Service Set Properties

Published: 2014-05-02

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

Service Set Properties

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

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at 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.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the **load** command, see the *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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xii 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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can 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: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Service Set Overview

Understanding Service Sets

Junos OS enables you to create service sets that define a collection of services to be performed by an Adaptive Services interface (AS) or Multiservices line cards (MS-DPC, MS-MIC, and MS-MPC). You can configure the service set either as an interface style service set or as a next-hop style service set.

An interface service set is used as an action modifier across an entire interface. You can use an interface style service set when you want to apply services to packets passing through an interface.

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 service interface 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 service sets, include the following statements at the **[edit services]** hierarchy level:

```
[edit services]
service-set service-set-name {
   (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);
   (ptsp-rules rule-names | ptsp-rule-sets rule-set-name);
   (stateful-firewall-rules rule-names | stateful-firewall-rule-sets rule-set-name);
   allow-multicast;
   extension-service service-name {
      provider-specific rules;
   }
   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;
    }
    max-flows number;
    next-hop-service {
      inside-service-interface interface-name.unit-number;
      outside-service-interface interface-name.unit-number;
      service-interface-pool name;
    }
    syslog {
      host hostname {
        services severity-level;
        facility-override facility-name;
        log-prefix prefix-value;
      }
    }
  }
  adaptive-services-pics {
    traceoptions {
      file filename <files number> <match regex> <size size> <(world-readable |
        no-world-readable)>;
      flag flag;
    }
  }
  logging {
    traceoptions {
      file filename <files number> <match regex> <size size> <(world-readable |
        no-world-readable)>;
      flag flag;
    }
  }
```

Related Documentation

- Configuring Service Sets to be Applied to Services Interfaces on page 7
- Configuring Service Rules on page 11
- Configuring IPsec Service Sets on page 13
- Configuring Service Set Limitations on page 18
- Configuring System Logging for Service Sets on page 19
- Enabling Services PICs to Accept Multicast Traffic on page 21
- Tracing Services PIC Operations on page 21
- Example: Configuring Service Sets on page 25

PART 2

Configuration

CHAPTER 2

Configuration Tasks

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

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;
```

The **post-service-filter** statement is not supported when the service interface is on an MS-MIC or MS-MPC.

For an example, see "Example: Configuring Service Sets" on page 25.

NOTE: With interface-style service sets that are configured with Junos OS extension-provide packages, the traffic fails to get serviced when the ingress interface is part of a VRF instance and the service interface is not part of the same VRF instance.

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 to Junos Application Aware (previously known as Dynamic Application Awareness) 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).

NOTE: You can create IFL indexes greater than 8000 only if the interface service set is not configured.

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.

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Rules on page 11
- Configuring IPsec Service Sets on page 13
- Configuring Service Set Limitations on page 18
- Configuring System Logging for Service Sets on page 19
- Example: Configuring Service Sets on page 25

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 *Junos VPN Site Secure*..
- You configure Network Address Translation (NAT) rules at the **[edit services nat]** hierarchy level; for more information, see *Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide*..
- You configure packet-triggered subscribers and policy control (PTSP) rules at the **[edit services ptsp]** hierarchy level; for more information, see *Packet-Triggered Subscribers and Policy Control Feature Guide*.
- You configure softwire rules for DS-Lite or 6rd softwires at the **[edit services softwire]** hierarchy level; for more information, see *Softwire Services*.
- You configure stateful firewall rules at the **[edit services stateful-firewall]** hierarchy level; for more information, see *Junos Network Secure*.

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);
([softwire-rules rule-names] | softwire-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 Junos Application Aware (previously known as Dynamic Application Awareness) 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 Junos Application Aware functionality is used. For more information, see *Intrusion Detection and Prevention*, *Application Identification*, and *Application-Aware Access List*.

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7

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;
copy-dont-fragment-bit
set-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

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 Administration Library for Routing Devices*. 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.

In packets that are transmitted through dynamic endpoint IPSec tunnels, you can enable the value set in the Don't Fragment (DF) bit of the packet entering the tunnel to be copied only to the outer header of the IPsec packet and to not cause any modification to the DF bit in the inner header of the IPsec packet. If the packet size exceeds the tunnel maximum transmission unit (MTU) value, the packet is fragmented before encapsulation. For IPsec tunnels, the default MTU value is 1500 regardless of the interface MTU setting. To copy the DF bit value to only the outer header and not modify the inner header, use the **copy-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level. You can also configure the DF bit to be set only in the outer IPv4 header of the IPsec packet and not be defined in the inner IPv4 header. To configure the DF bit in only the outer header of the IPsec packet and to leave the inner header unmodified, include the **set-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **copy-dont-fragment-bit** and **set-dont-fragment-bit** statements at the **[edit services**

ipsec-vpn rule *rule-name* term *term-name* then] hierarchy level to clear the DF bit in the IPv4 packets that enter the static tunnel. These functionalities are supported on MX Series routers with MS-MICs and MS-MPCs.

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.

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7
- Configuring Service Set Limitations on page 18
- Configuring System Logging for Service Sets on page 19

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*.

  

  NOTE: When an aggregated multiservices (AMS) interface is configured as the service interface for a service set, the max-flow value configured for the service set is applied to each of the member interfaces in the AMS interface. That is, if you have configured 1000 as the max-flow value for a service set that uses an AMS interface with four active member interfaces, each of the member interfaces can handle 1000 flows each, resulting in an effective max-flow value of 4000.

- 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 Administration Library for Routing Devices*.

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7
- Configuring Service Rules on page 11
- Configuring System Logging for Service Sets on page 19
- *Configuring SNMP Traps for Flow Limits*

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 class-name
    facility-override facility-name;
    log-prefix prefix-value;
    port port-number
    services severity-level;
    source-address source-address
  }
}
```

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. The **source-address** parameter is supported on the ms, rms, and mams interfaces.

Table 3 on page 19 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

Table 3: System Log Message Severity Levels *(continued)*

Severity Level	Description
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-rror 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;
```

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7
- Tracing Services PIC Operations on page 21

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.

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7
- Configuring Service Rules on page 11
- Example: Configuring Service Sets on page 25
- *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.2**, 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

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 23 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
init	Trace initialization events.	Off
interfaces	Trace interface events.	Off
mib	Trace GGSN SNMP MIB events.	Off
removed-client	Trace client cleanup events.	Off

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

Flag	Description	Default Setting
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
```

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7
- Configuring System Logging for Service Sets on page 19

CHAPTER 3

Example

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;
         }
      }
   }
}
```

Related Documentation

- Understanding Service Sets on page 3
- Configuring Service Sets to be Applied to Services Interfaces on page 7

CHAPTER 4

Configuration Statements

allow-multicast

Syntax allow-multicast;

Hierarchy Level [edit services service-set *service-set-name*]

Release Information Statement introduced in Junos OS Release 8.0.

Description Allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC.

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

Related Documentation
- Enabling Services PICs to Accept Multicast Traffic on page 21

adaptive-services-pics

Syntax

```
adaptive-services-pics {
  traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

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.

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

Related Documentation

- Tracing Services PIC Operations on page 21

anti-replay-window-size (Services Service Set)

Syntax anti-replay-window-size *bits*;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 10.0.

Description 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 **[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.

Options ***bits***—Size of the antireplay window, in bits.

Default: 64 bits (AS PICs), 128 bits (Multiservices PICs and DPCs)

Range: 64 through 4096 bits

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

Related Documentation

- Configuring IPsec Service Sets on page 13
- *Configuring IPsec Rules*

bypass-traffic-on-exceeding-flow-limits

Syntax bypass-traffic-on-exceeding-flow-limits;

Hierarchy Level [editservices service-set *service-set-name* 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 *service-set-name*]** hierarchy level.

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

Related Documentation
- Configuring Service Sets to be Applied to Services Interfaces on page 7

bypass-traffic-on-pic-failure

Syntax bypass-traffic-on-pic-failure;

Hierarchy Level [edit services service-set *service-set-name* service-set-options]

Release Information Statement introduced in Junos OS Release 10.1.

Description 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.

This issue applies only to Junos Application Aware (previously known as Dynamic Application Awareness) configurations with IDP service sets.

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

Related Documentation
- Configuring Service Sets to be Applied to Services Interfaces on page 7

class

Syntax

```
class {
  alg-logs;
  ids-logs;
  nat-logs;
  packet-logs;
  pcp-logs;
  session-logs <open | close>;
  stateful-firewall-logs ;
}
```

Hierarchy Level [edit services service-set *service-set-name* syslog host *hostname*]

Release Information Statement introduced in Junos OS Release 13.2.

Description Set the class of applications to be logged to the system log.

Options *class-name*—Enter one of the following values:

- **alg-logs**—Log application-level gateway events.
- **ids-logs**—Log intrusion detection system events.
- **nat-logs**—Log Network Address Translation events.
- **packet-logs**—Log general packet-related events.
- **session-logs**—Log session open and close events.
- **session-logs open**—Log session open events only.
- **session-logs close**—Log session close events.

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

Related Documentation

- See Configuring System Logging for Service Sets on page 19.

clear-dont-fragment-bit (Services Service Set)

Syntax clear-dont-fragment-bit;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 10.0.

Description 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 *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.

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

Related Documentation

- Configuring IPsec Service Sets on page 13
- *Configuring IPsec Rules*

copy-dont-fragment-bit (Services Set)

Syntax copy-dont-fragment-bit;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 14.1.

Description Copy the do not fragment (DF) bit value to only the outer header and not modify the inner header of the IPsec packet in dynamic endpoint tunnels. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **copy-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level to copy the DF bit value to only the outer header of the packet in a static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.

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

Related Documentation

- Configuring IPsec Service Sets on page 13
- *Configuring IPsec Rules*

facility-override

Syntax facility-override *facility-name*;

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 ***facility-name***—Name of the facility that overrides the default assignment. Valid entries are:

- **authorization**
- **daemon**
- **ftp**
- **kernel**
- **local0** through **local7**
- **user**

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

Related Documentation

- Configuring System Logging for Service Sets on page 19

host (service-set)

Syntax

```
host hostname {
  class {
    alg-logs;
    ids-logs;
    nat-logs;
    packet-logs;
    pcp-logs;
    session-logs <open | close>;
    stateful-firewall-logs ;
  }
  facility-override facility-name;
  interface-service prefix-value;
  log-prefixprefix-value
  port port-number
  services severity-level;
  source-addresssource-address
}
```

Hierarchy Level [edit services service-set *service-set-name* syslog]

Release Information Statement introduced before Junos OS Release 7.4.
class option introduced in Junos OS Release 13.2.

Description Specify the hostname for the system logging utility.

Options ***hostname***—Name of the system logging utility host machine.

The remaining statements are explained separately.

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

Related Documentation

- Configuring System Logging for Service Sets on page 19

ids-rules

Syntax (ids-rules *rule-name* | ids-rule-sets *rule-set-name*);

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 ***rule-name***—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

Related Documentation
- Configuring Service Rules on page 11

ike-access-profile

Syntax ike-access-profile *profile-name*;

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 ***profile-name***—Identifier for access profile, which must match the name configured at the **[edit access profile *name* client * ike]** hierarchy level.

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

Related Documentation
- *Configuring Dynamic Endpoints for IPsec Tunnels*
- Configuring IPsec Service Sets on page 13

interface-service

Syntax

```
interface-service {
  service-interface name;
}
```

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** *name*—Name of the service device associated with the interface-wide service set.

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

Related Documentation

- Configuring Service Sets to be Applied to Services Interfaces on page 7

ipsec-vpn-options

Syntax

```
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;
}
```

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.

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

Related Documentation

- Configuring Service Rules on page 11

ipsec-vpn-rules

Syntax (ipsec-vpn-rules *rule-name* | ipsec-vpn-rule-sets *rule-set-name*);

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 ***rule-name***—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

Related Documentation
- Configuring Service Rules on page 11

local-gateway

Syntax local-gateway *address*;

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 ***address***—Local address.

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

Related Documentation
- Configuring Service Rules on page 11

log-prefix (Services)

Syntax log-prefix *prefix-value*;

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 ***prefix-value***—System logging prefix value.

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

Related Documentation
- Configuring System Logging for Service Sets on page 19

logging (Services)

Syntax

```
logging {
  traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

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.

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

Related Documentation
- Tracing Services PIC Operations on page 21

max-drop-flows

Syntax

```
max-drop-flows {
  ingress ingress-flows;
  egress egress-flows;
}
```

Hierarchy Level [edit services service-set *service-set-name*]

Release Information Statement introduced in Junos OS Release 12.3

Description Configure the maximum drop flows allowed per ingress and egress direction. The configuration is per service set. The configured limits indicate the maximum number of drop flows that can be created at a given instance of time in both directions. If max drop flows ingress is 10 and egress is 5 then at a given instance of time maximum of 10 ingress drop flows and 5 egress drop flows can be present. Two counters, one for each direction ingress and egress, are to be added to service set stateful-firewall statistics to track the number of drop flows not created due to the drop flow limits exceeded. These limits applies to all types of drop flows i.e., TCP, UDP, ICMP etc. Ingress drop flows are forward flows for match-direction input rules and reverse flows for match-direction output rules. Similarly egress drop flows are reverse flows for match-direction input and forward flows for match-direction output rules. The limits are applied cumulatively on all the nat rules associated with the service-set.

Options ***ingress-flows***—Maximum number of drop flows on the ingress interface.

egress-flows—Maximum number of drop flows on the egress interface.

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

Related Documentation

- Configuring Service Set Limitations on page 18

max-flows

Syntax max-flows *number*;

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 *number*—Maximum number of flows.

NOTE: When an aggregated multiservices (AMS) interface is configured as the service interface for a service set, the **max-flow** value configured for the service set is applied to each of the member interfaces in the AMS interface. That is, if you have configured 1000 as the **max-flow** value for a service set that uses an AMS interface with four active member interfaces, each of the member interfaces can handle 1000 flows each, resulting in an effective **max-flow** value of 4000.

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

Related Documentation

- Configuring Service Set Limitations on page 18

max-drop-flows

Syntax

```
max-drop-flows {
  ingress ingress-flows;
  egress egress-flows;
}
```

Hierarchy Level [edit services service-set *service-set-name*]

Release Information Statement introduced in Junos OS Release 12.3

Description Configure the maximum drop flows allowed per ingress and egress direction. The configuration is per service set. The configured limits indicate the maximum number of drop flows that can be created at a given instance of time in both directions. If max drop flows ingress is 10 and egress is 5 then at a given instance of time maximum of 10 ingress drop flows and 5 egress drop flows can be present. Two counters, one for each direction ingress and egress, are to be added to service set stateful-firewall statistics to track the number of drop flows not created due to the drop flow limits exceeded. These limits applies to all types of drop flows i.e., TCP, UDP, ICMP etc. Ingress drop flows are forward flows for match-direction input rules and reverse flows for match-direction output rules. Similarly egress drop flows are reverse flows for match-direction input and forward flows for match-direction output rules. The limits are applied cumulatively on all the nat rules associated with the service-set.

Options ***ingress-flows***—Maximum number of drop flows on the ingress interface.

egress-flows—Maximum number of drop flows on the egress interface.

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

Related Documentation

- Configuring Service Set Limitations on page 18

message-rate-limit

Syntax message-rate-limit *messages-per-second*

Hierarchy Level

```
interfaces interface-name {
  services-options {
    cgn-pic;
    disable-global-timeout-override;
    ignore-errors <alg> <tcp>;
    inactivity-non-tcp-timeout seconds;
    inactivity-tcp-timeout seconds;
    inactivity-timeout seconds;
    open-timeout seconds;
    session-limit {
      maximum number;
      rate new-sessions-per-second;
    }
    session-timeout seconds;
    syslog {
    }
  }
}
```

Release Information Statement introduced Junos OS Release 11.1.

Description Maximum system log messages per second allowed from this interface.

NOTE: The message-rate-limit command can be configured only for physical service interfaces (sp-*x/x/x*) and not for redundancy services PIC interfaces (rsp*x*).

Options ***messages-per-second***——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.

Range: 0 through 2147483647

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

Related Documentation

- Configuring System Logging for Service Sets on page 19

nat-options

Syntax

```
nat-options {
  land-attack-check (ip-only | ip-port);
  max-sessions-per-subscriber session-number;
  stateful-nat64 {
    clear-dont-fragment-bit;
  }
}
```

Hierarchy Level [edit services service-set *service-set-name*]

Release Information Statement introduced with Junos OS Release 12.1.
land-attack-check and **max-sessions-per-subscriber** statements added in 13.3.

Description Specify parameters for NAT operation.

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

Related Documentation

- Configuring Service Rules on page 11
- *clear-dont-fragment-bit*
- *land-attack-check*
- *max-sessions-per-subscriber*
- *stateful-nat64*

nat-rules

Syntax (nat-rules *rule-name* | nat-rule-sets *rule-set-name*);

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 ***rule-name***—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

Related Documentation

- Configuring Service Rules on page 11

next-hop-service

Syntax

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

Hierarchy Level [edit services service-set *service-set-name*]

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

inside-service-interface ***interface-name.unit-number***—Name and logical unit number of the service interface associated with the service set applied inside the network.

outside-service-interface ***interface-name.unit-number***—Name and logical unit number of the service interface associated with the service set applied outside the network.

outside-service-interface-type ***interface-type***—Identifies the interface type of the service interface associated with the service set applied outside the network. For inline IP reassembly, set the interface type to local.

service-interface-pool ***name***—Name of the pool of logical interfaces configured at the **[edit services service-interface-pools pool *pool-name*]** 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.

NOTE: **service-interface-pool** is not applicable for IP reassembly configuration on L2TP.

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

Related Documentation

- Configuring Service Sets to be Applied to Services Interfaces on page 7

no-anti-replay (Services Service Set)

Syntax no-anti-replay;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 10.0.

Description 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 *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.

Usage Guidelines See or .

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

Related Documentation

- Configuring IPsec Service Sets on page 13
- *Configuring or Disabling IPsec Anti-Replay*

passive-mode-tunneling

Syntax passive-mode-tunneling;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 10.0.

Description 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.

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

Related Documentation
- Configuring IPsec Service Sets on page 13

pgcp-rules

Syntax (pgcp-rules *rule-name* | pgcp-rules-sets *rule-set-name*);

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 ***rule-name***—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

Related Documentation
- Configuring Service Sets to be Applied to Services Interfaces on page 7

port (syslog)

Syntax port *port-number*;

Hierarchy Level [edit interfaces *interface-name* services-options syslog host *hostname*]

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 ***port-number***—Port number for system log messages.

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

Related Documentation
- *Configuring System Logging for Services Interfaces*

ptsp-rules

Syntax (ptsp-rules *rule-name* | ptsp-rules-sets *rule-set-name*);

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 ***rule-name***—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

Related Documentation
- Configuring Service Sets to be Applied to Services Interfaces on page 7

service-interface

Syntax service-interface *interface-name*;

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 ***interface-name***—Identifier of the service interface.

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

Related Documentation

- Configuring Service Sets to be Applied to Services Interfaces on page 7

service-set (Services)

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;
  }
  ip-reassembly-rules rule-name};
  (ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
  max-flows number;
  max-drop-flows {
    ingress ingress-flows;
    egress egress-flows;
  }
  nat-options {
    land-attack-check (ip-only | ip-port);
    max-sessions-per-subscriber session-number;
    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;
    outside-service-interface-type local;
    service-interface-pool name;
  }
  (pgcp-rules rule-name | pgcp-rule-sets rule-set-name);
  (ptsp-rules rule-name | ptsp-rule-sets rule-set-name);
  service-set-options {
    bypass-traffic-on-exceeding-flow-limits;
    bypass-traffic-on-pic-failure;
    enable-asymmetric-traffic-processing;
    support-uni-directional-traffic;
  }
  snmp-trap-thresholds{
    flows high high-threshold | low low-threshold;
    nat-address-port high-threshold | low low-threshold;
    }
```

```
    }
    softwire-options {
      dslite-ipv6-prefix-length dslite-ipv6-prefix-length;
    }
    (softwire-rules rule-name | softwire-rule-sets rule-set-name);
    (stateful-firewall-rules rule-name | stateful-firewall-rule-sets rule-set-name);
    syslog {
      host hostname {
        class {
          alg-logs;
          ids-logs;
          nat-logs;
          packet-logs;
          pcp-logs;
          session-logs <open | close>;
          stateful-firewall-logs ;
        }
        services severity-level;
        facility-override facility-name;
        interface-service prefix-value;
      }
    }
}
```

Hierarchy Level [edit services]

Release Information Statement introduced before Junos OS Release 7.4.
pgcp-rules and **pgcp-rule-sets** options added in Junos OS Release 8.4.
server-set-options option added in Junos OS Release 10.1.
ptsp-rules and **ptsp-rule-sets** options added in Junos OS Release 10.2.
softwire-rules and **clear-rule-sets** options added in Junos OS Release 10.4.
softwire-options option added in Junos OS Release 14.1.

Description Define the service set.

Options ***service-set-name***—Name of the service set.

The remaining statements are explained separately.

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

Related Documentation

- *Service Set Properties*

service-set-options

Syntax

```
service-set-options {
  bypass-traffic-on-exceeding-flow-limits;
  bypass-traffic-on-pic-failure;
  enable-asymmetric-traffic-processing;
  support-uni-directional-traffic;
  header-integrity-check
}
```

Hierarchy Level [edit services service-set]

Release Information Statement introduced in Junos OS Release 10.1. The **enable-asymmetric-traffic-processing** and the **support-uni-directional-traffic** options were added in Release 11.2.

Description Specify the service set options to apply to a service set.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Service Sets to be Applied to Services Interfaces on page 7
- *Configuring APPID Support for Unidirectional Traffic*

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.

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

Related Documentation

- *Service Set Properties*

services (System Logging)

Syntax services *severity-level*;

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 ***severity-level***—Assigns a severity level to the facility. Valid entries are:

- **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.

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

Related Documentation

- Configuring System Logging for Service Sets on page 19

set-dont-fragment-bit (Services Set)

Syntax set-dont-fragment-bit;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 14.1.

Description Configure the do not fragment (DF) bit in only the outer header of the IPsec packet and leave the inner header unmodified for dynamic endpoint tunnels. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **set-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level to set the DF bit in the outer header of the IPv4 packets that enter the static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.

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

Related Documentation

- Configuring IPsec Service Sets on page 13
- *Configuring IPsec Rules*

source-address

Syntax source-address *source-address*

Hierarchy Level [edit services service-set *service-set-name* syslog host *hostname*]

Release Information Statement introduced in Junos OS Release 13.1.

Description Specify a source address to record in system log messages that are directed to a remote machine specified in the ***hostname*** statement.

NOTE: The supported interfaces are ms, rms, and mams interfaces. If you do not specify the interface parameter, the command loops on all supported interfaces.

Options ***source-address***—A valid IP address, which is recorded as the message source in messages sent to the remote machines specified in the **host *hostname*** statement

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

Related Documentation

- Configuring System Logging for Service Sets on page 19
- host on page 36
- service-set on page 51

stateful-firewall-rules

Syntax (stateful-firewall-rules *rule-names* | stateful-firewall-rule-sets *rule-set-name*);

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 ***rule-name***—Identifier for the collection of terms that make up this rule.

rule-set-name—Identifier for the set of rules to be included.

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

Related Documentation

- Configuring Service Rules on page 11

syslog (Services Service Set)

Syntax

```
syslog {
  host hostname {
    class {
      alg-logs;
      ids-logs;
      nat-logs;
      packet-logs;
      pcp-logs;
      session-logs <open | close>;
      stateful-firewall-logs ;
    }
    services severity-level;
    facility-override facility-name;
    interface-service prefix-value;
  }
}
```

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 **/var/log** 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.

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

Related Documentation

- Configuring System Logging for Service Sets on page 19

tcp-mss

Syntax tcp-mss *number*;

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 ***number***—MSS value.

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

Related Documentation

- Configuring Service Set Limitations on page 18

traceoptions (Services Logging)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression> <size size> <world-readable |
    no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

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

file *filename*—Name of the file to receive the output of the tracing operation. All files are placed in the directory **/var/log**.

files *number*—(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.

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

Range: 2 through 1000 files

Default: 3 files

flag *flag*—Tracing operation to perform:

- **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.

match *regex*—(Optional) Match output to a defined regular expression (regex).

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: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

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

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

Related Documentation
- Tracing Services PIC Operations on page 21

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.

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

Related Documentation
- Configuring IPsec Service Sets on page 13

tunnel-mtu (Services Service Set)

Syntax tunnel-mtu *bytes*;

Hierarchy Level [edit services service-set *service-set-name* ipsec-vpn-options]

Release Information Statement introduced in Junos OS Release 10.0.

Description 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 **[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.

Options ***bytes***—MTU size.

Default: 1500 bytes

Range: 256 through 9192 bytes

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

Related Documentation

- *mtu*
- Configuring IPsec Service Sets on page 13
- *Specifying the MTU for IPsec Tunnels*

PART 3

Administration

CHAPTER 5

Service Sets Operational Mode Commands

- clear services service-sets statistics integrity-drops
- clear services service-sets statistics packet-drops
- clear services service-sets statistics syslog
- show services service-sets cpu-usage
- show services service-sets memory-usage
- show services service-sets statistics packet-drops
- show services service-sets statistics syslog
- show services service-sets statistics tcp-mss
- show services service-sets summary

clear services service-sets statistics integrity-drops

Syntax clear services service-sets statistics integrity-drops
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 13.3

Description Clear integrity-drops statistics for one adaptive services interface, for all adaptive services interfaces, or for one service-set.

Options

none—Clear integrity-drops statistics for all configured adaptive service interfaces/ service-set.

Service-set *service-set-name* —(Optional) Clear integrity-drops statistics for the specified service-set

interface *interface-name*—(Optional) Clear integrity-drops statistics for the specified adaptive services interface.

Required Privilege Level network

Related Documentation

- show services service-sets statistics packet-drops on page 73
-

clear services service-sets statistics packet-drops

Syntax clear services service-sets statistics packet-drops
<interface *interface-name*>

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 *interface-name*—(Optional) Clear dropped-packet statistics for the specified adaptive services interface. On M Series and T Series routers, the ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port*** or **rsp*number***. On J Series routers, the ***interface-name*** is **sp-*pim*/0/*port***.

Required Privilege Level network

Related Documentation
- show services service-sets statistics packet-drops on page 73

List of Sample Output clear services service-sets statistics packet-drops on page 67

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services service-sets statistics packet-drops

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

clear services service-sets statistics syslog

Syntax clear services service-sets statistics syslog
<service-set *service-set-name*>
<interface *interface-name*>

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 **none**—Clear system log for all configured services interfaces and their service sets.

interface ***interface-name***—(Optional) Clear system log statistics for the specified services interface. On M Series, MX Series, and T Series routers, the ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***. On J Series routers, the ***interface-name*** is **sp-*pim*/0/*port***.

service-set ***service-set-name***—(Optional) Clear system log statistics for the specified services interface.

Required Privilege Level network

Related Documentation
- show services service-sets statistics syslog on page 75

List of Sample Output clear services service-sets statistics syslog on page 68

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services service-sets statistics syslog

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


show services service-sets cpu-usage

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

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 **none**—Display CPU usage for all adaptive services interfaces and service sets.

interface *interface-name*—(Optional) Display CPU usage for a particular interface. On M Series and T Series routers, the ***interface-name*** parameter can have the value **sp-*fpc/pic/port*** or **rsp*number***. On J Series routers, ***interface-name*** is **sp-*pim*/0/*port***.

service-set *service-set-name*—(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.

Required Privilege Level view

List of Sample Output show services service-sets cpu-usage on page 69

Output Fields Table 5 on page 69 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: • 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 **rsp*number***. 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 72
show services service-sets memory-usage zone on page 72
show services service-sets memory-usage interface on page 72

Output Fields

Table 6 on page 71 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	Memory zone in which the adaptive services interface is currently operating: • **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 service-sets memory-usage

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

show services service-sets memory-usage zone

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

show services service-sets memory-usage interface

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

show services service-sets statistics packet-drops

Syntax show services service-sets statistics packet-drops
<interface *interface-name*>

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

none—Display the number of dropped service sets packets for all adaptive services interfaces.

interface *interface-name*—(Optional) Display the number of dropped service sets packets for a particular interface. On M Series and T Series routers, *interface-name* can be *ms-fpc/pic/port*, *sp-fpc/pic/port*, or *rspnumber*. On J Series routers, *interface-name* is *sp-pim/0/port*.

Required Privilege Level view

Related Documentation

- *clear services flow-collector statistics*

List of Sample Output show services service-sets statistics packet-drops interface on page 73

Output Fields Table 7 on page 73 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 service-sets statistics packet-drops interface

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

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

show services service-sets statistics syslog

Syntax
show services service-sets statistics syslog
<interface *interface-name*>
<service-set *service-set-name*>
<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
none—Display the system log statistics for all services interfaces and all service sets.

brief—(Default) Display abbreviated system log statistics.

detail—Display detailed system log statistics.

interface *interface-name*—(Optional) Display the system log statistics for a specific adaptive service interface. On M Series and T Series routers, ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***. On J Series routers, ***interface-name*** is **sp-*pim*/0/*port***.

service-set *service-set name*—(Optional) Display the system log statistics for a specific named service-set.

Required Privilege Level
view

Related Documentation
- clear services service-sets statistics syslog on page 68

List of Sample Output
show services service-sets statistics syslog brief on page 76
show services service-sets statistics syslog detail on page 76

Output Fields
Table 8 on page 75 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

class name	Logs created for events for each of the following classes:
	• **Session open logs**
	• **Session close logs**
	• **Packet logs**
	• **Stateful firewall logs**
	• **ALG logs**
	• **NAT logs**
	• **IDS logs**
	• **All other logs**
	The following information is displayed for system log messages for each class of event that is logged:
	• **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:
	  ◦ **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 *interface-name*>

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 **none**—Display service set TCP MSS information for all adaptive services interfaces.

interface ***interface-name***—(Optional) Display TCP MSS statistics for a particular interface. The ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp** ***number***.

Required Privilege Level view

List of Sample Output show services service-sets statistics tcp-mss on page 78

Output Fields Table 9 on page 78 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 service-sets statistics tcp-mss

```
user@host> show services 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 *interface-name*>

Release Information Command introduced before Junos OS Release 7.4.

Description Display service set summary information.

Options **none**—Display service set summary information for all adaptive services interfaces.

interface *interface-name*—(Optional) Display service set summary information for a particular interface. On M Series and T Series routers, ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***. On J Series routers, ***interface-name*** is **sp-*pim*/0/*port***.

Required Privilege Level view

List of Sample Output show services service-sets summary on page 79
show services service-sets summary interface on page 80

Output Fields Table 10 on page 79 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                                                  CPU
Interface    configured            Bytes used    Policy bytes used  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 service-sets summary interface

```
user@host> show services service-sets summary interface sp-1/3/0
Interface: sp-1/3/0
                 Service sets                          CPU
  Service type   configured             Bytes used   utilization
  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 4

Index

Index

Symbols

A

B

C

D

E

F

H

I

L

M

N

O

P

S

T

W