JUNIPER NETWORKS

Stateful Firewalls in SDK Applications

Published: 2014-04-30

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

Stateful Firewalls in SDK Applications

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
- J 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x 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

Stateful Firewall

Loading the Stateful Firewall Plug-In

As of Junos OS Release 9.5, a stateful firewall plug-in is provided as part of the jbundle package. To load this plug-in on the PIC, include the **package jservices-sfw** statement at the **[edit chassis fpc *slot-number* pic *slot-number* adaptive-services service-package extension-provider]** hierarchy level. For example:

```
user@host# show chassis
fpc 0 {
    pic 2 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 7;
                    object-cache-size 512;
                    package jservices-sfw; #Loads stateful firewall plug-in.
                    policy-db-size 64;
                }
            }
        }
    }
}
```

You can load both the **jservices-sfw** package and a Junos SDK application package on the same PIC.

The following example demonstrates the stateful firewall plug-in coexisting with a provider's plug-in:

```
[edit]
services {
  service-set sset {
    stateful-firewall-rules rule1;
    interface-service {
      service-interface ms-0/0/0;
    }
    extension-service customer-plugin;
    service-order {
      forward-flow [ stateful-firewall customer-plugin ];
    }
```

```
}
stateful-firewall {
  rule rule1 {
    match-direction input-output;
    term term1 {
      from {
        applications junos-ftp;
      }
      then {
        accept;
      }
    }
  }
  rule rule2 {
    match-direction input;
    term term1 {
      from {
        source-address {
          192.1.1.2/32;
        }
        then {
          reject;
          syslog;
        }
      }
    }
  }
}
```

The following stateful firewall operational commands support the **ms-** interface:

- **show services stateful-firewall flows**—Display stateful firewall flow table entries.
- **show services stateful-firewall statistics**—Display stateful firewall statistics. For this command, only rule and ALG statistics are given. In the extensive option, other statistics appear but do not populate correctly; those values are all zeroes.
- **clear services stateful-firewall flows**—Remove established flows from the flow table.

The commands are described in the CLI Explorer.

Related Documentation

- Configuring Memory for the Stateful Firewall Plug-In on page 7
- extension-provider on page 12

PART 2

Configuration

CHAPTER 2

Configuration Tasks

Configuring Memory for the Stateful Firewall Plug-In

When configuring the stateful firewall internal plug-in, some questions remain regarding the upper limit to specify for the **policy-db-size**, **object-cache-size**, and **forwarding-db-size** statements when the application needs to use a large number of rules, causing the total memory required to approach the size of the object cache configured. The following limits, which are specific to the stateful firewall configuration, await additional review:

- Maximum number of terms (with one rule per term) per service set: 1200
- Maximum number of service sets per Multiservices PIC: 4000 (Juniper Networks M Series Multiservice Edge Routers and T Series Core Routers), 6000 (Juniper Networks MX Series 3D Universal Edge Routers and M120 Multiservice Edge Routers)
- Maximum object cache size: 1280 MB (Multiservices 400 PICs and DPCs), 512 MB (Multiservices 100 PICs)
- Maximum policy database size: Still to be determined.

If the policy database is set too small, an error message is logged in the router message file even though the commit may appear to be successful. It is necessary to check the logs to make sure that no message file error is found to be sure that the stateful firewall commit was indeed successful. The remedial action is to increase the size of the policy database.

Related Documentation

- extension-provider on page 12

Configuring rsh, rlogin, rexec for Stateful Firewall

Some implementations of the rsh, rlogin, rexec mechanism require the remote host to authenticate the request by opening a separate TCP session to port 113 on the client host. By default, the stateful firewall does not allow this authentication flow to go through.

To open the authentication flow, include the **applications junos-ident** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* from]** hierarchy level:

```
[edit]
services {
  stateful-firewall {
    rule rule1 {
      term term1 {
        from {
          (source-address | destination-address);
          applications junos-ident;
        }
        then {
          accept;
        }
      }
    }
  }
}
```

To allow Kerberos-enabled rsh, rlogin, rexec through the stateful firewall, configure the following additional applications and include them in the stateful firewall terms:

```
[edit]
applications {
  application test-kerberos-kshell {
    Protocol tcp;
    destination-port kshell;
  }
  application test kerberos-klogin {
    protocol tcp;
    destination-port klogin;
  }
}
```

```
services {
  stateful-firewall {
    rule rule1 {
      term term1 {
        from {
          applications [kerberos-klogin kerberos-kshell];
        }
        then {
          accept;
        }
      }
    }
  }
}
```

Related Documentation

- Configuring Memory for the Stateful Firewall Plug-In on page 7

CHAPTER 3

Configuration Statements

control-cores

Syntax control-cores *control-number*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure control cores. Any cores not configured as either control or data cores are treated as user cores. When the number of control cores is changed, the PIC reboots.

Options ***control-number***—Number of control cores. At least one core must be a control core.

Range: 1 through 8

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

Related Documentation
- *Configuring Control and Data Cores*
- data-cores on page 10

data-cores

Syntax data-cores *data-number*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure data cores. Any cores not configured as either data or control cores are treated as user cores. When the number of data cores is changed, the PIC reboots.

Options ***data-number***—Number of data cores. Although it is not mandatory to dedicate any cores as data cores, it is advisable, depending on the nature of the application, to dedicate a minimum of five as data cores to achieve good performance.

Range: 0 through 7

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

Related Documentation
- *Configuring Control and Data Cores*
- control-cores on page 9

data-flow-affinity

Syntax
```
data-flow-affinity {
  hash-key (layer-3 | layer-4);
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.5.

Description Enable flow affinity distribution for packets over data CPUs on the PIC. Once enabled, the default behavior distributing data packets changes from a round-robin distribution to a flow affinity distribution based on a hash distribution. Adding or deleting this statement causes the PIC to reboot.

The 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 Packet Distribution Settings*

destination (Chassis)

Syntax destination *destination*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider syslog *facility*]

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure where log messages go. By default, all messages go to the **/var/log** directory on the Routing Engine. Enhancements to the existing infrastructure make debugging on the Multiservices PIC easier by giving the user the option of redirecting log messages. When the **syslog destination** statement is configured to redirect the log messages, you can use the **set system syslog** command, a command available in the native Junos OS CLI, to override the syslog settings made on the Multiservices PIC.

Options ***destination***—Choose one of the following options:

- **routing-engine**—Forward log messages to the Routing Engine.
- **pic-console**—Forward log messages to the console of the PIC.

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

Related Documentation

- *Configuring System Log Messages*
- extension-provider on page 12

extension-provider

Syntax

```
extension-provider {
  control-cores control-number;
  data-cores data-number;
  data-flow-affinity {
    hash-key (layer-3 | layer-4);
  }
  forwarding-db-size size;
  object-cache-size size;
  package package-name;
  policy-db-size size;
  syslog {
    facility {
      severity;
      destination destination;
    }
  }
  wired-max-processes num-procs;
  wired-process-mem-size mem-size;
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure an application on a PIC. When the **extension-provider** statement is first configured, the PIC reboots.

The 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 Control and Data Cores*
- *Configuring Packet Distribution Settings*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*
- *Configuring System Log Messages*

forwarding-db-size

Syntax forwarding-db-size *size*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure the size of the forwarding database (FDB). When this setting is changed, the PIC reboots.

NOTE: You need to enable the forwarding-options sampling statement for the FDB to be created.

Options ***size***—Size of the FDB, in megabytes (MB). The size of the FDB and the size of the policy database together must be smaller than the size of the object cache.

Range: 0 through 12879 MB

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

Related Documentation

- *Configuring Memory Settings*
- policy-db-size on page 17
- wired-process-mem-size on page 19
- object-cache-size on page 15

hash-key (Chassis)

Syntax hash-key (layer-3 | layer-4);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider data-flow-affinity]

Release Information Statement introduced in Junos OS Release 10.2.

Description Set the hashing distribution of flow affinity. This is an optional setting. Once the **data-flow-affinity** statement is enabled, you may need to choose the hashing distribution. Modifying this statement causes the PIC to reboot.

Default If you do not configure the **hash-key** statement, the hashing distribution is 5-tuple hashing, or **layer-4**.

Options **layer-3**—3-tuple hashing (source IP address, destination IP address, and IP protocol).

layer-4—5-tuple hashing (3-tuple plus source and destination TCP or UDP ports).

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

Related Documentation

- *Configuring Packet Distribution Settings*
- extension-provider on page 12

object-cache-size

Syntax object-cache-size *value*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure the size of the object cache. When this setting is changed, the PIC reboots.

Options *value*—Amount of object cache, in MB. Only values in increments of 128 MB are allowed.

Range: For Multiservices 100 PIC, range is 128 MB through 512 MB. If the **wired-process-mem-size** statement at the same hierarchy level has a value of 512 MB, the maximum value for this statement is 128 MB.

Range: For Multiservices 400 PIC, range is 128 MB through 1280 MB. If the **wired-process-mem-size** statement at the same hierarchy level has a value of 512 MB, the maximum value for this statement is 512 MB.

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

Related Documentation

- *Configuring Memory Settings*
- forwarding-db-size on page 13
- policy-db-size on page 17
- wired-process-mem-size on page 19

package (Loading on PIC)

Syntax package *package-name*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.1.

Description Identify a package to be loaded on the PIC. When a package is added or removed, the PIC reboots.

Options ***package-name***—Name of the package to be loaded on the PIC. There can be up to eight packages loaded on a PIC; however, only one data package is allowed per PIC. An error message is displayed if more than eight packages are specified.

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

Related Documentation

- *Configuring Packages on the PIC*

policy-db-size

Syntax policy-db-size *size*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.3.

Description Configure the size of the policy database. When this setting is changed, the PIC reboots.

NOTE: At least one data core must be configured to configure the size of the policy database.

Options ***size***—Size of the policy database, in megabytes (MB). The size of the forwarding database and the size of the policy database together must be smaller than the size of the object cache.

Range: 0 through 1279 MB

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

Related Documentation

- *Configuring Memory Settings*
- forwarding-db-size on page 13
- object-cache-size on page 15
- wired-process-mem-size on page 19

syslog (Chassis)

Syntax

```
syslog {
  facility {
    severity;
    destination destination;
  }
}
```

Hierarchy Level

[edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information

Statement introduced in Junos OS Release 9.2.
Options **daemon** and **kernel** (for ***facility***) introduced in Junos OS Release 9.5.

Description

Enable PIC system logging to record or view system log messages on a specific PIC. The system log information is passed to the kernel for logging in the **/var/log** directory.

Options

facility—Group of messages that are either generated by the same software process or concern a similar condition or activity. Possible values include the following: **daemon**, **external**, **kernel**, and **pfe**.

severity—Classification of effect on functioning. Possible values are the following options:

- **any**—Include all severity levels.
- **none**—Disable logging of the associated facility to a destination.
- **emergency**—System panic or other condition that causes the routing platform to stop functioning.
- **alert**—Conditions that require immediate correction, such as a corrupted system database.
- **critical**—Critical conditions, such as hard 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 nonerror conditions of interest.

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

- *Configuring System Log Messages*

wired-process-mem-size

Syntax wired-process-mem-size *mem-size*;

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]

Release Information Statement introduced in Junos OS Release 9.3.

Description Configure the size of the reserved wired process memory. You can also configure object cache. If this setting is changed, the PIC reboots.

Options ***megabytes***—Size of the reserved wired process memory, in MB. The only size you can set for this statement is 512 MB.

Default: 512 MB

Range: 0 through 512 MB

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

Related Documentation

- *Configuring Memory Settings*
- forwarding-db-size on page 13
- object-cache-size on page 15
- policy-db-size on page 17
- wired-max-processes

PART 3

Index

Index