical-system
 service-set
 start
 tenant <tenant-name>
 to-zone <zone-name>
 unknown-source-identity
 zone-context

Release Information Command modified in Junos OS Release 9.2.
 Support for IPv6 addresses is added in Junos OS Release 10.2.
 Support for wildcard addresses is added in Junos OS Release 11.1.
 Support for global policy and services offloading is added in Junos OS Release 11.4.
 Support for source-identities and the **Description** output field is added in Junos OS Release 12.1.
 Support for negated address added in Junos OS Release 12.1X45-D10.
 The output fields for Policy Statistics expanded, and the output fields for the **global** and **policy-name** options are expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10.
 Support for the **initial-tcp-mss** and **reverse-tcp-mss** options is added in Junos OS Release 12.3X48-D20.
 Output field and description for **source-end-user-profile** option is added in Junos OS Release 15.1x49-D70.
 Output field and description for **dynamic-applications** option is added in Junos OS Release 15.1x49-D100.
 Output field and description for **dynapp-redir-profile** option is added in Junos OS Release 18.2R1.
 The **tenant** option is introduced in Junos OS Release 18.3R1.

Description Displays a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy. The existing show commands for displaying the policies configured with multiple tenant support are enhanced. A security policy controls the traffic flow from one zone to another zone. The security policies allow you to deny, permit, reject (deny and send a TCP RST or ICMP port unreachable message to the source host), encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another.

Options	<ul style="list-style-type: none">• application-firewall—Displays the information of application-firewall.• count—Displays the number of policies. Range is 1 through 65,535.• detail—(Optional) Displays a detailed view of all of the policies configured on the device.• from-zone—Displays the policy information matching the given source zone.• global—(Optional) Displays information about global policies.• hit-count—Displays the policies hit count.• interface—Displays the name of the adaptive services interface.• logical-system—Displays the logical system name.• policy-name—(Optional) Displays the information about a specified policy.• root-logical-system—Displays root logical system as default.• service-set—Displays the name of the service set.• start—Displays the policies from a given position. Range is 1 through 65,535.• tenant—Displays the name of the tenant system.• to-zone—Displays the policy information matching the given destination zone.• unknown-source-identity—Displays the unknown-source-identity of a policy.• zone-context—Displays the count of policies in each context (from-zone and to-zone).
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>Security Policies Overview</i>• <i>Understanding Security Policy Rules</i>• <i>Understanding Security Policy Elements</i>• <i>Unified Policies Configuration Overview</i>
List of Sample Output	<p>show security policies on page 727</p> <p>show security policies (Dynamic Applications) on page 728</p> <p>show security policies policy-name detail on page 729</p> <p>show security policies (Services-Offload) on page 730</p> <p>show security policies (Device Identity) on page 730</p> <p>show security policies detail on page 730</p> <p>show security policies detail (TCP Options) on page 732</p> <p>show security policies policy-name (Negated Address) on page 733</p> <p>show security policies policy-name detail (Negated Address) on page 733</p> <p>show security policies global on page 733</p> <p>show security policies detail tenant on page 734</p>

Output Fields Table 76 on page 725 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 76: 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.
Source identities	One or more user roles specified for a policy.

Table 76: show security policies Output Fields (continued)

Field Name	Field Description
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.
Action or Action-type	<ul style="list-style-type: none"> • The action taken for a packet that matches the policy's tuples. Actions include the following: <ul style="list-style-type: none"> • permit • firewall-authentication • tunnel ipsec-vpn vpn-name • pair-policy pair-policy-name • source-nat pool pool-name • pool-set pool-set-name • interface • destination-nat name • deny • reject • services-offload

Table 76: show security policies Output Fields (continued)

Field Name	Field Description
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.
dynapp-redir-profile	Displays unified policy redirect profile. See <i>profile(dynamic-application)</i> .
Per policy TCP Options	Configured syn and sequence checks, and the configured TCP MSS value for the initial direction, the reverse direction or, both.

Sample Output

show security policies

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

```

From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
Source addresses:
sa-1-ipv4: 198.51.100.11/24
sa-2-ipv6: 2001:db8:a0b:12f0::1/32
```

```

sa-3-ipv6: 2001:db8:a0b:12f0::22/32
sa-4-wc: 203.0.113.1/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.2/24
da-2-ipv6: 2001:db8:a0b:12f0::8/32
da-3-ipv6: 2001:db8:a0b:12f0::9/32
da-4-wc: 192.168.22.11/255.255.0.255
Source identities: role1, role2, role4
Applications: any
Action: permit, application services, log, scheduled
Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
Source addresses:
sa-1-ipv4: 198.51.100.11/24
sa-2-ipv6: 2001:db8:a0b:12f0::1/32
sa-3-ipv6: 2001:db8:a0b:12f0::22/32
Destination addresses:
da-1-ipv4: 2.2.2.2/24
da-2-ipv6: 2001:db8:a0b:12f0::1/32
da-3-ipv6: 2001:db8:a0b:12f0::9/32
Source identities: role1, role4
Applications: any
Action: deny, scheduled

```

show security policies (Dynamic Applications)

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

```

Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses: any
Destination addresses: any
Applications: any
Dynamic Applications: junos:YAHOO
Action: deny, log
Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
Source addresses: any
Destination addresses: any
Applications: any
Dynamic Applications: junos:web, junos:web:social-networking:facebook,
junos:TFTP, junos:QQ
Action: permit, log
Policy: p3, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 3
Source addresses: any
Destination addresses: any
Applications: any
Dynamic Applications: junos:HTTP, junos:SSL
Action: permit, application services, log

```

The following example displays the output with unified policies configured.

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

```

Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses: any
Destination addresses: any
Applications: junos-defaults
Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
dynapp-redir-profile: profile1

```


show security policies policy-name detail

```
user@host> show security policies policy-name p1 detail
```

```

Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
  sa-1-ipv4: 198.51.100.11/24
  sa-2-ipv6: 2001:db8:a0b:12f0::1/32
  sa-3-ipv6: 2001:db8:a0b:12f0::9/32
  sa-4-wc: 203.0.113.1/255.255.0.255
Destination addresses:
  da-1-ipv4: 192.0.2.0/24
  da-2-ipv6: 2001:db8:a0b:12f0::1/32
  da-3-ipv6: 2001:db8:a0b:12f0::9/32
  da-4-wc: 192.168.22.11/255.255.0.255
Source identities:
  role1
  role2
  role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Destination Address Translation: drop translated
Application firewall :
Rule-set: my_ruleset1
  Rule: rule1
    Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
    Dynamic Application groups: junos:web, junos:chat
    Action: deny
  Default rule: permit
Session log: at-create, at-close
Scheduler name: sch20
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
  Input bytes      : 18144      545 bps
  Initial direction: 9072      272 bps
  Reply direction  : 9072      272 bps
  Output bytes     : 18144      545 bps
  Initial direction: 9072      272 bps
  Reply direction  : 9072      272 bps
  Input packets    : 216        6 pps
  Initial direction: 108        3 bps
  Reply direction  : 108        3 bps
  Output packets   : 216        6 pps
  Initial direction: 108        3 bps
  Reply direction  : 108        3 bps
  Session rate     : 108        3 sps
  Active sessions  : 93
  Session deletions: 15
  Policy lookups   : 108

```

The following example displays the output with unified policies configured.

```
user@host> show security policies policy-name p1 detail
```

```

Default policy: permit-all
Pre ID default policy: permit-all

```

```
From zone: trust, To zone: trust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses: any
Destination addresses: any
Applications: any
Action: reject
dynapp-redir-profile: profile1
```

show security policies (Services-Offload)

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

```
Policy: p1, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
dynapp-redir-profile: profile1(1)
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies (Device Identity)

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

```
From zone: trust, To zone: untrust
Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0,
Sequence number: 1
Source addresses: any
Destination addresses: any
source-end-user-profile: marketing-profile
Applications: any
Action: permit
```

show security policies detail

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

```
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
4, Scope Policy: 0
Policy Type: Configured
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
  role1
```

```

role2
role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
  Input bytes      :          18144          545 bps
  Initial direction:          9072          272 bps
  Reply direction  :          9072          272 bps
  Output bytes     :          18144          545 bps
  Initial direction:          9072          272 bps
  Reply direction  :          9072          272 bps
  Input packets    :           216           6 pps
  Initial direction:          108           3 bps
  Reply direction  :          108           3 bps
  Output packets   :           216           6 pps
  Initial direction:          108           3 bps
  Reply direction  :          108           3 bps
  Session rate     :          108           3 sps
  Active sessions  :           93
  Session deletions:           15
  Policy lookups    :          108
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
5, Scope Policy: 0
Policy Type: Configured
Description: The policy p2 is for the sales team
Sequence number: 1
From zone: untrust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
role1
role2
role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

The following example displays the output with unified policies configured.

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

```

Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0

```

```

any-ipv6(global): ::/0
Application: junos-defaults
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [443-443]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [5432-5432]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [80-80]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [3128-3128]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [8000-8000]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [8080-8080]
IP protocol: 17, ALG: 0, Inactivity timeout: 60
  Source port range: [0-0]
  Destination port range: [1-65535]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [443-443]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [5432-5432]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [80-80]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [3128-3128]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [8000-8000]
IP protocol: 6, ALG: 0, Inactivity timeout: 1800
  Source port range: [0-0]
  Destination port range: [8080-8080]
IP protocol: 17, ALG: 0, Inactivity timeout: 60
  Source port range: [0-0]
  Destination port range: [1-65535]
Dynamic Application:
  junos:FACEBOOK-CHAT: 10704
  junos:GMAIL: 51
dynapp-redir-profile: profile1(1)
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No

```

show security policies detail (TCP Options)

```

user@host> show security policies policy-name p2 detail
node0:

```

```

-----
Policy:p2, action-type:permit, State: enabled,Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0

```

```

any-ipv6(global): ::/0
Destination addresses:
any-ipv4(global): 0.0.0.0/0
any-ipv6(global): ::/0
Application: junos-defaults
IP protocol: tcp, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [80-80]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Dynamic-application: junos:HTTP

```

show security policies policy-name (Negated Address)

```

user@host> show security policies policy-name p1
node0:
-----
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit

```

show security policies policy-name detail (Negated Address)

```

user@host> show security policies policy-name p1 detail
node0:
-----
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses(excluded):
ad1(ad): 255.255.255.255/32
ad2(ad): 198.51.100.1/24
ad3(ad): 198.51.100.6 ~ 198.51.100.56
ad4(ad): 192.0.2.8/24
ad5(ad): 198.51.100.99 ~ 198.51.100.199
ad6(ad): 203.0.113.9/24
ad7(ad): 203.0.113.23/24
Destination addresses(excluded):
ad13(ad2): 198.51.100.76/24
ad12(ad2): 198.51.100.88/24
ad11(ad2): 192.0.2.23 ~ 192.0.2.66
ad10(ad2): 192.0.2.93
ad9(ad2): 203.0.113.76 ~ 203.0.113.106
ad8(ad2): 203.0.113.199
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

show security policies global

```

user@host> show security policies global policy-name Pa
node0:
-----
Global policies:
Policy: Pa, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1

```

```

From zones: any
To zones: any
Source addresses: H0
Destination addresses: H1
Applications: junos-http
Action: permit

```

show security policies detail tenant

```
user@host> show security policies detail tenant TN1
```

```

Default policy: deny-all
Pre ID default policy: permit-all
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses: any
Destination addresses: any
Application: junos-ping
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input bytes      : 0 0 bps
Initial direction: 0 0 bps
Reply direction  : 0 0 bps
Output bytes     : 0 0 bps
Initial direction: 0 0 bps
Reply direction  : 0 0 bps
Input packets    : 0 0 pps
Initial direction: 0 0 bps
Reply direction  : 0 0 bps
Output packets   : 0 0 pps
Initial direction: 0 0 bps
Reply direction  : 0 0 bps
Session rate     : 0 0 sps
Active sessions  : 0
Session deletions: 0
Policy lookups   : 0

```

show security screen statistics

Syntax	<pre>show security screen statistics <zone <i>zone-name</i> interface <i>interface-name</i>> logical-system <<i>logical-system-name</i> all> root-logical-system tenant <<i>tenant-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 8.5.</p> <p>The node option added in Junos OS Release 9.0.</p> <p>The logical-system all option added in Junos OS Release 11.2R6.</p> <p>Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10.</p> <p>The tenant option is introduced in Junos OS Release 18.3R1.</p>
Description	Display intrusion detection service (IDS) security screen statistics.
Options	<ul style="list-style-type: none"> • zone <i>zone-name</i>—Display screen statistics for this security zone. • interface <i>interface-name</i> —Display screen statistics for this interface. • <i>logical-system-name</i>—Display screen statistics for the named logical system. • root-logical-system—(Optional) Display screen statistics for the master logical system only. • tenant—Display the name of the tenant system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>clear security screen statistics</i> • <i>clear security screen statistics interface</i> • <i>clear security screen statistics zone</i> • <i>Example: Configuring Multiple Screening Options</i>
List of Sample Output	<p>show security screen statistics zone scrzone on page 738</p> <p>show security screen statistics zone untrust (IPv6) on page 738</p> <p>show security screen statistics interface ge-0/0/3 on page 739</p> <p>show security screen statistics interface ge-0/0/1 (IPv6) on page 739</p> <p>show security screen statistics interface ge-0/0/1 node primary on page 740</p> <p>show security screen statistics zone trust logical-system all on page 740</p> <p>show security screen statistics zone trust tenant TN1 on page 742</p> <p>show security screen statistics zone trust tenant all on page 743</p>
Output Fields	<p>Table 77 on page 736 lists the output fields for the show security screen statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 77: show security screen statistics Output Fields

Field Name	Field Description
ICMP flood	Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP flood	User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP port scan	Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP address sweep	Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.
IP tear drop	Number of teardrop attacks. Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN flood	Number of TCP SYN attacks.
IP spoofing	Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP ping of death	ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP source route option	Number of IP source route attacks.
TCP address sweep	Number of TCP address sweeps.
TCP land attack	Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN fragment	Number of TCP SYN fragments.
TCP no flag	Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set.
IP unknown protocol	Number of IPs.
IP bad options	Number of invalid options.
IP record route option	Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels.
IP timestamp option	Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.

Table 77: show security screen statistics Output Fields (continued)

Field Name	Field Description
IP security option	Number of IP security option attacks.
IP loose source route option	Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination.
IP strict source route option	Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination.
IP stream option	Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP fragment	Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP large packet	Number of large ICMP packets.
TCP SYN FIN	Number of TCP SYN FIN packets.
TCP FIN no ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.
Source session limit	Number of concurrent sessions that can be initiated from a source IP address.
TCP SYN-ACK-ACK proxy	Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold and SRX Series devices running Junos OS reject further connection requests from that IP address.
IP block fragment	Number of IP block fragments.
Destination session limit	Number of concurrent sessions that can be directed to a single destination IP address.
UDP address sweep	Number of UDP address sweeps.
IPv6 extension header	Number of packets filtered for the defined IPv6 extension headers.
IPv6 extension hop by hop option	Number of packets filtered for the defined IPv6 hop-by-hop option types.
IPv6 extension destination option	Number of packets filtered for the defined IPv6 destination option types.
IPv6 extension header limit	Number of packets filtered for crossing the defined IPv6 extension header limit.
IPv6 malformed header	Number of IPv6 malformed headers defined for the intrusion detection service (IDS).
ICMPv6 malformed packet	Number of ICMPv6 malformed packets defined for the IDS options.

Sample Output

show security screen statistics zone scrzone

```
user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                   0
UDP flood                                    0
TCP winnuke                                  0
TCP port scan                               91
ICMP address sweep                           0
TCP sweep                                    0
UDP sweep                                    0
IP tear drop                                0
TCP SYN flood                                0
IP spoofing                                  0
ICMP ping of death                           0
IP source route option                       0
TCP land attack                              0
TCP SYN fragment                             0
TCP no flag                                  0
IP unknown protocol                          0
IP bad options                               0
IP record route option                       0
IP timestamp option                          0
IP security option                           0
IP loose source route option                 0
IP strict source route option                0
IP stream option                             0
ICMP fragment                               0
ICMP large packet                            0
TCP SYN FIN                                  0
TCP FIN no ACK                               0
Source session limit                         0
TCP SYN-ACK-ACK proxy                        0
IP block fragment                           0
Destination session limit                    0
```

Sample Output

show security screen statistics zone untrust (IPv6)

```
user@host> show security screen statistics zone untrust
Screen statistics:
IDS attack type                               Statistics
ICMP flood                                   0
UDP flood                                    0
TCP winnuke                                  0
.....
IPv6 extension header                        0
IPv6 extension hop by hop option             0
IPv6 extension destination option            0
IPv6 extension header limit                  0
IPv6 malformed header                        0
ICMPv6 malformed packet                      0
```

Sample Output

show security screen statistics interface ge-0/0/3

```

user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
TCP winnuke               0
TCP port scan             91
ICMP address sweep        0
TCP sweep                 0
UDP sweep                 0
IP tear drop              0
TCP SYN flood             0
IP spoofing               0
ICMP ping of death        0
IP source route option    0
TCP land attack           0
TCP SYN fragment          0
TCP no flag               0
IP unknown protocol       0
IP bad options            0
IP record route option    0
IP timestamp option       0
IP security option        0
IP loose source route option 0
IP strict source route option 0
IP stream option          0
ICMP fragment             0
ICMP large packet         0
TCP SYN FIN               0
TCP FIN no ACK            0
Source session limit      0
TCP SYN-ACK-ACK proxy     0
IP block fragment         0
Destination session limit 0

```

Sample Output

show security screen statistics interface ge-0/0/1 (IPv6)

```

user@host> show security screen statistics interface ge-0/0/1

Screen statistics:

IDS attack type           Statistics
ICMP flood                0
UDP flood                 0
.....
IPv6 extension header      0
IPv6 extension hop by hop option 0
IPv6 extension destination option 0
IPv6 extension header limit 0
IPv6 malformed header     0
ICMPv6 malformed packet   0

```

Sample Output

show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
```

```
-----
Screen statistics:
IDS attack type          Statistics
ICMP flood               1
UDP flood                 1
TCP winnuke              1
TCP port scan            1
ICMP address sweep       1
TCP sweep                 1
UDP sweep                 1
IP tear drop             1
TCP SYN flood            1
IP spoofing              1
ICMP ping of death       1
IP source route option   1
TCP land attack          1
TCP SYN fragment         1
TCP no flag              1
IP unknown protocol      1
IP bad options           1
IP record route option   1
IP timestamp option      1
IP security option       1
IP loose source route option 1
IP strict source route option 1
IP stream option         1
ICMP fragment            1
ICMP large packet        1
TCP SYN FIN              1
TCP FIN no ACK           1
Source session limit     1
TCP SYN-ACK-ACK proxy    1
IP block fragment        1
Destination session limit 1
```

Sample Output

show security screen statistics zone trust logical-system all

```
user@host> show security screen statistics zone trust logical-system all
Logical system: root-logical-system
Screen statistics:
```

```
IDS attack type          Statistics
ICMP flood               0
UDP flood                 0
TCP winnuke              0
TCP port scan            0
ICMP address sweep       0
TCP sweep                 0
UDP sweep                 0
IP tear drop             0
TCP SYN flood            0
IP spoofing              0
```

ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls1

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

Logical system: ls2

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0

show security screen statistics zone trust tenant TN1

```
user@host> show security screen statistics zone trust tenant TN1
```

Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
UDP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
SYN flood source	0
SYN flood destination	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0

IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0
IPv6 extension header	0
IPv6 extension hop by hop option	0
IPv6 extension destination option	0
IPv6 extension header limit	0
IPv6 malformed header	0
ICMPv6 malformed packet	0
IP tunnel summary	0

show security screen statistics zone trust tenant all

```
user@host> show security screen statistics zone trust tenant all
```

```
Logical system: root-logical-system
screen statistics:
```

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
UDP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
SYN flood source	0
SYN flood destination	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0

IP block fragment	0
Destination session limit	0
IPv6 extension header	0
IPv6 extension hop by hop option	0
IPv6 extension destination option	0
IPv6 extension header limit	0
IPv6 malformed header	0
ICMPv6 malformed packet	0
IP tunnel summary	0

Tenant: TN1
Screen statistics:

IDS attack type	Statistics
ICMP flood	0
UDP flood	0
TCP winnuke	0
TCP port scan	0
UDP port scan	0
ICMP address sweep	0
TCP sweep	0
UDP sweep	0
IP tear drop	0
TCP SYN flood	0
SYN flood source	0
SYN flood destination	0
IP spoofing	0
ICMP ping of death	0
IP source route option	0
TCP land attack	0
TCP SYN fragment	0
TCP no flag	0
IP unknown protocol	0
IP bad options	0
IP record route option	0
IP timestamp option	0
IP security option	0
IP loose source route option	0
IP strict source route option	0
IP stream option	0
ICMP fragment	0
ICMP large packet	0
TCP SYN FIN	0
TCP FIN no ACK	0
Source session limit	0
TCP SYN-ACK-ACK proxy	0
IP block fragment	0
Destination session limit	0
IPv6 extension header	0
IPv6 extension hop by hop option	0
IPv6 extension destination option	0
IPv6 extension header limit	0
IPv6 malformed header	0
ICMPv6 malformed packet	0
IP tunnel summary	0

show services user-identification authentication-table

Syntax show services user-identification authentication-table
 <authentication-source | counter | ip-address>
 show services user-identification authentication-table authentication-source
 <active-directory | all | aruba-clearpass | identity-management>
 show services user-identification authentication-table authentication-source active-directory
 <brief | domain | extensive | group | logical-system | root-logical-system |summary |user>
 show services user-identification authentication-table authentication-source all
 <brief | domain | extensive |group | logical-system | root-logical-system |summary |user>
 <domain *domain*>
 <group (group-name | brief | domain | extensive | logical-system | root-logical-system |
 summary)>
 <logical-system (*logical-system-name*| all)>
 <node (node-id | all | local | primary)>
 <root-logical-system (enter |brief | domain | extensive | node)>
 <user (user-name | brief | domain | extensive | logical-system | node | root-logical-system |
 summary)>
 show services user-identification authentication-table authentication-source active-directory
 <brief | domain | extensive | group | logical-system | root-logical-system |summary |user>
 show services user-identification authentication-table authentication-source
 identity-management source-name
 show services user-identification authentication-table counter
 show services user-identification authentication-table ip-address
 <summary>
 <logical-system *logical-system-name*>
 <root-logical-system>
 <node *node-id*>
 <IP address *ip-address*>

Release Information Command introduced in Junos OS Release 12.1X47-D10 for active directory. Support for Aruba ClearPass added in Junos OS release 12.3X48-D30 for Aruba ClearPass. Support added for identity-management as an authentication source in Junos OS Release 15.1X49-D100. Support added for logical-system for authentication-source all in Junos OS Release 18.2R1.

Description Display the user identity information authentication table entries for the specified authentication source. You can display the entire contents of the specified authentication source's authentication table, or you can constrain the displayed information to a specific domain, group, or user based on the user name. You can also display identity information for a user based on the IP address of the user's device. You can show brief or extensive information for all of these instances.

authentication-source—User authentication source whose authentication table or identity management server entries are to be displayed.

Authentication sources include:

active-directory—Display the SRX Series active-directory table contents. You can display all of the table's contents or you can delimit the display of user identity information by domain, group, or user name. You can display brief or extensive information for each of these categories.

- **domain**—Display the entries in the authentication table for the specified domain. You can display summary, group, or user entries for the specified domain.
- **group**—Display the entries from the authentication table for the specified group.
- **user**—Display the entries from the authentication table for the specified user based on the user name.

aruba-clearpass—Display the SRX Series Aruba ClearPass authentication table contents. You can display all of the table's contents or you can delimit the display of user information by domain, group, or user name. You can display brief or extensive information for each of these categories.

- **domain**—Display the entries in the authentication table for the specified domain. You can display summary, group, or user entries for the specified domain.
- **group**—Display the entries from the authentication table for the specified group.
- **user**—Display the entries from the authentication table for the specified user based on the user name.

identity-management —Display user identity entries contained in the identity-management authentication system.

- **source-name**—Name of the identity -management source. This could be the Juniper Identity Management Service (JIMS) or any third-party authentication source.
 - If you specify a source, such as "JIMS – Active Directory" for Juniper Identity Management Service, the SRX Series device will show entries only for that authentication source.

Possible values include:

- For JIMS: "JIMS – Active Directory", "JIMS – Exchange"
- For ClearPass: "Aruba ClearPass"
- **domain**—Display the entries in the identity management system for the specified domain. You can display summary, group, or user entries for the specified domain.
- **group**—Display the entries in the identity management system for the specified group.
- **user**—Display the entries in the identity management system for the specified user based on the user name.

- Options**
- **all**—Summary of the authentication entry information for all entries.
 - **group *group-name***—Entries from the authentication table or identity management system for the specified group.
 - **ip-address *ip-address***—Entries from the authentication table or identity management system for the specified IP address.
 - **user *name***—Entries from the authentication table for the specified username.
 - **domain *name***—Summary, group, or user entries for the specified domain.
 - **node**—(Optional) For chassis cluster configurations, the summary, IP address, or user entries for a specific node.
 - **node-id**—Identification number of the node. It can be 0 or 1.
 - **all**—Display information about all nodes.
 - **local**—Display information about the local node.
 - **primary**—Display information about the primary node.
 - **brief | extensive**—Display the specified level of output (the default is brief).
 - **logical-system**—Display the authentication entries based on the logical system name.
 - **root-logical-system**—Display the authentication entries based on the root logical system.

Required Privilege Level

view

List of Sample Output

[show services user-identification active-directory-access active-directory-authentication-table ip-address on page 749](#)
[show services user-identification authentication-table ip-address on page 750](#)
[show services user-identification active-directory-access active-directory-authentication-table all on page 750](#)
[show services user-identification active-directory-access active-directory-authentication-table all extensive on page 750](#)
[show services user-identification active-directory-access active-directory-authentication-table all domain on page 751](#)
[All Authentication Sources on page 751](#)
[Aruba ClearPass on page 753](#)
[show services user-identification authentication-table authentication-source aruba-clearpass domain brief on page 755](#)
[show services user-identification authentication-table authentication-source aruba-clearpass extensive on page 755](#)
[show services user-identification authentication-table authentication-source identity-management brief on page 757](#)
[show services user-identification authentication-table authentication-source identity-management extensive on page 757](#)
[show services user-identification authentication-table authentication-source all extensive on page 758](#)

[show services user-identification authentication-table authentication-source all](#)
[extensive on page 758](#)

Field Name	Field Description
Domain Output Fields	Name of the domain that the users belong to. User identity and authentication information is display for all users who belong to the domain and for whom there are entries in the specified authentication source table or repository.
Total entries	Number of user entries in the authentication table, by domain.
For each entry:	
Source IP	The IP address of the user's device. If a user is logged in to the network with more than one device, a separate entry is created for the user for each device. It showing the devices IP address.
Username	The name by which the user is logged in to the network.
Groups	A list of the groups that the user belongs to. The list can include a group that identifies the device posture.
State	<p>The state of the entry. There are four states for an authentication entry: initial, valid, invalid, and pending.</p> <ul style="list-style-type: none"> • An initial state is a temporary state, and it can be created from either a valid or an invalid entry. The entry had not been pushed to the Packet Forwarding Engine. • A valid state indicates that the authentication entry has a valid IP address, domain, and username. The authentication entry is pushed to the Packet Forwarding Engine. • An invalid state indicates that the entry does not have a valid IP address, domain, and username. If the entry is invalid, it is put in the null domain. • A pending state indicates that the entry was created after the user query was sent and before the response was received. The IP address is being probed.
Source	Authentication source.
Access start date	The date when the authentication entry was created by the SRX Series device.
Access start time	The time when the authentication entry was created by the SRX Series device.
Last updated timestamp	The time when the user information was created. This value is taken from the timestamp field in the user information.
Age time:	The time, in minutes, after which the entry expires, as configured by the authentication-entry-timeout statement. If a value of 0 was specified, the entry never expires.
Forced Age time:	<p>The rest value and the forced value.</p> <p>This information is made available if you configure the firewall-authentication-forced-timeout statement for active directory.</p>

Active Directory

show services user-identification active-directory-access active-directory-authentication-table ip-address

Output of this command displays authentication and identity information for a specific user based on the IP address of the user's device.

```
user@host> show services user-identification active-directory-access
active-directory-authentication-table ip-address 198.51.100.3.
Domain: ad.example.net
Source-ip: 198.51.100.3
Username: user1
Groups:group1
State: Valid
Source: wmic
Access start date: 2014-03-10
Access start time: 13:59:56
Age time: 1437
```

show services user-identification authentication-table ip-address

Output of this command displays authentication and identity information for a specific user based on the IP address of the user's device.

```
user@host> show services user-identification authentication-table ip-address 2001:db8::1:1
Domain: ac.example.net
Source-ip: 2001:db8::1:1
Username: user1
Groups:group1
State: Valid
Source: wmic
Access start date: 2017-05-10
Access start time: 13:59:56
Age time: 1437
```

show services user-identification active-directory-access active-directory-authentication-table all

Output of this command displays user authentication and identity information for all users for whom there are entries in the active directory authentication table.

```
user@host> show services user-identification active-directory-access
active-directory-authentication-table all
Domain: www.engineering-example.net
Total count: 2
Source IP      Username      Groups        State
198.51.100.22  u2            r1, r3, r4    initial
198.51.100.23  u3            r5, r6, r4    pending

Domain: www.hr-example.net
Total count: 2
Source IP      Username      Groups        State
198.51.100.26  u4            r1, r3, r4    initial
198.51.100.27  u5            r5, r6, r4    pending
```

show services user-identification active-directory-access active-directory-authentication-table all extensive

Output of this command, which specifies the **extensive** option, shows state and access information for all entries in the active directory authentication table, in addition to basic information displayed when the **brief** option is used and by default.

```
user@host> show services user-identification active-directory-access
active-directory-authentication-table all extensive
```

```
Domain: www.mycompany-example.com
Total entries: 2
```

```
Source IP: 198.51.100.29
Username: u2
Groups: r1, r3, r4
State: initial
Access start date: 2013-05-22
Access start time: 10:56:58
Age time: 20 min
```

```
Source IP: 198.51.100.30
Username: u3
Groups: r5, r6, r4
State: pending
Access start date: 2013-05-22
Access start time: 10:56:58
Age time: 20 min
```

```
Domain: www.hr-example.net
Total entries: 2
```

```
Source IP: 198.51.100.31
Username: u2
Groups: r1, r3, r4
State: initial
Access start date: 2013-05-22
Access start time: 10:56:58
Age time: 20 min
```

```
Source IP: 198.51.100.32
Username: u3
Groups: r5, r6, r4
State: pending
Access start date: 2013-05-22
Access start time: 10:56:58
Age time: 20
```

show services user-identification active-directory-access active-directory-authentication-table all domain

Output of this command shows by default brief user identity and authentication information for all users for whom there are entries in the active directory authentication table and whose devices belong to the specified domain.

```
user@host> show services user-identification active-directory-access
active-directory-authentication-table all domain www.mydomain-example.com
```

```
Domain: www.mydomain-example.com
Total count: 2
```

Source IP	Username	Groups	State
198.51.100.36	u2	r1, r3, r4	initial
198.51.100.37	u3	r5, r6, r4	pending

All Authentication Sources

Output of this command shows extensive user identity and authentication information for all users with entries in authentication tables of any authentication source. This

example shows only one entry to illustrate the content that is displayed with the extensive option.

```
user@host> show services user-identification authentication-table authentication-source all
extensive
```

```
Domain: ad-userfw-example.net
Total entries: 1
Source-ip: 198.51.100.1/24
Username: administrator
State: Valid
Source: firewall-authentication
Access start date: 2016-10-27
Access start time: 09:30:27
Age time: 30
```

```
user@host> show services user-identification authentication-table authentication-source all
logical-system
```

```
lsys1
node0:
```

```
-----
Logical System: root-logical-system
```

```
Domain: ad2012.jims.com
Total entries: 18003
Source IP      Username      groups(Ref by policy)      state
bbbb:bbbb:bbbb: jimsuser18000      Valid
bbbb:bbbb:bbbb: jimsuser17999      Valid
bbbb:bbbb:bbbb: jimsuser17998      Valid
bbbb:bbbb:bbbb: jimsuser17997      Valid
bbbb:bbbb:bbbb: jimsuser17996      Valid
bbbb:bbbb:bbbb: jimsuser17995      Valid
bbbb:bbbb:bbbb: jimsuser17994      Valid
bbbb:bbbb:bbbb: jimsuser17993      Valid
```

```
user@host> show services user-identification authentication-table authentication-source all
root-logical-system
```

```
node0:
```

```
-----
Logical System: root-logical-system
```

```
Domain: ad2012.jims.com
Total entries: 18003
Source IP      Username      groups(Ref by policy)      state
bbbb:bbbb:bbbb: jimsuser10745      Valid
bbbb:bbbb:bbbb: jimsuser18000      Valid
bbbb:bbbb:bbbb: jimsuser17999      Valid
bbbb:bbbb:bbbb: jimsuser17998      Valid
bbbb:bbbb:bbbb: jimsuser17997      Valid
bbbb:bbbb:bbbb: jimsuser17996      Valid
bbbb:bbbb:bbbb: jimsuser17995      Valid
bbbb:bbbb:bbbb: jimsuser17994      Valid
bbbb:bbbb:bbbb: jimsuser17993      Valid
bbbb:bbbb:bbbb: jimsuser17992      Valid
```

```
user@host> show services user-identification authentication-table
authentication-source all node 0
```

```
node0:
```

```
-----
Logical System: root-logical-system
```



```

Domain: ad2012.jims.com
Total entries: 18003
Source IP      Username      groups(Ref by policy)      state
bbbb:bbbb:bbbb: jimsuser14716
bbbb:bbbb:bbbb: jimsuser18000      Valid
bbbb:bbbb:bbbb: jimsuser17999      Valid
bbbb:bbbb:bbbb: jimsuser17998      Valid
bbbb:bbbb:bbbb: jimsuser17997      Valid
bbbb:bbbb:bbbb: jimsuser17996      Valid
bbbb:bbbb:bbbb: jimsuser17995      Valid
bbbb:bbbb:bbbb: jimsuser17994      Valid
bbbb:bbbb:bbbb: jimsuser17993      Valid

```

```

user@host> show services user-identification authentication-table authentication-source all
node 0 logical-system lsysl
node0:

```

```
-----
Logical System: root-logical-system

```

```

Domain: ad2012.jims.com
Total entries: 18003
Source IP      Username      groups(Ref by policy)      state
bbbb:bbbb:bbbb: jimsuser18000      Valid
bbbb:bbbb:bbbb: jimsuser17999      Valid
bbbb:bbbb:bbbb: jimsuser17998      Valid
bbbb:bbbb:bbbb: jimsuser17997      Valid
bbbb:bbbb:bbbb: jimsuser17996      Valid
bbbb:bbbb:bbbb: jimsuser17995      Valid
bbbb:bbbb:bbbb: jimsuser17994      Valid
bbbb:bbbb:bbbb: jimsuser17993      Valid
bbbb:bbbb:bbbb: jimsuser17992      Valid

```

```

user@host> show services user-identification authentication-table authentication-source all
node 0
node0:

```

```
-----
Logical System: root-logical-system

```

```

Domain: ad2012.jims.com
Total entries: 18003
Source IP      Username      groups(Ref by policy)      state
bbbb:bbbb:bbbb: jimsuser1213
bbbb:bbbb:bbbb: jimsuser18000      Valid
bbbb:bbbb:bbbb: jimsuser17999      Valid
bbbb:bbbb:bbbb: jimsuser17998      Valid
bbbb:bbbb:bbbb: jimsuser17997      Valid
bbbb:bbbb:bbbb: jimsuser17996      Valid
bbbb:bbbb:bbbb: jimsuser17995      Valid
bbbb:bbbb:bbbb: jimsuser17994      Valid
bbbb:bbbb:bbbb: jimsuser17993      Valid

```

Aruba ClearPass

```

show services user-identification authentication-table authentication-source
aruba-clearpass domain extensive

```

Output of this command shows extensive user identity and authentication information, when Aruba ClearPass is used as the authentication source, for all users whose devices belong to the GLOBAL domain.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass domain GLOBAL extensive
Domain: GLOBAL
Total entries: 7
Source-ip: 203.0.113.21
  Username: vikiyr
  Groups: posture-healthy, accounting-grp, accounting-grp-and-company-device,
  corporate-limited, [user authenticated]
  Groups referenced by policy: accounting-grp-and-company-device,
  corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:20:30
  Last updated timestamp: 2015-12-22 04:02:48
  Age time: 0
Source-ip: 203.0.113.89
  Username: abewhfy
  Groups: posture-unknown, marketing-access-limited-grp, [user authenticated]
  Groups referenced by policy: marketing-access-limited-grp
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:31:40
  Last updated timestamp: 2015-12-22 04:18:48
  Age time: 0
Source-ip: 203.0.113.52
  Username: jjxchan
  Groups: posture-healthy, marketing-access-for-pcs-limited-group,
  marketing-general, sales-limited, corporate-limited, [user authenticated]
  Groups referenced by policy: marketing-access-for-pcs-limited-group,
  corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:22:48
  Last updated timestamp: 2015-12-22 05:46:21
  Age time: 0
Source-ip: 203.0.113.53
  Username: ltchen1
  Groups: posture-healthy, human-resources-grp, accounting-limited,
  corporate-limited, [user authenticated]
  Groups referenced by policy: corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:21:37
  Last updated timestamp: 2015-12-22 05:41:18
  Age time: 0
Source-ip: 203.0.113.54
  Username: guest1
  Groups: posture-healthy, guest, [user authenticated]
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:23:10
  Last updated timestamp: 2015-12-22 05:50:47
```

```

Age time: 0
Source-ip: 203.0.113.55
Username: guest2
Groups:posture-healthy, guest-device-byod, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0
Source-ip: 2001:db8:4136:e378:8000:63bf:3fff:fdd2
Username: guest3
Groups:posture-healthy, guest-device-grp, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0

```

show services user-identification authentication-table authentication-source aruba-clearpass domain brief

Output of this command shows brief user identity and authentication information for users whose devices belong to the GLOBAL domain.

If you do not specify brief, the same information would be displayed. The default behavior is to show brief output.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass domain GLOBAL brief
```

```

Domain: GLOBAL
Total entries: 6
Source IP                               Username      groups(Ref by policy)
state
203.0.113.71                             taviki2
accounting-grp-and-company-dev Valid
203.0.113.89                             gabewb1
marketing-access-limited-grp Valid
203.0.113.92                             tljxchan
marketing-access-for-pcs-limit Valid
203.0.113.93                             tjlchen1      corporate-limited
Valid
203.0.113.94                             guest1
Valid
203.0.113.95                             guest2
Valid
2001:db8:4136:e378:8000:63bf:3fff:fdd2 guest2
Valid

```

show services user-identification authentication-table authentication-source aruba-clearpass extensive

Output of the following command shows extensive user identity and authentication information for all users authenticated by Aruba ClearPass for whom entries exist in the aruba-clearpass authentication table.

```
user@host> show services user-identification authentication-table authentication-source
aruba-clearpass extensive
```

```

Domain: GLOBAL
Total entries: 7
Source-ip: 203.0.113.31
  Username: vjki2
  Groups:posture-healthy, accounting-grp, accounting-grp-and-company-device,
  corporate-limited, [user authenticated]
  Groups referenced by policy:accounting-grp-and-company-device,
  corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:20:30
  Last updated timestamp: 2015-12-22 04:02:48
  Age time: 0
Source-ip: 203.0.113.89
  Username: labew11
  Groups:posture-unknown, marketing-access-limited-grp, [user authenticated]
  Groups referenced by policy:marketing-access-limited-grp
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:31:40
  Last updated timestamp: 2015-12-22 04:18:48
  Age time: 0
Source-ip: 203.0.113.62
  Username: dxchan45
  Groups:posture-healthy, marketing-access-for-pcs-limited-group,
  marketing-general, sales-limited, corporate-limited, [user authenticated]
  Groups referenced by policy:marketing-access-for-pcs-limited-group,
  corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:22:48
  Last updated timestamp: 2015-12-22 05:46:21
  Age time: 0
Source-ip: 2001:db8:4136:e378:8000:63bf:3fff:fdd2
  Username: efchan47
  Groups:posture-healthy, marketing-access-for-pcs-limited-group,
  marketing-general, sales-limited, corporate-limited, [user authenticated]
  Groups referenced by policy:marketing-access-for-pcs-limited-group,
  corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:22:48
  Last updated timestamp: 2015-12-22 05:46:21
  Age time: 0
Source-ip: 203.0.113.83
  Username: ljhen1
  Groups:posture-healthy, human-resources-grp, accounting-limited,
  corporate-limited, [user authenticated]
  Groups referenced by policy:corporate-limited
  State: Valid
  Source: Aruba ClearPass
  Access start date: 2016-03-08
  Access start time: 17:21:37
  Last updated timestamp: 2015-12-22 05:41:18
  Age time: 0
Source-ip: 203.0.113.34

```

```

Username: guest1
Groups:posture-healthy, guest, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:10
Last updated timestamp: 2015-12-22 05:50:47
Age time: 0
Source-ip: 203.0.113.95
Username: guest2
Groups:posture-healthy, guest-device-byod, [user authenticated]
State: Valid
Source: Aruba ClearPass
Access start date: 2016-03-08
Access start time: 17:23:21
Last updated timestamp: 2015-12-22 05:52:44
Age time: 0

```

Identity Management

show services user-identification authentication-table authentication-source identity-management brief

Output of this command displays brief user authentication and identity information for all users for whom there are entries in the identity-management authentication source.

```

user@host> show services user-identification authentication-table authentication-source
identity-management brief
Domain: ad-domaine-example.net
Total entries: 5
Source IP      Username      groups(Ref by policy)      state
198.51.100.63  N/A          administrator              Valid
203.0.113.30   administrator
203.0.113.18   N/A          administrator              Valid
198.51.100.69  N/A          administrator              Valid
198.51.100.66  administrator
Domain: NULL
Total entries: 1
Source IP      Username      groups(Ref by policy)

```

show services user-identification authentication-table authentication-source identity-management extensive

Output of this command displays extensive user authentication and identity information for all users for whom there are entries in the identity-management authentication source.

```

user@host> show services user-identification authentication-table authentication-source
identity-management extensive
Domain: ad-domain2-example.net
Total entries: 5
Source-ip: 198.51.100.63
Username: N/A
Groups:posture-healthy
State: Valid
Source: JIMS - Active Directory
Access start date: 2017-06-05
Access start time: 09:28:45
Last updated timestamp: 2017-06-06 08:41:56
Age time: 0
Source-ip: 198.51.100.66

```

```
Username: administrator
Groups:posture-healthy, group policy creator owners, enterprise admins, schema
admins, domain admins,
administrators, denied rod password replication group
State: Valid
Source: JIMS - Active Directory
Access start date: 2017-06-05
Access start time: 09:23:44
Last updated timestamp: 2017-06-06 08:11:45
Age time: 0
```

show services user-identification authentication-table authentication-source all extensive

Output of this command, which specifies the extensive option, shows state and access information for all entries.

```
user@host> show services user-identification authentication-table authentication-source
identity-management extensive
Domain: jims-dom1.local
Total entries: 1
Source-ip: 2001:db8:4136:e378:8000:63bf:3fff:fdd2
Username: user1
Groups:posture-healthy
Groups referenced by policy:posture-healthy
State: Valid
Source: JIMS - Active Directory
Access start date: 2017-08-23
Access start time: 15:06:32
Last updated timestamp: 2017-06-07 02:50:10
Age time: 30
```

Firewall Authentication Forced Age Timeout

Output shows the “Forced Age timeout” value is displayed when the firewall authentication forced timeout function is configured, but only for when the extensive option is used. The value shows the remaining time left based on the forced timeout setting.

show services user-identification authentication-table authentication-source all extensive

```
user@host> show services user-identification authentication-table
authentication-source all extensive
Domain: ad-userfw.net
Total entries: 1
Source-ip: 198.51.100.98
Username: administrator
State: Valid
Source: firewall-authentication
Access start date: 2016-10-27
Access start time: 09:30:27
Age time: 30
Forced Age time: 30/180
```

show system security-profile

Syntax show system security-profile (all-resource | *resource*)
detail | *terse*
 logical-system (*logical-system-name*)
 root-logical-system
 tenant (*tenant-name*)

Release Information Command introduced in Junos OS Release 11.2.
 Support for application firewall added in Junos OS Release 11.3.
 Option to display all resources for a logical system added in Junos OS Release 11.
 Resource information for ports in source NAT pools with port translation added in Release Junos OS 11.4.
 The tenant option is introduced in Junos OS Release 18.3R1.
 The icap redirect profile option is introduced in Junos OS Release 18.3R1.

Description Display information about a resource allocated to the logical system in a security profile. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

The **show system security-profile** command can be used by the master administrator to display resource information for the master logical system or user logical system. This command can also be used by the user logical system administrator to display resource information for a user logical system.

Options Either specify **all-resource** to display information about all resources allocated for the logical system, or specify one of the following resources:

- address-book—Address books.
- appfw-rule-set—Application firewall rule set entries.
- appfw-rule—Application firewall rule entries.
- auth-entry—Firewall authentication entries.
- cpu—CPU utilization.
- flow-gate—Flow gates, also known as pinholes.
- flow-session—Flow sessions.
- icap-redirect-profile—ICAP redirect profile resource information.
- nat-cone-binding—Network Address Translation (NAT) cone bindings.
- nat-destination-pool—NAT destination pools.
- nat-destination-rule—NAT destination rules.
- nat-nopat-address—NAT without port address translations.
- nat-pat-address—NAT with port address translations.
- nat-pat-portnum—NAT source port numbers for port translation

- nat-port-ol-ipnumber—NAT port overloading IP numbers.
- nat-rule-referenced-prefix—NAT rule referenced IP-prefixes.
- nat-source-pool—NAT source pools.
- nat-source-rule—NAT source rules.
- nat-static-rule—NAT static rules.
- policy—Security policies.
- policy-with-count—Security policies with a count.
- scheduler—Schedulers.
- zone—Security zones.

detail | terse—(Optional) Display the specified level of output.

The following options are available only to the master administrator:

- logical-system—Display resource information for a specified user logical system. Specify **all** to display resource information for all logical systems, including the master logical system.
- root-logical-system—Display resource information for the master (root) logical system.
- summary—Display summary information about the resource for all logical systems.
- tenant—Display resource information for a specified tenant system. Specify **all** to display resource information for all tenant systems.

Required Privilege Level

view

Related Documentation

- [security-profile-resources on page 546](#)

List of Sample Output

[show system security-profile all-resource on page 761](#)
[show system security-profile all-resource tenant all on page 762](#)
[show system security-profile policy on page 762](#)
[show system security-profile cpu on page 762](#)
[show system security-profile cpu logical-system all on page 763](#)
[show system security-profile cpu summary on page 763](#)
[show system security-profile nat-pat-portnum on page 763](#)
[show system security-profile nat-pat-portnum summary on page 764](#)
[show system security-profile icap-redirect-profile logical-system all on page 764](#)

Output Fields

[Table 78 on page 761](#) lists the output fields for the **show system security-profile** command. Output fields are listed in the approximate order in which they appear.

Table 78: show system security-profile Output Fields

Field Name	Field Description
logical system name	Name of the logical system.
tenant name	Name of the tenant system.
security profile name	Name of the security profile bound to the logical system.
usage	Number of resources that are currently being used by the logical system.
reserved	Number of resources that are guaranteed to be available to the logical system.
maximum	Number of resources that the logical system can use. The maximum does not guarantee that the amount specified for the resource in the security profile is available. The maximum is not applicable for CPU resources.
CPU control	TRUE if CPU control is enabled or FALSE if CPU control is not enabled.
CPU control target	Upper limit for CPU utilization on the device. The default value is 80 percent.
CPU name	Central point (CP) or services processing unit (SPU). CP utilization and average utilization of all SPUs is shown. The detail option shows CPU utilization on each SPU.
drop rate	Packets dropped for CPU control.

Sample Output

show system security-profile all-resource

```
user@host> show system security-profile all-resource
```

```

resource                               usage    reserved    maximum

[logical system name:  root-logical-system]
[security profile name: Default-Profile]
address-book                           0         0         512
auth-entry                             0         0  2147483647
cpu on CP                             0.00%     1.00%     80.00%
cpu on SPU                             0.00%     1.00%     80.00%
flow-gate                              0         0     524288
flow-session                           2         0    6291456
nat-cone-binding                       0         0     65536
nat-destination-pool                   0         0     4096
nat-destination-rule                   0         0     8192
nat-nopat-address                      0         0    1048576
nat-pat-address                        0         0     2048
nat-port-ol-ipnumber                   0         0         4
nat-rule-referenced-prefix             0         0    1048576
nat-source-pool                        0         0     2048
nat-source-rule                        0         0     8192
nat-static-rule                        0         0    20480
policy                                 0         0    40000
policy-with-count                       0         0     1024

```

scheduler	0	0	64
zone	0	0	512

show system security-profile all-resource tenant all

```
user@host> show system security-profile all-resource tenant all
```

resource	usage	reserved	maximum
[logical system or tenant name: tn1]			
[security profile name: SP1]			
address-book	0	0	2000
appfw-profile	0	0	2048
appfw-rule	0	0	114688
appfw-rule-set	0	0	57344
auth-entry	0	0	50000
cpu on CP	0.00%	0.00%	80.00%
cpu on SPU	0.00%	0.00%	80.00%
ds-lite-software-initiator	0	0	100000
flow-gate	0	0	524288
flow-session	0	0	119537664
icap-redirect-profile	0	0	64
nat-cone-binding	0	0	2097152
nat-destination-pool	0	0	8192
nat-destination-rule	0	0	30720
nat-interface-port-ol	0	0	256
nat-nopat-address	0	0	4194304
nat-pat-address	0	0	1048576
nat-pat-portnum	0	0	2576980378
nat-port-ol-ipnumber	0	0	128
nat-rule-referenced-prefix	0	0	1048576
nat-source-pool	0	0	12288
nat-source-rule	0	0	30720
nat-static-rule	0	0	30720
policy	0	0	80000
policy-with-count	0	0	1024
scheduler	0	0	64
security-log-stream-number	1	0	3
sla-policy	0	0	1024
zone	0	0	2000

show system security-profile policy

```
user@host> show system security-profile policy
```

logical system name	security profile name	usage	reserved	maximum
ls-product-design	ls-design-profile	0	40	50

show system security-profile cpu

```
user@host> show system security-profile cpu
```

```
CPU control: TRUE
```

```
CPU control target: 80.00%
```

logical system name	profile name	CPU name	usage(%)	reserved(%)
drop rate(%)				
root-logical-system	Default-Profile	CP	0.00%	1.00%
0.00%				
root-logical-system	Default-Profile	SPU	0.00%	1.00%
0.00%				

show system security-profile cpu logical-system all

```

user@host> show system security-profile cpu logical-system all
CPU control: TRUE
CPU control target: 80.00%
logical system name  profile name  CPU name  usage(%)  reserved(%)
drop rate(%)
root-logical-system  Default-Profile CP          0.00%      1.00%
0.00%
root-logical-system  Default-Profile SPU        0.00%      1.00%
0.00%
ls-product-design    ls-design-profile CP          0.00%      0.00%
0.00%
ls-product-design    ls-design-profile SPU        0.00%      0.00%
0.00%
ls-marketing-dept    ls-acct-mrkt-profile CP      0.00%      0.00%
0.00%
ls-marketing-dept    ls-acct-mrkt-profile SPU      0.00%      0.00%
0.00%

logical system name  security profile name  usage  reserved  maximum
root-logical-system  Default-Profile        67108864  0  134217728
lsys1                profile1                193536   6000  134217728

```

show system security-profile cpu summary

```

user@host> show system security-profile cpu summary
CPU control: TRUE
CPU control target: 80.00%

CPU type      :    CP
global used amount : 0.00%
global maximum quota : 80.00%
global available amount : 80.00%
total logical systems :    3
total security profiles :    3
heaviest usage / user : 0.00%      / root-logical-system
lightest usage / user : 0.00%      / root-logical-system

CPU type      :    SPU
global used amount : 0.00%
global maximum quota : 80.00%
global available amount : 80.00%
total logical systems :    3
total security profiles :    3
heaviest usage / user : 0.00%      / root-logical-system
lightest usage / user : 0.00%      / root-logical-system

```

show system security-profile nat-pat-portnum

```

user@host> show system security-profile cpu nat-pat-portnum
CPU control: TRUE
CPU control target: 80.00%
logical system name  security profile name  usage(%)  reserved(%)
maximum
root-logical-system  Default-Profile CP      67108864      0
134217728

```

show system security-profile nat-pat-portnum summary

```
user@host> show system security-profile nat-pat-portnum summary
global used amount      :67302400
global maximum quota    :134217728
global available amount  :66915328
total logical systems    :2
total security profiles  :1
heaviest usage / user    :193536 / lsys1
```

show system security-profile icap-redirect-profile logical-system all

```
user@host> show system security-profile icap-redirect-profile logical-system all
logical-system tenant name  security profile name      usage   reserved
maximum
root-logical-system        Default-Profile              2       0
64
LSYS1                      SP1                          1       30
64
LSYS2                      SP2                          1       30
64
```

show system security-profile scheduler

Syntax	<pre>show system security-profile scheduler detail logical-system <logical-system-name> root-logical-system summary tenant <tenant-name> terse</pre>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>The tenant option is added in Junos OS Release 18.3R1.</p>
Description	<p>Displays the number of schedulers that the user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. The existing show command for the security-profile scheduler is enhanced with tenant support.</p>
Options	<ul style="list-style-type: none"> • detail—Displays the detailed output. • logical-system—Displays the name of the logical system. • root-logical-system—Displays root logical system as default. • summary—Displays the summary output. • tenant—Displays the name of the tenant system. • terse—Displays the terse output.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show security policies on page 723
List of Sample Output	<p>show system security-profile scheduler on page 766</p> <p>show system security-profile scheduler detail on page 766</p> <p>show system security-profile scheduler summary on page 767</p> <p>show system security-profile scheduler terse on page 767</p> <p>show system security-profile scheduler tenant all on page 767</p>
Output Fields	<p>Table 79 on page 765 lists the output fields for the show system security-profile scheduler command. Output fields are listed in the approximate order in which they appear.</p>

Table 79: show security-profile scheduler Output Fields

Field Name	Field Description
logical-system tenant name	Name of the logical system or tenant system name.

Table 79: show security-profile scheduler Output Fields (continued)

Field Name	Field Description
security profile name	Name of the security profile bound to the logical system or tenant system.
usage/used amount	Number of resources that are currently being used.
reserved amount	Number of resources that are guaranteed to be available to the logical system or the tenant system.
maximum quota	Number of resources that the logical system or the tenant system can use. The maximum does not guarantee that the amount specified for the resource in the security profile is available. The maximum is not applicable for CPU resources.
global maximum quota	If a logical system or the tenant system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems or tenant system.
global available amount	Number of resources available across all the logical systems or tenant system.
total logical systems/tenants	Total number of logical systems and tenant systems.
heaviest usage/user	Using the most security log streams with the detailed number.
lightest usage/user	Using the least security log streams with the detailed number.
total security profiles	Total number of the resources configured for the security profile.
global used amount	Number of resources used across all the logical systems or tenant systems.

Sample Output

show system security-profile scheduler

```

root@host> show system security-profile scheduler
logical-system tenant name  security profile name  usage  reserved
maximum
root-logical-system      Default-Profile        0      0
256

```

Sample Output

show system security-profile scheduler detail

```

root@host> show system security-profile scheduler detail
logical-system tenant name : root-logical-system
security profile name      : Default-Profile
used amount                : 0
reserved amount            : 0
maximum quota              : 256

```

Sample Output

show system security-profile scheduler summary

```

root@host> show system security-profile scheduler summary
global used amount      : 0
global maximum quota    : 256
global available amount  : 256
total logical systems/tenants : 2
total security profiles  : 2
heaviest usage / user    : 0      / root-logical-system ...(2 logical system
& tenants)
lightest usage / user    : 0      / root-logical-system ...(2 logical system
& tenants)

```

Sample Output

show system security-profile scheduler terse

```

root@host> show system security-profile scheduler terse
logical-system tenant name  security profile name      usage    reserved
maximum

root-logical-system        Default-Profile            0         0
256

```

Sample Output

show system security-profile scheduler tenant all

```

root@host> show system security-profile scheduler tenant all
logical-system tenant name  security profile name      usage    reserved
maximum

root-logical-system        Default-Profile            0         0
256

```

show system security-profile security-log-stream-number detail logical-system all

Syntax	show system security-profile security-log-stream-number detail logical-system (all logical-system-name)
Release Information	Command introduced in Junos OS Release 18.2R1.
Description	Display information about a resource allocated to the logical system in a security profile with security-log-stream number.
Options	<p>logical-system-name—Name of the logical system.</p> <p>all—Display resource information for all logical systems, including the master logical system.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> security-profile-resources on page 546
Output Fields	Table 80 on page 768 lists the output fields for the show system security-profile security-log-stream-number summary command. Output fields are listed in the approximate order in which they appear.

Table 80: show system security-profile security-log-stream-number summary Output Fields

Field Name	Field Description
logical system name	Displays the logical system name
security profile name	Name of the security profile
used amount	Number of resources that are currently being used by the logical system.
reserved amount	Reserved quota that guarantees that the resource amount specified is always available to the logical system.
maximum quota	Maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize 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.

Sample Output

`show system security-profile security-log-stream-number detail logical-system all`

```
user@host> show system security-profile security-log-stream-number detail logical-system all
logical system name      : root-logical-system
security profile name    : Default-Profile
used amount              : 0
reserved amount         : 0
maximum quota           : 8

logical system name      : lsys0
security profile name    : lsys_profile
used amount              : 0
reserved amount         : 0
maximum quota           : 8

logical system name      : lsys1
security profile name    : lsys_profile
used amount              : 0
reserved amount         : 0
maximum quota           : 8

logical system name      : lsys2
security profile name    : lsys_profile
used amount              : 0
reserved amount         : 0
maximum quota           : 8
```

show system security-profile security-log-stream-number logical-system all

Syntax	show system security-profile security-log-stream-number logical-system (all logical-system-name)
Release Information	Command introduced in Junos OS Release 18.2R1.
Description	Display information about a resource allocated to the logical system in a security profile. This command can be used by the master administrator to display resource information for the master logical system or user logical system.
Options	<p>logical-system—Display resource information for a specified user logical system.</p> <p>all—Display resource information for all logical systems, including the master logical system.</p> <p>logical-system-name—Specify the logical system name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>security-profile-resources</i>
Output Fields	Table 81 on page 770 lists the output fields for the show system security-profile security-log-stream-number logical-system all command. Output fields are listed in the approximate order in which they appear.

Table 81: show system security-profile security-log-stream-number logical-system all Output Fields

Field Name	Field Description
logical system name	Name of the logical system
security profile name	Name of the security profile bound to the logical system
usage	Number of resources that are currently being used by the logical system.
reserved	Number of resources that are guaranteed to be available to the logical system.
maximum	Number of resources that the logical system can use. The maximum does not guarantee that the amount specified for the resource in the security profile is available. The maximum is not applicable for CPU resources.
root-logical-system	Display resource information for the master (root) logical system
Default-Profile	Specify the authentication profile to use if no profile is specified

Sample Output

`show system security-profile security-log-stream-number logical-system all`

```
user@host> show system security-profile security-log-stream-number logical-system all
logical system name  security profile name  usage  reserved  maximum
root-logical-system  Default-Profile        1       0         3
LSYS1                sp1                     0       1         3
LSYS2                sp2                     1       0         3
```

show system security-profile security-log-stream-number summary

Syntax	show system security-profile security-log-stream-number summary (detail terse)
Release Information	Command introduced in Junos OS Release 18.2R1.
Description	Display summary information about the resource for all logical systems.
Options	detail —Display detailed output. terse —Display terse output (default).
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> security-profile-resources
Output Fields	Table 82 on page 772 lists the output fields for the show system security-profile security-log-stream-number summary command. Output fields are listed in the approximate order in which they appear.

Table 82: show system security-profile security-log-stream-number summary Output Fields

Field Name	Field Description
global used amount	Number of resources that are currently being used by the logical system.
global maximum quota	Number of resources that the logical system can use. The maximum does not guarantee that the amount specified for the resource in the security profile is available. The maximum is not applicable for CPU resources.
global available amount	Number of resources that are guaranteed to be available to the logical system.
total logical systems	Total number of logical systems
total security profiles	Total number of resources configured for the security profile
heaviest usage / user	Using the most security log streams with the detailed number
lightest usage / user	Using the least security log streams with the detailed number

Sample Output

show system security-profile security-log-stream-number summary

```

user@host> show system security-profile security-log-stream-number summary
global used amount      : 0
global maximum quota    : 32

```

```
global available amount : 32
total logical systems   : 1
total security profiles : 0
heaviest usage / user   : 0    / root-logical-system
lightest usage / user   : 0    / root-logical-system
```

show security softwires

Syntax	<code>show security softwires <software-name <i>software-name</i>> <logical-system (all <i>logical-system-name</i>)></code>
Release Information	Command introduced in Junos OS Release 10.4. The logical-system option introduced in Junos OS Release 12.1.
Description	Display a summary of information of all the software concentrators and details on concentrators with specified name.
Options	<p>software-name <i>software-name</i>—Display the details of the specified software concentrator.</p> <p>logical-system (all <i>logical-system-name</i>)—Display software information for all logical systems or for a specified logical system. This option is only available to the master administrator.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Understanding Traffic Processing on Security Devices</i>

Sample Output

```

user@host> show security softwires
Software Name      SC Address      Status  Number of SI connected
SC-CSSI-1         3001::1        Connected  2
SC-CSSI-str00     3100::1        Active    0
SC-CSSI-str01     3101::1        Inactive  0
SC-CSSI-str02     3001::1        Connected 2520

user@host> show security softwires software-name SC-CSSI-1
Name of software: SC-CSSI-1
  SC status: Connected
  SC address: 3001::1
  Zone: trust
  VR ID: 0
  SI Address      SI Status      SPU
  3001::2         Active         spu-1
  3001::2         Active         spu-21
  SI number: 2

user@host> show security softwires logical-system ls-product-design
Software Name      SC Address      Status  Number of SI connected
sc_1               3000::1        Connected  1

```

show security zones

Syntax	<pre>show security zones <zone-name> detail logical-system <logical-system-name> root-logical-system tenant <tenant-name> terse type</pre>
Release Information	<p>Command introduced in Junos OS Release 8.5.</p> <p>The Description output field added in Junos OS Release 12.1.</p> <p>The tenant option is introduced in Junos OS Release 18.3R1.</p>
Description	<p>Displays the information about the security zones. You can define a security zone, which allows you to divide the network into different segments and apply different security options to each segment. The existing show commands for displaying the zones configured with multiple tenant support are enhanced.</p>
Options	<ul style="list-style-type: none"> • detail—(Optional) Displays the detail level of output. • terse—(Optional) Displays the specified level of output. • zone-name—(Optional) Displays information about the specified zone. • logical-system—Displays logical system name. • root-logical-system—Displays root logical system as default. • tenant—Displays the name of the tenant system. • type—Displays the information for zones of a specified type.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Security Zones Overview</i> • <i>Supported System Services for Host Inbound Traffic</i> • <i>security-zone</i>
List of Sample Output	<p>show security zones on page 776</p> <p>show security zones abc on page 777</p> <p>show security zones abc detail on page 777</p> <p>show security zones terse on page 777</p> <p>show security zone tenant all on page 777</p>
Output Fields	<p>Table 83 on page 776 lists the output fields for the show security zones command. Output fields are listed in the approximate order in which they appear.</p>

Table 83: show security zones Output Fields

Field Name	Field Description	Level of Output
Functional zone	Name of the functional zone.	none
Security zone	Name of the security zone.	detail none
Description	Description of the security zone.	detail none
Policy configurable	Whether the policy can be configured or not.	detail none
Interfaces bound	Number of interfaces in the zone.	detail none
Interfaces	List of the interfaces in the zone.	detail none
Zone	Name of the zone.	terse
Type	Type of the zone.	terse
Tenant	Name of the tenant system.	detail

Sample Output

show security zones

```

user@host> show security zones
Functional zone: management
  Description: This is the management zone.
  Policy configurable: No
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0
Security zone: Host
  Description: This is the host zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    fxp0.0
Security zone: abc
  Description: This is the abc zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:

```



```

    ge-0/0/1.0
Security zone: def
Description: This is the def zone.
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
    ge-0/0/2.0

```

Sample Output

show security zones abc

```

user@host> show security zones abc
Security zone: abc
Description: This is the abc zone.
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
    ge-0/0/1.0

```

Sample Output

show security zones abc detail

```

user@host> show security zones abc detail
Security zone: abc
Description: This is the abc zone.
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
    ge-0/0/1.0

```

Sample Output

show security zones terse

```

user@host> show security zones terse
Zone                Type
my-internal         Security
my-external         Security
dmz                 Security

```

show security zone tenant all

```

user@host show security zone tenant all

Tenant: TN1

Security zone: Host
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:

Security zone: abc

```

Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:xe-0/0/1.0

Security zone: def
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:xe-0/0/3.0