JUNIPER NETWORKS

Intrusion Detection Properties

Published: 2012-11-27

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

Intrusion Detection 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 ix defines notice icons used in this guide.

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration 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)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify 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.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web 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 J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

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

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Configuration

CHAPTER 1

Configuration Tasks

Configuring IDS Rules

IDS rules identify traffic for which you want the router software to count events. Because IDS is based on stateful firewall properties, you must configure at least one stateful firewall rule and include it in the service set with the IDS rules; for more information, see Configuring Stateful Firewall Rules.

To configure an IDS rule, include the **rule *rule-name*** statement at the **[edit services ids]** hierarchy level:

```
[edit services ids]
rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (address | any-unicast) <except>;
            destination-address-range low minimum-value high maximum-value <except>;
            destination-prefix-list list-name <except>;
            source-address (address | any-unicast) <except>;
            source-address-range low minimum-value high maximum-value <except>;
            source-prefix-list list-name <except>;
        }
        then {
            aggregation {
                destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
                source-prefix prefix-value | source-prefix-ipv6 prefix-value;
            }
            (force-entry | ignore-entry);
            logging {
                syslog;
                threshold rate;
            }
            session-limit {
                by-destination {
                    hold-time seconds;
```

```
            maximum number;
            packets number;
            rate number;
          }
          by-pair {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
          }
          by-source {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
          }
        }
        syn-cookie {
          mss value;
          threshold rate;
        }
      }
    }
  }
```

Each IDS rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections describe IDS rule content in more detail:

- Configuring Match Direction for IDS Rules on page 4
- Configuring Match Conditions in IDS Rules on page 5
- Configuring Actions in IDS Rules on page 6

Configuring Match Direction for IDS Rules

Each rule must include a **match-direction** statement that specifies whether the match is applied on the input or output side of the interface. To configure where the match is applied, include the **match-direction (input | input-output | output)** statement at the **[edit services ids rule *rule-name*]** hierarchy level:

```
[edit services ids rule rule-name]
match-direction (input | output | input-output);
```

If you configure **match-direction input-output**, bidirectional rule creation is allowed.

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the AS or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output. For more information on inside and outside interfaces, see Configuring Service Sets to be Applied to Services Interfaces.

On the AS or Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that match the packet direction are considered.

Configuring Match Conditions in IDS Rules

To configure IDS match conditions, include the **from** statement at the **[edit services ids rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ids rule rule-name term term-name]
from {
  application-sets set-name;
  applications [ application-names ];
  destination-address (address | any-unicast) <except>;
  destination-address-range low minimum-value high maximum-value <except>;
  destination-prefix-list list-name <except>;
  source-address (address | any-unicast) <except>;
  source-address-range low minimum-value high maximum-value <except>;
  source-prefix-list list-name <except>;
}
```

If you omit the **from** statement, the software accepts all events and places them in the IDS cache for processing.

The source address and destination address can be either IPv4 or IPv6. You can use the destination address, a range of destination addresses, a source address, or a range of source addresses as a match condition, in the same way that you would configure a firewall filter; for more information, see the Routing Policy Configuration Guide.

Alternatively, you can specify a list of source or destination prefixes by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or **source-prefix-list** statement in the IDS rule. For an example, see Examples: Configuring Stateful Firewall Rules.

You can also include application protocol definitions that you have configured at the **[edit applications]** hierarchy level; for more information, see Configuring Application Protocol Properties.

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services ids rule *rule-name* term *term-name* from]** hierarchy level.
- To apply one or more sets of application protocol definitions that you have defined, include the **application-sets** statement at the **[edit services ids rule *rule-name* term *term-name* from]** hierarchy level.

NOTE: If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions.

If a match occurs on an application, the application protocol is displayed separately in the **show services ids** command output. For more information, see the Junos OS Operational Mode Commands.

Configuring Actions in IDS Rules

To configure IDS actions, include the **then** statement at the **[edit services ids rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ids rule rule-name term term-name]
then {
  aggregation {
    destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
    source-prefix prefix-value | source-prefix-ipv6 prefix-value;
  }
  (force-entry | ignore-entry);
  logging {
    syslog;
    threshold rate;
  }
  session-limit {
    by-destination {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
    by-pair {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
    by-source {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
  }
  syn-cookie {
    mss value;
    threshold rate;
  }
}
```

You can configure the following possible actions:

- **aggregation**—The router aggregates traffic labeled with the specified source or destination prefixes before passing the events to IDS processing. This is helpful if you want to examine all the traffic connected with a particular source or destination host. To collect traffic with some other marker, such as a particular application or port, configure that value in the match conditions.

  To configure aggregation prefixes, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level and specify values for **source-prefix**, **destination-prefix source-prefix-ipv6**, or **destination-prefix-ipv6**:

  ```
  [edit services ids rule rule-name term term-name then]
    aggregation {
    destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
    source-prefix prefix-value | source-prefix-ipv6 prefix-value;
  }
  ```

  The value of **source-prefix** and **destination-prefix** must be an integer between 1 and 32. The value of **source-prefix-ipv6** and **destination-prefix-ipv6** must be an integer between 1 and 128.

- **(force-entry | ignore-entry)**—**force-entry** provides a permanent spot in IDS caches for subsequent events after one event is registered. By default, the IDS software does not record information about "good" packets that do not exhibit suspicious behavior. You can use the **force-entry** statement to record all traffic from a suspect host, even traffic that would not otherwise be counted.

  ignore-entry ensures that all IDS events are ignored. You can use this statement to disregard all traffic from a host you trust, including any temporary anomalies that IDS would otherwise count as events.

  To configure an entry behavior different from the default, include the **force-entry** or **ignore-entry** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

  ```
  [edit services ids rule rule-name term term-name then]
  (force-entry | ignore-entry);
  ```

- **logging**—The event is logged in the system log file.

  To configure logging, include the **logging** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

  ```
  [edit services ids rule rule-name term term-name then]
  logging {
    syslog;
    threshold rate;
  }
  ```

  You can optionally include a threshold rate to trigger the generation of system log messages. The threshold rate is specified in events per second. IDS logs are generated once every 60 seconds for each anomaly that is reported. The logs are generated as long as the events continue.

- **session-limit**—The router limits open sessions when the specified threshold is reached.

  To configure a threshold, include the **session-limit** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ids rule rule-name term term-name then]
session-limit {
  by-destination {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
  by-pair {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
  by-source {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
}
```

You configure the thresholds for flow limitation based on traffic direction:

- To limit the number of outgoing sessions from one internal host or subnet, configure the **by-source** statement.
- To limit the number of sessions between a pair of IP addresses, subnets, or applications, configure the **by-pair** statement.
- To limit the number of incoming sessions to one external public IP address or subnet, configure the **by-destination** statement.

For each direction, you can configure the following threshold values:

- **hold-time** *seconds*—When the **rate** or **packets** measurement reaches the threshold value, stop all new flows for the specified number of seconds. Once **hold-time** is in effect, the traffic is blocked for the specified time even if the rate subsides below the specified limit. By default, **hold-time** has a value of 0; the range is 0 through 60 seconds.
- **maximum** *number*—Maximum number of open sessions per IP address or subnet per application. The range is 1 through 32,767.
- **packets** *number*—Maximum number of packets per second (pps) per IP address or subnet per application. The range is 4 through 2,147,483,647.
- **rate** *number*—Maximum number of sessions per second per IP address or subnet per application. The range is 4 through 32,767.

  If you include more than one source address in the match conditions configured at the **[edit services ids rule** *rule-name* **term** *term-name* **from]** hierarchy level, limits are applied for each source address independently. For example, the following configuration allows 20 connections from each source address (**10.1.1.1** and **10.1.1.2**),

not 20 connections total. The same logic applies to the **applications** and **destination-address** match conditions.

```
[edit services ids rule rule-name term term-name]
  from {
  source-address 10.1.1.1;
  source-address 10.1.1.2;
  }
  then {
  session-limit by-source {
    maximum 20;
  }
}
```

NOTE: IDS limits are applied to packets that are accepted by stateful firewall rules. They are not applied to packets discarded or rejected by stateful firewall rules. For example, if the stateful firewall accepts 75 percent of the incoming traffic and the remaining 25 percent is rejected or discarded, the IDS limit applies only to 75 percent of the traffic.

- **syn-cookie**—The router activates SYN-cookie defensive mechanisms.

  To configure SYN-cookie values, include the **syn-cookie** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

  ```
  [edit services ids rule rule-name term term-name then]
  syn-cookie {
    mss value;
    threshold rate;
  }
  ```

  If you enable SYN-cookie defenses, you must include both a threshold rate to trigger SYN-cookie activity and a Transmission Control Protocol (TCP) maximum segment size (MSS) value for TCP delayed binding. The threshold rate is specified in SYN attacks per second. By default, the TCP MSS value is 1500; the range is from 128 through 8192.

Configuring IDS Rule Sets

The **rule-set** statement defines a collection of IDS rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services ids]** hierarchy level with a **rule** statement for each rule:

```
[edit services ids]
rule-set rule-set-name {
  rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing

continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

CHAPTER 2

Example

Examples: Configuring IDS Rules

The following configuration adds a permanent entry to the IDS anomaly table when it encounters a flow with the destination address 10.410.6.2:

```
[edit services ids]
rule simple_ids {
   term 1 {
      from {
         destination-address 10.410.6.2/32;
      }
      then {
         force-entry;
         logging {
            threshold 1;
            syslog;
         }
      }
   }
   term default {
      then {
         aggregation {
            source-prefix 24;
         }
      }
   }
   match-direction input;
}
```

The IDS configuration works in conjunction with the stateful firewall mechanism and relies heavily on the anomalies reported by the stateful firewall. The following configuration example shows this relationship:

```
[edit services ids]
rule simple_ids {
   term 1 {
      from {
         source-address 10.30.20.2/32;
         destination-address {
```

```
            10.30.10.2/32;
            10.30.1.2/32 except;
          }
          applications appl-ftp;
        }
        then {
          force-entry;
          logging {
            threshold 5;
            syslog;
          }
          syn-cookie {
            threshold 10;
          }
        }
      }
      match-direction input;
    }
```

The following example shows configuration of flow limits:

```
[edit services ids]
rule ids-all {
  match-direction input;
  term t1 {
    from {
      application-sets alg-set;
    }
    then {
      aggregation {
        destination-prefix 30; /* IDS action aggregation */
      }
      logging {
        threshold 10;
      }
      session-limit {
        by-destination {
          hold-time 0;
          maximum 10;
          packets 200;
          rate 100;
        }
        by-pair {
          hold-time 0;
          maximum 10;
          packets 200;
          rate 100;
        }
        by-source {
          hold-time 5;
          maximum 10;
          packets 200;
          rate 100;
        }
      }
    }
```



```
    }
}
```

CHAPTER 3

Configuration Statements

aggregation

Syntax

```
aggregation {
  destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
  source-prefix prefix-value | source-prefix-ipv6 prefix-value;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the type of data to be aggregated.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring IDS Rules" on page 3.

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

application-sets (Services IDS)

Syntax application-sets *set-name*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define one or more target application sets.

Options ***set-name***—Name of the target application set.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

applications (Services IDS)

Syntax applications [*application-names*];

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define one or more applications to which IDS applies.

Options ***application-name***—Name of the target application.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

by-destination

Syntax

```
by-destination {
  hold-time seconds;
  maximum number;
  packets number;
  rate number;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then session-limit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Apply limit to sessions based on numbers generated from the configured destination (IP or subnet) or application.

Options **hold-time** ***seconds***—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the **maximum**, **packets**, or **rate** statements.

maximum ***number***—Maximum number of open sessions per application or IP address.

packets ***number***—Maximum peak packets per second per application or IP address.

rate ***number***—Maximum number of sessions per second per application or IP address.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

by-pair

Syntax

```
by-pair {
  hold-time seconds;
  maximum number;
  packets number;
  rate number;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then session-limit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Apply limit to paired stateful firewall and NAT flows (forward and reverse).

Options

hold-time ***seconds***—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the **maximum**, **packets**, or **rate** statements.

maximum ***number***—Maximum number of open sessions per application or IP address.

packets ***number***—Maximum peak packets per second per application or IP address.

rate ***number***—Maximum number of sessions per second per application or IP address.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

by-source

Syntax

```
by-source {
  hold-time seconds;
  maximum number;
  packets number;
  rate number;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then session-limit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Apply limit to sessions based on numbers generated from the configured source (IP or subnet) or application.

Options

hold-time ***seconds***—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the **maximum**, **packets**, or **rate** statements.

maximum ***number***—Maximum number of open sessions per application or IP address.

packets ***number***—Maximum peak packets per second per application or IP address.

rate ***number***—Maximum number of sessions per second per application or IP address.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

Required Privilege Level

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

destination-address (Services IDS)

Syntax destination-address (*address* | any-unicast) <except>;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.
address option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description Specify the destination address for rule matching.

Options ***address***—Destination IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Exempt the specified address, prefix, or unicast packets from rule matching.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

destination-address-range (Services IDS)

Syntax destination-address-range low *minimum-value* high *maximum-value* <except>;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description Specify the destination address range for rule matching.

Options ***minimum-value***—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exempt the specified address range from rule matching.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

destination-prefix (Services IDS)

Syntax destination-prefix *prefix-value*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then aggregation]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the prefix value for destination IPv4 address aggregation.

Options ***prefix-value***—Integer value.
Range: 1 through 32

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

destination-prefix-ipv6

Syntax destination-prefix-ipv6 *prefix*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then aggregation]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the prefix value for destination IPv6 address aggregation.

Options ***prefix-value***—Integer value.
Range: 1 through 128

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

destination-prefix-list (Services IDS)

Syntax destination-prefix-list *list-name* <except>;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 8.2.

Description Specify the destination prefix list for rule matching. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level.

Options ***list-name***—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

Related Documentation

- Routing Policy Configuration Guide

force-entry

Syntax (force-entry | ignore-entry);

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify handling of entries in the IDS events cache:

- **force-entry**—Ensure that the entry has a permanent place in the IDS cache after one event is registered.
- **ignore-entry**—Ensure that all IDS events are ignored.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

from (Services IDS)

Syntax

```
from {
  application-sets set-name;
  applications [ application-names ];
  destination-address (address | any-unicast) <except>;
  destination-address-range low minimum-value high maximum-value <except>;
  source-address (address | any-unicast) <except>;
  source-address-range low minimum-value high maximum-value <except>;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify input conditions for the IDS term.

Options For information on match conditions, see the description of firewall filter match conditions in the Routing Policy Configuration Guide.

The remaining statements are explained separately.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

ignore-entry

See force-entry

logging (Services IDS)

Syntax

```
logging {
  syslog;
  threshold rate;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set logging values for this IDS term.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

match-direction (Services IDS)

Syntax match-direction (input | output | input-output);

Hierarchy Level [edit services ids rule *rule-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the direction in which the rule match is applied.

Options
input—Apply the rule match on input.

output—Apply the rule match on output.

input-output—Apply the rule match bidirectionally.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

mss

Syntax mss *value*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then syn-cookie]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the maximum segment size (MSS) value used in Transmission Control Protocol (TCP) delayed binding.

Options
value—MSS value.
Default: 1500
Range: 128 through 8192

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

rule (Services IDS)

Syntax

```
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
    }
    then {
      aggregation {
        destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-value | source-prefix-ipv6 prefix-value;
      }
      (force-entry | ignore-entry);
      logging {
        syslog;
        threshold rate;
      }
      session-limit {
        by-destination {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
        by-pair {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
        by-source {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
      }
      syn-cookie {
        mss value;
        threshold rate;
      }
    }
  }
}
```

Hierarchy Level

[edit services ids],
[edit services ids rule-set *rule-set-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the rule the router uses when applying this service.

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

Usage Guidelines See "Configuring IDS Rules" on page 3.

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

rule-set (Services IDS)

Syntax

```
rule-set rule-set-name {
    [ rule rule-names ];
}
```

Hierarchy Level [edit services ids]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the rule set the router uses when applying this service.

Options ***rule-set-name***—Identifier for the collection of rules that constitute this rule set.

Usage Guidelines See "Configuring IDS Rule Sets" on page 9.

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

services (IDS)

Syntax services ids { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the service rules to be applied to traffic.

Options **ids**—Identifies the IDS set of rules statements.

Usage Guidelines See "Configuring IDS Rules" on page 3.

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

session-limit

Syntax

```
session-limit {
  by-destination {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
  by-pair {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
  by-source {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable flow limitation by configuring thresholds on source, destination, or stateful firewall and network address translation (NAT) paired traffic flows.

Options The remaining statements are described separately.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

source-address (Services IDS)

Syntax source-address (*address* | any-unicast) <except>;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.
address option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description Specify the source address for rule matching.

Options ***address***—Source IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Exempt the specified address, prefix, or unicast packets from rule matching.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

source-address-range (Services IDS)

Syntax source-address-range low *minimum-value* high *maximum-value* <except>;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description Specify the source address range for rule matching.

Options ***minimum-value***—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exempt the specified address range from rule matching.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

source-prefix (Services IDS)

Syntax source-prefix *prefix-value*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then aggregation]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the prefix value for source IPv4 address aggregation.

Options ***prefix-value***—Integer value.
Range: 1 through 32

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

source-prefix-ipv6

Syntax source-prefix-ipv6 *prefix-value*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then aggregation]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the prefix value for source IPv6 address aggregation.

Options ***prefix-value***—Integer value.
Range: 1 through 128

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

source-prefix-list (Services IDS)

Syntax source-prefix-list *list-name* <except>;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 8.2.

Description Specify the source prefix list for rule matching. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level.

Options ***list-name***—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Usage Guidelines See "Configuring Match Conditions in IDS Rules" on page 5.

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

Related Documentation
- Routing Policy Configuration Guide

syn-cookie

Syntax
```
syn-cookie {
  mss value;
  threshold rate;
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable SYN-cookie defenses against SYN attacks. By default, SYN-cookie techniques are not applied.

Options The remaining statements are described separately.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

syslog (Services IDS)

Syntax syslog;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then logging]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable system logging. The system log information from the Adaptive Services or Multiservices Physical Interface Card (PIC) is passed to the kernel for logging in the **/var/log** directory.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

term (Services IDS)

Syntax

```
term term-name {
  from {
    application-sets set-name;
    applications [ application-names ];
    destination-address (address | any-unicast) <except>;
    destination-address-range low minimum-value high maximum-value <except>;
    source-address (address | any-unicast) <except>;
    source-address-range low minimum-value high maximum-value <except>;
  }
  then {
    aggregation {
      destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
      source-prefix prefix-value | source-prefix-ipv6 prefix-value;
    }
    (force-entry | ignore-entry);
    logging {
      syslog;
      threshold rate;
    }
    session-limit {
      by-destination {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
      by-pair {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
      by-source {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
    }
    syn-cookie {
      mss value;
      threshold rate;
    }
  }
}
```

Hierarchy Level [edit services ids rule *rule-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IDS term properties.

Options ***term-name***—Identifier for the term.

The remaining statements are explained separately.

Usage Guidelines See "Configuring IDS Rules" on page 3.

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

then (Services IDS)

Syntax

```
then {
  aggregation {
    destination-prefix prefix-number | destination-prefix-ipv6 prefix-value;
    source-prefix prefix-number | source-prefix-ipv6 prefix-value;
  }
  (force-entry | ignore-entry);
  logging {
    syslog;
    threshold rate;
  }
  session-limit {
    by-destination {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
    by-pair {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
    by-source {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
  }
  syn-cookie {
    mss value;
    threshold rate;
  }
}
```

Hierarchy Level [edit services ids rule *rule-name* term *term-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IDS term actions.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring IDS Rules" on page 3.

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

threshold (Services)

Syntax threshold *rate*;

Hierarchy Level [edit services ids rule *rule-name* term *term-name* then logging],
[edit services ids rule *rule-name* term *term-name* then syn-cookie]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the threshold for logging or applying SYN-cookie defenses.

Options ***rate***—Logging threshold number of events per second.

rate—SYN-cookie defense number of SYN attacks per second.

Usage Guidelines See "Configuring Actions in IDS Rules" on page 6.

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

PART 2

Administration

CHAPTER 4

Intrusion Detection Service Operational Mode Commands

clear services ids

Syntax clear services ids
<interface *interface-name*>
<service-set *service-set-name*>

Release Information Command introduced before Junos OS Release 7.4.

Description Clear intrusion detection service (IDS) events.

Options **none**—Clear all IDS events for all adaptive services interfaces for all service sets, and clear and reset IDS.

interface ***interface-name***—(Optional) On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number*.** On the J Series , the ***interface-name*** is **sp-*pim*/0/*port***.

service-set ***service-set-name***—(Optional) Clear all IDS events for a particular service set.

Required Privilege Level view

List of Sample Output clear services ids on page 38

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

Sample Output

clear services ids

```
user@host> clear services ids
```


clear services ids destination-table

Syntax
clear services ids destination-table
<destination-prefix *destination-prefix-name*>
<interface *interface-name*>
<service-set *service-set-name*>

Release Information
Command introduced before Junos OS Release 7.4.

Description
Clear the intrusion detection service (IDS) events for a particular address that might be under attack.

Options
none—Clear the attack destination address table.

destination-prefix *destination-prefix-name*—(Optional) Clear the attack destination table for a particular destination prefix.

interface *interface-name*—(Optional) Clear the attack destination table for a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***. On the J Series routers, the ***interface-name*** is **sp-*pim*/0/*port***.

service-set *service-set-name*—(Optional) Clear the attack destination table for a particular service set.

Required Privilege Level
view

List of Sample Output
clear services ids destination-table on page 39

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

Sample Output

clear services ids destination-table

```
user@host> clear services ids destination-table
```

clear services ids pair-table

Syntax clear services ids pair-table
<destination-prefix *destination-prefix-name*>
<interface *interface-name*>
<service-set *service-set-name*>
<source-prefix *source-prefix-name*>

Release Information Command introduced before Junos OS Release 7.4.

Description Clear the intrusion detection service (IDS) attack source and destination address pair table.

Options **none**—Clear the attack source and destination address pair table.

destination-prefix *destination-prefix-name*—(Optional) Clear the attack source and destination address pair table for a particular destination prefix.

interface *interface-name*—(Optional) Clear the attack destination table for a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***. On the J Series routers, the ***interface-name*** is **sp-*pim*/0/*port***.

service-set *service-set-name*—Optional) Clear the attack source and destination address pair table for a particular service set.

source-prefix *source-prefix-name*—(Optional) Clear the attack source and destination address pair table for a particular source prefix.

Required Privilege Level view

List of Sample Output clear services ids pair-table on page 40

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

Sample Output

clear services ids pair-table

```
user@host> clear services ids pair-table
```


clear services ids source-table

Syntax
clear services ids source-table
<interface *interface-name*>
<service-set *service-set-name*>
<source-prefix *source-prefix-name*>

Release Information
Command introduced before Junos OS Release 7.4.

Description
Clear all intrusion detection service (IDS) events for addresses that are suspected attackers.

Options
none—Clear the attack source address table.

interface *interface-name*—(Optional) On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***. On the J Series routers, the ***interface-name*** is **sp-*pim*/0/*port*.**

service-set *service-set-name*—(Optional) Clear the attack source address table for a particular service set.

source-prefix source-prefix-name—(Optional) Clear the attack source address table for a particular source prefix.

Required Privilege Level
view

List of Sample Output
clear services ids source-table on page 41

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

Sample Output

clear services ids source-table

```
user@host> clear services ids source-table
```

show services ids

Syntax show services ids (destination-table | pair-table | source-table)
<brief | extensive | terse>
<destination-prefix *destination-prefix-name*>
<interface *interface-name*>
<limit *number*>
<order (anomalies | bytes | flows | packets)>
<service-set *service-set-name*>
<source-prefix *source-prefix-name*>
<threshold *number*>

Release Information Command introduced before Junos OS Release 7.4.

Description Display information about intrusion detection service (IDS) events. All events gathered by IDS are reported as anomalies. For example, events such as **create forward or watch flow**, **FTP passive**, and **FTP active** are genuinely allowed by the stateful firewall but are logged as anomalies to track the rates and number for these events.

Options **destination-table**—Display information for an address under possible attack.

pair-table—Display information for a particular suspected attack source and destination address pair.

source-table—Display information for an address that is a suspected attacker.

brief | extensive | terse—(Optional) Display the specified level of output.

destination-prefix ***destination-prefix-name***—(Optional) Display information for a particular destination prefix.

interface ***interface-name***—(Optional) 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*.

limit ***number***—(Optional) Maximum number of entries to display. By default, all tables display the top 32 entries sorted by the number of events for the criteria chosen. To display additional entries, configure the limit option to set up to 256 entries.

order—(Optional) Display events according to one of the following table-ordering criteria. The default is anomalies.

- **anomalies**—Display information for particular anomalies.
- **bytes**—Order output by number of bytes received.
- **flows**—Order output by number of flows.
- **packets**—Order output by number of packets received.

service-set ***service-set-name***—(Optional) Display information about a particular service set.

source-prefix ***source-prefix-name***—(Optional) Display information about a particular source prefix.

threshold ***number***—(Optional) Limit the display to events with this number of anomalies, bytes, flows, or packets, whichever criterion you specify for order. For example, to display all events with more than 100 flows, specify order flows and threshold 100.

Required Privilege Level view

List of Sample Output

show services ids destination-table on page 46
show services ids destination-table extensive on page 46
show services ids destination-table extensive order anomalies on page 46
show services ids pair-table extensive on page 47
show services ids pair-table extensive limit on page 47
show services ids source-table extensive on page 48
show services ids source-table extensive limit on page 48

Output Fields Table 3 on page 43 lists the output fields for the **show services ids** command. Output fields are listed in the approximate order in which they appear.

Table 3: show services ids Output Fields

Field Name	Field Description	Output Level
Interface	Name of an adaptive services interface.	All levels
Service set	Name of a service set. Individual empty service sets are not displayed, but if no service set has any flows, a flow table header is printed for each service set.	All levels
Sorting order	Primary mode to display information: **Anomalies**, **Bytes**, **Flows**, or **Packets**.	All levels
Source address	Name of the source address.	All levels
Dest address	Name of the destination address.	All levels
Time	Total time the information has been in the table.	All levels
Flags	**Flags** can be **Forced**, **F** (terse output only), **SYNcookie**, **S** (terse output only), **Forced+SYNcookie**, and **F+S** (terse output only). The **SYNcookie** flag is visible only in the destination table.	All levels
Application	Configured application, such as **FTP** or **Telnet**.	All levels
Bytes	Total number of bytes sent from the source to the destination address, in thousands (**k**) or millions (**m**).	All levels
Packets	Total number of packets sent from the source to the destination address, in thousands (**k**) or millions (**m**).	All levels
Flows	Total number of flows of packets sent from the source to the destination address, in thousands (**k**) or millions (**m**).	All levels

Table 3: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Anomalies	Total number of packets in the anomaly table, in thousands (**k**) or millions (**m**).	All levels
Anomaly description	One or more of the following types of anomalies. For more information, see the detailed descriptions in the stateful firewall section of the *Junos OS System Log Messages Reference*. • First packet of TCP session not SYN • ICMP echo request dropped, because sequence number duplicated • ICMP echo reply dropped. No matching sequence number • ICMP echo request dropped. Too many echo requests without echo reply • ICMP header length check failed • ICMP packet length greater than 64K • IP fragment assembly timeout • IP fragment length error • IP fragment overlap • IP packet length greater than 64K • IP packet too short • IP packet with broadcast destination address • IP packet with checksum error • IP packet with incorrect length • IP packet with TTL equal to 0	**extensive**

Table 3: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Anomaly description (continued)	• IP packet with version other than 4 • Land attack (IP src address = dest address) • No matching SFW rule; attempting to create discard flow • Number of open sessions exceeds IDS limit; packet dropped • Packet rate exceeds IDS limit; packet dropped • Session creation rate exceeds IDS limit; packet dropped • SFW application message too long • SFW discard packet contains non-configured IP option types • SFW drop packet because of discard flow • SFW dropped TCP watch packet • SFW rules request FTP active mode data packets to be accepted; attempting to create forward flow • SFW rules request FTP passive mode data packets to be accepted; attempting to create forward flow • SFW rules request packet to be accepted; attempting to create forward or watch flow • SFW rules request packet to be discarded; attempting to create discard flow • SFW rules request packet to be rejected; attempting to create reject flow • SFW discard flow requires packet to be dropped • SFW SYN defense • Smurf attack (ping to IP broadcast address) • TCP FIN/RST or SYN/(URG|FIN|RST) flags set • TCP header length check failed • TCP port scan (port not in LISTEN state) • TCP seq number zero and FIN/PSH/RST flags set • TCP seq number zero and no flags set • TCP source or destination port zero • TCP SYN flood attack • UDP header length check failed • UDP port scan (port not in LISTEN state) • UDP source or destination port zero	extensive
Count	Number of times that a particular anomaly occurred, in thousands (k) or millions (M).	extensive
Rate (eps)	Anomaly events per second. The IDS subsystem attempts to maintain a weighted average of rates, which might not reflect the exact incoming rate of attack at low rates. However, at high rates exceeding 160 events per second, the rates generally match.	extensive
Elapsed	Time since the same type of event last occurred.	extensive
Total IDS table entries	Number of entries in the IDS table. This number is not necessarily the sum of all entries displayed.	All levels

Table 3: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Total failed IDS table entry insertions	Number of IDS entries not allowed into the table because the table was full	All levels
Total number of events (closed flows and anomalies detected)	Total number of events since the system was started or since the **show ids services** command was executed.	All levels

Sample Output

show services ids destination-table

```
user@host> show services ids destination-table
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags             Application

any             ->   10.58.255.146   36m12s SYN cookie
  Bytes:   35.0 m, Packets:  822.0 k, Flows:  274.0 k, Anomalies: 2251.0 k


Total IDS table entries: 87
Total failed IDS table entry insertions 0
Total number of events (closed flows and anomalies detected): 2606018
```

show services ids destination-table extensive

```
user@host> show services ids destination-table extensive
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags             Application

any             ->   10.58.255.146   35m52s SYN cookie
  Bytes:   34.0 m, Packets:  798.0 k, Flows:  266.0 k, Anomalies: 2251.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    First packet of TCP session not SYN              160.0 k       0       14s
    TCP source or destination port zero              634.0 k   154.6     3m37s
    UDP source or destination port zero              633.0 k   170.0     3m37s
    ICMP header length check failed                     2875     0.9     3m37s
    IP fragment assembly timeout                     820.0 k    12.8     3m18s
    UDP header length check failed                       385     0.5     3m53s
    TCP header length check failed                       383     0.5     3m53s

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2598063
```

show services ids destination-table extensive order anomalies

```
user@host> show services ids destination-table extensive order anomalies
Interface: sp-0/2/0, Service set: ss1
IDS sorting order: Anomalies
Source address       Dest address      Time Flags             Application
15.1.1.1        ->    15.99.1.1          1m28s               junos-ftp
  Bytes: 1065, Packets: 18, Flows: 1, Anomalies: 10
```

```
   Anomaly description                                Count   Rate(eps)  Elapsed
   creating forward or watch flow                       1        15.6       1m28s
   Number of open sessions exceeds IDS limit            9         0.8         18s

Total IDS table entries:                                        3
Total failed IDS table entry insertions                         0
Total number of events (closed flows and anomalies):            11
```

show services ids pair-table extensive

```
user@host> show services ids pair-table extensive
Interface: sp-3/2/0, Service set: ss_all_limits
IDS sorting order: Packets
Source address       Dest address      Time Flags             Application
15.1.1.4        ->      15.99.1.4     2m20s                  junos-ftp

  Bytes: 5.7k, Packets: 102.0, Flows: 41.0, Anomalies: 462.0
    Anomaly description                              Count     Rate   Elapsed
    creating forward or watch flow                    41.0      8.8     2m17s

    Packet rate exceeds IDS src limit                 21.0      7.1     2m17s

    Session creation rate exceeds IDS src limit      359.0     99.7     2m16s

    TCP SYN flood attack                              41.0      1.9     1m30s



Total IDS table entries:                                        3
Total failed IDS table entry insertions                         0
Total number of events (closed flows and anomalies):            462
```

show services ids pair-table extensive limit 3

```
user@host> show services ids pair-table extensive limit 3
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags             Application
10.58.255.18    ->   10.58.255.146   38m41s SYN cookie
  Bytes:  286.0 m, Packets: 2823.0 k, Flows:  324.0 k, Anomalies:  387.0 k
    Anomalies                                       Count   Rate(eps) Elapsed
    First packet of TCP session not SYN             160.0 k     0.1       25s
    TCP source or destination port zero              69.0 k    14.1     6m26s
    UDP source or destination port zero              68.0 k    12.7     6m26s
    ICMP header length check failed                     318     0.1      7m6s
    IP fragment assembly timeout                     88.0 k     1.3      6m7s
    UDP header length check failed                       39     0.0     6m58s
    TCP header length check failed                       46     0.0     6m45s

10.58.255.23    ->   10.58.255.146   18m48s SYN cookie
  Bytes:  104.0 m, Packets:  421.0 k, Flows:      230, Anomalies:  124.0 k
    Anomalies                                       Count   Rate(eps) Elapsed
    TCP source or destination port zero              37.0 k     9.8     6m26s
    UDP source or destination port zero              37.0 k     8.4     6m26s
    IP fragment assembly timeout                     48.0 k     1.0      6m7s
    ICMP header length check failed                     190     0.2     6m47s
    UDP header length check failed                       29     0.0     6m51s
    TCP header length check failed                       23     0.0     6m59s

10.58.255.25    ->   10.58.255.146   18m48s SYN cookie
  Bytes:  104.0 m, Packets:  420.0 k, Flows:      232, Anomalies:  123.0 k
    Anomalies                                       Count   Rate(eps) Elapsed
    TCP source or destination port zero              37.0 k     9.8      6m26s
    UDP source or destination port zero              37.0 k     8.6      6m26s
    IP fragment assembly timeout                     48.0 k     1.5       6m7s
```

```
    ICMP header length check failed                    173     0.1      6m43s
    UDP header length check failed                      24     0.0      6m43s
    TCP header length check failed                      19     0.0      6m56s

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2659291
```

show services ids source-table extensive

```
user@host> show services ids source-table extensive
Interface: sp-3/2/0, Service set: ss_all_limits
IDS sorting order: Packets
Source address       Dest address      Time Flags             Application
15.1.1.4        ->            any     2m43s                 junos-ftp

  Bytes: 5.7k, Packets: 102.0, Flows: 41.0, Anomalies: 462.0
    Anomaly description                               Count     Rate   Elapsed
    creating forward or watch flow                     41.0      8.8     2m40s

    Packet rate exceeds IDS src limit                  21.0      7.1     2m40s

    Session creation rate exceeds IDS src limit       359.0     99.7     2m39s

    TCP SYN flood attack                               41.0      1.9     1m53s



Total IDS table entries:                                  3
Total failed IDS table entry insertions                   0
Total number of events (closed flows and anomalies):      462
```

show services ids source-table extensive limit

```
user@host> show services ids source-table extensive limit 3
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags             Application

10.58.255.18    ->             any   40m 0s SYN cookie
  Bytes:  250.0 m, Packets: 1978.0 k, Flows:  356.0 k, Anomalies:  387.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    TCP source or destination port zero             37.0 k     9.8     6m26s
    First packet of TCP session not SYN            160.0 k     0.0       40s
    TCP source or destination port zero             69.0 k    62.5     7m45s
    UDP source or destination port zero             68.0 k    56.2     7m45s
    ICMP header length check failed                    319     0.1     7m49s
    IP fragment assembly timeout                    89.0 k     4.4     7m26s
    UDP header length check failed                     39     0.0     8m17s
    TCP header length check failed                     46     0.0      8m4s

10.58.255.30    ->             any   20m 7s SYN cookie
  Bytes:  107.0 m, Packets:  427.0 k, Flows:      264, Anomalies:  125.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    UDP source or destination port zero             38.0 k    65.5     7m45s
    TCP source or destination port zero             37.0 k    38.1     7m45s
    IP fragment assembly timeout                    49.0 k     4.1     7m26s
    TCP header length check failed                     24     0.0     9m23s
    ICMP header length check failed                   165     0.1      8m6s
    UDP header length check failed                     26     0.0     8m13s

10.58.255.17    ->             any   20m10s SYN cookie
```

```
  Bytes:  107.0 m, Packets:  426.0 k, Flows:      262, Anomalies:  125.0 k
    Anomalies                                      Count   Rate(eps) Elapsed
    TCP source or destination port zero             38.0 k    55.      7m45s
    UDP source or destination port zero             38.0 k    55.1     7m45s
    ICMP header length check failed                    147    0.1      7m50s
    IP fragment assembly timeout                    49.0 k    2.8      7m26s
    TCP header length check failed                      22    0.0      9m33s
    UDP header length check failed                      22    0.0       8m1s
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2691423
Interface: sp-1/3/0, Service set: blue
NAT pool                  Address                   Port         Ports in use
d2-pool             10.59.16.100-10.59.16.100     4000-4002          1
```

PART 3

Index

Index

Symbols

A

B

C

D

F

I