

Service Set Properties



Published: 2012-02-28

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Service Set Properties
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Supported Platforms	ix
	Using the Examples in This Manual	ix
	Merging a Full Example	x
	Merging a Snippet	x
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiv
Part 1	Configuration	
Chapter 1	Configuration Tasks	3
	Configuring Service Sets to be Applied to Services Interfaces	3
	Configuring Interface Service Sets	3
	Configuring Next-Hop Service Sets	5
	Determining Traffic Direction	6
	Interface Style Service Sets	6
	Next-Hop Style Service Sets	6
	Configuring Service Rules	7
	Configuring IPsec Service Sets	8
	Configuring the Local Gateway Address for IPsec Service Sets	9
	IKE Addresses in VRF Instances	9
	Configuring IKE Access Profiles for IPsec Service Sets	10
	Configuring Certification Authorities for IPsec Service Sets	10
	Configuring or Disabling Antireplay Service	10
	Clearing the Don't-Fragment Bit	11
	Configuring Passive-Mode Tunneling	12
	Configuring the Tunnel MTU Value	12
	Configuring Service Set Limitations	13
	Configuring System Logging for Service Sets	13
	Enabling Services PICs to Accept Multicast Traffic	15
	Tracing Services PIC Operations	15
	Configuring the Adaptive Services Log Filename	16
	Configuring the Number and Size of Adaptive Services Log Files	16
	Configuring Access to the Log File	17
	Configuring a Regular Expression for Lines to Be Logged	17
	Configuring the Trace Operations	17

Chapter 2	Example	19
	Example: Configuring Service Sets	19
Chapter 3	Configuration Statements	21
	allow-multicast	21
	adaptive-services-pics	22
	anti-replay-window-size	23
	bypass-traffic-on-exceeding-flow-limits	24
	bypass-traffic-on-pic-failure	24
	clear-dont-fragment-bit	25
	facility-override	26
	host	26
	ids-rules	27
	ike-access-profile	27
	interface-service	28
	ipsec-vpn-options	28
	ipsec-vpn-rules	29
	local-gateway	29
	log-prefix	30
	logging	30
	max-flows	31
	message-rate-limit	32
	nat-rules	33
	next-hop-service	34
	no-anti-replay	35
	passive-mode-tunneling	35
	pgcp-rules	36
	port (syslog)	36
	ptsp-rules	37
	service-interface	37
	service-set	38
	services (Hierarchy)	39
	services (System Logging)	40
	stateful-firewall-rules	41
	syslog	41
	tcp-mss	42
	traceoptions	43
	trusted-ca	44
	tunnel-mtu	45
Part 2	Administration	
Chapter 4	Service Sets Operational Mode Commands	49
	clear services service-sets statistics packet-drops	50
	clear services service-sets statistics syslog	51
	show services service-sets cpu-usage	52
	show services service-sets memory-usage	54
	show services service-sets statistics packet-drops	56
	show services service-sets statistics syslog	58

show services service-sets statistics tcp-mss	61
show services service-sets summary	62

Part 3

Index

Index	67
-----------------	----

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	xi
	Table 2: Text and Syntax Conventions	xi
Part 1	Configuration	
Chapter 1	Configuration Tasks	3
	Table 3: System Log Message Severity Levels	14
	Table 4: Adaptive Services Tracing Flags	17
Part 2	Administration	
Chapter 4	Service Sets Operational Mode Commands	49
	Table 5: show services service-sets cpu-usage Output Fields	52
	Table 6: show services service-sets memory-usage Output Fields	54
	Table 7: show services service-sets packet-drops Output Fields	56
	Table 8: show services service-sets statistics syslog Output Fields	58
	Table 9: show services service-sets statistics tcp-mss Output Fields	61
	Table 10: show services service-sets summary Output Fields	62

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

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

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

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

Supported Platforms

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

- M Series
- T Series
- MX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the **load** command, see the [Junos OS CLI User Guide](#).

Documentation Conventions

Table 1 on page xi 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.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book 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 System Basics Configuration 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; interface names; 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)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Configuration

- [Configuration Tasks on page 3](#)
- [Example on page 19](#)
- [Configuration Statements on page 21](#)

CHAPTER 1

Configuration Tasks

- [Configuring Service Sets to be Applied to Services Interfaces on page 3](#)
- [Configuring Service Rules on page 7](#)
- [Configuring IPsec Service Sets on page 8](#)
- [Configuring Service Set Limitations on page 13](#)
- [Configuring System Logging for Service Sets on page 13](#)
- [Enabling Services PICs to Accept Multicast Traffic on page 15](#)
- [Tracing Services PIC Operations on page 15](#)

Configuring Service Sets to be Applied to Services Interfaces

You configure a services interface to specify the adaptive services interface on which the service is to be performed. Services interfaces are used with either of the service set types described in the following sections.

- [Configuring Interface Service Sets on page 3](#)
- [Configuring Next-Hop Service Sets on page 5](#)
- [Determining Traffic Direction on page 6](#)

Configuring Interface Service Sets

An interface service set is used as an action modifier across an entire interface. To configure the services interface, include the **interface-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

```
[edit services service-set service-set-name]  
  interface-service {  
    service-interface interface-name;  
  }
```

Only the device name is needed, because the router software manages logical unit numbers automatically. The services interface must be an adaptive services interface for which you have configured **unit 0 family inet** at the **[edit interfaces *interface-name*]** hierarchy level.

When you have defined and grouped the service rules by configuring the service-set definition, you can apply services to one or more interfaces installed on the router. When

you apply the service set to an interface, it automatically ensures that packets are directed to the PIC.

To associate a defined service set with an interface, include a **service-set** statement with the **input** or **output** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service]
input {
  service-set service-set-name <service-filter filter-name>;
  post-service-filter filter-name;
}
output {
  service-set service-set-name <service-filter filter-name>;
}
```

If a packet is entering the interface, the match direction is **input**. If a packet is leaving the interface, the match direction is **output**. The service set retains the input interface information even after services are applied, so that functions such as filter-class forwarding and destination class usage (DCU) that depend on input interface information continue to work.

You configure the same service set on the input and output sides of the interface. You can optionally include filters associated with each service set to refine the target and additionally process the traffic. If you include the **service-set** statement without a **service-filter** definition, the router software assumes the match condition is true and selects the service set for processing automatically.



NOTE: If you configure service sets with filters, they must be configured on the input and output sides of the interface.

You can include more than one service set definition on each side of the interface. If you include multiple service sets, the router software evaluates them in the order in which they appear in the configuration. The system executes the first service set for which it finds a match in the service filter and ignores the subsequent definitions. A maximum of six service sets can be applied to an interface. When you apply multiple service sets to an interface, you must also configure and apply a service filter to the interface.

An additional statement allows you to specify a filter for processing the traffic after the input service set is executed. To configure this type of filter, include the **post-service-filter** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service input]** hierarchy level:

```
post-service-filter filter-name;
```

For an example, see [“Example: Configuring Service Sets” on page 19](#).



NOTE: When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the `bypass-traffic-on-pic-failure` statement at the `[edit services service-set service-set-name service-set-options]` hierarchy level. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured. This issue applies only Dynamic Application Awareness for Junos OS configurations using IDP service sets. This forwarding feature worked only with the Packet Forwarding Engine (PFE) initially. Starting with Junos OS Release 11.3, the packet-forwarding feature is extended to packets generated by the Routing Engine for bypass service sets as well.

Configuring Next-Hop Service Sets

A next-hop service set is a route-based method of applying a particular service. Only packets destined for a specific next hop are serviced by the creation of explicit static routes. This configuration is useful when services need to be applied to an entire virtual private network (VPN) routing and forwarding (VRF) table, or when routing decisions determine that services need to be performed.

When a next-hop service is configured, the AS or Multiservices PIC is considered to be a two-legged module with one leg configured to be the inside interface (inside the network) and the other configured as the outside interface (outside the network).

To configure the domain, include the `service-domain` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
service-domain (inside | outside);
```

The `service-domain` setting must match the configuration for the next-hop service inside and outside interfaces. To configure the inside and outside interfaces, include the `next-hop-service` statement at the `[edit services service-set service-set-name]` hierarchy level. The interfaces you specify must be logical interfaces on the same AS PIC. You cannot configure `unit 0` for this purpose, and the logical interface you choose must not be used by another service set.

```
next-hop-service {
  inside-service-interface interface-name.unit-number;
  outside-service-interface interface-name.unit-number;
}
```

Traffic on which the service is applied is forced to the inside interface using a static route. For example:

```
routing-options {
  static {
    route 10.1.2.3 next-hop sp-1/1/0.1;
  }
}
```

After the service is applied, traffic exits by way of the outside interface. A lookup is then performed in the Packet Forwarding Engine (PFE) to send the packet out of the AS or Multiservices PIC.

The reverse traffic enters the outside interface, is serviced, and sent to the inside interface. The inside interface forwards the traffic out of the AS or Multiservices PIC.

Determining Traffic Direction

When you configure next-hop service sets, the AS PIC functions as a two-part interface, in which one part is the *inside* interface and the other part is the *outside* interface. The following sequence of actions takes place:

1. To associate the two parts with logical interfaces, you configure two logical interfaces with the **service-domain** statement, one with the **inside** value and one with the **outside** value, to mark them as either an inside or outside service interface.
2. The router forwards the traffic to be serviced to the inside interface, using the next-hop lookup table.
3. After the service is applied, the traffic exits from the outside interface. A route lookup is then performed on the packets to be sent out of the router.
4. When the reverse traffic returns on the outside interface, the applied service is undone; for example, IPsec traffic is decrypted or NAT addresses are unmasked. The serviced packets then emerge on the inside interface, the router performs a route lookup, and the traffic exits the router.

A service rule's match direction, whether input, output, or input/output, is applied with respect to the traffic flow through the AS PIC, not through a specific inside or outside interface.

When a packet is sent to an AS PIC, packet direction information is carried along with it. This is true for both interface style and next-hop style service sets.

Interface Style Service Sets

Packet direction is determined by whether a packet is entering or leaving any Packet Forwarding Engine interface (with respect to the forwarding plane) on which the **interface-service** statement is applied. This is similar to the input and output direction for stateless firewall filters.

The match direction can also depend on the network topology. For example, you might route all the external traffic through one interface that is used to protect the other interfaces on the router, and configure various services on this interface specifically. Alternatively, you might use one interface for priority traffic and configure special services on it, but not care about protecting traffic on the other interfaces.

Next-Hop Style Service Sets

Packet direction is determined by the AS PIC interface used to route packets to the AS PIC. If you use the **inside-interface** statement to route traffic, then the packet direction is **input**. If you use the **outside-interface** statement to direct packets to the AS PIC, then the packet direction is **output**.

The interface to which you apply the service sets affects the match direction. For example, apply the following configuration:

```
sp-1/1/0 unit 1 service-domain inside;
sp-1/1/0 unit 2 service-domain outside;
```

If you configure **match-direction input**, you include the following statements:

```
[edit]
services service-set test1 next-hop-service inside-service-interface sp-1/0/0.1;
services service-set test1 next-hop-service outside-service-interface sp-1/0/0.2;
services ipsec-vpn rule test-ipsec-rule match-direction input;
routing-options static route 10.0.0.0/24 next-hop sp-1/1/0.1;
```

If you configure **match-direction output**, you include the following statements:

```
[edit]
services service-set test2 next-hop-service inside-service-interface sp-1/0/0.1;
services service-set test2 next-hop-service outside-service-interface sp-1/0/0.2;
services ipsec-vpn rule test-ipsec-rule match-direction output;
routing-options static route 10.0.0.0/24 next-hop sp-1/1/0.2;
```

The essential difference between the two configurations is the change in the match direction and the static routes' next hop, pointing to either the AS PIC's inside or outside interface.

Configuring Service Rules

You specify the collection of rules and rule sets that constitute the service set. The router performs rule sets in the order in which they appear in the configuration. You can include only one rule set for each service type. You configure the rule names and content for each service type at the **[edit services *name*]** hierarchy level for each type:

- You configure intrusion detection service (IDS) rules at the **[edit services ids]** hierarchy level; for more information, see Configuring IDS Rules.
- You configure IP Security (IPsec) rules at the **[edit services ipsec-vpn]** hierarchy level; for more information, see IPsec Properties.
- You configure Network Address Translation (NAT) rules at the **[edit services nat]** hierarchy level; for more information, see Network Address Translation.
- You configure Packet Gateway Control Protocol (PGCP) rules at the **[edit services pgcp]** hierarchy level; for more information, see Border Gateway Function (BGF).
- You configure packet-triggered subscribers and policy control (PTSP) rules at the **[edit services ptsp]** hierarchy level; for more information, see PTSP for Subscriber Access.
- You configure software rules for DS-Lite or 6rd softwires at the **[edit services software]** hierarchy level; for more information, see Software Services for Juniper Service Framework (JSF).
- You configure stateful firewall rules at the **[edit services stateful-firewall]** hierarchy level; for more information, see Stateful Firewall.

To configure the rules and rule sets that constitute a service set, include the following statements at the `[edit services service-set service-set-name]` hierarchy level:

```
([ ids-rules rule-names ] | ids-rule-sets rule-set-name);  
([ ipsec-vpn-rules rule-names ] | ipsec-vpn-rule-sets rule-set-name);  
([ nat-rules rule-names ] | nat-rule-sets rule-set-name);  
([ pgcp-rules rule-names ] | pgcp-rule-sets rule-set-name);  
([software-rules rule-names] | software-rule-sets rule-set-name);  
([ stateful-firewall-rules rule-names ] | stateful-firewall-rule-sets rule-set-name);
```

For each service type, you can include one or more individual rules, or one rule set.

If you configure a service set with IPsec rules, it must not contain rules for any other services. You can, however, configure another service set containing rules for the other services and apply both service sets to the same interface.



NOTE: You can also include Dynamic Application Awareness for Junos OS functionality within service sets. To do this, you must include an `idp-profile` statement at the `[edit services service-set]` hierarchy level, along with application identification (APPID) rules, and, as appropriate, application-aware access list (AACL) rules and a `policy-decision-statistics-profile`. Only one service sets can be applied to a single interface when Dynamic Application Awareness functionality is used. For more information, see [Intrusion Detection and Prevention, Application Identification, and Application-Aware Access List](#).

Configuring IPsec Service Sets

IPsec service sets require additional specifications that you configure at the `[edit services service-set service-set-name ipsec-vpn-options]` hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]  
anti-replay-window-size bits;  
clear-dont-fragment-bit;  
ike-access-profile profile-name;  
local-gateway address;  
no-anti-replay;  
passive-mode-tunneling;  
trusted-ca [ ca-profile-names ];  
tunnel-mtu bytes;
```

Configuration of these statements is described in the following sections:

- [Configuring the Local Gateway Address for IPsec Service Sets on page 9](#)
- [Configuring IKE Access Profiles for IPsec Service Sets on page 10](#)
- [Configuring Certification Authorities for IPsec Service Sets on page 10](#)
- [Configuring or Disabling Antireplay Service on page 10](#)
- [Clearing the Don't-Fragment Bit on page 11](#)

- [Configuring Passive-Mode Tunneling on page 12](#)
- [Configuring the Tunnel MTU Value on page 12](#)

Configuring the Local Gateway Address for IPsec Service Sets

If you configure an IPsec service set, you must also configure a local IPv4 or IPv6 address by including the **local-gateway** statement:

- If the Internet Key Exchange (IKE) gateway IP address is in **inet.0** (the default situation), you configure the following statement:

```
local-gateway address;
```

- If the IKE gateway IP address is in a VPN routing and forwarding (VRF) instance, you configure the following statement:

```
local-gateway address routing-instance instance-name;
```

You can configure all the link-type tunnels that share the same local gateway address in a single next-hop-style service set. The value you specify for the **inside-service-interface** statement at the **[edit services service-set service-set-name]** hierarchy level should match the **ipsec-inside-interface** value, which you configure at the **[edit services ipsec-vpn rule rule-name term term-name from]** hierarchy level. For more information about IPsec configuration, see [Configuring IPsec Rules](#).

IKE Addresses in VRF Instances

You can configure Internet Key Exchange (IKE) gateway IP addresses that are present in a VPN routing and forwarding (VRF) instance as long as the peer is reachable through the VRF instance.

For next-hop service sets, the key management process (kmd) places the IKE packets in the routing instance that contains the **outside-service-interface** value you specify, as in this example:

```
routing-instances vrf-nxthop {
  instance-type vrf;
  interface sp-1/1/0.2;
  ...
}
services service-set service-set-1 {
  next-hop-service {
    inside-service-interface sp-1/1/0.1;
    outside-service-interface sp-1/1/0.2;
  }
  ...
}
```

For interface service sets, the **service-interface** statement determines the VRF, as in this example:

```
routing-instances vrf-intf {
  instance-type vrf;
  interface sp-1/1/0.3;
  interface ge-1/2/0.1; # interface on which service set is applied
```

```
...
}
services service-set service-set-2 {
  interface-service {
    service-interface sp-1/1/0.3;
  }
  ...
}
```

Configuring IKE Access Profiles for IPsec Service Sets

For dynamic endpoint tunneling only, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level. To do this, include the **ike-access-profile** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
ike-access-profile profile-name;
```

The **ike-access-profile** statement must reference the same name as the **profile** statement you configured for IKE access at the **[edit access]** hierarchy level. You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.



NOTE: If you configure an IKE access profile in a service set, no other service set can share the same local-gateway address.

Also, you must configure a separate service set for each VRF. All interfaces referenced by the **ipsec-inside-interface** statement within a service set must belong to the same VRF.

Configuring Certification Authorities for IPsec Service Sets

You can specify one or more trusted certification authorities by including the **trusted-ca** statement:

```
trusted-ca [ ca-profile-names ];
```

When you configure public key infrastructure (PKI) digital certificates in the IPsec configuration, each service set can have its own set of trusted certification authorities. The names you specify for the **trusted-ca** statement must match profiles configured at the **[edit security pki]** hierarchy level; for more information, see the [Junos OS System Basics Configuration Guide](#). For more information about IPsec digital certificate configuration, see Configuring IPsec Rules.

Configuring or Disabling Antireplay Service

You can include the **anti-replay-window-size** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to specify the size of the antireplay window.

```
anti-replay-window-size bits;
```


This statement is useful for dynamic endpoint tunnels for which you cannot configure the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

For static IPsec tunnels, this statement sets the antireplay window size for all the static tunnels within this service set. If a particular tunnel needs a specific value for antireplay window size, set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level. If antireplay check has to be disabled for a particular tunnel in this service set, set the **no-anti-replay** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.



NOTE: The **anti-replay-window-size** and **no-anti-replay** settings at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level override the settings specified at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

You can also include the **no-anti-replay** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to disable IPsec antireplay service. It occasionally causes interoperability issues for security associations.

```
no-anti-replay;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **no-anti-reply** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

For static IPsec tunnels, this statement disables the antireplay check for all the tunnels within this service set. If antireplay check has to be enabled for a particular tunnel, then set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.



NOTE: Setting the **anti-replay-window-size** and **no-anti-replay** statements at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level overrides the settings specified at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

Clearing the Don't-Fragment Bit

You can include the **clear-dont-fragment-bit** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation.

```
clear-dont-fragment-bit;
```

This statement is useful for dynamic endpoint tunnels, for which you cannot configure the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, setting this statement clears the DF bit on packets entering all the static tunnels within this service set. If you want to clear the DF bit on packets entering a specific tunnel, set the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

Configuring Passive-Mode Tunneling

You can include the **passive-mode-tunneling** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to enable the service set to tunnel malformed packets.

```
[edit services service-set service-set-name ipsec-vpn-options]
passive-mode-tunneling;
```

This functionality bypasses the active IP checks, such as version, TTL, protocol, options, address and other land attack checks, and tunnels the packets as is. If this statement is not configured, packets failing the IP checks are dropped in the PIC. In passive mode, the inner packet is not touched; hence, an ICMP error is not generated, if the packet size exceeds the tunnel MTU value.

The IPsec tunnel is not treated as a next hop and TTL is not decremented. Because an ICMP error is not generated if the packet size exceeds the tunnel MTU value, the packet will be tunnelled even if it crosses the tunnel MTU threshold.



NOTE: This functionality is similar to that provided by the **no-ipsec-tunnel-in-traceroute** statement, described in Disabling IPsec Tunnel Endpoint in Traceroute.

Configuring the Tunnel MTU Value

You can include the **tunnel-mtu** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to set the maximum transmission unit (MTU) value for IPsec tunnels.

```
tunnel-mtu bytes;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement sets the tunnel MTU value for all the tunnels within this service set. If you need a specific value for a particular tunnel, then set the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.



NOTE: The `tunnel-mtu` setting at the `[edit services ipsec-vpn rule rule-name term term-name then]` hierarchy level overrides the value specified at the `[edit services service-set service-set-name ipsec-vpn-options]` hierarchy level.

Configuring Service Set Limitations

You can set the following limitations on service set capacity:

- You can limit the maximum number of flows allowed per service set. To configure the maximum value, include the `max-flows` statement at the `[edit services service-set service-set-name]` hierarchy level:

```
max-flows number;
```

The `max-flows` statement permits you to assign a single flow limit value. For IDS service sets only, you can specify various types of flow limits with a finer degree of control. For more information, see the description of the `session-limit` statement in *Configuring IDS Rule Sets*.

- You can limit the maximum segment size (MSS) allowed by the Transmission Control Protocol (TCP). To configure the maximum value, include the `tcp-mss` statement at the `[edit services service-set service-set-name]` hierarchy level:

```
tcp-mss number;
```

The TCP protocol negotiates an MSS value during session connection establishment between two peers. The MSS value negotiated is primarily based on the MTU of the interfaces to which the communicating peers are directly connected to. However in the network, due to variation in link MTU on the path taken by the TCP packets, some packets which are still well within the MSS value may be fragmented when the concerned packet's size exceeds the link's MTU.

If the router receives a TCP packet with the SYN bit and MSS option set and the MSS option specified in the packet is larger than the MSS value specified by the `tcp-mss` statement, the router replaces the MSS value in the packet with the lower value specified by the `tcp-mss` statement. The range for the `tcp-mss mss-value` parameter is from **536** through **65535**.

To view statistics of SYN packets received and SYN packets whose MSS value, is modified, issue the `show services service-sets statistics tcp-mss` operational mode command. For more information on this topic, see the *Junos OS System Basics Configuration Guide*.

Configuring System Logging for Service Sets

You specify properties that control how system log messages are generated for the service set. These values override the values configured at the `[edit interfaces interface-name services-options]` hierarchy level.

To configure service-set-specific system logging values, include the `syslog` statement at the `[edit services service-set service-set-name]` hierarchy level:

```

syslog {
  host hostname {
    class
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
  }
}

```

Configure the **host** statement with a hostname or an IP address that specifies the system log target server. The hostname **local** directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing instance to which the initial data packet (that triggered session establishment) is delivered. You can specify only one system logging hostname.

Table 3 on page 14 lists the severity levels that you can specify in configuration statements at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Table 3: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
emergency	System panic or other condition that causes the router to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or non-error conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific service set. To debug a configuration or log NAT functionality, set the level to **info**.

For more information about system log messages, see the [Junos OS System Log Messages Reference](#).

To select the class of messages to be logged to the specified system log host, include the **class** statement at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level:

```
class class-name;
```

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level:

```
facility-override facility-name;
```

The supported facilities are: **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level:

```
log-prefix prefix-value;
```

Enabling Services PICs to Accept Multicast Traffic

To allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC, include the **allow-multicast** statement at the **[edit services service-set service-set-name]** hierarchy level. If this statement is not included, multicast traffic is dropped by default. This statement applies only to multicast traffic using a next-hop service set; interface service set configuration is not supported. Only unidirectional flows are created for multicast packets. For a configuration example, see Example: Configuring NAT for Multicast Traffic.

Tracing Services PIC Operations

Tracing operations track all adaptive services operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, no events are traced. If you include the **traceoptions** statement at the **[edit services adaptive-services-pics]** or **[edit services logging]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **serviced** located in the **/var/log** directory.
- When the file **serviced** reaches 128 kilobytes (KB), it is renamed **serviced.0**, then **serviced.1**, and so on, until there are three trace files. Then the oldest trace file (**serviced.2**) is overwritten. (For more information about how log files are created, see the [Junos OS System Log Messages Reference](#).)
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements:

```
file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
```

```
flag {  
    all;  
    command-queued;  
    config;  
    handshake;  
    init;  
    interfaces;  
    mib;  
    removed-client;  
    show;  
}
```

You include these statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level.

These statements are described in the following sections:

- [Configuring the Adaptive Services Log Filename on page 16](#)
- [Configuring the Number and Size of Adaptive Services Log Files on page 16](#)
- [Configuring Access to the Log File on page 17](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 17](#)
- [Configuring the Trace Operations on page 17](#)

Configuring the Adaptive Services Log Filename

By default, the name of the file that records trace output is **serviced**. You can specify a different name by including the **file** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file filename;
```

Configuring the Number and Size of Adaptive Services Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed ***filename.0***, then ***filename.1***, and so on, until there are three trace files. Then the oldest trace file (***filename.2***) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (***filename***) reaches 2 MB, ***filename*** is renamed ***filename.0***, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename.0*** is renamed ***filename.1*** and ***filename*** is renamed ***filename.0***. This process repeats until there are 20 trace files. Then the oldest file (***filename.19***) is overwritten by the newest file (***filename.0***).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit services adaptive-services-pics traceoptions file filename]** or **[edit services logging traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
file <filename> match regular-expression;
```

Configuring the Trace Operations

By default, if the **traceoptions** configuration is present, only important events are logged. You can configure the trace operations to be logged by including the following statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
flag {
  all;
  configuration;
  routing-protocol;
  routing-socket;
  snmp;
}
```

Table 4 on page 17 describes the meaning of the adaptive services tracing flags.

Table 4: Adaptive Services Tracing Flags

Flag	Description	Default Setting
all	Trace all operations.	Off
command-queued	Trace command enqueue events.	Off
config	Log reading of the configuration at the [edit services] hierarchy level.	Off
handshake	Trace handshake events.	Off

Table 4: Adaptive Services Tracing Flags (*continued*)

Flag	Description	Default Setting
init	Trace initialization events.	Off
interfaces	Trace interface events.	Off
mib	Trace GGSN SNMP MIB events.	Off
removed-client	Trace client cleanup events.	Off
show	Trace CLI command servicing.	Off

To display the end of the log, issue the **show log serviced | last** operational mode command:

[edit]

user@host# run show log serviced | last

CHAPTER 2

Example

- [Example: Configuring Service Sets on page 19](#)

Example: Configuring Service Sets

Apply two service sets, **my-input-service-set** and **my-output-service-set**, on an interface-wide basis. All traffic has **my-input-service-set** applied to it. After the service set is applied, additional filtering is done using **my_post_service_input_filter**.

```
[edit interfaces fe-0/1/0]
unit 0 {
  family inet {
    service {
      input {
        service-set my-input-service-set;
        post-service-filter my_post_service_input_filter;
      }
      output {
        service-set my-output-service-set;
      }
    }
  }
}
```


CHAPTER 3

Configuration Statements


allow-multicast

Syntax	allow-multicast;
Hierarchy Level	[edit services service-set <i>service-set-name</i>]
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC.
Usage Guidelines	See “Enabling Services PICs to Accept Multicast Traffic” on page 15.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

adaptive-services-pics

Syntax	<pre>adaptive-services-pics { traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; } }</pre>
Hierarchy Level	[edit services]
Release Information	Statement introduced before Junos OS Release 7.4. The file option was added in Release 8.0.
Description	Define global services properties.
Options	The remaining statement is explained separately.
Usage Guidelines	See “Tracing Services PIC Operations” on page 15 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

anti-replay-window-size

Syntax	<code>anti-replay-window-size <i>bits</i>;</code>
Hierarchy Level	<code>[edit services service-set <i>service-set-name</i> ipsec-vpn-options]</code>
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Specify the size of the IPsec antireplay window. This statement is useful for dynamic endpoint tunnels for which you cannot configure the anti-replay-window-size statement at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level.</p> <p>For static IPsec tunnels, this statement sets the antireplay window size for all the static tunnels within this service set. If a particular tunnel needs a specific value for antireplay window size, set the anti-replay-window-size statement at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level. If antireplay check has to be disabled for a particular tunnel in this service set, set the no-anti-replay statement at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level.</p>
	<div>  <p>NOTE: The anti-replay-window-size and no-anti-replay settings at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level override the settings specified at the <code>[edit services service-set <i>service-set-name</i> ipsec-vpn-options]</code> hierarchy level.</p> </div>
Options	<p>bits—Size of the antireplay window, in bits.</p> <p>Default: 64 bits (AS PICs), 128 bits (Multiservices PICs and DPCs)</p> <p>Range: 64 through 4096 bits</p>
Usage Guidelines	See “Configuring IPsec Service Sets” on page 8 or Configuring IPsec Rules.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

bypass-traffic-on-exceeding-flow-limits

Syntax	bypass-traffic-on-exceeding-flow-limits;
Hierarchy Level	[edit services service-set <i>service-set-name</i> service-set-options]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Enable packets to bypass without creating a new session when the flow in the service set exceeds the limit that is set by the max-flows statement at the [edit services service-set <i>service-set-name</i>] hierarchy level.
Usage Guidelines	See “Configuring Service Sets to be Applied to Services Interfaces” on page 3 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

bypass-traffic-on-pic-failure

Syntax	bypass-traffic-on-pic-failure;
Hierarchy Level	[edit services service-set <i>service-set-name</i> service-set-options]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	<p>When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the bypass-traffic-on-pic-failure statement. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured.</p> <p>This issue applies only to Dynamic Application Awareness for Junos OS configurations with IDP service sets.</p>
Usage Guidelines	See “Configuring Service Sets to be Applied to Services Interfaces” on page 3 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

clear-dont-fragment-bit

Syntax	clear-dont-fragment-bit;
Hierarchy Level	[edit services service-set <i>service-set-name</i> ipsec-vpn-options]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This statement is useful for dynamic endpoint tunnels, for which you cannot configure the clear-dont-fragment-bit statement at the [edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then] hierarchy level.</p> <p>For static IPsec tunnels, setting this statement clears the DF bit on packets entering all the static tunnels within this service set. If you want to clear the DF bit on packets entering a specific tunnel, set the clear-dont-fragment-bit statement at the [edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then] hierarchy level.</p>
Usage Guidelines	See “Configuring IPsec Service Sets” on page 8 or Configuring IPsec Rules.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

facility-override

Syntax	<code>facility-override <i>facility-name</i>;</code>
Hierarchy Level	[edit services service-set service-set-name syslog host hostname]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Override the default facility for system log reporting.
Options	<i>facility-name</i> —Name of the facility that overrides the default assignment. Valid entries are: authorization daemon ftp kernel local0 through local7 user
Usage Guidelines	See “ Configuring System Logging for Service Sets ” on page 13.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

host

Syntax	<code>host <i>hostname</i> { facility-override <i>facility-name</i>; interface-service <i>prefix-value</i>; services severity-level; }</code>
Hierarchy Level	[edit services service-set service-set-name syslog]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the hostname for the system logging utility.
Options	<i>hostname</i> —Name of the system logging utility host machine. The remaining statements are explained separately.
Usage Guidelines	See “ Configuring System Logging for Service Sets ” on page 13.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ids-rules

Syntax	(ids-rules <i>rule-name</i> ids-rule-sets <i>rule-set-name</i>);
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the intrusion detection service (IDS) rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
Options	<p><i>rule-name</i>—Identifier for the collection of terms that constitute this rule.</p> <p><i>rule-set-name</i>—Identifier for the set of rules to be included.</p>
Usage Guidelines	See “ Configuring Service Rules ” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

ike-access-profile

Syntax	ike-access-profile <i>profile-name</i> ;
Hierarchy Level	[edit services service-set service-set-name ipsec-vpn-options]
Release Information	Statement introduced in Junos OS Release 7.4.
Description	Define the access profile for the IPsec traffic on dynamic tunnels.
Options	<i>profile-name</i> —Identifier for access profile, which must match the name configured at the [edit access profile <i>name</i> client * ike] hierarchy level.
Usage Guidelines	See Configuring Dynamic Endpoints for IPsec Tunnels or “ Configuring IPsec Service Sets ” on page 8.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

interface-service

Syntax	interface-service { service-interface <i>name</i> ; }
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the device name for the interface service Physical Interface Card (PIC).
Options	service-interface <i>name</i> —Name of the service device associated with the interface-wide service set.
Usage Guidelines	See “ Configuring Service Sets to be Applied to Services Interfaces ” on page 3.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ipsec-vpn-options

Syntax	ipsec-vpn-options { anti-replay-window-size <i>bits</i> ; clear-dont-fragment-bit; ike-access-profile <i>profile-name</i> ; local-gateway <i>address</i> ; no-anti-replay; passive-mode-tunneling; trusted-ca [<i>ca-profile-names</i>]; tunnel-mtu <i>bytes</i> ; }
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify IP Security (IPsec) service options.
Options	The remaining statements are explained separately.
Usage Guidelines	See “ Configuring Service Rules ” on page 7.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ipsec-vpn-rules

Syntax	(ipsec-vpn-rules <i>rule-name</i> ipsec-vpn-rule-sets <i>rule-set-name</i>);
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the IPsec rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
Options	<p><i>rule-name</i>—Identifier for the collection of terms that constitute this rule.</p> <p><i>rule-set-name</i>—Identifier for the set of rules to be included.</p>
Usage Guidelines	See “ Configuring Service Rules ” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

local-gateway

Syntax	local-gateway <i>address</i> ;
Hierarchy Level	[edit services service-set service-set-name ipsec-vpn-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the local IPv4 or IPv6 address for the IPsec traffic.
Options	<i>address</i> —Local address.
Usage Guidelines	See “ Configuring Service Rules ” on page 7.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

log-prefix

Syntax	<code>log-prefix <i>prefix-value</i>;</code>
Hierarchy Level	[edit services service-set service-set-name syslog host hostname]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Set the system logging prefix value.
Options	<i>prefix-value</i> —System logging prefix value.
Usage Guidelines	See “ Configuring System Logging for Service Sets ” on page 13.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.


logging

Syntax	<pre>logging { traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; } }</pre>
Hierarchy Level	[edit services]
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Define global services properties.
Options	The remaining statement is explained separately.
Usage Guidelines	See “ Tracing Services PIC Operations ” on page 15.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

max-flows

Syntax	<code>max-flows <i>number</i>;</code>
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Maximum number of flows allowed for the service set.
Options	<i>number</i> —Maximum number of flows.
Usage Guidelines	See “Configuring Service Set Limitations” on page 13 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

message-rate-limit

Syntax	<code>message-rate-limit <i>messages-per-second</i></code>
Hierarchy Level	<pre>interfaces <i>interface-name</i> { services-options { cgn-pic; disable-global-timeout-override; ignore-errors <alg> <tcp>; inactivity-non-tcp-timeout <i>seconds</i>; inactivity-tcp-timeout <i>seconds</i>; inactivity-timeout <i>seconds</i>; open-timeout <i>seconds</i>; session-limit { maximum <i>number</i>; rate <i>new-sessions-per-second</i>; } session-timeout <i>seconds</i>; syslog { } } }</pre>
Release Information	Statement introduced Junos OS Release 11.1.
Description	Maximum system log messages per second allowed from this interface.
	<div><p>NOTE: The <code>message-rate-limit</code> command can be configured only for physical service interfaces (<code>sp-x/x/x</code>) and not for redundancy services PIC interfaces (<code>rspx</code>).</p></div>
Options	<i>messages-per-second</i> —This option configures the maximum number of system log messages per second that can be formatted and sent from the PIC to either the Routing Engine (local) or to an external server (remote). The default rates are 10,000 for the Routing Engine and 200,000 for an external server.
Usage Guidelines	See “Configuring System Logging for Service Sets” on page 13 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.


nat-rules

Syntax	(nat-rules <i>rule-name</i> nat-rule-sets <i>rule-set-name</i>);
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the Network Address Translation (NAT) rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
Options	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule. <i>rule-set-name</i> —Identifier for the set of rules to be included.
Usage Guidelines	See “ Configuring Service Rules ” on page 7.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

next-hop-service

Syntax	<pre>next-hop-service { inside-service-interface <i>interface-name.unit-number</i>; outside-service-interface <i>interface-name.unit-number</i>; service-interface-pool <i>name</i>; }</pre>
Hierarchy Level	[edit services service-set <i>service-set-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. service-interface-pool option added in Junos OS Release 9.3.
Description	Specify interface names or a service interface pool for the forwarding next-hop service set. You cannot specify both a service interface pool and an inside or outside interface.
Options	<p>inside-service-interface <i>interface-name.unit-number</i>—Name and logical unit number of the service interface associated with the service set applied inside the network.</p> <p>outside-service-interface <i>interface-name.unit-number</i>—Name and logical unit number of the service interface associated with the service set applied outside the network.</p> <p>service-interface-pool <i>name</i>—Name of the pool of logical interfaces configured at the [edit services service-interface-pools pool <i>pool-name</i>] hierarchy level. You can configure a service interface pool only if the service set has a PGCP rule configured. The service set cannot contain any other type of rule.</p>
Usage Guidelines	See “Configuring Service Sets to be Applied to Services Interfaces” on page 3 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

no-anti-replay

Syntax	no-anti-replay;
Hierarchy Level	[edit services service-set <i>service-set-name</i> ipsec-vpn-options]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Disable IPsec antireplay service for this service set, which occasionally causes interoperability issues for security associations. This statement is useful for dynamic endpoint tunnels for which you cannot configure the no-anti-reply statement at the [edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then] hierarchy level.</p> <p>For static IPsec tunnels, this statement disables the antireplay check for all the tunnels within this service set. If antireplay check has to be enabled for a particular tunnel, then set the anti-replay-window-size statement at the [edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then] hierarchy level.</p>
	<div>  <p>NOTE: Setting the anti-replay-window-size and no-anti-replay statements at the [edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then] hierarchy level overrides the settings specified at the [edit services service-set <i>service-set-name</i> ipsec-vpn-options] hierarchy level.</p> </div>
Usage Guidelines	See “ Configuring IPsec Service Sets ” on page 8 or Configuring or Disabling IPsec Anti-Replay.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

passive-mode-tunneling

Syntax	passive-mode-tunneling;
Hierarchy Level	[edit services service-set <i>service-set-name</i> ipsec-vpn-options]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Allows tunneling of malformed packets. When this statement is enabled, traffic bypasses the usual active IP checks. The IPsec tunnel is not treated as a next hop and TTL is not decremented. If the packet size exceeds the tunnel MTU value, an ICMP error is not generated.</p>
Usage Guidelines	See “ Configuring IPsec Service Sets ” on page 8.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

pgcp-rules

Syntax	<code>(pgcp-rules <i>rule-name</i> pgcp-rules-sets <i>rule-set-name</i>);</code>
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Specify the Packet Gateway Control Protocol (PGCP) rules or rule set included in this service set. You can configure multiple rules but only one rule set for each service.
Options	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule. <i>rule-set-name</i> —Identifier for the set of rules to be included.
Usage Guidelines	See “ Configuring Service Sets to be Applied to Services Interfaces ” on page 3.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

port (syslog)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> services-options syslog host <i>hostname</i>]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	UDP port for system log messages on the host. The default port is 514.
Options	<i>port-number</i> —Port number for system log messages.
Usage Guidelines	See Configuring System Logging for Services Interfaces .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ptsp-rules

Syntax	(ptsp-rules <i>rule-name</i> ptsp-rules-sets <i>rule-set-name</i>);
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the PTSP rules or rule set included in this service set. You can configure multiple rules but only one rule set for each service.
Options	<p><i>rule-name</i>—Identifier for the collection of terms that constitute this rule.</p> <p><i>rule-set-name</i>—Identifier for the set of rules to be included.</p>
Usage Guidelines	See “ Configuring Service Sets to be Applied to Services Interfaces ” on page 3.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

service-interface

Syntax	service-interface <i>interface-name</i> ;
Hierarchy Level	[edit services service-set service-set-name interface-service]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the name for the adaptive services interface associated with an interface-wide service set.
Options	<i>interface-name</i> —Identifier of the service interface.
Usage Guidelines	See “ Configuring Service Sets to be Applied to Services Interfaces ” on page 3.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

service-set

```
Syntax  service-set service-set-name {
        allow-multicast;
        extension-service service-name {
            provider-specific-rules-configuration;
        }
        (ids-rules rule-name | ids-rule-sets rule-set-name);
        interface-service {
            service-interface interface-name;
        }
        ipsec-vpn-options {
            anti-replay-window-size bits;
            clear-dont-fragment-bit;
            ike-access-profile profile-name;
            local-gateway address;
            no-anti-replay;
            passive-mode-tunneling;
            trusted-ca [ ca-profile-names ];
            tunnel-mtu bytes;
        }
        (ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
        max-flows number;
        nat-options {
            stateful-nat64 {
                clear-dont-fragment-bit
            }
        }
        (nat-rules rule-name | nat-rule-sets rule-set-name);
        next-hop-service {
            inside-service-interface interface-name.unit-number;
            outside-service-interface interface-name.unit-number;
            service-interface-pool name;
        }
        (pgcp-rules rule-name | pgcp-rule-sets rule-set-name);
        (ptsp-rules rule-name | ptsp-rule-sets rule-set-name);
        (software-rules rule-name | software-rule-sets rule-set-name);
        (stateful-firewall-rules rule-name | stateful-firewall-rule-sets rule-set-name);
        syslog {
            host hostname {
                class class-name;
                facility-override facility-name;
                log-prefix prefix-value;
                port port-number;
                services severity-level;
            }
        }
    }
```

Hierarchy Level [edit services]

Release Information Statement introduced before Junos OS Release 7.4. The **pgcp-rules** and **pgcp-rule-sets** options were added in Release 8.4. The **ptsp-rules** and **ptsp-rule-sets** options were added

in Release 10.2. The **software-rules** and **software-rule-sets** options were added in Release 10.4.

Description Define the service set.

Options *service-set-name*—Identifies the service set.

The remaining statements are explained separately.

Usage Guidelines See Service Set Properties.

Required Privilege interface—To view this statement in the configuration.

Level interface-control—To add this statement to the configuration.

services (Hierarchy)

Syntax services { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the service rules to be applied to traffic.

Usage Guidelines See Service Set Properties.

Required Privilege interface—To view this statement in the configuration.

Level interface-control—To add this statement to the configuration.

services (System Logging)

Syntax	<code>services severity-level;</code>
Hierarchy Level	[edit services service-set service-set-name syslog host hostname]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the severity level for system logging messages.
Options	<p>severity-level—Assigns a severity level to the facility. Valid entries are:</p> <ul style="list-style-type: none">• alert—Conditions that should be corrected immediately.• any—Matches any level.• critical—Critical conditions.• emergency—Panic conditions.• error—Error conditions.• info—Informational messages.• notice—Conditions that require special handling.• warning—Warning messages.
Usage Guidelines	See “Configuring System Logging for Service Sets” on page 13.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

stateful-firewall-rules

Syntax	(stateful-firewall-rules <i>rule-names</i> stateful-firewall-rule-sets <i>rule-set-name</i>);
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the stateful firewall rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
Options	<p><i>rule-name</i>—Identifier for the collection of terms that make up this rule.</p> <p><i>rule-set-name</i>—Identifier for the set of rules to be included.</p>
Usage Guidelines	See “ Configuring Service Rules ” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

syslog

Syntax	<pre> syslog { host <i>hostname</i> { services <i>severity-level</i>; facility-override <i>facility-name</i>; interface-service <i>prefix-value</i>; } } </pre>
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure generation of system log messages for the service set. The system log information is passed to the kernel for logging in the <code>/var/log</code> directory. These settings override the values defined at the [edit interfaces interface-name services-options] hierarchy level; for more information on configuring those values, see Configuring System Logging for Services Interfaces .
Options	The remaining statements are described separately.
Usage Guidelines	See “ Configuring System Logging for Service Sets ” on page 13.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

tcp-mss

Syntax	<code>tcp-mss <i>number</i>;</code>
Hierarchy Level	[edit services service-set service-set-name]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Specify the TCP Maximum Segment Size (MSS) allowed for the service set.
Options	<i>number</i> —MSS value.
Usage Guidelines	See “ Configuring Service Set Limitations ” on page 13.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; } </pre>
Hierarchy Level	[edit services adaptive-services-pics], [edit services logging]
Release Information	Statement introduced before Junos OS Release 7.4. file option added in Release 8.0.
Description	Configure Adaptive Services or Multiservices PIC tracing operations. The messages are output to /var/log/serviced .
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform:</p> <ul style="list-style-type: none"> • all—Trace everything. • command-queued—Trace command enqueue events. • config—Trace configuration events. • handshake—Trace handshake events. • init—Trace initialization events. • interfaces—Trace interface events. • mib—Trace GGSN SNMP MIB events. • removed-client—Trace client cleanup events. • show—Trace CLI command servicing. <p>match <i>regex</i>—(Optional) Match output to a defined regular expression (regex).</p>

Default: If you do not include this option, the trace operation output includes all lines relevant to the logged events.

no-world-readable—(Optional) Prevent any user from reading the log file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Allow any user to read the log file.

Usage Guidelines See [“Tracing Services PIC Operations” on page 15](#).

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

trusted-ca

Syntax `trusted-ca ca-profile-name;`

Hierarchy Level [edit [services service-set service-set-name ipsec-vpn-options](#)]

Release Information Statement introduced in Junos OS Release 7.5.


Description Identify one or more trusted IPsec certification authorities.

Options **ca-profile-name**—Name of certification authority profile, which is configured at the [edit [security pki](#)] hierarchy level.

Usage Guidelines See [“Configuring IPsec Service Sets” on page 8](#).

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

tunnel-mtu

Syntax	<code>tunnel-mtu bytes;</code>
Hierarchy Level	<code>[edit services service-set <i>service-set-name</i> ipsec-vpn-options]</code>
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Maximum transmission unit (MTU) size for IPsec tunnels. This statement is useful for dynamic endpoint tunnels for which you cannot configure the tunnel-mtu statement at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level.</p> <p>For static IPsec tunnels, this statement sets the tunnel MTU value for all the tunnels within this service set. If you need a specific value for a particular tunnel, then set the tunnel-mtu statement at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level.</p>
	<div>  <p>NOTE: The tunnel-mtu setting at the <code>[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]</code> hierarchy level overrides the value specified at the <code>[edit services service-set <i>service-set-name</i> ipsec-vpn-options]</code> hierarchy level.</p> </div>
Options	<p><i>bytes</i>—MTU size.</p> <p>Default: 1500 bytes</p> <p>Range: 256 through 9192 bytes</p>
Usage Guidelines	See “ Configuring IPsec Service Sets ” on page 8 or Specifying the MTU for IPsec Tunnels.
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"> mtu

PART 2

Administration

- [Service Sets Operational Mode Commands on page 49](#)

CHAPTER 4

Service Sets Operational Mode Commands

clear services service-sets statistics packet-drops

Syntax	clear services service-sets statistics packet-drops <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 7.4.
Description	Clear dropped-packet statistics for one adaptive services interface or for all adaptive services interfaces.
Options	none —Clear dropped-packet statistics for all configured adaptive services interfaces. interface <i>interface-name</i> —(Optional) Clear dropped-packet statistics for the specified adaptive services interface. On M Series and T Series routers, the <i>interface-name</i> can be <i>ms-fpc/pic/port</i> , <i>sp-fpc/pic/port</i> or <i>rspnumber</i> . On J Series routers, the <i>interface-name</i> is <i>sp-pim/0/port</i> .
Required Privilege Level	network
Related Documentation	<ul style="list-style-type: none">• show services service-sets statistics packet-drops on page 56
List of Sample Output	clear services service-sets statistics packet-drops on page 50
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services	user@host> clear services service-sets statistics packet-drops interface sp-5/0/0
service-sets statistics	Flow collector interface: cp-5/0/0
packet-drops	Interface state: Collecting flows
	Statistics cleared successfully

clear services service-sets statistics syslog

Syntax	clear services service-sets statistics syslog <service-set <i>service-set-name</i> > <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 11.1.
Description	Clear system log statistics for one services interface or for all services interfaces, and for one named service set or all service sets on the interface or interfaces.
Options	<p>none—Clear system log for all configured services interfaces and their service sets.</p> <p>interface <i>interface-name</i>—(Optional) Clear system log statistics for the specified services interface. On M Series, MX Series, and T Series routers, the <i>interface-name</i> can be <i>ms-fpc/pic/port</i>, <i>sp-fpc/pic/port</i>, or <i>rspnumber</i>. On J Series routers, the <i>interface-name</i> is <i>sp-pim/O/port</i>.</p> <p>service-set <i>service-set-name</i>—(Optional) Clear system log statistics for the specified services interface.</p>
Required Privilege Level	network
Related Documentation	<ul style="list-style-type: none"> • show services service-sets statistics syslog on page 58
List of Sample Output	clear services service-sets statistics syslog on page 51
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```

clear services user@host> clear services service-sets statistics syslog interface sp-5/0/0
service-sets statistics Flow collector interface: cp-5/0/0
syslog      Interface state: Collecting flows
            Statistics cleared successfully

```

show services service-sets cpu-usage

Syntax	show services service-sets cpu-usage <interface <i>interface-name</i> > <service-set <i>service-set-name</i> >
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display service set CPU usage as a percentage. The command is supported only on Adaptive Services PICs (SP PICs).
Options	<p>none—Display CPU usage for all adaptive services interfaces and service sets.</p> <p>interface <i>interface-name</i>—(Optional) Display CPU usage for a particular interface. On M Series and T Series routers, the <i>interface-name</i> parameter can have the value <i>sp-fpc/pic/port</i> or <i>rspnumber</i>. On J Series routers, <i>interface-name</i> is <i>sp-pim/O/port</i>.</p> <p>service-set <i>service-set-name</i>—(Optional) Display CPU usage for a particular service set. For the Layer 2 Tunneling Protocol (L2TP), you can use a tunnel group to represent a service set.</p>
Required Privilege Level	view
List of Sample Output	show services service-sets cpu-usage on page 52
Output Fields	Table 5 on page 52 lists the output fields for the show services service-sets cpu-usage command. Output fields are listed in the approximate order in which they appear.

Table 5: show services service-sets cpu-usage Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface
Service set (system category)	Name of the CPU usage category: <ul style="list-style-type: none"> • idp_recommended—Name of the service sets (displays all the service sets attached to the service PICs) • Idle • System • Receive • Transmit
CPU utilization %	Percentage of the CPU resources being used

Sample Output

```

show services service-sets cpu-usage user@host> show services service-sets cpu-usage
Interface  Service set (system category)  CPU utilization %
sp-4/1/0   idp_recommended                18.20 %
sp-4/1/0   Idle                          44.69 %

```

sp-4/1/0	System	7.01 %
sp-4/1/0	Receive	15.10 %
sp-4/1/0	Transmit	15.00 %

show services service-sets memory-usage

Syntax show services service-sets memory-usage
 <interface *interface-name*>
 <service-set *service-set-name*>
 <zone>

Release Information Command introduced before Junos OS Release 7.4.

Description Display service set memory usage.

Options none—Display service set memory usage.

interface *interface-name*—(Optional) Display memory usage for a particular interface. On M Series and T Series routers, the *interface-name* can be *sp-fpc/pic/port*, or *rspnumber*. On J Series routers, the *interface-name* is *sp-pim/0/port*.



NOTE: This command is not supported on Multilink Protocol-based services PICs.

The interface option is not supported on Multiservice PICs.

service-set *service-set-name*—(Optional) Display memory usage for a particular service set. For Layer 2 Tunneling Protocol (L2TP), you can use a tunnel group to represent a service set.

zone—(Optional) Display the memory usage zone of the adaptive services interface or an individual service set.

Required Privilege Level view

List of Sample Output [show services service-sets memory-usage on page 55](#)
[show services service-sets memory-usage zone on page 55](#)
[show services service-sets memory-usage interface on page 55](#)

Output Fields [Table 6 on page 54](#) lists the output fields for the **show services service-sets memory-usage** command. Output fields are listed in the approximate order in which they appear.

Table 6: show services service-sets memory-usage Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface
Service set	Name of a service set
Bytes Used	Number of bytes of memory being used

Table 6: show services service-sets memory-usage Output Fields (continued)

Field Name	Field Description
Memory zone	<p>Memory zone in which the adaptive services interface is currently operating:</p> <ul style="list-style-type: none"> • Green—All new flows are allowed. • Yellow—Unused memory is reclaimed. All new flows are allowed. • Orange—New flows are allowed only for service sets that are using less than their equal share of memory. • Red—No new flows are allowed.

Sample Output

```

show services user@host> show services service-sets memory-usage
service-sets Interface Service set Bytes Used
memory-usage ms-4/0/0 N/A 14817036
ms-4/1/0 N/A 14691700

```

```

show services user@host> show services service-sets memory-usage zone
service-sets Interface Memory zone
memory-usage zone

```

```

show services user@host> show services service-sets memory-usage interface ms-4/1/0
service-sets Interface Service Set Bytes Used
memory-usage ms-4/1/0 N/A 14691700
interface

```

show services service-sets statistics packet-drops

Syntax	show services service-sets statistics packet-drops <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 7.4.
Description	Display the number of dropped packets for service sets exceeding CPU limits or memory limits.
Options	<p>none—Display the number of dropped service sets packets for all adaptive services interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Display the number of dropped service sets packets for a particular interface. On M Series and T Series routers, <i>interface-name</i> can be <i>ms-fpc/pic/port</i>, <i>sp-fpc/pic/port</i>, or <i>rspnumber</i>. On J Series routers, <i>interface-name</i> is <i>sp-pim/0/port</i>.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear services flow-collector statistics
List of Sample Output	show services service-sets statistics packet-drops interface on page 56
Output Fields	Table 7 on page 56 lists the output fields for the show services service-sets packet-drops command. Output fields are listed in the approximate order in which they appear.

Table 7: show services service-sets packet-drops Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
CPU limit Drops	Number of packets dropped because the service set exceeded the average CPU limit.
Memory limit Drops	Number of packets dropped because the service set exceeded the memory limit.
Flow limit Drops	Number of packets dropped because the service set exceeded the flow limit.

Sample Output

```

show services user@host> show services service-sets statistics packet-drops interface sp-1/0/0
service-sets statistics
packet-drops interface

```

Interface	Service Set	Cpu limit Drops	Memory limit Drops	Flow limit Drops
sp-1/0/0	sset1	0	0	0

show services service-sets statistics syslog

Syntax	show services service-sets statistics syslog <interface <i>interface-name</i> > <service-set <i>service-set-name</i> > <brief detail>
Release Information	Command introduced in Junos OS Release 11.1.
Description	Display the system log statistics with optional filtering by interface and service set name..
Options	<p>none—Display the system log statistics for all services interfaces and all service sets.</p> <p>brief—(Default) Display abbreviated system log statistics.</p> <p>detail—Display detailed system log statistics.</p> <p>interface <i>interface-name</i>—(Optional) Display the system log statistics for a specific adaptive service interface. On M Series and T Series routers, <i>interface-name</i> can be <i>ms-fpc/pic/port</i>, <i>sp-fpc/pic/port</i>, or <i>rspnumber</i>. On J Series routers, <i>interface-name</i> is <i>sp-pim/0/port</i>.</p> <p>service-set <i>service-set name</i>—(Optional) Display the system log statistics for a specific named service-set.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear services service-sets statistics syslog on page 51
List of Sample Output	show services service-sets statistics syslog brief on page 59 show services service-sets statistics syslog detail on page 59
Output Fields	Table 8 on page 58 lists the output fields for the show services service-sets statistics syslog command. Output fields are listed in the approximate order in which they appear.

Table 8: show services service-sets statistics syslog Output Fields

Field Name	Field Description	Level
Interface	Name of a services interface.	all
Message rate limit	Maximum number of messages per second written to the interface's system log.	all
Service set	Name of a service set.	all
Messages sent	Number of messages sent.	brief
Messages dropped	Number of messages dropped.	brief

Table 8: show services service-sets statistics syslog Output Fields (*continued*)

Field Name	Field Description	Level
<i>class name</i>	<p>Logs created for events for each of the following classes:</p> <ul style="list-style-type: none"> • Session open logs • Session close logs • Packet logs • Stateful firewall logs • ALG logs • NAT logs • IDS logs • All other logs <p>The following information is displayed for system log messages for each class of event that is logged:</p> <ul style="list-style-type: none"> • Messages sent—Number of messages sent for session open events. • Messages dropped—Number of messages dropped for session open events. Counts are given for these drop reasons: <ul style="list-style-type: none"> • low priority—The priority of the message was too low for the message to be sent. • no class set—Specific classes of event messages were configured and this class was not selected. • above rate limit—The maximum number of system log messages per second was exceeded. 	detail

Sample Output

```

show services service-sets statistics syslog brief
user@host> show services service-sets statistics syslog brief
Interface: sp-1/1/0
  Message rate limit: 200000
  Service-set: sset-sfw-sp1
    Messages sent: 20
    Messages dropped: 3488
  Service-set: sset-nat-sp1
    Messages sent: 18
    Messages dropped: 91
Interface: sp-1/2/0
  Message rate limit: 15000
  Service-set: sset-sfw-sp2
    Messages sent: 210
    Messages dropped: 579

```

Sample Output

```

show services service-sets statistics syslog detail
user@host> show services service-sets statistics syslog detail
Interface: sp-1/2/0
  Message rate limit: 10
  Service-set: sset-sfw
    Messages sent: 0
    Messages dropped: 1600
  Session open logs:

```

```
Sent: 0
Dropped: 1277 (low priority: 1277, no class set: 0, above rate limit: 0)
Session close logs:
Sent: 0
Dropped: 0 (low priority: 0, no class set: 0, above rate limit: 0)
Packet logs:
Sent: 0
Dropped: 323 (low priority: 323, no class set: 0, above rate limit: 0)
Stateful firewall logs:
Sent: 0
Dropped: 0 (low priority: 0, no class set: 0, above rate limit: 0)
ALG logs:
Sent: 0
Dropped: 0 (low priority: 0, no class set: 0, above rate limit: 0)
NAT logs:
Sent: 0
Dropped: 0 (low priority: 0, no class set: 0, above rate limit: 0)
IDS logs:
Sent: 0
Dropped: 0 (low priority: 0, no class set: 0, above rate limit: 0)
Other logs:
Sent: 0
Dropped: 0 (low priority: 0, no class set: 0, above rate limit: 0)
```

show services service-sets statistics tcp-mss

Syntax	show services service-sets statistics tcp-mss <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 9.5.
Description	(M Series and T Series routers only) Display TCP maximum segment size (MSS) statistics for service sets.
Options	<p>none—Display service set TCP MSS information for all adaptive services interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Display TCP MSS statistics for a particular interface. The <i>interface-name</i> can be <i>ms-fpc/pic/port</i>, <i>sp-fpc/pic/port</i>, or <i>rsp number</i>.</p>
Required Privilege Level	view
List of Sample Output	show services service-sets statistics tcp-mss on page 61
Output Fields	Table 9 on page 61 lists the output fields for the show services service-sets statistics tcp-mss command. Output fields are listed in the approximate order in which they appear.

Table 9: show services service-sets statistics tcp-mss Output Fields

Field Name	Field Description
Interface	Name of the adaptive services interface.
Service Set	Name of the configured service set.
SYN Received	Number of TCP SYN packets received.
SYN Modified	Number of TCP SYN packets with the MSS value modified to match the MSS value specified in the TCP MSS configuration.

Sample Output

```

show services user@host> show services service-sets statistics tcp-mss
service-sets statistics
tcp-mss      Interface  Service Set      SYN Received  SYN Modified
              sp-1/2/0      asq_ipsec_svc_0      500           220

```

show services service-sets summary

Syntax	show services service-sets summary <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display service set summary information.
Options	<p>none—Display service set summary information for all adaptive services interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Display service set summary information for a particular interface. On M Series and T Series routers, <i>interface-name</i> can be <i>ms-fpc/pic/port</i>, <i>sp-fpc/pic/port</i>, or <i>rspnumber</i>. On J Series routers, <i>interface-name</i> is <i>sp-pim/O/port</i>.</p>
Required Privilege Level	view
List of Sample Output	show services service-sets summary on page 62 show services service-sets summary interface on page 63
Output Fields	Table 10 on page 62 lists the output fields for the show services service-sets summary command. Output fields are listed in the approximate order in which they appear.

Table 10: show services service-sets summary Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface
Service type	Type of adaptive service, such as stateful firewall (SFW), Network Address Translation (NAT), intrusion detection service (IDS), Layer 2 Tunneling Protocol (L2TP), Compressed Real-Time Transport Protocol (CRTP), or IP Security (IPsec)
Service sets configured	Total number of service sets configured on the PIC that use internal service set IDs and do not consume external service sets, including CRTP and L2TP
Bytes used	Bytes used by a particular service or all services
Policy bytes used	Policy bytes used by a particular service or all services
CPU utilization	Percentage of the CPU resources being used

Sample Output

```

show services service-sets summary user@host> show services service-sets summary
Service sets
Interface configured Bytes used Policy bytes used CPU utilization

```

ms-4/0/0	1	14821556 (4.53 %)	855124 (0.40 %)	N/A
ms-4/1/0	1	14691700 (4.49 %)	855068 (0.40 %)	N/A

```

show services user@host> show services service-sets summary interface sp-1/3/0
service-sets summary Interface: sp-1/3/0
interface
  Service type  Service sets  Bytes used  CPU
                configured
  SFW/NAT/IDS   1            54 ( 0.00 %)  N/A
  L2TP          1            58 ( 0.00 %)  N/A
  CRTP          1            58 ( 0.00 %)  N/A
  System        0           920831 ( 0.44 %)  N/A
  Idle          0             0 ( 0.00 %)  N/A
  Total        3           921001 ( 0.44 %)  N/A

```


PART 3

Index

- [Index on page 67](#)

Index

Symbols

#, comments in configuration statements.....	xii
(), in syntax descriptions.....	xii
< >, in syntax descriptions.....	xii
[], in configuration statements.....	xii
{ }, in configuration statements.....	xii
(pipe), in syntax descriptions.....	xii

A

adaptive-services-pics statement.....	22
alert (system logging severity level).....	14
allow-multicast statement.....	21
usage guidelines.....	15
anti-replay-window-size statement.....	23
usage guidelines.....	10
any (system logging severity level).....	14
applying service set to interface.....	3
AS PIC	
multicast traffic.....	15

B

braces, in configuration statements.....	xii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xii
bypass-traffic-on-exceeding-flow-limits	
statement.....	24
bypass-traffic-on-pic-failure statement.....	24
usage guidelines.....	3

C

clear services service-sets statistics packet-drops	
command.....	50
clear services service-sets statistics syslog	
command.....	51
clear-dont-fragment-bit statement	
service-set.....	25
usage guidelines.....	11
comments, in configuration statements.....	xii
conventions	
text and syntax.....	xi

critical (system logging severity level).....	14
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

D

documentation	
comments on.....	xiii

E

emergency (system logging severity level).....	14
error (system logging severity level).....	14
event policy	
all (tracing flag).....	17
configuration (tracing flag).....	17
database (tracing flag).....	17
events (tracing flag).....	17
policy (tracing flag).....	17

F

facility-override statement.....	26
usage guidelines.....	13
filters	
used with services.....	3
flow collector services	
statistics	
dropped-packet, clearing.....	50, 51
flow limiting.....	13
font conventions.....	xi

H

host statement.....	26
usage guidelines.....	13

I

ids-rule-sets statement	
usage guidelines.....	7
ids-rules statement.....	27
usage guidelines.....	7
ike-access-profile statement.....	27
usage guidelines.....	10
info (system logging severity level).....	14
input statement	
interfaces	
usage guidelines.....	3
inside and outside interfaces.....	6
inside-service-interface statement	
usage guidelines.....	6
interface style service sets.....	6

interface-service statement.....	28	passive-mode-tunneling statement.....	35
usage guidelines.....	3	usage guidelines.....	12
ipsec-vpn-options statement.....	28	pgcp-rule-sets statement	
usage guidelines.....	9	usage guidelines.....	7
ipsec-vpn-rule-sets statement		pgcp-rules statement	
usage guidelines.....	7	service-set.....	36
ipsec-vpn-rules statement.....	29	usage guidelines.....	7
usage guidelines.....	7	post-service-filter statement	
		usage guidelines.....	3
L		ptsp-rule-sets statement	
limiting flows per service set.....	13	usage guidelines.....	7
local-gateway statement.....	29	ptsp-rules statement.....	37
usage guidelines.....	9	usage guidelines.....	7
log output			
adaptive services.....	16	S	
log-prefix statement.....	30	service interface configuration.....	3
usage guidelines.....	13	service rules configuration.....	7
logging statement.....	30	service sets	
		example configuration.....	19
M		service-domain statement	
manuals		usage guidelines.....	5
comments on.....	xiii	service-filter statement	
match direction usage in service sets.....	6	interfaces	
max-flows statement.....	31	usage guidelines.....	3
usage guidelines.....	13	service-interface statement.....	37
multicast traffic		usage guidelines.....	3
AS PIC.....	15	service-set statement.....	38
		services sets	
N		CPU usage, displaying.....	52
nat-rule-sets statement		dropped packet statistics	
usage guidelines.....	7	clearing.....	50
nat-rules statement.....	33	displaying.....	56
usage guidelines.....	7	memory usage, displaying.....	54
next-hop style service sets.....	6	summary information, displaying.....	62
next-hop-service statement.....	34	syslog statistics	
usage guidelines.....	5	clearing.....	51
no-anti-replay statement.....	35	displaying.....	58
usage guidelines.....	10	services statement	
notice (system logging severity level).....	14	service sets	
		usage guidelines.....	13
O		show services service-sets cpu-usage	
output statement		command.....	52
usage guidelines.....	3	show services service-sets memory-usage	
outside-service-interface statement		command.....	54
usage guidelines.....	6	show services service-sets statistics packet-drops	
		command.....	56
P		show services service-sets statistics syslog	
parentheses, in syntax descriptions.....	xii	command.....	58

show services service-sets statistics tcp-mss	
command.....	61
show services service-sets summary	
command.....	62
software-rules statement	
usage guidelines.....	7
stateful-firewall-rule-sets statement	
usage guidelines.....	7
stateful-firewall-rules statement.....	41
usage guidelines.....	7
support, technical See technical support	
syntax conventions.....	xi
syslog statement	
service sets.....	41
usage guidelines.....	13

T

tcp-mss	
statistics, displaying.....	61
tcp-mss statement.....	42
technical support	
contacting JTAC.....	xiii
trace-options	
server (tracing flag).....	17
timer-events (tracing flag).....	17
traceoptions statement	
services.....	43
tracing flags	
event policy	
all.....	17
configuration.....	17
database.....	17
events.....	17
policy.....	17
server.....	17
timer-events.....	17
tracing operations	
adaptive services.....	15
trusted-ca statement.....	44
usage guidelines.....	10
tunnel-mtu statement.....	45
usage guidelines.....	12

W

warning (system logging severity level).....	14
--	----

