ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308
CLI Reference Manual
Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR
Phone (Other Countries): Check the list of phone numbers at http://support.netgear.com/app/answers/detail/a_id/984.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Version</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-11138-01</td>
<td>1.0</td>
<td>August 2012</td>
<td>First publication</td>
</tr>
</tbody>
</table>
### Contents

#### Chapter 1  Introduction

- Command Syntax and Conventions ................................... 7
- Command Conventions .................................................. 7
- Description of a Command ............................................ 8
- Common Parameters .................................................... 9
- The Four Categories of Commands .................................... 9
- The Four Main Modes for Configuration Commands ............... 10
- Save Commands .......................................................... 12
- Global Commands ....................................................... 13
- The Three Basic Types of Commands ................................ 14
- Command Autocompletion and Command Abbreviation .......... 15
  - CLI Line-Editing Conventions ...................................... 15
- Access the CLI ........................................................... 16

#### Chapter 2  Overview of the Configuration Commands

- Network Settings (Net Mode) Configuration Commands .......... 17
- Security Settings (Security Mode) Configuration Commands .... 20
- Administrative and Monitoring Settings (System Mode)       
  - Configuration Commands .......................................... 23
- VPN Settings (VPN Mode) Configuration Commands .............. 24

#### Chapter 3  Net Mode Configuration Commands

- General WAN Commands .............................................. 27
- IPv4 WAN Commands .................................................. 31
- IPv6 WAN Commands .................................................. 46
- IPv6 Tunnel Commands ............................................... 50
- Dynamic DNS Commands ............................................. 53
- IPv4 LAN Commands .................................................. 54
- IPv6 LAN Commands .................................................. 66
- IPv4 DMZ Setup Commands ......................................... 74
- IPv6 DMZ Setup Commands ......................................... 76
- WAN QoS Commands .................................................. 80
- IPv4 Routing Commands ............................................. 93
- IPv6 Routing Commands ............................................. 98

#### Chapter 4  Security Mode Configuration Commands

- Security Services Commands ........................................ 101
- Security Schedules Commands ...................................... 110
Chapter 5  System Mode Configuration Commands

Remote Management Commands .......................... 186
SNMP Commands ........................................... 191
Time Zone Command ..................................... 192
WAN Traffic Meter Command ............................ 198
Firewall Logs and Email Alerts Commands ........... 201

Chapter 6  VPN Mode Configuration Commands

IPSec VPN Wizard Command ............................. 208
IPSec IKE Policy Commands ............................ 210
IPSec VPN Policy Commands ........................... 216
IPSec VPN Mode Config Commands ..................... 228
SSL VPN Portal Layout Commands ....................... 231
SSL VPN Authentication Domain Commands .......... 234
SSL VPN Authentication Group Commands ............ 238
SSL VPN User Commands ............................... 239
SSL VPN Port Forwarding Commands .................. 246
SSL VPN Client and Client Route Commands ........ 248
SSL VPN Resource Commands ........................... 252
SSL VPN Policy Commands ............................. 256
RADIUS Server Command ............................... 263
PPTP Server Commands .................................. 265
L2TP Server Commands .................................. 266

Chapter 7  Overview of the Show Commands

Network Settings (Net Mode) Show Commands ......... 267
Security Settings (Security Mode) Show Commands .... 269
Administrative and Monitoring Settings (System Mode)
Show Commands ......................................... 270
VPN Settings (VPN Mode) Show Commands .......... 270

Chapter 8  Show Commands

Network Settings (Net Mode) Show Commands ........ 273
WAN IPv4 and WAN IPv6 Show Commands .......... 273
Network Settings (Net Mode) Show Commands ......................... 273
WAN IPv4 and WAN IPv6 Show Commands ............................. 273
IPv6 Mode, IPv6 Tunnel, and SIIT Show Commands ................. 277
LAN DHCP Show Commands ........................................ 278
Dynamic DNS Show Commands ...................................... 279
IPv4 LAN Show Commands .......................................... 280
IPv6 LAN Show Commands .......................................... 284
DMZ Show Commands ................................................ 286
Routing Show Commands ............................................. 288
Network Statistics Show Commands .................................. 289
Security Settings (Security Mode) Show Commands ................ 290
Services Show Command ............................................. 290
Schedules Show Command .......................................... 292
Firewall Rules Show Command ..................................... 292
Attack Checks Show Commands .................................... 294
Session Limits Show Commands .................................... 295
Advanced Firewall Show Commands ................................ 296
Address Filter Show Commands ..................................... 296
Port Triggering Show Commands ................................... 297
UPnP Show Commands .............................................. 298
Bandwidth Profiles Show Command ................................ 298
Content Filtering Show Commands .................................. 299
Administrative and Monitoring Settings (System Mode)
Show Commands ....................................................... 300
Remote Management Show Command ................................ 301
SNMP Show Commands ............................................. 301
Time Show Command ................................................. 302
Firmware Version Show Command .................................. 302
Status Show Command .............................................. 303
WAN Traffic Meter Show Command .................................. 306
Logging Configuration Show Commands ................................ 307
Logs Show Commands ................................................ 309
VPN Settings (VPN Mode) Show Commands ......................... 311
IPSec VPN Show Commands ........................................ 311
SSL VPN Show Commands .......................................... 313
SSL VPN User Show Commands .................................... 316
RADIUS Server Show Command .................................... 319
PPTP Server Show Commands ....................................... 320
L2TP Server Show Commands ....................................... 320

Chapter 9 Utility Commands

Overview Util Commands ............................................. 321
Firmware Backup, Restore, and Upgrade Commands .............. 322
Diagnostic Commands ............................................... 323

CLI Command Index
Introduction

This document describes the command-line interface (CLI) for the NETGEAR ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308.

This chapter introduces the CLI interface. It includes the following sections:

- Command Syntax and Conventions
- The Four Categories of Commands
- The Four Main Modes for Configuration Commands
- Global Commands
- The Three Basic Types of Commands
- Command Autocompletion and Command Abbreviation
- Access the CLI

**Note:** For more information about the topics covered in this manual, visit the support website at [http://support.netgear.com](http://support.netgear.com).

**Note:** For more information about the features that you can configure using the CLI, see the ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 Reference Manual.

**Note:** You cannot generate and upload a certificate through the CLI. You need to access the web management interface to manage these tasks.
Command Syntax and Conventions

A command is one or more words that can be followed by one or more keywords and parameters. Keywords and parameters can be required or optional:

- A keyword is a predefined string (word) that narrows down the scope of a command. A keyword can be followed by an associated parameter or by associated keywords. In many cases, these associated keywords are mutually exclusive, so you need to select one of them. In some cases, this manual refers to a group of words as a keyword.
- A parameter is a variable for which you need to type a value. You need to replace the parameter name with the appropriate value, which might be a name or number. A parameter can be associated with a command or with a keyword.

This manual lists each command by its full command name and provides a brief description of the command. In addition, for each command, the following information is provided:

- **Format.** Shows the command keywords and the required and optional parameters.
- **Mode.** Identifies the command mode you need to be in to access the command. (With some minor exceptions, the mode is always described using lower-case letters.)
- **Related show command or commands.** Identifies and links to the show command or commands that can display the configured information.

For more complicated commands, in addition to the format, mode, and related show command or commands, the following information is provided:

- **Table.** Explains the keywords and parameters that you can use for the command.
- **Example.** Shows a CLI example for the command.

Command Conventions

In this manual, the following type font conventions are used:

- A command name is stated in **bold** font.
- A keyword name is stated in **bold** font.
- A parameter name is stated in *italic* font.

The keywords and parameters for a command might include mandatory values, optional values, or choices. The following table describes the conventions that this manual uses to distinguish between value types:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&gt; angle brackets</td>
<td>&lt;value&gt;</td>
<td>Indicate that you need to enter a value in place of the brackets and text inside them. <em>(value is the parameter.)</em></td>
</tr>
<tr>
<td>[] square brackets</td>
<td>[value]</td>
<td>Indicate an optional parameter that you can enter in place of the brackets and text inside them. <em>(value is the parameter.)</em></td>
</tr>
</tbody>
</table>
Description of a Command

The following example describes the `net radvd pool lan edit <row id>` command:

```
net radvd pool lan edit is the command name.
<row id> is the required parameter for which you need to enter a value after you type the command words.
```

The command lets you enter the net-config [radvd-pool-lan] mode, from which you can issue the following keywords and parameters:

```
prefix_type {6To4 {sla_id <id number>} | {Global-Local-ISATAP}
    {prefix_address <ipv6-address>} {prefix_length
    <prefix length>}}
```

```
prefix_life_time <seconds>
```

Explanation of the keywords and parameters:

```
prefix_type is a keyword. The required associated keyword that you need to select is either 6To4 or Global-Local-ISATAP.
```

- If you select 6To4, you also need to issue the `sla_id` keyword and enter a value for the `<id number>` parameter.
- If you select Global-Local-ISATAP, you also need to issue the `prefix_address` keyword and enter a value for the `<ipv6-address>` parameter, and you need to issue the `prefix_length` keyword and enter a value for the `<prefix length>` parameter.

```
prefix_life_time is a keyword. <seconds> is the required parameter for which you need to enter a value.
```

Command example:

```
SRX5308> net radvd pool lan edit 12
net-config[radvd-pool-lan]> prefix_type Global-Local-ISATAP
net-config[radvd-pool-lan]> prefix_address 10FA:2203:6145:4201::
net-config[radvd-pool-lan]> prefix_length 10
net-config[radvd-pool-lan]> prefix_life_time 3600
net-config[radvd-pool-lan]> save
```
Common Parameters

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. The following table describes common parameter values and value formatting:

Table 2. Common parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ipaddr         | This parameter is a valid IPv4 address. You need to enter the IP address in the a.b.c.d format, in which each octet is a number in the range from 0 to 255 (both inclusive), for example, 10.12.140.218. The CLI accepts decimal, hexadecimal, and octal formats through the following input formats (where n is any valid decimal, hexadecimal, or octal number):  
  • 0xn (CLI assumes hexadecimal format)  
  • 0n (CLI assumes octal format with leading zeros)  
  • n (CLI assumes decimal format) |
| ipv6-address   | This parameter is a valid IPv6 address. You can enter the IPv6 address in the following formats:  
  • FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or  
  • FE80:0:0:0:20F:24FF:FEBF:DBCB, or  
  • FE80::20F:24FF:FEBF:DBCB, or  
  • FE80:0:0:0:20F:24FF:128:141:49:32  
  For additional information, see RFC 3513. |
| Character strings | Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid. |

The Four Categories of Commands

There are four CLI command categories:

- Configuration commands with four main configuration modes. For more information, see the following section, The Four Main Modes for Configuration Commands. Save commands also fall into this category (see Save Commands on page 12).
- Show commands that are available for the four main configuration modes (see Chapter 7, Overview of the Show Commands and Chapter 8, Show Commands).
- Utility commands (see Chapter 9, Utility Commands).
- Global commands (see Global Commands on page 13).
The Four Main Modes for Configuration Commands

For the configuration commands, there are four main modes in the CLI: net, security, system, and vpn. *Chapter 2, Overview of the Configuration Commands* lists all commands in these modes, and each of these modes is described in detail in a separate chapter (see *Chapter 3* through *Chapter 6*).

The following table lists the *main* configuration modes, the configuration modes, the features that you can configure in each configuration mode, and, for orientation, the basic web management interface (GUI) path to the feature.

**Table 3. Main configuration modes**

<table>
<thead>
<tr>
<th>Main Mode</th>
<th>Submode</th>
<th>Feature That You Can Configure</th>
<th>Basic Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network configuration commands</td>
<td>net</td>
<td>ddns</td>
<td>Dynamic DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dmz</td>
<td>DMZ for IPv4&lt;br&gt;DMZ for IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ethernet</td>
<td>VLAN assignment to LAN interface</td>
</tr>
<tr>
<td></td>
<td>ipv6</td>
<td>IPv4 or IPv4/IPv6 mode</td>
<td>Network Configuration &gt; WAN Settings</td>
</tr>
<tr>
<td></td>
<td>ipv6_tunnel</td>
<td>IPv6 tunnels</td>
<td>Network Configuration &gt; WAN Settings</td>
</tr>
<tr>
<td></td>
<td>lan</td>
<td>IPv4 LAN settings and VLANs&lt;br&gt;LAN groups for IPv4&lt;br&gt;Secondary IPv4 LAN addresses&lt;br&gt;Advanced IPv4 LAN settings&lt;br&gt;Fixed and reserved DHCP IPv4 addresses&lt;br&gt;LAN IPv4 traffic meter profiles&lt;br&gt;IPv6 LAN settings&lt;br&gt;Secondary IPv6 LAN addresses&lt;br&gt;IPv6 LAN DHCP address pools&lt;br&gt;IPv6 prefix delegation for the LAN</td>
<td>Network Configuration &gt; LAN Setup</td>
</tr>
<tr>
<td></td>
<td>protocol_binding</td>
<td>Protocol bindings</td>
<td>Network Configuration &gt; Protocol Binding</td>
</tr>
<tr>
<td></td>
<td>qos</td>
<td>WAN QoS profiles</td>
<td>Network Configuration &gt; QoS</td>
</tr>
<tr>
<td></td>
<td>radvd</td>
<td>IPv6 RADVD and pools for the LAN&lt;br&gt;IPv6 RADVD and pools for the DMZ</td>
<td>Network Configuration &gt; LAN Setup&lt;br&gt;Network Configuration &gt; DMZ Setup</td>
</tr>
<tr>
<td></td>
<td>routing</td>
<td>Dynamic IPv4 routes&lt;br&gt;Static IPv4 routes&lt;br&gt;Static IPv6 routes</td>
<td>Network Configuration &gt; Routing</td>
</tr>
</tbody>
</table>
### Table 3. Main configuration modes (continued)

<table>
<thead>
<tr>
<th>Main Mode</th>
<th>Submode</th>
<th>Feature That You Can Configure</th>
<th>CLI</th>
<th>Web Management Interface (GUI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>net (continued)</td>
<td>siit</td>
<td>Stateless IP/ICMP Translation</td>
<td></td>
<td>Network Configuration &gt; SIIT</td>
</tr>
<tr>
<td></td>
<td>wan</td>
<td>IPv4 WAN (Internet) settings</td>
<td></td>
<td>Network Configuration &gt; WAN Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secondary IPv4 WAN addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 WAN (Internet) settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MTU, port speed, and MAC address, failure detection method, and upload/download settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>wan_settings</td>
<td>NAT or Classical Routing Load balancing settings for IPv4</td>
<td></td>
<td>Network Configuration &gt; WAN Settings</td>
</tr>
</tbody>
</table>

### Security configuration commands

- **security address_filter**: Source MAC filters
  - IP/MAc bindings for IPv4
  - IP MAC bindings for IPv6
  - Security > Address Filter
- **bandwidth**: Bandwidth profiles
  - Security > Bandwidth Profile
- **content_filter**: Group filtering
  - Blocked keywords
  - Web components
  - Trusted domains
  - Security > Content Filtering
- **firewall**: All IPv4 firewall rules
  - All IPv6 firewall rules
  - Attack checks
  - Session limits and time-outs
  - SIP ALG
  - Security > Firewall
- **porttriggering_rules**: Security > Port Triggering
- **schedules**: Security > Schedule
- **services**: Custom services
  - LAN and WAN IP groups
  - LAN QoS profiles
  - Security > Services
- **upnp**: Security > UPnP

### Administration and monitoring configuration commands

- **system logging**: Monitoring > Firewall Logs & E-mail
- **remote_management**: Administration > Remote Management
- **snmp**: Administration > SNMP
Table 3. Main configuration modes (continued)

<table>
<thead>
<tr>
<th>Main Mode</th>
<th>Submode</th>
<th>Feature That You Can Configure</th>
<th>Basic Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>system (continued)</td>
<td>time</td>
<td>Time Zone</td>
<td>Administration &gt; Time Zone</td>
</tr>
<tr>
<td>traffic_meter</td>
<td></td>
<td>WAN traffic meters</td>
<td>Monitoring &gt; Traffic Meter</td>
</tr>
</tbody>
</table>

VPN configuration commands

<table>
<thead>
<tr>
<th>Main Mode</th>
<th>Submode</th>
<th>Feature That You Can Configure</th>
<th>Basic Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn</td>
<td>ipsec</td>
<td>IKE policies</td>
<td>VPN &gt; IPSec VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN IPSec Wizard</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode Config records</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RADIUS servers</td>
<td></td>
</tr>
<tr>
<td>l2tp</td>
<td></td>
<td>L2TP server</td>
<td>VPN &gt; L2TP Server</td>
</tr>
<tr>
<td>pptp</td>
<td></td>
<td>PPTP server</td>
<td>VPN &gt; PPTP Server</td>
</tr>
<tr>
<td>sslvpn</td>
<td></td>
<td>SSL policies</td>
<td>VPN &gt; SSL VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources and resource objects</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Portal layouts</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL VPN clients</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Client routes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domains</td>
<td>Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User login and IP policies</td>
<td></td>
</tr>
</tbody>
</table>

Save Commands

The following table describes the configuration commands that let you save or cancel configuration changes in the CLI. You can use these commands in any of the four main configuration modes. These commands are not preceded by a period.

Table 4. Save commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>save</td>
<td>Save the configuration changes.</td>
</tr>
<tr>
<td>exit</td>
<td>Save the configuration changes and exit the current configuration mode.</td>
</tr>
<tr>
<td>cancel</td>
<td>Roll back the configuration changes.</td>
</tr>
</tbody>
</table>
**Commands That Require Saving**

After you have issued a command that includes the word `configure`, `add`, or `edit`, you enter a configuration mode from which you can issue keywords and associated parameters. These are examples of commands for which you need to save your changes:

- `net lan ipv4 configure <vlan id>` lets you enter the net-config [lan-ipv4] configuration mode. After you made your changes, issue `save` or `exit` to save your changes.

- `security content_filter trusted_domain add` lets you enter the security-config [approved-urls] configuration mode. After you made your changes, issue `save` or `exit` to save your changes.

- `vpn sslvpn users groups add` lets you enter the vpn-config [user-groups] configuration mode. After you made your changes, issue `save` or `exit` to save your changes.

**Commands That Do Not Require Saving**

You do not need to save your changes after you have issued a command that deletes, disables, or enables a row ID, name, IP address, or MAC address, or that lets you make a configuration change without entering another configuration mode. These are examples of commands that you do not need to save:

- `net lan dhcp reserved_ip delete <mac address>`
- `vpn ipsec vpnpolicy disable <vpn policy name>`
- `security firewall ipv4 enable <row id>`
- `security firewall ipv4 default_outbound_policy {Allow | Block}`

**Global Commands**

The following table describes the global commands that you can use anywhere in the CLI. These commands need to be preceded by a period.

**Table 5. Global CLI commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.exit</td>
<td>Exit the current session.</td>
</tr>
<tr>
<td>.help</td>
<td>Display an overview of the CLI syntax.</td>
</tr>
<tr>
<td>.top</td>
<td>Return to the default command mode or root.</td>
</tr>
<tr>
<td>.reboot</td>
<td>Reboot the system.</td>
</tr>
<tr>
<td>.history</td>
<td>Display the command-line history of the current session.</td>
</tr>
</tbody>
</table>
The Three Basic Types of Commands

You can encounter the following three basic types of commands in the CLI:

- **Entry commands to enter a configuration mode.** Commands that let you enter a configuration mode from which you can configure various keywords and associated parameters and keywords. For example, the `net wan wan1 ipv4 configure` command lets you enter the net-config [wan1-ipv4] mode, from which you can configure the IPv4 WAN settings.

  This type of command is the most common in the CLI and is always indicated by two steps in this manual, each one showing the format and mode:

  **Step 1** Format: `net wan wan ipv4 configure <wan interface>`
  Mode: `net`

  **Step 2** Format: This section shows the keywords and associated parameters, for example:
  
  `isp_connection_type {STATIC | DHCPC | PPPoE | PPTP}`
  Mode: `net-config [wan1-ipv4]`

  Sometimes, you need to enter a parameter to enter a configuration mode. For example, `security schedules edit <row id>` requires you to enter the row ID parameter to enter the security-config [schedules] mode, from which you can modify various keywords and associated parameters and keywords.

- **Commands with a single parameter.** Commands that require you to supply one or more parameters and that do not let you enter another configuration mode. The parameter is usually a row ID or a name. For example, `security firewall ipv4 delete <row id>` requires you to enter the row ID parameter to delete the firewall rule.

  For this type of command, the format and mode are shown in this manual:

  Format: `security firewall ipv4 delete <row id>`
  Mode: `security`

- **Commands without parameters.** Commands that do not require you to supply a parameter after the command and that do not let you enter another configuration mode. For example, `util restore_factory_defaults` does not require parameters.

  For this type of command also, the format and mode are shown in this manual:

  Format: `util restore_factory_defaults`
  Mode: `util`
Command Autocompletion and Command Abbreviation

Command autocompletion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. You need to type all of the required keywords and parameters before you can use autocompletion.

The following keys both perform autocompletion for the current command. If the command prefix is not unique, a subsequent repeat of the key displays possible completions.

- **Enter or Return key.** Autocompletes, syntax-checks, and then executes the command. If there is a syntax error, the offending part of the command is highlighted and explained.
- **Spacebar.** Autocompletes, or if the command is already resolved, inserts a space.

CLI Line-Editing Conventions

The following table describes the key combinations that you can use to edit commands or increase the speed of command entry. Access this list from the CLI by issuing `.help`.

Table 6. CLI editing conventions

<table>
<thead>
<tr>
<th>Key or Key Sequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Invoking context-sensitive help</strong></td>
<td></td>
</tr>
<tr>
<td>?</td>
<td>Displays context-sensitive help. The information that displays consists either of a list of possible command completions with summaries or of the full syntax of the current command. When a command has been resolved, a subsequent repeat of the help key displays a detailed reference.</td>
</tr>
<tr>
<td><strong>Autocompleting</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Command autocompletion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. However, you need to type all of the required keywords and parameters before you use autocompletion.</td>
<td></td>
</tr>
<tr>
<td>Enter (or Return)</td>
<td>Autocompletes, syntax-checks, and then executes a command. If there is a syntax error, the offending part of the command line is highlighted and explained. If the command prefix is not unique, a subsequent repeat of the key displays possible completions.</td>
</tr>
<tr>
<td>Spacebar</td>
<td>Autocompletes, or if the command is already resolved, inserts a space. If the command prefix is not unique, a subsequent repeat of the key displays possible completions.</td>
</tr>
<tr>
<td><strong>Moving around</strong></td>
<td></td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Go to the beginning of the line.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Go to the end of the line.</td>
</tr>
<tr>
<td>Up arrow</td>
<td>Go to the previous line in the history buffer.</td>
</tr>
<tr>
<td>Down arrow</td>
<td>Go to the next line in the history buffer.</td>
</tr>
<tr>
<td>Left arrow</td>
<td>Go backward one character.</td>
</tr>
</tbody>
</table>
You can access the CLI by logging in with the same user credentials (user name and password) that you use to access the web management interface. **SRX5308>** is the CLI prompt.

```
SRX5308 login: admin
Password:  
******************************************
Welcome to SRX5308 Command Line Interface
******************************************
SRX5308>
```
Overview of the Configuration Commands

This chapter provides an overview of all configuration commands in the four configuration command modes. The keywords and associated parameters that are available for these commands are explained in the following chapters. The chapter includes the following sections:

- Network Settings (Net Mode) Configuration Commands
- Security Settings (Security Mode) Configuration Commands
- Administrative and Monitoring Settings (System Mode) Configuration Commands
- VPN Settings (VPN Mode) Configuration Commands

Network Settings (Net Mode) Configuration Commands

Enter the `net ?` command at the CLI prompt to display the submodes in the net mode. The following table lists the submodes and their commands in alphabetical order:

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddns</td>
<td><code>net ddns configure</code></td>
<td>Enable, configure, or disable DDNS service.</td>
</tr>
<tr>
<td>dmz</td>
<td><code>net dmz ipv4 configure</code></td>
<td>Enable, configure, or disable the IPv4 DMZ.</td>
</tr>
<tr>
<td></td>
<td><code>net dmz ipv6 configure</code></td>
<td>Enable, configure, or disable the IPv6 DMZ.</td>
</tr>
<tr>
<td></td>
<td><code>net dmz ipv6 pool configure &lt;ipv6 address&gt;</code></td>
<td>Configure a new or existing IPv6 DMZ DHCP address pool.</td>
</tr>
<tr>
<td></td>
<td><code>net dmz pool ipv6 delete &lt;ipv6 address&gt;</code></td>
<td>Delete an IPv6 DMZ DHCP address pool.</td>
</tr>
<tr>
<td>ethernet</td>
<td><code>net ethernet configure &lt;interface name or number&gt;</code></td>
<td>Configure a VLAN for a LAN interface.</td>
</tr>
<tr>
<td>ipv6</td>
<td><code>net ipv6 ipmode configure</code></td>
<td>Configure the IP mode (IPv4 only or IPv4/IPv6).</td>
</tr>
<tr>
<td>ipv6_tunnel</td>
<td><code>net ipv6_tunnel isatap add</code></td>
<td>Configure a new IPv6 ISATAP tunnel.</td>
</tr>
<tr>
<td></td>
<td><code>net ipv6_tunnel isatap delete &lt;row id&gt;</code></td>
<td>Delete an IPv6 ISATAP tunnel.</td>
</tr>
</tbody>
</table>
### Table 7. Net mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6_tunnel</td>
<td>net ipv6_tunnel isatap edit &lt;row id&gt;</td>
<td>Configure an existing IPv6 ISATAP tunnel.</td>
</tr>
<tr>
<td></td>
<td>net ipv6_tunnel six_to_four configure</td>
<td>Enable or disable automatic (6to4) tunneling.</td>
</tr>
<tr>
<td>lan</td>
<td>net lan dhcp reserved_ip configure &lt;mac address&gt;</td>
<td>Bind a MAC address to an IP address for DHCP reservation or change an existing binding, and assign a LAN group.</td>
</tr>
<tr>
<td></td>
<td>net lan dhcp reserved_ip delete &lt;mac address&gt;</td>
<td>Delete the binding of a MAC address to an IP address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 advanced configure</td>
<td>Configure advanced LAN settings such as the MAC address for VLANs and ARP broadcast.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 configure &lt;vlan id&gt;</td>
<td>Configure a new or existing VLAN.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 default_vlan</td>
<td>Configure the default VLAN for each port.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 delete &lt;vlan id&gt;</td>
<td>Delete a VLAN.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 disable &lt;vlan id&gt;</td>
<td>Disable a VLAN.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 enable &lt;vlan id&gt;</td>
<td>Enable a VLAN.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 multi_homing add</td>
<td>Configure a new secondary IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 multi_homing delete &lt;row id&gt;</td>
<td>Delete a secondary IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 multi_homing edit &lt;row id&gt;</td>
<td>Configure an existing secondary IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 traffic_meter configure &lt;ip address&gt;</td>
<td>Configure a traffic meter profile for an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv4 traffic_meter delete &lt;row id&gt;</td>
<td>Delete a traffic meter profile.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 configure</td>
<td>Configure the IPv6 LAN address settings and DHCPv6.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 multi_homing add</td>
<td>Configure a new secondary IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 multi_homing delete &lt;row id&gt;</td>
<td>Delete a secondary IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 multi_homing edit &lt;row id&gt;</td>
<td>Configure an existing secondary IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 pool add</td>
<td>Configure a new IPv6 LAN DHCP address pool.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 pool delete &lt;row id&gt;</td>
<td>Delete an IPv6 LAN DHCP address pool.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 pool edit &lt;row id&gt;</td>
<td>Configure an existing IPv6 LAN DHCP address pool.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 prefix_delegation add</td>
<td>Configure a new prefix for IPv6 LAN prefix delegation.</td>
</tr>
</tbody>
</table>
Table 7. Net mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan (continued)</td>
<td>net lan ipv6 prefix_delegation delete &lt;row id&gt;</td>
<td>Delete a prefix for IPv6 LAN prefix delegation.</td>
</tr>
<tr>
<td></td>
<td>net lan ipv6 prefix_delegation edit &lt;row id&gt;</td>
<td>Configure an existing prefix for IPv6 LAN prefix delegation.</td>
</tr>
<tr>
<td></td>
<td>net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt;</td>
<td>Change an existing LAN default group name.</td>
</tr>
<tr>
<td>protocol binding</td>
<td>net protocol_binding add</td>
<td>Configure a new protocol binding.</td>
</tr>
<tr>
<td></td>
<td>net protocol_binding delete</td>
<td>Delete a protocol binding.</td>
</tr>
<tr>
<td></td>
<td>net protocol_binding disable</td>
<td>Disable a protocol binding.</td>
</tr>
<tr>
<td></td>
<td>net protocol_binding edit &lt;row id&gt;</td>
<td>Configure an existing protocol binding.</td>
</tr>
<tr>
<td></td>
<td>net protocol_binding enable &lt;row id&gt;</td>
<td>Enable a protocol binding.</td>
</tr>
<tr>
<td>qos</td>
<td>net qos configure</td>
<td>Configure the QoS mode for the WAN interfaces.</td>
</tr>
<tr>
<td></td>
<td>net qos profile add</td>
<td>Configure a new WAN QoS profile.</td>
</tr>
<tr>
<td></td>
<td>net qos profile delete &lt;row id&gt;</td>
<td>Delete a WAN QoS profile.</td>
</tr>
<tr>
<td></td>
<td>net qos profile disable &lt;row id&gt;</td>
<td>Disable a WAN QoS profile.</td>
</tr>
<tr>
<td></td>
<td>net qos profile edit &lt;row id&gt;</td>
<td>Configure an existing WAN QoS profile.</td>
</tr>
<tr>
<td></td>
<td>net qos profile enable &lt;row id&gt;</td>
<td>Enable a WAN QoS profile.</td>
</tr>
<tr>
<td>radvd</td>
<td>net radvd configure dmz</td>
<td>Configure the IPv6 RADVD for the DMZ.</td>
</tr>
<tr>
<td></td>
<td>net radvd configure lan</td>
<td>Configure the IPv6 RADVD for the LAN.</td>
</tr>
<tr>
<td>routing</td>
<td>net routing dynamic configure</td>
<td>Configure RIP and the associated MD5 key information.</td>
</tr>
<tr>
<td></td>
<td>net routing static ipv4 configure &lt;route name&gt;</td>
<td>Configure a new or existing IPv4 static route.</td>
</tr>
<tr>
<td></td>
<td>net routing static ipv4 delete &lt;route name&gt;</td>
<td>Delete an IPv4 static route.</td>
</tr>
<tr>
<td></td>
<td>net routing static ipv4 delete_all</td>
<td>Delete all IPv4 routes.</td>
</tr>
<tr>
<td></td>
<td>net routing static ipv6 configure &lt;route name&gt;</td>
<td>Configure a new or existing IPv6 static route.</td>
</tr>
<tr>
<td></td>
<td>net routing static ipv6 delete &lt;route name&gt;</td>
<td>Delete an IPv6 static route.</td>
</tr>
<tr>
<td></td>
<td>net routing static ipv6 delete_all</td>
<td>Delete all IPv6 routes.</td>
</tr>
<tr>
<td>siit</td>
<td>net siit configure</td>
<td>Configure Stateless IP/ICMP Translation</td>
</tr>
</tbody>
</table>
### Security Settings (Security Mode) Configuration Commands

Enter the `security ?` command at the CLI prompt to display the submodes in the security mode. The following table lists the submodes and their commands in alphabetical order:

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan</td>
<td><code>net wan port_setup configure &lt;wan interface&gt;</code></td>
<td>Configure the MTU, port speed, and MAC address of the VPN firewall.</td>
</tr>
<tr>
<td></td>
<td><code>net wan wan_ipv4 configure &lt;wan interface&gt;</code></td>
<td>Configure the IPv4 settings of the WAN interface.</td>
</tr>
<tr>
<td></td>
<td><code>net wan wan_ipv4 secondary_address add &lt;wan interface&gt;</code></td>
<td>Configure a secondary IPv4 WAN address.</td>
</tr>
<tr>
<td></td>
<td><code>net wan wan_ipv4 secondary_address delete &lt;row id&gt;</code></td>
<td>Delete a secondary IPv4 WAN address.</td>
</tr>
<tr>
<td></td>
<td><code>net wan wan_ipv6 configure &lt;wan interface&gt;</code></td>
<td>Configure the IPv6 settings of the WAN interface.</td>
</tr>
<tr>
<td>wan_settings</td>
<td><code>net wan_settings load_balancing configure</code></td>
<td>Configure the load balancing settings for two WAN interfaces that are configured for IPv4.</td>
</tr>
<tr>
<td></td>
<td><code>net wan_settings wanmode configure</code></td>
<td>Configure the mode of IPv4 routing (NAT or classical routing) between the WAN interface and LAN interfaces.</td>
</tr>
</tbody>
</table>

---

Table 7. Net mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>address_filter</td>
<td><code>security address_filter ip_or_mac_binding add</code></td>
<td>Configure a new IP/MAC binding rule.</td>
</tr>
<tr>
<td></td>
<td><code>security address_filter ip_or_mac_binding delete &lt;row id&gt;</code></td>
<td>Delete an IP/MAC binding rule.</td>
</tr>
<tr>
<td></td>
<td><code>security address_filter ip_or_mac_binding edit &lt;row id&gt;</code></td>
<td>Configure an existing IP/MAC binding rule.</td>
</tr>
<tr>
<td></td>
<td><code>security address_filter ip_or_mac_binding enable_email_log &lt;ip version&gt;</code></td>
<td>Configure the email log for IP/MAC Binding violations.</td>
</tr>
<tr>
<td></td>
<td><code>security address_filter mac_filter configure</code></td>
<td>Configure the source MAC address filter.</td>
</tr>
<tr>
<td></td>
<td><code>security address_filter mac_filter source add</code></td>
<td>Configure a new MAC source address.</td>
</tr>
<tr>
<td></td>
<td><code>security address_filter mac_filter source delete &lt;row id&gt;</code></td>
<td>Delete a MAC source address.</td>
</tr>
</tbody>
</table>
Table 8. Security mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>security bandwidth profile add</td>
<td>Configure a new bandwidth profile.</td>
</tr>
<tr>
<td></td>
<td>security bandwidth profile delete &lt;row id&gt;</td>
<td>Delete a bandwidth profile.</td>
</tr>
<tr>
<td></td>
<td>security bandwidth profile edit &lt;row id&gt;</td>
<td>Configure an existing bandwidth profile.</td>
</tr>
<tr>
<td></td>
<td>security bandwidth enable_bandwidth_profiles {Y</td>
<td>N}</td>
</tr>
<tr>
<td>content_filter</td>
<td>security content_filter block_group disable</td>
<td>Remove content filtering from groups.</td>
</tr>
<tr>
<td></td>
<td>security content_filter block_group enable</td>
<td>Apply content filtering to groups.</td>
</tr>
<tr>
<td></td>
<td>security content_filter blocked_keywords add</td>
<td>Configure a new blocked keyword.</td>
</tr>
<tr>
<td></td>
<td>security content_filter blocked_keywords delete &lt;row id&gt;</td>
<td>Delete a blocked keyword.</td>
</tr>
<tr>
<td></td>
<td>security content_filter blocked_keywords edit &lt;row id&gt;</td>
<td>Configure an existing blocked keyword.</td>
</tr>
<tr>
<td></td>
<td>security content_filter content_filtering configure</td>
<td>Configure web content filtering.</td>
</tr>
<tr>
<td></td>
<td>security content_filter trusted_domain add</td>
<td>Configure a new trusted domain.</td>
</tr>
<tr>
<td></td>
<td>security content_filter trusted_domain delete &lt;row id&gt;</td>
<td>Delete a trusted domain.</td>
</tr>
<tr>
<td></td>
<td>security content_filter trusted_domain edit &lt;row id&gt;</td>
<td>Configure an existing trusted domain.</td>
</tr>
<tr>
<td></td>
<td>security firewall advanced algs</td>
<td>Configure SIP support for the ALG.</td>
</tr>
<tr>
<td></td>
<td>security firewall attack_checks configure ipv4</td>
<td>Configure WAN and LAN security attack checks for IPv4 traffic.</td>
</tr>
<tr>
<td></td>
<td>security firewall attack_checks configure ipv6</td>
<td>Configure WAN security attack checks for IPv6 traffic.</td>
</tr>
<tr>
<td></td>
<td>security firewall attack_checks igmp configure</td>
<td>Enable or disable multicast pass-through for IPv4 traffic.</td>
</tr>
<tr>
<td></td>
<td>security firewall ipv4 add_rule dmz_wan inbound</td>
<td>Configure a new IPv4 DMZ WAN inbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td>security firewall ipv4 add_rule dmz_wan outbound</td>
<td>Configure a new IPv4 DMZ WAN outbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td>security firewall ipv4 add_rule lan_dmz inbound</td>
<td>Configure a new IPv4 LAN DMZ inbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td>security firewall ipv4 add_rule lan_dmz outbound</td>
<td>Configure a new IPv4 LAN DMZ outbound firewall rule.</td>
</tr>
</tbody>
</table>
### Table 8. Security mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>security firewall ipv4 add_rule lan_wan inbound</code></td>
<td>Configure a new IPv4 LAN WAN inbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 add_rule lan_wan outbound</code></td>
<td>Configure a new IPv4 LAN WAN outbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td>`security firewall ipv4 default_outbound_policy {Allow</td>
<td>Block}`</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 delete &lt;row id&gt;</code></td>
<td>Delete an IPv4 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 disable &lt;row id&gt;</code></td>
<td>Disable an IPv4 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 edit_rule dmz_wan inbound &lt;row id&gt;</code></td>
<td>Configure an existing IPv4 DMZ WAN inbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 edit_rule dmz_wan outbound &lt;row id&gt;</code></td>
<td>Configure an existing IPv4 DMZ WAN outbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 edit_rule lan_dmz inbound &lt;row id&gt;</code></td>
<td>Configure an existing IPv4 LAN DMZ inbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 edit_rule lan_dmz outbound &lt;row id&gt;</code></td>
<td>Configure an existing IPv4 LAN DMZ outbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 edit_rule lan_wan inbound &lt;row id&gt;</code></td>
<td>Configure an existing IPv4 LAN WAN inbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 edit_rule lan_wan outbound &lt;row id&gt;</code></td>
<td>Configure an existing IPv4 LAN WAN outbound firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv4 enable &lt;row id&gt;</code></td>
<td>Enable an IPv4 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv6 configure</code></td>
<td>Configure a new IPv6 firewall rule.</td>
</tr>
<tr>
<td></td>
<td>`security firewall ipv6 default_outbound_policy {Allow</td>
<td>Block}`</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv6 delete &lt;row id&gt;</code></td>
<td>Delete an IPv6 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv6 disable &lt;row id&gt;</code></td>
<td>Disable an IPv6 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv6 edit &lt;row id&gt;</code></td>
<td>Configure an existing IPv6 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall ipv6 enable &lt;row id&gt;</code></td>
<td>Enable an IPv6 firewall rule.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall session_limit configure</code></td>
<td>Configure global session limits.</td>
</tr>
<tr>
<td></td>
<td><code>security firewall session_settings configure</code></td>
<td>Configure global session time-outs.</td>
</tr>
<tr>
<td></td>
<td><code>security porttriggering_rules add</code></td>
<td>Configure a new port triggering rule.</td>
</tr>
<tr>
<td></td>
<td><code>security porttriggering_rules delete &lt;row id&gt;</code></td>
<td>Delete a port triggering rule.</td>
</tr>
<tr>
<td></td>
<td><code>security porttriggering_rules edit &lt;row id&gt;</code></td>
<td>Configure an existing port triggering rule.</td>
</tr>
</tbody>
</table>
Table 8. Security mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedules</td>
<td>security schedules edit {1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>security services add</td>
<td>Configure a new custom service.</td>
</tr>
<tr>
<td></td>
<td>security services delete &lt;row id&gt;</td>
<td>Delete a custom service.</td>
</tr>
<tr>
<td></td>
<td>security services edit &lt;row id&gt;</td>
<td>Configure an existing custom service.</td>
</tr>
<tr>
<td></td>
<td>security services ip_group add</td>
<td>Configure a new LAN or WAN IP group.</td>
</tr>
<tr>
<td></td>
<td>security services ip_group add_ip_to &lt;group name&gt;</td>
<td>Add an IP address to a LAN or WAN IP group.</td>
</tr>
<tr>
<td></td>
<td>security services ip_group delete &lt;row id&gt;</td>
<td>Delete a LAN or WAN IP group.</td>
</tr>
<tr>
<td></td>
<td>security services ip_group delete_ip &lt;row id&gt;</td>
<td>Remove an IP address from a LAN or WAN IP group.</td>
</tr>
<tr>
<td></td>
<td>security services ip_group edit &lt;row id&gt;</td>
<td>Configure an existing LAN or WAN IP group.</td>
</tr>
<tr>
<td></td>
<td>security services qos_profile add</td>
<td>Add a QoS profile.</td>
</tr>
<tr>
<td></td>
<td>security services qos_profile delete &lt;row id&gt;</td>
<td>Delete a QoS profile.</td>
</tr>
<tr>
<td></td>
<td>security services qos_profile edit &lt;row id&gt;</td>
<td>Configure an existing QoS profile.</td>
</tr>
<tr>
<td>upnp</td>
<td>security upnp configure</td>
<td>Configure UPnP.</td>
</tr>
</tbody>
</table>

Administrative and Monitoring Settings (System Mode) Configuration Commands

Enter the system ? command at the CLI prompt to display the submodes in the system mode. The following table lists the submodes and their commands in alphabetical order:

Table 9. System mode configuration commands

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging</td>
<td>system logging configure</td>
<td>Configure routing logs for accepted and dropped IPv4 and IPv6 packets.</td>
</tr>
<tr>
<td></td>
<td>system logging remote configure</td>
<td>Configure email logs and alerts, schedule email logs and alerts, and configure a syslog server.</td>
</tr>
</tbody>
</table>
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Table 9. System mode configuration commands (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_management</td>
<td>system remote_management https configure</td>
<td>Configure remote management over HTTPS.</td>
</tr>
<tr>
<td></td>
<td>system remote_management telnet configure</td>
<td>Configure remote management over Telnet.</td>
</tr>
<tr>
<td>snmp</td>
<td>system snmp sys configure</td>
<td>Configure the SNMP system information.</td>
</tr>
<tr>
<td>time</td>
<td>system time configure</td>
<td>Configure the system time, date, and NTP servers.</td>
</tr>
<tr>
<td>traffic_meter</td>
<td>system traffic_meter configure &lt;wan interface&gt;</td>
<td>Configure the WAN traffic meter.</td>
</tr>
</tbody>
</table>

VPN Settings (VPN Mode) Configuration Commands

Enter the `vpn ?` command at the CLI prompt to display the submodes in the vpn mode. The following table lists the submodes and their commands in alphabetical order:

Table 10. Configuration commands: vpn mode

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec</td>
<td>vpn ipsec ikepolicy configure &lt;ike policy name&gt;</td>
<td>Configure a new or existing manual IPSec IKE policy.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec ikepolicy delete &lt;ike policy name&gt;</td>
<td>Delete an IPSec policy.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec mode_config configure &lt;record name&gt;</td>
<td>Configure a new or existing Mode Config record.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec mode_config delete &lt;record name&gt;</td>
<td>Delete a Mode Config record.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec radius configure</td>
<td>Configure the RADIUS servers.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec vpnpolicy configure &lt;vpn policy name&gt;</td>
<td>Configure a new or existing auto IPSec VPN policy or manual IPSec VPN policy.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec vpnpolicy connect &lt;vpn policy name&gt;</td>
<td>Establish a VPN connection.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec vpnpolicy delete &lt;vpn policy name&gt;</td>
<td>Delete an IPSec VPN policy.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec vpnpolicy disable &lt;vpn policy name&gt;</td>
<td>Disable an IPSec VPN policy.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec vpnpolicy drop &lt;vpn policy name&gt;</td>
<td>Terminate an IPSec VPN connection.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec vpnpolicy enable &lt;vpn policy name&gt;</td>
<td>Enable an IPSec VPN policy.</td>
</tr>
<tr>
<td></td>
<td>vpn ipsec wizard configure &lt;Gateway</td>
<td>VPN_Client&gt;</td>
</tr>
<tr>
<td>l2tp</td>
<td>vpn l2tp server configure</td>
<td>Configure the L2TP server.</td>
</tr>
</tbody>
</table>
**Overview of the Configuration Commands**

## Overview of the Configuration Commands

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>pptp</td>
<td><code>vpn pptp server configure</code></td>
<td>Configure the PPTP server.</td>
</tr>
<tr>
<td>radius</td>
<td><code>vpn ipsec radius configure</code></td>
<td>Configure the RADIUS server.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn client ipv4</code></td>
<td>Configure the SSL client IPv4 address range.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn client ipv6</code></td>
<td>Configure the SSL client IPv6 address range.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn policy add</code></td>
<td>Configure a new SSL VPN policy.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn policy delete &lt;row id&gt;</code></td>
<td>Delete an SSL VPN policy.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn policy edit &lt;row id&gt;</code></td>
<td>Configure an existing SSL VPN policy.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portal_layouts add</code></td>
<td>Configure a new SSL VPN portal layout.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portal_layouts delete &lt;row id&gt;</code></td>
<td>Delete an SSL VPN portal layout.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portal_layouts edit &lt;row id&gt;</code></td>
<td>Configure an existing SSL VPN portal layout.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portal_layouts set-default &lt;row id&gt;</code></td>
<td>Configure the default SSL VPN portal layout.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portforwarding appconfig add</code></td>
<td>Configure a new SSL port forwarding application.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portforwarding appconfig delete &lt;row id&gt;</code></td>
<td>Delete an SSL VPN port forwarding application.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portforwarding hostconfig add</code></td>
<td>Configure a new host name for an SSL port forwarding application.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn portforwarding hostconfig delete &lt;row id&gt;</code></td>
<td>Delete a host name for an SSL port forwarding application.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn resource add</code></td>
<td>Add a new SSL VPN resource.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn resource configure add &lt;resource name&gt;</code></td>
<td>Configure an SSL VPN resource object.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn resource configure delete &lt;row id&gt;</code></td>
<td>Deletes an SSL VPN resource object.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn resource delete &lt;row id&gt;</code></td>
<td>Delete an SSL VPN resource.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn route add</code></td>
<td>Add an SSL VPN client route.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn route delete &lt;row id&gt;</code></td>
<td>Delete an SSL VPN client route.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn users domains add</code></td>
<td>Configure a new authentication domain.</td>
</tr>
<tr>
<td>sslvpn</td>
<td><code>vpn sslvpn users domains delete &lt;row id&gt;</code></td>
<td>Delete an authentication domain.</td>
</tr>
<tr>
<td>sslvpn</td>
<td>`vpn sslvpn users domains disable_Local_Authentication {Y</td>
<td>N}`</td>
</tr>
</tbody>
</table>
Table 10. Configuration commands: vpn mode (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslvpn (continued)</td>
<td>vpn sslvpn users domains edit &lt;row id&gt;</td>
<td>Configure an existing authentication domain.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users groups add</td>
<td>Configure a new authentication group.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users groups delete &lt;row id&gt;</td>
<td>Delete an authentication group.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users groups edit &lt;row id&gt;</td>
<td>Configure an existing authentication group.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users add</td>
<td>Add a new user account.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users browser_policies &lt;row id&gt;</td>
<td>Configure the client browsers from which a user is either allowed or denied access.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users delete &lt;row id&gt;</td>
<td>Delete a user account.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users edit &lt;row id&gt;</td>
<td>Configure an existing user account.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users ip_policies configure &lt;row id&gt;</td>
<td>Configure source IP addresses from which a user is either allowed or denied access.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users ip_policies delete &lt;row id&gt;</td>
<td>Delete a source IP address for a user.</td>
</tr>
<tr>
<td></td>
<td>vpn sslvpn users users login_policies &lt;row id&gt;</td>
<td>Configure the login policy for a user.</td>
</tr>
</tbody>
</table>
This chapter explains the configuration commands, keywords, and associated parameters in the net mode. The chapter includes the following sections:

- General WAN Commands
- IPv4 WAN Commands
- IPv6 WAN Commands
- IPv6 Tunnel Commands
- Dynamic DNS Commands
- IPv4 LAN Commands
- IPv6 LAN Commands
- IPv4 DMZ Setup Commands
- IPv6 DMZ Setup Commands
- WAN QoS Commands
- IPv4 Routing Commands
- IPv6 Routing Commands

**IMPORTANT:**

After you have issued a command that includes the word configure, add, or edit, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 12.

**General WAN Commands**

```
net wan port_setup configure <wan interface>
```

This command configures the advanced WAN settings for a WAN interface, that is, the MTU, port speed, MAC address, failure detection method, and upload and download settings of the VPN firewall. After you have issued the `net wan port_setup configure` command to specify one of the four WAN interfaces (that is, WAN1, WAN2, WAN3, or WAN4), you enter the `net-config [port_setup]` mode, and then you can configure the advanced settings for the specified interface in the order that you prefer.
Step 1 Format  
net wan port_setup configure <wan interface>

Mode  
net

Step 2 Format  
def_mtu {Default | Custom | mtu_size <number>}

def_mtu  

mtu_size  

Step 2 Format  
port_speed {Auto_Sense | 10_BaseT_Half_Duplex | 10_BaseT_Full_Duplex | 100_BaseT_Half_Duplex | 100_BaseT_Full_Duplex | 1000_BaseT_Full_Duplex}

mac_type {Use-Default-Mac | Use-This-Computers-Mac | Use-This-Mac | mac_address <mac address>}

failover_method type {None | WAN-DNS | CUSTOM-DNS | Ping | CUSTOM-DNS | CRM}

upload_download wan_conn_type {DSL | ADSL | T1 | T3 | Other}

upload_download upload_speed_type {56-Kbps | 128-Kbps | 256-Kbps | 384-Kbps | 512-Kbps | 768-Kbps | 1500-Kbps | 1544-Kbps | 10-Mbps | 44.736-Mbps | 100-Mbps | 1-Gbps | Custom | upload_download upload_speed <speed>}

upload_download download_speed_type {56-Kbps | 128-Kbps | 256-Kbps | 384-Kbps | 512-Kbps | 768-Kbps | 1500-Kbps | 1544-Kbps | 10-Mbps | 44.736-Mbps | 100-Mbps | 1-Gbps | Custom | upload_download download_speed <speed>}

Mode  
net-config [port_setup]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>def_mtu</td>
<td>Default or Custom</td>
<td>Specifies whether the default MTU or a custom MTU is used. If you select Custom, you need to issue the mtu_size keyword and specify the size of the MTU.</td>
</tr>
</tbody>
</table>
| mtu_size| number                                           | The size of the default MTU in bytes for the WAN port:  
• If you have configured IPv4 mode, type a number between 68 and 1500 bytes.  
• If you have configured IPv4/IPv6 mode, type a number between 1280 and 1500 bytes. |
## Port speed

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port_speed</td>
<td>Auto_Sense, 10_BaseT_Half_Duplex, 10_BaseT_Full_Duplex, 100_BaseT_Half_Duplex, 100_BaseT_Full_Duplex, or 1000_BaseT_Full_Duplex</td>
<td>Specifies the port speed and duplex mode of the WAN port. The keywords are self-explanatory.</td>
</tr>
</tbody>
</table>

## MAC address

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_type</td>
<td>Use-Default-Mac, Use-This-Computers-Mac, or Use-This-Mac</td>
<td>Specifies the source for the MAC address. The default setting is Use-Default-Mac. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, select either Use-This-Computers-Mac or select Use-This-Mac. If you select the latter keyword, you need to issue the mac_address keyword and specify the MAC address that is expected by your ISP.</td>
</tr>
<tr>
<td>mac_address</td>
<td></td>
<td>The MAC address that the ISP requires for MAC authentication when the mac_type keyword is set to Use-This-Mac.</td>
</tr>
</tbody>
</table>

## Failure detection method

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| failover_method type | None, WAN-DNS, CUSTOM-DNS, or Ping | Specifies the type of failover method for IPv4 connections. You can specify only one type of method:  
• None. There is no failover method configured.  
• WAN-DNS. DNS queries are sent to the DNS server that you configure through the `net wan wan ipv4 configure <wan interface>` command.  
• CUSTOM-DNS. DNS queries are sent to the DNS server that you need to specify with the failover_method dns_ipaddress_wan keyword.  
• Ping. Pings are sent to a server with a public IP address that you need to specify with the failover_method ping_ipaddress_wan keyword.  
For all three failover methods, you also need to issue the failover_method retry_interval keyword to specify and interval and the and failover_method retry_attempts keywords to specify the number of attempts. |
| failover_method retry_interval | seconds | The retry interval in seconds, from 5 to 999 seconds. The DNS query or ping is sent periodically after every test period. |
### Net Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Command example:**

```
SRX5308> net wan port_setup configure WAN1
net-config[port_setup]> def_mtu Custom
net-config[port_setup]> mtu_size 1498
net-config[port_setup]> port_speed 1000_BaseT_Full_Duplex
net-config[port_setup]> mac_type Use-This-Computers-Mac
net-config[port_setup]> failover_method type Ping
net-config[port_setup]> failover_method ping_ipaddress_wan 10.147.38.217
net-config[port_setup]> failover_method retry_interval 30
net-config[port_setup]> failover_method retry_attempts 4
net-config[port_setup]> upload_download wan_conn_type DSL
net-config[port_setup]> upload_download upload_speed_type 1-Gbps
```
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

```plaintext
net-config[port_setup]> upload_download download_speed_type 1-Gbps
net-config[port_setup]> save
```

Related show command: `show net wan port_setup <wan interface>`

---

**IPv4 WAN Commands**

**net wan_settings wanmode configure**

This command configures the mode of IPv4 routing between the WAN interface and LAN interfaces. After you have issued the `net wan_settings wanmode configure` command, you enter the `net-config [routing-mode]` mode, and then you can configure NAT or classical routing.

**WARNING!**

Changing the mode of IPv4 routing causes all LAN–WAN and DMZ–WAN inbound firewall settings to revert to default settings.

Step 1 Format: `net wan_settings wanmode configure`

Mode: `net`

Step 2 Format: `type {NAT | Classical_Routing}`

Mode: `net-config [routing-mode]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>NAT or Classical_Routing</td>
<td>Specifies the IPv4 routing mode.</td>
</tr>
</tbody>
</table>

Command example:

```
FVS318N> net wan_settings wanmode configure
net-config[routing-mode]> NAT
net-config[routing-mode]> save
```

Related show command: `show net wan_settings wanmode`
**Net Mode Configuration Commands**

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**net wan wan ipv4 configure <wan interface>**

This command configures the IPv4 settings for a WAN interface. After you have issued the `net wan wan ipv4 configure` command to specify one of the four WAN interfaces (that is, WAN1, WAN2, WAN3, or WAN4), you enter the net-config [wan-ipv4] mode. First, specify the ISP connection type (you can select only a single type). Then, for the selected ISP connection type, configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. If you select a static ISP connection type, there is no further configuration required.

**Step 1 Format**

```
net wan wan ipv4 configure <wan interface>
```

**Step 2 Format**

```
isp_connection_type {static | dhcp | pppoe | pptp} Yes
isp_login_required {Y | N}
```

- `static ip_address <ip_address>`
- `static subnet_mask <subnet_mask>`
- `static gateway_address <ip_address>`
- `static primary_dns <ip_address>`
- `static secondary_dns <ip_address>`

```
dhcpc account_name <account name>
dhcpc domain_name <domain name>
dhcpc client_identifier {Y | N}
dhcpc vendor_identifier {Y | N}
dhcpc get_dns_from_isp {Y | N} {dhcpc primary_dns <ipaddress>}
    {dhcpc secondary_dns <ipaddress>}
```

```
pppoe username <user name>
pppoe password <password>
pppoe AccountName <account name>
pppoe DomainName <domain name>
pppoe connectivity_type {keepalive | idletimeout {idletime <minutes>}}
```

```
pppoe connection_reset {N | Y} {reset_hour <hour>}
    {reset_min <minutes>} {delay_in_reset <seconds>}
```

```
pppoe get_ip_dynamically {Y | N} {static_ip <ipaddress>
    {subnet_mask <subnet_mask>}}
```

```
pppoe get_dns_from_isp {Y | N} {primary_dns <ipaddress>
    {secondary_dns <ipaddress>}}
```
Net Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

```
pptp username <user name>
pptp password <password>
pptp AccountName <account name>
pptp DomainName <domain name>
pptp connectivity_type {keepalive | idletimeout
   {pptp idle_time <seconds>}}
pptp my_address <ipaddress>
pptp server_address <ipaddress>
pptp get_dns_from_isp {Y | N {pptp primary_dns <ipaddress>
   [pptp secondary_dns <ipaddress>]}}
```

**Mode**
```
net-config [wan-ipv4]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isp_connection_type</td>
<td>static, dhcp, pppoe, or pptp</td>
<td>Specifies the type of ISP connection. You can specify only one type of connection:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• static. Configure the keywords and parameters in the STATIC section of this table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dhcp. Configure the keywords and parameters in the DHCPC section of this table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• pppoe. Configure the keywords and parameters in the PPPoE section of this table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• pptp. Configure the keywords and parameters in the PPTP section of this table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You need to confirm your selection by typing Yes (that is, Yes, and not just Y).</td>
</tr>
<tr>
<td>isp_login_required</td>
<td>Y or N</td>
<td>Enables or disables the ISP login requirement if the type of ISP connection is PPPoE or PPTP.</td>
</tr>
</tbody>
</table>

**Static**

- **static ip_address**
  - `ipaddress`
  - The static IP address.

- **static subnet_mask**
  - `subnet mask`
  - The subnet mask that is associated with the static IP address.

- **static gateway_address**
  - `ipaddress`
  - The IP address of the ISP gateway.

- **static primary_dns**
  - `ipaddress`
  - The IP address of the primary DNS server.

- **static secondary_dns**
  - `ipaddress`
  - The IP address of the optional secondary DNS server.
### Net Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCPC (These keywords consist of two separate words)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dhcpc account_name</td>
<td>account name</td>
<td>The ISP account name (alphanumeric string).</td>
</tr>
<tr>
<td>dhcpc domain_name</td>
<td>domain name</td>
<td>The ISP domain name (alphanumeric string).</td>
</tr>
<tr>
<td>dhcpc client_identifier</td>
<td>Y or N</td>
<td>Enables or disables the DHCP client-identifier option. If enabled, the DHCP client-identifier is sent to the ISP server. By default, the option is not sent.</td>
</tr>
<tr>
<td>dhcpc vendor_identifier</td>
<td>Y or N</td>
<td>Enables or disables the DHCP vendor-class-identifier option. If enabled, the DHCP vendor-class-identifier is sent to the ISP server. By default, the option is not sent.</td>
</tr>
<tr>
<td>dhcpc get_dns_from_isp</td>
<td>Y or N</td>
<td>Specifies whether or not the IP address of the DNS server is dynamically received from the ISP. If you select N, you need to issue the dhcpc primary_dns keyword and enter the IP address of the primary DNS server. For a secondary DNS server, issue the dhcpc secondary_dns keyword, and enter the IP address.</td>
</tr>
<tr>
<td>dhcpc primary_dns</td>
<td>ipaddress</td>
<td>The IP address of the primary DNS server if your IP address is not dynamically received from the ISP.</td>
</tr>
<tr>
<td>dhcpc secondary_dns</td>
<td>ipaddress</td>
<td>The IP address of the optional secondary DNS server if your IP address is not dynamically received from the ISP.</td>
</tr>
<tr>
<td><strong>PPPoE (These keywords consist of two separate words)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pppoe username</td>
<td>user name</td>
<td>The user name (alphanumeric string) to log in to the PPPoE service, if required.</td>
</tr>
<tr>
<td>pppoe password</td>
<td>password</td>
<td>The password (alphanumeric string) to log in to the PPPoE service, if required.</td>
</tr>
<tr>
<td>pppoe AccountName</td>
<td>account name</td>
<td>The PPPoE account name (alphanumeric string).</td>
</tr>
<tr>
<td>pppoe DomainName</td>
<td>domain name</td>
<td>The PPPoE domain name (alphanumeric string).</td>
</tr>
<tr>
<td>pppoe connectivity_type</td>
<td>keepalive or idletimeout</td>
<td>Specifies the type of PPPoE connection. If you select idletimeout, you need to issue the idletimeout keyword and enter the idle time-out in minutes.</td>
</tr>
<tr>
<td>pppoe idletime</td>
<td>minutes</td>
<td>The idle time-out period in minutes, from 5 to 999 minutes.</td>
</tr>
</tbody>
</table>
### Net Mode Configuration Commands

**pppoe connection_reset**  
Specifies whether or not the PPPoE connection is automatically reset. If it is reset, you need to issue the `reset_hour` and `reset_min` keywords and enter the hour and minutes after which the connection is reset. You also need to issue the `delay_in_reset` keyword and enter the number of seconds of delay.

- **Y** or **N**

**pppoe reset_hour**  
The hour at which the PPPoE connection is reset.

- **hour**

**pppoe reset_min**  
The minutes at which the PPPoE connection is reset.

- **minutes**

**pppoe delay_in_reset**  
After the connection has been reset, the number of seconds of delay before an PPPoE connection attempt is made.

- **seconds**

**pppoe get_ip_dynamically**  
Specifies whether or not the IP address is dynamically received from the ISP. If it is not, you need to issue the `static_ip` keyword and enter the static IP address, and issue the `subnet_mask` keyword and enter the subnet mask.

- **Y** or **N**

**pppoe static_ip**  
The static IP address if your IP address is not dynamically received from the ISP.

- **ipaddress**

**pppoe subnet_mask**  
The subnet mask if your IP address is not dynamically received from the ISP.

- **subnet mask**

**pppoe get_dns_from_isp**  
Specifies whether or not the IP address of the DNS server is dynamically received from the ISP. If you select **N**, you need to issue the `primary_dns` keyword and enter the IP address of the primary DNS server. For a secondary DNS server, issue the `secondary_dns` keyword, and enter the IP address.

- **Y** or **N**

**pppoe primary_dns**  
The IP address of the primary DNS server if your IP address is not dynamically received from the ISP.

- **ipaddress**

**pppoe secondary_dns**  
The IP address of the optional secondary DNS server if your IP address is not dynamically received from the ISP.

- **ipaddress**

**PPTP (These keywords consist of two separate words)**

**pptp username**  
The user name (alphanumeric string) to log in to the PPTP service, if required.

- **user name**
Command example:

SRX5308> net wan wan ipv4 configure WAN2
net-config[wan-ipv4]> isp_connection_type dhcp
net-config[wan-ipv4]> dhcpc client_identifier Y
net-config[wan-ipv4]> dhcpc get_dns_from_isp N
net-config[wan-ipv4]> dhcpc primary_dns 10.124.56.118
net-config[wan-ipv4]> dhcpc secondary_dns 10.124.56.132
net-config[wan-ipv4]> save
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Related show commands: *show net wan wan ipv4 setup <wan interface>* and *show net wan wan ipv4 status <wan interface>*

**net wan wan ipv4 secondary_address add <wan interface>**

This command configures a secondary IPv4 WAN address. After you have issued the `net wan wan ipv4 secondary_address add` command to specify one of the four WAN interfaces (that is, WAN1, WAN2, WAN3, or WAN4), you enter the net-config [wan-secondary-address] mode, and then you can configure the secondary WAN address and subnet mask in the order that you prefer.

| Step 1 Format | net lan ipv4 multi_homing add {WAN1 | WAN2 | WAN3 | WAN4} |
| Mode          | net |

| Step 2 Format | ip_address <ipaddress> |
| subnet_mask <subnet mask> |
| Mode          | net-config [wan-secondary-address] |

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>ipaddress</td>
<td>The secondary IPv4 address for the selected WAN interface.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>subnet mask</td>
<td>The subnet mask for the secondary IP address.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> net wan wan ipv4 secondary_address add WAN2
net-config[wan-secondary-address]> ip_address 10.168.50.1
net-config[wan-secondary-address]> subnet_mask 255.255.255.0
net-config[wan-secondary-address]> save

Related show commands: *show net wan wan ipv4 secondary_addresses <wan interface>*

**net wan wan ipv4 secondary_address delete <row id>**

This command deletes a secondary IPv4 WAN address by deleting its row ID.

| Format       | net wan wan ipv4 secondary_address delete <row id> |
| Mode         | net |

Related show commands: *show net wan wan ipv4 secondary_addresses <wan interface>*
**net wan_settings load_balancing configure**

This command configures the load balancing settings for two WAN interfaces that are configured for IPv4. After you have issued the `net wan_settings load_balancing configure` command, you enter the net-config [load-balancing] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `wan_mode_type` keyword determines which other keywords and parameters can you can apply.

---

**Note:** You can configure the load balancing settings only if the `net ipv6 ipmode configure` command is set to IPv4 Only.

---

**Step 1**  
**Format:** `net wan_settings load-balancing configure`  
**Mode:** `net`

**Step 2**  
**Format:**  
```
wan_mode_type {Primary-WAN | primary_wan_interface {WAN1 | WAN2 | WAN3 | WAN4} | auto_rollover {N | Y} | secondary_wan_interface {WAN1 | WAN2 | WAN3 | WAN4} | Load-Balancing | loadbal_algo {Round-Robin | Weighted-LB})
```

**Mode:** `net-config [load-balancing]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common settings</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| `wan_mode_type`    | `Primary-WAN` or `Load-Balancing`               | Specifies the load balancing settings:  
  • **Primary-WAN**. One WAN interface is made the primary interface. The other three interfaces are disabled. As an option, another WAN interface can be made the rollover link. The remaining two interfaces are disabled. Configure the keywords and parameters in the Primary WAN mode and auto-rollover mode settings section of this table.  
  • **Load-Balancing**. The VPN firewall distributes the outbound traffic equally among the WAN interfaces that are functional. Configure the keywords and parameters in the Load balancing settings section of this table, that is, issue the `loadbal_algo` keyword and specify the load balancing method. |
| `primary_wan_interface` | `WAN1, WAN2, WAN3, or WAN4` | Specifies the interface that functions as the primary WAN interface. |
**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**Net Mode Configuration Commands**

### Net WAN Settings Configuration

#### Command example:

```
SRX5308> net wan_settings load_balancing configure WAN1
net-config[load-balancing]> wan_mode_type Primary-WAN
net-config[load-balancing]> primary_wan_interface WAN1
net-config[load-balancing]> auto_rollover Y
net-config[load-balancing]> secondary_wan_interface WAN2
net-config[load-balancing]> save
```

**Related show command:** `show net wan port_setup <wan interface>`

---

**net protocol_binding add**

This command configures a new protocol binding, that is, it binds a service to a WAN interface. After you have issued the `net protocol_binding add` command, you enter the net-config [protocol-binding] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>net protocol_binding add</td>
<td>net</td>
</tr>
</tbody>
</table>
Step 2 Format  
\[\text{service}_\text{name} \{\text{default}_\text{services} \text{<default service name>} | \{\text{custom}_\text{services} \text{<custom service name>}\}\right\}\]

local gateway [WAN1 | WAN2 | WAN3 | WAN4]

source_network_type [address_wise {ANY | SINGLE_ADDRESS
  \{source_network_start_ip \text{<ipaddress>}\} | ADDRESS_RANGE
  \{source_network_start_ip \text{<ipaddress>}\}
  \{source_network_end_ip \text{<ipaddress>}\}]} | group_wise
  \{group \text{name}\}

destination_network_type [address_wise {ANY | SINGLE_ADDRESS
  \{destination_network_start_ip \text{<ipaddress>}\} | ADDRESS_RANGE
  \{destination_network_start_ip \text{<ipaddress>}\}
  \{destination_network_end_ip \text{<ipaddress>}\}]} | group_wise
  \{group \text{name}\}

Mode  net-config [protocol-binding]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_name</td>
<td>ANY, AIM, BGP, BOOTP_CLIENT, BOOTP_SERVER,</td>
<td>Specifies the default service and protocol to which the protocol binding</td>
</tr>
<tr>
<td>default_services</td>
<td>CU-SEEEME:UDP, CU-SEEEME:TCP, DNS:UDP, DNS:TCP,</td>
<td>applies.</td>
</tr>
<tr>
<td></td>
<td>FINGER, FTP, HTTP, HTTPS, ICMP-TYPE-3, ICMP-TYPE-4,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICMP-TYPE-5, ICMP-TYPE-6, ICMP-TYPE-7, ICMP-TYPE-8,</td>
<td></td>
</tr>
<tr>
<td>service_name</td>
<td>custom_service name</td>
<td>The custom service that you have configured with the security services add</td>
</tr>
<tr>
<td>custom_services</td>
<td></td>
<td>command and to which the protocol binding applies.</td>
</tr>
</tbody>
</table>
### Keyword

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_gateway</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the interface to which the service is bound.</td>
</tr>
<tr>
<td>source_network_type</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN source address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>address_wise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source_network_start_ip</td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td>source_network_end_ip</td>
<td>ipaddress</td>
<td>• The IP address if the source_network_type address_wise keywords are set to SINGLE_ADDRESS.</td>
</tr>
<tr>
<td>destination_network_type</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN destination address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>address_wise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source_network_start_ip</td>
<td>ipaddress</td>
<td>• The start IP address if the source_network_type address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>destination_network_start_ip</td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td>destination_network_end_ip</td>
<td>ipaddress</td>
<td>• The IP address if the source_network_type address_wise keywords are set to SINGLE_ADDRESS.</td>
</tr>
<tr>
<td>source_network_end_ip</td>
<td>ipaddress</td>
<td>• The start IP address if the source_network_type address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
</tbody>
</table>

**Description**

- **local_gateway**: Specifies the interface to which the service is bound.
- **source_network_type**: Specifies the type of LAN source address. The address_wise and group_wise keywords are mutually exclusive.
- **source_network_start_ip**: There are two options:
  - The IP address if the source_network_type address_wise keywords are set to SINGLE_ADDRESS.
  - The start IP address if the source_network_type address_wise keywords are set to ADDRESS_RANGE.
- **source_network_end_ip**: The end IP address if the source_network_type address_wise keywords are set to ADDRESS_RANGE.
- **source_network_type group_wise**: The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the `net lan lan_groups edit <row id> <new group name>` command. The LAN IP group name is a name that you have specified with the `security services ip_group add` command.
- **destination_network_type**: Specifies the type of WAN destination address. The address_wise and group_wise keywords are mutually exclusive.
- **destination_network_start_ip**: There are two options:
  - The IP address if the source_network_type address_wise keywords are set to SINGLE_ADDRESS.
  - The start IP address if the source_network_type address_wise keywords are set to ADDRESS_RANGE.
**Net Mode Configuration Commands**

---

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**Command example:**

SRX5308> `net protocol_binding add`
net-config[protocol-binding]> `service_name default_services FTP`
net-config[protocol-binding]> `local_gateway WAN1`
net-config[protocol-binding]> `source_network_type address_wise ANY`
net-config[protocol-binding]> `destination_network_type address_wise SINGLE_ADDRESS`
net-config[protocol-binding]> `destination_network_start_ip 10.122.178.214`
net-config[protocol-binding]> `save`

Related show command: `show net protocol_binding setup`

---

**net protocol_binding edit <row id>**

This command configures an existing protocol binding, that is, it binds a service to a WAN interface. After you have issued the `net protocol_binding edit` command to specify the row to be edited, you enter the net-config [protocol-binding] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

Mode: `net`

---

**Net Mode Configuration Commands**

42
Step 2 Format

```
service_name {default_services <default service name> | 
  [custom_services <custom service name>]}
local_gateway | WAN1 | WAN2 | WAN3 | WAN4
source_network_type {address_wise {ANY | SINGLE_ADDRESS
  {source_network_start_ip <ipaddress> | ADDRESS_RANGE
  {source_network_start_ip <ipaddress>}
  {source_network_end_ip <ipaddress>}} | group_wise
  <group name>}
destination_network_type {address_wise {ANY | SINGLE_ADDRESS
  {destination_network_start_ip <ipaddress> | ADDRESS_RANGE
  {destination_network_start_ip <ipaddress>}
  {destination_network_end_ip <ipaddress>}} | group_wise
  <group name>}
```

Mode

```
net-config [protocol-binding]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_name custom_services</td>
<td>custom service name</td>
<td>The custom service that you have configured with the security services add command and to which the protocol binding applies.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>local_gateway</code></td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the interface to which the service is bound.</td>
</tr>
<tr>
<td><code>source_network_type</code></td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN source address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><code>source_network_start_ip</code></td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The IP address if the <code>source_network_type address_wise</code> keywords are set to <code>SINGLE_ADDRESS</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The start IP address if the <code>source_network_type address_wise</code> keywords are set to <code>ADDRESS_RANGE</code>.</td>
</tr>
<tr>
<td><code>source_network_end_ip</code></td>
<td>ipaddress</td>
<td>The end IP address if the <code>source_network_type address_wise</code> keywords are set to <code>ADDRESS_RANGE</code>.</td>
</tr>
<tr>
<td><code>source_network_type group_wise</code></td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that you have specified with the <code>net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt;</code> command. The LAN IP group name is a name that you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>have specified with the <code>security services ip_group add</code> command. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><code>destination_network_type</code></td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN destination address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><code>destination_network_start_ip</code></td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The IP address if the <code>source_network_type address_wise</code> keywords are set to <code>SINGLE_ADDRESS</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The start IP address if the <code>source_network_type address_wise</code> keywords are set to <code>ADDRESS_RANGE</code>.</td>
</tr>
</tbody>
</table>
### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Net Mode Configuration Commands**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination_network_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the source_network_type address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>destination_network_type</td>
<td>group name</td>
<td>The name of the WAN IP group. The WAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>

**Related show command:** `show net protocol_binding setup`

**net protocol_binding delete**

This command deletes a protocol binding by deleting its row ID.

**Format**  
`net protocol_binding delete <row id>`

**Mode**  
net

**Related show command:** `show net protocol_binding setup`

---

**net protocol_binding disable**

This command disables a protocol binding by specifying its row ID.

**Format**  
`net protocol binding disable <row id>`

**Mode**  
security

**Related show command:** `show net protocol_binding setup`
**Net protocol_binding enable**

This command enables a protocol binding by specifying its row ID.

**Format**
```
net protocol binding enable <row id>
```

**Mode**
security

**Related show command:** `show net protocol_binding setup`

---

**IPv6 WAN Commands**

**net ipv6 ipmode configure**

This command configures the IPv6 mode. After you have issued the `net ipv6 ipmode configure` command, you enter the net-config [mode] mode, and then you can configure the IP mode. You can select support for IPv4 only or for both IPv4 and IPv6.

⚠️ **WARNING!**

Changing the IP mode causes the VPN firewall to reboot.

**Step 1**
**Format**
```
net ipv6 ipmode configure
```

**Mode**
net

**Step 2**
**Format**
```
ip_type {IPv4_Only | IPv4/IPv6}
```

**Mode**
net-config [mode]

**Keyword | Associated Keyword to Select | Description**
--- | --- | ---

| ip_type | IPv4_Only or IPv4/IPv6 | Specifies the IPv6 routing mode. |

**Command example:**
```
FVS318N> net ipv6 ipmode configure
net-config[mode]> ip_type IPv4/IPv6
net-config[mode]> save
```

**Related show command:** `show net ipv6 ipmode setup`
**net wan wan ipv6 configure <wan interface>**

This command configures the IPv6 settings for a WAN interface. After you have issued the `net wan wan ipv6 configure` command to specify one of the four WAN interfaces (that is, WAN1, WAN2, WAN3, or WAN4), you enter the `net-config [wan-ipv6]` mode. First, specify the ISP connection type (you can select only a single type). Then, for the selected ISP connection type, configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
net wan wan ipv6 configure
```

**Step 2 Format**

```
isp type {STATIC | DHCPC | PPPoE}
```

```
static ip_address <ipv6-address>
static prefix <prefix-length>
static gateway_address <ipv6-address>
static primary_dns <ipv6-address>
static secondary_dns <ipv6-address>
```

```
dhcpc stateless_mode_enable {StatelessAddrAutoConfig
| prefix_delegation_enable {Y | N} | StatefulAddrAutoConfig}
```

```
pppoe user_name <user name>
pppoe password <password>
pppoe dhcpv6_option {Disable-DHCPv6 {pppoe primary_dns <ipv6-address> | pppoe secondary_dns <ipv6-address>} | DHCPv6-StatelessMode | DHCPv6-StatefulMode | DHCPv6-Prefix-Delegation}
```

**Mode**

```
net-config [wan-ipv6]
```

<table>
<thead>
<tr>
<th>Keyword (consists of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| isp type                               | STATIC, DHCPC, or PPPoE                         | Specifies the type of ISP connection:  
  • STATIC. Configure the keywords and parameters in the Static section of this table.  
  • DHCPC. Configure the keywords and parameters in the DHCPC section of this table.  
  • PPPoE. Configure the keywords and parameters in the PPPoE section of this table. |
<table>
<thead>
<tr>
<th>Keyword (consists of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static ip_address</td>
<td>ipv6-address</td>
<td>The IPv6 address of the WAN interface.</td>
</tr>
<tr>
<td>static prefix</td>
<td>prefix-length</td>
<td>The prefix length (integer) for the static address.</td>
</tr>
<tr>
<td>static gateway_address</td>
<td>ipv6-address</td>
<td>The IPv6 address of the gateway.</td>
</tr>
<tr>
<td>static primary_dns</td>
<td>ipv6-address</td>
<td>The IPv6 address of the primary DNS server.</td>
</tr>
<tr>
<td>static secondary_dns</td>
<td>ipv6-address</td>
<td>The IPv6 address of the secondary DNS server.</td>
</tr>
<tr>
<td>DHCPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dhcpc stateless_mode_enable</td>
<td>StatelessAddrAutoConfig or StatefulAddrAutoConfig</td>
<td>Specifies the type of DHCPv6 mode (stateless or stateful). If you set the dhcpc stateless_mode_enable keywords to StatelessAddrAutoConfig, you have the option to set the dhcpc prefix_delegation_enable keywords and associated parameter.</td>
</tr>
<tr>
<td>prefix_delegation_enable</td>
<td>Y or N</td>
<td>Enables or disables prefix delegation if the dhcpc stateless_mode_enable keywords are set to StatelessAddrAutoConfig. Prefix delegation allows the ISP's stateful DHCPv6 server to assign a prefix.</td>
</tr>
<tr>
<td>PPPoE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pppoe user_name</td>
<td>user name</td>
<td>The PPPoE user name that is provided by the ISP.</td>
</tr>
<tr>
<td>pppoe password</td>
<td>password</td>
<td>The PPPoE password that is provided by the ISP.</td>
</tr>
</tbody>
</table>
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (consists of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| pppoe dhcpv6_option                     | Disable-DHCPv6, DHCPv6-StatelessMode, DHCPv6-StatefulMode, or DHCPv6-Prefix-Delegation | Specifies the DHCPv6 server options for the PPPoE configuration:  
  * Disable-DHCPv6. DHCPv6 is disabled. You need to issue the pppoe primary_dns and pppoe secondary_dns keywords and specify DNS servers to receive an IP address from the ISP.  
  * DHCPv6-StatelessMode. The VPN firewall generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from the ISP's DHCPv6 server. Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed by combining this prefix and the MAC address of the WAN port. The IP address is a dynamic address.  
  * DHCPv6-StatefulMode. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from the ISP's DHCPv6 server. The IP address is a dynamic address.  
  * DHCPv6-Prefix-Delegation. The VPN firewall obtains a prefix from the ISP's DHCPv6 server through prefix delegation. The VPN firewall's own stateless DHCPv6 server can assign this prefix to its IPv6 LAN clients. |
| pppoe primary_dns                       | ipv6-address                                   | The IPv6 address of the primary DNS server if the DHCPv6 server option is Disable-DHCPv6. |
| pppoe secondary_dns                     | ipv6-address                                   | The IPv6 address of the secondary DNS server if the DHCPv6 server option is Disable-DHCPv6. |

**Command example:**

SRX5308> net wan wan ipv6 configure WAN2  
net-config[wan-ipv6]> isp type DHCP  
net-config[wan-ipv6]> dhcpc stateless_mode_enable StatelessAddrAutoConfig  
net-config[wan-ipv6]> prefix_delegation_enable Y  
net-config[wan-ipv6]> save
Related show commands: `show net wan wan ipv6 setup <wan interface>` and `show net wan wan ipv6 status <wan interface>`

**net siit configure**

This command enables and configures Stateless IP/ICMP Translation (SIIT). After you have issued the `net siit configure` command, you enter the net-config [siit] mode, and then you can enable SIIT and configure the IPv4 address.

<table>
<thead>
<tr>
<th>Step 1 Format</th>
<th>net siit configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>net</td>
</tr>
</tbody>
</table>

**Step 2 Format**

```plaintext
enable {Y | N}  
ipv4_address <ipaddress>
```

<table>
<thead>
<tr>
<th>Mode</th>
<th>net-config [siit]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables SIIT.</td>
</tr>
<tr>
<td>ipv4_address</td>
<td>subnet mask</td>
<td>The IPv4 address for the SIIT configuration.</td>
</tr>
</tbody>
</table>

**Command example:**

```plaintext
SRX5308> net siit configure  
net-config[siit]> enable Y  
net-config[siit]> ipv4_address 192.168.5.117  
net-config[siit]> save
```

**Related show command:** `show net siit setup`

---

**IPv6 Tunnel Commands**

**net ipv6_tunnel isatap add**

This command configures a new ISATAP tunnel. After you have issued the `net ipv6_tunnel isatap add` command, you enter the net-config [isatap-tunnel] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.
Note: To be able to configure an ISATAP tunnel, you first need to set the IP mode to IPv4/IPv6 (see net ipv6 ipmode configure).

Command example:
SRX5308> net ipv6_tunnel isatap add
net-config[isatap-tunnel]> subnet_prefix 2004::
net-config[isatap-tunnel]> end_point_type Other_IP [ipv4_address 10.29.33.4]
net-config[isatap-tunnel]> save

Related show commands: show net ipv6_tunnel setup and show net ipv6_tunnel status

net ipv6_tunnel isatap edit <row id>

This command configures an existing ISATAP tunnel. After you have issued the net ipv6_tunnel isatap edit command to specify the row to be edited, you enter the net-config [isatap-tunnel] mode, and then you can change the subnet prefix only.

Step 1 Format net ipv6_tunnel isatap edit <row id>
Mode net

### Keyword | Associated Keyword to Select or Parameter to Type | Description
--- | --- | ---
subnet_prefix | subnet prefix | The IPv6 64-bit subnet prefix (string) that is assigned to the logical ISATAP subnet for this intranet.
end_point_type | LAN or Other_IP | Specifies the local endpoint IP address for the tunnel that is initiated on the VPN firewall. The endpoint can be the LAN interface or a specific LAN IPv4 address. If you select Other_IP, you also need to issue the ipv4_address keyword to specify an IPv4 address.
ipv4_address | ipaddress | The IPv4 address of a local endpoint that is not a LAN IPv4 address.
Step 2  Format  `subnet_prefix <subnet prefix>`  
Mode  `net-config [isatap-tunnel]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>subnet_prefix</code></td>
<td><code>subnet prefix</code></td>
<td>The IPv6 64-bit subnet prefix (string) that is assigned to the logical ISATAP subnet for this intranet.</td>
</tr>
</tbody>
</table>

Related show commands: `show net ipv6_tunnel setup` and `show net ipv6_tunnel status`

`net ipv6_tunnel isatap delete <row id>`

This command deletes an ISATAP tunnel by deleting its row ID.

**Note:** To be able to delete an ISATAP tunnel, you first need to set the IP mode to IPv4/IPv6 (see `net ipv6 ipmode configure`).

Format  `net ipv6_tunnel isatap delete <row id>`  
Mode  `net`

Related show commands: `show net ipv6_tunnel setup` and `show net ipv6_tunnel status`

`net ipv6_tunnel six_to_four configure`

This command enables or disables automatic tunneling, which allows traffic from an IPv6 LAN to be tunneled through an IPv4 WAN to reach an IPv6 network. After you have issued the `net ipv6_tunnel six_to_four configure` command, you enter the net-config [six-to-four-tunnel] mode, and then you can configure automatic tunneling.

Step 1  Format  `net ipv6_tunnel six_to_four configure`  
Mode  `net`

Step 2  Format  `automatic_tunneling_enable {Y | N}`  
Mode  `net-config [six-to-four-tunnel]`
**Net Mode Configuration Commands**

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**Command example:**

```
FVS318N> net ipv6_tunnel six_to_four configure
net-config[six-to-four-tunnel]> automatic_tunneling_enable Y
net-config[six-to-four-tunnel]> save
```

**Related show commands:** *show net ipv6_tunnel setup* and *show net ipv6_tunnel status*

---

**Dynamic DNS Commands**

`net ddns configure`

This command enables, configures, or disables Dynamic DNS (DDNS) service. After you have issued the `net ddns configure` command, you enter the net-config [ddns] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. Before you specify a keyword, you need to specify the WAN interface to which the configuration applies.

**Step 1 Format**

```
net ddns configure
```

**Mode**

```
et`
```

**Step 2 Format**

```
{wan1 | wan2 | wan3 | wan4} enable {Disable | DynDNS | TZO | DNS_Oray | 3322_DDNS}
{wan1 | wan2 | wan3 | wan4} hostname <host name>
{wan1 | wan2 | wan3 | wan4} username <user name>
{wan1 | wan2 | wan3 | wan4} password <password>
{wan1 | wan2 | wan3 | wan4} wild_flag_enable {Y | N}
{wan1 | wan2 | wan3 | wan4} time_update_enable {Y | N}
```

**Mode**

```
net-config [ddns]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{wan1</td>
<td>wan2</td>
<td>wan3</td>
</tr>
<tr>
<td>{wan1</td>
<td>wan2</td>
<td>wan3</td>
</tr>
</tbody>
</table>
Command example:

SRX5308> net ddns configure
net-config[ddns]> wan2 enable DynDNS
net-config[ddns]> wan2 hostname adminnetgear.dyndns.org
net-config[ddns]> wan2 username jaybrown
net-config[ddns]> wan2 password 4hg!RA278s
net-config[ddns]> wan2 wild_flag_enable N
net-config[ddns]> wan2 time_update_enable Y
net-config[ddns]> save

Related show command: show net ddns setup

IPv4 LAN Commands

net lan ipv4 configure <vlan id>

This command configures a new or existing VLAN, that is, a VLAN ID and a VLAN profile. After you have issued the net lan ipv4 configure command to specify a new or existing VLAN ID, you enter the net-config [lan-ipv4] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 Format net lan ipv4 configure <vlan id>

Mode net
Step 2 Format

```
profile_name <name>
port_membership {port 1 [Y | N]} | {port 2 [Y | N]} | {port 3 [Y | N]} | {port 4 [Y | N]}
static address <ipaddress>
static subnet_mask <subnet mask>
dhcp mode {None | DHCP-Server | DHCP-Relay}
proxy dns_enable {Y | N}
dhcp domain_name <domain name>
dhcp start_address <ipaddress>
dhcp end_address <ipaddress>
dhcp primary_dns <ipaddress>
dhcp secondary_dns <ipaddress>
dhcp wins_server <ipaddress>
dhcp lease_time <hours>
enable_ldap {Y | N}
ldap_serverip <ipaddress>
ldap_search_base <search base>
ldap_port <number>
dhcp relay_gateway <ipaddress>
inter_vlan_routing {Y | N}
```

Mode

```
net-config [lan-ipv4]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>name</td>
<td>The name of the VLAN profile.</td>
</tr>
<tr>
<td>port_membership port1</td>
<td>ipaddress</td>
<td>Specifies whether or not the port is a member of the VLAN. You need to specify each port individually.</td>
</tr>
<tr>
<td>port_membership port2</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>port_membership port3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>port_membership port4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static address</td>
<td></td>
<td>The static IPv4 address for the VLAN.</td>
</tr>
<tr>
<td>static subnet_mask</td>
<td></td>
<td>The IPv4 subnet mask for the VLAN profile.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| dhcp_mode                                     | None, DHCP-Server, or DHCP-Relay                 | Specifies the DHCP mode for the devices that are connected to the VLAN:  
• None. The DHCP server is disabled. No further DHCP configuration is required.  
• DHCP-Server. Configure the keywords and parameters in the DHCP server section of this table.  
• DHCP-Relay. Configure the keywords and parameters in the DHCP relay section of this table. |
| proxy_dns_enable                              | Y or N                                          | Enables or disables the LAN DNS proxy. |
| inter_vlan_routing                            | Y or N                                          | Enables or disables inter-VLAN routing. |

### DHCP Server

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp_domain_name</td>
<td>domain name</td>
<td>The FQDN or domain name of the DHCP server.</td>
</tr>
<tr>
<td>dhcp_start_address</td>
<td>ipaddress</td>
<td>The start IP address for the DHCP address range.</td>
</tr>
<tr>
<td>dhcp_end_address</td>
<td>ipaddress</td>
<td>The end IP address for the DHCP address range.</td>
</tr>
<tr>
<td>dhcp_primary_dns</td>
<td>ipaddress</td>
<td>The IP address of the primary DNS server for the DHCP server.</td>
</tr>
<tr>
<td>dhcp_secondary_dns</td>
<td>ipaddress</td>
<td>The IP address of the secondary DNS server for the DHCP server.</td>
</tr>
<tr>
<td>dhcpWins_server</td>
<td>ipaddress</td>
<td>The IP address of the WINS server for the DHCP server.</td>
</tr>
<tr>
<td>dhcp_lease_time</td>
<td>hours</td>
<td>The DHCP lease time in hours.</td>
</tr>
<tr>
<td>enable_ldap</td>
<td>Y or N</td>
<td>Enables or disables LDAP.</td>
</tr>
<tr>
<td>ldap_serverip</td>
<td>ipaddress</td>
<td>The IP address of the LDAP server.</td>
</tr>
<tr>
<td>ldap_search_base</td>
<td>search base</td>
<td>The search base (string) for LDAP</td>
</tr>
<tr>
<td>ldap_port</td>
<td>number</td>
<td>The port number for the LDAP server.</td>
</tr>
</tbody>
</table>

### DHCP Relay

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcprelay_gateway</td>
<td>ipaddress</td>
<td>The IP address of the DHCP relay gateway.</td>
</tr>
</tbody>
</table>

**Command example:**

SRX5308> net lan ipv4 configure 4  
net-config[lan-ipv4]> profile_name Marketing  
net-config[lan-ipv4]> port_membership port 1 Y  
net-config[lan-ipv4]> port_membership port 3 Y  
net-config[lan-ipv4]> port_membership port 4 Y
net-config[lan-ipv4]> static address 192.168.1.1
net-config[lan-ipv4]> static subnet_mask 255.255.255.0
net-config[lan-ipv4]> dhcp mode DHCP-Relay
net-config[lan-ipv4]> proxy dns_enable N
net-config[lan-ipv4]> inter_vlan_routing Y
net-config[lan-ipv4]> save

Related show command: show net lan ipv4 setup

net lan ipv4 delete <vlan id>
This command deletes a VLAN by deleting its ID. You cannot delete VLAN 1, the default VLAN.

Format net lan ipv4 delete <vlan id>
Mode net

Related show command: show net lan ipv4 setup

net lan ipv4 disable <vlan id>
This command disables a VLAN by specifying its ID. You cannot disable VLAN 1, the default VLAN.

Format net lan ipv4 disable <vlan id>
Mode net

Related show command: show net lan ipv4 setup

net lan ipv4 enable <vlan id>
This command enables a VLAN by specifying its ID. VLAN 1, the default VLAN, is always enabled.

Format net lan ipv4 enable <vlan id>
Mode net
**Related show command:** `show net lan ipv4 setup`

---

**net ethernet configure <interface name or number>**

This command configures a VLAN for a LAN interface. After you have issued the `net ethernet configure` command to specify a LAN interface, you enter `net-config [ethernet]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
net ethernet configure <interface name or number>
```

**Mode**

net

**Step 2 Format**

```
vlanid <number>
vlan-enable {Y | N}
native-vlan {Y | N}
```

**Mode**

net-config [ethernet]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlanid</td>
<td>number</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>vlan-enable</td>
<td>Y or N</td>
<td>Enables or disables the VLAN for this interface.</td>
</tr>
<tr>
<td>native-vlan</td>
<td>Y or N</td>
<td>Enables or disables the default (native) VLAN for this interface.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> net ethernet configure eth0
net-config[ethernet]> vlanid 12
net-config[ethernet]> vlan-enable Y
net-config[ethernet]> native-vlan N
net-config[ethernet]> save
```

---

**Note:** To enter the `net-config [ethernet]` mode, you can issue the `net ethernet configure` command with either an interface name such as `eth0` or an interface number such as `0`.

---

**Related show command:** `show net ethernet {interface name | all}`
net lan ipv4 default_vlan

This command configures the default VLAN for each port. After you have issued the `net lan ipv4 default_vlan` command, you enter the net-config [lan-ipv4-defvlan] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1  Format  net lan ipv4 default_vlan  
Mode   net

Step 2  Format  
port1 <vlan name>
port2 <vlan name>
port3 <vlan name>
port4 <vlan name>

Mode   net-config [lan-ipv4-defvlan]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>port2</td>
<td>&lt;vlan name&gt;</td>
<td></td>
</tr>
<tr>
<td>port3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>port4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Command example:

SRX5308> net lan ipv4 default_vlan
net-config[lan-ipv4-defvlan]> port1 Default
net-config[lan-ipv4-defvlan]> port2 Default
net-config[lan-ipv4-defvlan]> port3 Management
net-config[lan-ipv4-defvlan]> port4 Sales
net-config[lan-ipv4-defvlan]> save

Related show command: `show net lan ipv4 setup`

net lan ipv4 advanced configure

This command configures advanced LAN settings such as the MAC address for VLANs and ARP broadcast. After you have issued the `net lan ipv4 advanced configure` command, you enter the net-config [lan-ipv4-adv] mode, and then you can configure one
keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**  Format  net lan ipv4 advanced configure

  Mode  net

**Step 2**  Format  vlan_mac_offset_type {Same | Unique}

  enable_arp_broadcast {Y | N}

  Mode  net-config [lan-ipv4-adv]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
</table>
| vlan_mac_offset_type    | Same or Unique               | Specifies the MAC address for VLANs:
|                         |                              | • **Same**. All VLAN profiles use the same MAC address as the LAN ports. (All LAN ports share the same MAC address.)                          |
|                         |                              | • **Unique**. Each VLAN (up to 16 VLANs) is assigned a unique MAC address.                                                                     |
| enable_arp_broadcast    | Y or N                       | Enables or disables ARP broadcast.                                                                                                           |

**Command example:**

SRX5308> net lan ipv4 advanced configure
net-config[lan-ipv4-adv]> vlan_mac_offset_type Same
net-config[lan-ipv4-adv]> enable_arp_broadcast Y
net-config[lan-ipv4-adv]> save

**Related show command:** show net lan ipv4 advanced setup

---

**net lan dhcp reserved_ip configure <mac address>**

This command binds a MAC address to an IP address for DHCP reservation or lets you edit an existing binding. The command also assigns the device or computer to which the MAC address belongs to one of eight LAN groups. After you have issued the **net lan dhcp reserved_ip configure** command to configure the MAC address, you enter the net-config [dhcp-reserved-ip] mode, and then you can configure the IP address for the binding configuration.

**Step 1**  Format  net lan dhcp reserved_ip configure <mac address>

  Mode  net
**Step 2 Format**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_mac_name</td>
<td>device name</td>
<td>The name of the computer or device.</td>
</tr>
<tr>
<td>ip_addr_type</td>
<td>Fixed_set_on_PC or Dhcp_Reserved_IP</td>
<td>Specifies the IP address type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed_set_on_PC. The IP address is statically assigned on the computer or device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dhcp_Reserved_IP. The DHCP server of the wireless VPN firewall always assigns the specified IP address to this client during the DHCP negotiation.</td>
</tr>
<tr>
<td>ip_address</td>
<td>ipaddress</td>
<td>The IP address that needs to be bound to the specified MAC address. The IP address needs to be in the IP subnet of the VLAN to which the computer or device is assigned.</td>
</tr>
<tr>
<td>group_name</td>
<td>Group1, Group2, Group3, Group4, Group5, Group6, Group7, or Group8, or custom group name</td>
<td>Specifies the group to which the computer or device needs to be assigned. You can also enter a custom group name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command.</td>
</tr>
<tr>
<td>vlan_profile</td>
<td>vlan name</td>
<td>The name of the VLAN to which the computer or device needs to be assigned.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> net lan dhcp reserved_ip configure AA:BB:CC:1A:2B:3C
net-config[dhcp-reserved-ip]> ip_addr_type Dhcp_Reserved_IP
net-config[dhcp-reserved-ip]> ip_address 192.168.27.219
net-config[dhcp-reserved-ip]> group_name Group3
net-config[dhcp-reserved-ip]> vlan_profile Default
net-config[dhcp-reserved-ip]> save
```

**Related show commands:** show net lan dhcp reserved_ip setup and show net lan dhcp leased_clients list
**Net Mode Configuration Commands**

**net lan dhcp reserved_ip delete <mac address>**

This command deletes the binding of a MAC address to an IP address.

**Format**    net lan dhcp reserved_ip delete <mac address>

**Mode**      net

**Related show commands:** show net lan dhcp reserved_ip setup and show net lan dhcp leased_clients list

**net lan lan_groups edit <row id> <new group name>**

This command specified an IPv4 LAN group name, that is, it changes a default group name such as Group1, Group2, or Group3. You need to specify both the row id that represents the group (for example, 2 for Group2, or 5 for Group5) and the new name for the group.

**Format**    net lan lan_group edit <row id> <new group name>

**Mode**      net

**Related show command:** show net lan lan_groups

**net lan ipv4 multi_homing add**

This command configures a new IPv4 alias, that is, a secondary IPv4 address. After you have issued the **net lan ipv4 multi_homing add** command, you enter the net-config [lan-ipv4-multihoming] mode, and then you can configure the secondary address and subnet mask in the order that you prefer.

**Step 1**  Format    net lan ipv4 multi_homing add

**Mode**      net

**Step 2**  Format    ip_address <ipaddress>

**Mode**      net-config [lan-ipv4-multihoming]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>ipaddress</td>
<td>The secondary IPv4 address for the LAN.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>subnet mask</td>
<td>The subnet mask for the secondary IPv4 address.</td>
</tr>
</tbody>
</table>
Command example:

SRX5308> net lan ipv4 multi_homing add
net-config[lan-ipv4-multihoming]> ip_address 192.168.16.110
net-config[lan-ipv4-multihoming]> subnet_mask 255.255.255.248
net-config[lan-ipv4-multihoming]> save

Related show command: show net lan ipv4 multiHoming

---

net lan ipv4 multi_homing edit <row id>

This command configures an existing IPv4 alias, that is, a secondary IPv4 address. After you have issued the net lan ipv4 multi_homing edit command to specify the row to be edited, you enter the net-config [lan-ipv4-multihoming] mode, and then you can configure the secondary address and subnet mask in the order that you prefer.

**Step 1 Format**
net lan ipv4 multi_homing edit

**Mode**
net

**Step 2 Format**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>ipaddress</td>
<td>The secondary IPv4 address for the LAN.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>subnet mask</td>
<td>The subnet mask for the secondary IPv4 address.</td>
</tr>
</tbody>
</table>

**Mode**
net-config [lan-ipv4-multihoming]

Related show command: show net lan ipv4 multiHoming

---

net lan ipv4 multi_homing delete <row id>

This command deletes a secondary IPv4 address by specifying its row ID.

**Format**
net lan ipv4 multi_homing delete <row id>

**Mode**
net

Related show command: show net lan ipv4 multiHoming
net lan ipv4 traffic_meter configure <ip address>

This command configures a LAN traffic meter profile for an IP address. When the traffic limit has been reached, further traffic for that IP address is blocked. After you have issued the `net lan ipv4 traffic_meter configure` command to specify the IP address, you enter the net-config [lan-ipv4-traffic-meter] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**
```
net lan ipv4 traffic_meter configure <ip address>
```

**Mode**
```
net
```

**Step 2 Format**
```
direction {Downloadonly | BothDirections}
limit <number>

counter {RestartCounter | SpecificTime {day_of_month <day>} 
{time_hour <hour>} {time_meridian AM | PM} {time_minute <minute>}}

send_email_report {Y | N}

send_email_alert {Y | N}
```

**Mode**
```
net-config [lan-ipv4-traffic-meter]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic meter configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>direction</td>
<td>Downloadonly or BothDirections</td>
<td>Specifies the type of traffic limit:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Downloadonly. The traffic limit applies to downloaded traffic only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BothDirections. The traffic limit applies to both downloaded and uploaded traffic.</td>
</tr>
<tr>
<td>limit</td>
<td>number</td>
<td>The limit for the traffic meter in MB.</td>
</tr>
<tr>
<td><strong>Traffic counter configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>counter</td>
<td>SpecificTime or RestartCounter</td>
<td>Specifies how the traffic counter is restarted:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SpecificTime. Restarts the traffic counter on a specific day and time. You need to set the day_of_month, time_hour, time_meridian, and time_minute keywords and associated parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RestartCounter. Restarts the traffic counter after you have saved the command.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>day_of_month</td>
<td>day</td>
<td>The day in the format DD (01 to 31) that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>time_hour</td>
<td>hour</td>
<td>The hour in the format HH (00 to 12) that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>time_meridian</td>
<td>AM or PM</td>
<td>Specifies the meridiem for the hour that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>time_minute</td>
<td>minutes</td>
<td>The minutes in the format MM (00 to 59) that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>send_email_report</td>
<td>Y or N</td>
<td>Specifies whether or not an email report is sent when the traffic counter restarts.</td>
</tr>
</tbody>
</table>

**Action when limit is reached**

| send_email_alert        | Y or N                                            | Specifies whether or not an email alert is sent when the traffic limit is reached and further traffic is blocked.                          |

**Command example:**

SRX5308> `net lan ipv4 traffic_meter configure 192.168.11.204`
net-config[lan-ipv4-traffic-meter]> `direction BothDirections`
net-config[lan-ipv4-traffic-meter]> `limit 45000`
net-config[lan-ipv4-traffic-meter]> `counter RestartCounter`
net-config[lan-ipv4-traffic-meter]> `send_email_report N`
net-config[lan-ipv4-traffic-meter]> `send_email_alert N`
net-config[lan-ipv4-traffic-meter]> `save`

**Related show command:** `show net lan ipv4 traffic_meter setup` and `show net lan ipv4 traffic_meter detailed_setup <row id>`
**Net Mode Configuration Commands**

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

---

**net lan ipv4 traffic_meter delete <row id>**

This command deletes a LAN traffic meter profile by specifying its row ID.

**Format**

```bash
net lan ipv4 traffic_meter delete <row id>
```

**Mode**

`net`

**Related show command:** `show net lan ipv4 traffic_meter setup`

---

**IPv6 LAN Commands**

**net lan ipv6 configure**

This command configures the IPv6 LAN address settings and DHCPv6. After you have issued the `net lan ipv6 configure` command, you enter the net-config [lan-ipv6] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

**Format**

```bash
net lan ipv6 configure
```

**Mode**

`net`

**Step 2**

**Format**

```bash
static address <ipv6-address>
static prefix_length <prefix length>
dhcp server_enable {N | Y {dhcp mode {Stateless | Stateful}}}
prefix delegation_enable {Y | N}
dhcp domain name <domain name>
dhcp server_preference <number>
dhcp dns_type {useDnsProxy | useDnsFromISP | useEnteredDns
  {dhcp primary_dns <ipv6-address>} [dhcp secondary_dns <ipv6-address>]}
dhcp rebind_time <seconds>
```

**Mode**

`net-config [lan-ipv6]`

---

<table>
<thead>
<tr>
<th>Keyword (consists of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static address</td>
<td>ipv6-address</td>
<td>The link-local IPv6 address.</td>
</tr>
<tr>
<td>static prefix_length</td>
<td>prefix length</td>
<td>The IPv6 prefix length (integer) of the link-local IPv6 address.</td>
</tr>
<tr>
<td>dhcp server_enable</td>
<td>Y or N</td>
<td>Enables or disables DHCPv6. If you enable DHCPv6, you also need to issue the <code>dhcp mode</code> keywords to specify a stateless or stateful DHCPv6 server, and configure the server.</td>
</tr>
</tbody>
</table>
### Net Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword (consists of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp mode</td>
<td>Stateless or Stateful</td>
<td>Specifies the DHCPv6 mode (stateless or stateful).</td>
</tr>
<tr>
<td>dhcp prefix_delegation_enable</td>
<td>Y or N</td>
<td>Enables or disables prefix delegation. This option is available only if the dhcp mode keywords are set to Stateless. To configure prefixes, see the net lan ipv6 prefix_delegation add command.</td>
</tr>
<tr>
<td>dhcp domain_name</td>
<td>domain name</td>
<td>The server domain name (string) or FQDN for the DHCP server.</td>
</tr>
<tr>
<td>dhcp server_preference</td>
<td>number</td>
<td>The preference number (integer) of the DHCP server.</td>
</tr>
<tr>
<td>dhcp dns_type</td>
<td>useDnsProxy, useDnsFromISP, or useEnteredDns</td>
<td>Specifies the DNS server type. If you select useEnteredDns, you also need to issue the dhcp primary_dns keyword and associated parameter. The dhcp secondary_dns keyword and associated parameter are optional.</td>
</tr>
<tr>
<td>dhcp primary_dns</td>
<td>ipv6-address</td>
<td>The IPv6 address for the primary DNS server in the DHCP configuration if the dhcp dns_type keywords are set to useEnteredDns.</td>
</tr>
<tr>
<td>dhcp secondary_dns</td>
<td>ipv6-address</td>
<td>The IPv6 address for the secondary DNS server in the DHCP configuration if the dhcp dns_type keywords are set to useEnteredDns.</td>
</tr>
<tr>
<td>dhcp rebind_time</td>
<td>seconds</td>
<td>The lease time in seconds (integer), from 0 to 604800 seconds.</td>
</tr>
</tbody>
</table>

### Command example:

```
SRX5308> net lan ipv6 configure
net-config[lan-ipv6]> static address fec0::3
net-config[lan-ipv6]> static prefix_length 64
net-config[lan-ipv6]> dhcp server_enable Y
net-config[lan-ipv6]> dhcp mode Stateless
net-config[lan-ipv6]> dhcp prefix_delegation_enable Y
net-config[lan-ipv6]> dhcp domain name netgear.com
net-config[lan-ipv6]> dhcp server_preference 236
net-config[lan-ipv6]> dhcp dns_type useDnsProxy
net-config[lan-ipv6]> dhcp rebind_time 43200
net-config[lan-ipv6]> save
```

### Related show command:

```
show net lan ipv6 setup
```
**net lan ipv6 pool add**

This command configures a new IPv6 DHCP address pool for the LAN. After you have issued the `net lan ipv6 pool add` command, you enter the net-config [lan-ipv6-pool] mode, and then you can configure the IPv6 start and end addresses and the IPv6 prefix length for the IPv6 pool in the order that you prefer.

**Step 1 Format**

```
net lan ipv6 pool add
```

**Mode**

```
net
```

**Step 2 Format**

```
start_address <ipv6-address>
end_address <ipv6-address>
prefix_length <prefix length>
```

**Mode**

```
net-config [lan-ipv6-pool]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_address</td>
<td>ipv6-address</td>
<td>The start address of the IPv6 address pool.</td>
</tr>
<tr>
<td>end_address</td>
<td>ipv6-address</td>
<td>The end address of the IPv6 address pool.</td>
</tr>
<tr>
<td>prefix_value</td>
<td>prefix length</td>
<td>The prefix length for the IPv6 address pool.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> net lan ipv6 pool add
net-config[lan-ipv6-pool]> start_address 2001::1025
net-config[lan-ipv6-pool]> end_address 2001::1030
net-config[lan-ipv6-pool]> prefix_length 56
net-config[lan-ipv6-pool]> save
```

**Related show command:** `show net lan ipv6 setup`

---

**net lan ipv6 pool edit <row id>**

This command configures an existing IPv6 DHCP address pool for the LAN. After you have issued the `net lan ipv6 pool edit` command to specify the row to be edited, you enter the net-config [lan-ipv6-pool] mode, and then you can configure the IPv6 start and end addresses and the IPv6 prefix length for the IPv6 pool in the order that you prefer.

**Step 1 Format**

```
net lan ipv6 pool edit <row id>
```

**Mode**

```
net
```
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Net Mode Configuration Commands

---

**Step 2 Format**

```
start_address <ipv6-address>
end_address <ipv6-address>
prefix_length <prefix_length>
```

**Mode**

net-config [lan-ipv6-pool]

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_address</td>
<td>ipv6-address</td>
<td>The start address of the IPv6 address pool.</td>
</tr>
<tr>
<td>end_address</td>
<td>ipv6-address</td>
<td>The end address of the IPv6 address pool.</td>
</tr>
<tr>
<td>prefix_value</td>
<td>prefix length</td>
<td>The prefix length for the IPv6 address pool.</td>
</tr>
</tbody>
</table>

Related show command: `show net lan ipv6 setup`

---

**net lan ipv6 pool delete <row id>**

This command deletes an IPv6 DHCP address pool by specifying its row ID.

**Format**

```
net lan ipv6 pool delete <row id>
```

**Mode**

net

Related show command: `show net lan ipv6 setup`

---

**net lan ipv6 multi_homing add**

This command configures a new IPv6 alias, that is, a secondary IPv6 address. After you have issued the `net lan ipv6 multi_homing add` command, you enter the net-config [lan-ipv6-multihoming] mode, and then you can configure the secondary address and IPv6 prefix length in the order that you prefer.

**Step 1 Format**

```
net lan ipv6 multi_homing add
```

**Mode**

net

**Step 2 Format**

```
ip_address <ipv6-address>
prefix_length <prefix_length>
```

**Mode**

net-config [lan-ipv6-multihoming]
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Net Mode Configuration Commands**

**Command example:**

SRX5308> net lan ipv6 multi_homing add
net-config[lan-ipv6-multihoming]> ip_address 2002::1006
net-config[lan-ipv6-multihoming]> prefix_length 10
net-config[lan-ipv6-multihoming]> save

**Related show command:** *show net lan ipv6 multiHoming*

---

**net lan ipv6 multi_homing edit <row id>**

This command configures an existing IPv6 alias, that is, a secondary IPv6 address. After you have issued the `net lan ipv6 multi_homing edit` command to specify the row to be edited, you enter the net-config [lan-ipv6-multihoming] mode, and then you can configure the secondary address and IPv6 prefix length in the order that you prefer.

**Step 1**  
Format: `net lan ipv6 multi_homing edit <row id>`  
Mode: `net`

**Step 2**  
Format:  
- `ip_address <ipv6-address>`  
- `prefix_length <prefix length>`  
Mode: `net-config [lan-ipv6-multihoming]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>ipv6-address</td>
<td>The secondary IPv6 address for the LAN.</td>
</tr>
<tr>
<td>prefix_length</td>
<td>prefix length</td>
<td>The prefix length for the secondary IPv6 address.</td>
</tr>
</tbody>
</table>

**Related show command:** *show net lan ipv6 multiHoming*
**net lan ipv6 multi_homing delete <row id>**

This command deletes a secondary IPv6 address by specifying its row ID.

**Format**

```
net lan ipv6 multi_homing delete <row id>
```

**Mode**

```
net
```

**Related show command:** `show net lan ipv6 multiHoming`

---

**net radvd configure lan**

This command configures the Router Advertisement Daemon (RADVD) for the link-local advertisements of IPv6 router addresses and prefixes in the LAN. After you have issued the `net radvd configure lan` command, you enter the net-config [radvd-lan] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

**Format**

```
net radvd configure lan
```

**Mode**

```
net
```

**Step 2**

**Format**

```
enable {Y | N}
mode {Unsolicited-Multicast | Unicast-Only}
interval <seconds>
flags {Managed | Other}
preference {Low | Medium | High}
mtu <number>
life_time <seconds>
```

**Mode**

```
net-config [radvd-lan]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables the RADVD process to allow stateless autoconfiguration of the IPv6 LAN or disables the RADVD process.</td>
</tr>
</tbody>
</table>
| mode                                        | Unsolicited-Multicast or Unicast-Only          | Specifies the advertisement mode:  
  - **Unsolicited-Multicast**. Allows unsolicited multicast and unicast communication with the hosts. Router advertisements (RAs) are sent to all interfaces at the rate that is defined by the `interval` keyword and parameter.  
  - **Unicast-Only**. Responds to unicast packet requests only. No unsolicited packets are advertised. |
### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

#### Net Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**Command example:**

```
SRX5308> net radvd configure lan
net-config[radvd-lan]> enable Y
net-config[radvd-lan]> mode Unsolicited-Multicast
net-config[radvd-lan]> interval 60
net-config[radvd-lan]> flags Managed
net-config[radvd-lan]> preference Medium
net-config[radvd-lan]> mtu 1496
net-config[radvd-lan]> life_time 7200
net-config[radvd-lan]> save
```

**Related show command:** `show net radvd lan setup`

---

**net lan ipv6 prefix_delegation add**

This command configures a new IPv6 prefix for LAN prefix delegation. To enable prefix delegation for the IPv6 LAN, see the `net lan ipv6 configure` command. After you have issued the `net lan ipv6 prefix_delegation add` command, you enter the net-config [lan-prefix-delegation] mode, and then you can configure the IPv6 prefix and IPv6 prefix length in the order that you prefer.

**Step 1**

Format: `net lan ipv6 prefix_delegation add`

Mode: `net`
Step 2     Format  prefix <prefix>
            prefix_length <prefix_length>
        Mode  net-config [lan-prefix-delegation]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>prefix</td>
<td>The IPv6 prefix.</td>
</tr>
<tr>
<td>prefix_length</td>
<td>prefix length</td>
<td>The prefix length for IPv6 prefix.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> net lan ipv6 prefix_delegation add
net-config[lan-prefix-delegation]> prefix 2001:db8::
net-config[lan-prefix-delegation]> prefix_length 64
net-config[lan-prefix-delegation]> save

Related show command: show net lan ipv6 setup

net lan ipv6 prefix_delegation edit <row id>

This command configures an existing IPv6 prefix for LAN prefix delegation. After you have issued the net lan ipv6 prefix_delegation edit command to specify the row to be edited, you enter the net-config [lan-prefix-delegation] mode, and then you can configure the IPv6 prefix and IPv6 prefix length in the order that you prefer.

Step 1     Format  net lan ipv6 prefix_delegation edit <row id>
        Mode  net
Step 2     Format  prefix <prefix>
            prefix_length <prefix length>
        Mode  net-config [lan-prefix-delegation]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>prefix</td>
<td>The IPv6 prefix.</td>
</tr>
<tr>
<td>prefix_length</td>
<td>prefix length</td>
<td>The prefix length for IPv6 prefix.</td>
</tr>
</tbody>
</table>

Related show command: show net lan ipv6 setup
**net lan ipv6 prefix_delegation delete <row id>**

This command deletes an IPv6 prefix for LAN prefix delegation by deleting its row ID.

**Format**

```
net lan ipv6 prefix_delegation delete <row id>
```

**Mode**

```
net
```

**Related show command:** `show net lan ipv6 setup`

---

**IPv4 DMZ Setup Commands**

**net dmz ipv4 configure**

This command enables, configures, or disables the IPv4 DMZ. After you have issued the `net dmz ipv4 configure` command, you enter the net-config [dmz-ipv4] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

**Format**

```
net dmz ipv4 configure
```

**Mode**

```
net
```

**Step 2**

**Format**

```
enable_dmz {Y | N}
ip_address <ipaddress>
subnet_mask <subnet mask>
dhcp_mode {None | DHCP-Server | DHCP-Relay}
dns_proxy_enable {Y | N}
domain_name <domain name>
starting_ip_address <ipaddress>
ending_ip_address <ipaddress>
primary_dns_server <ipaddress>
secondary_dns_server <ipaddress>
wins_server <ipaddress>
lease_time <hours>
enable_ldap {Y | N}
ldap_serverip <ipaddress>
ldap_search_base <search base>
ldap_port <number>
```

**Mode**

```
net-config [dmz-ipv4]
```
### Net Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_dmz</td>
<td>Y or N</td>
<td>Enables or disables the DMZ.</td>
</tr>
<tr>
<td>ip_address</td>
<td>ipaddress</td>
<td>The IP address of the DMZ port.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>subnet mask</td>
<td>The subnet mask of the DMZ port.</td>
</tr>
</tbody>
</table>
| dhcp_mode       | None, DHCP-Serves or DHCP-Relay                   | Specifies the DHCP mode:  
|                 | • None. DHCP is disabled for the DMZ.             |             |
|                 | • DHCP-Server. DHCP is enabled for the DMZ.       |             |
|                 | • DHCP-Relay. Addresses are assigned in the       |             |
|                 | DMZ by a DHCP Relay. Configure the relay_gateway  |             |
|                 | keyword and associated parameter.                 |             |
| dns_proxy_enable| Y or N                                            | Enables or disables the DNS proxy. |

#### DHCP server

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>domain name</td>
<td>The server domain name (string) or FQDN for the DHCP server.</td>
</tr>
<tr>
<td>starting_ip_address</td>
<td>ipaddress</td>
<td>The start IP address for the DHCP address pool.</td>
</tr>
<tr>
<td>ending_ip_address</td>
<td>ipaddress</td>
<td>The end IP address for the DHCP address pool.</td>
</tr>
<tr>
<td>primary_dns_server</td>
<td>ipaddress</td>
<td>The IP address of the primary DNS server in the DMZ DHCP configuration.</td>
</tr>
<tr>
<td>secondary_dns_server</td>
<td>ipaddress</td>
<td>The IP address of the secondary DNS server in the DMZ DHCP configuration.</td>
</tr>
<tr>
<td>wins_server</td>
<td>ipaddress</td>
<td>The IP address of the WINS server in the DMZ DHCP configuration.</td>
</tr>
<tr>
<td>lease_time</td>
<td>hours</td>
<td>The duration in hours for which an IP address is leased.</td>
</tr>
<tr>
<td>enable_ldap</td>
<td>Y or N</td>
<td>Enables or disables LDAP.</td>
</tr>
<tr>
<td>ldap_serverip</td>
<td>ipaddress</td>
<td>The IP address of the LDAP server.</td>
</tr>
<tr>
<td>ldap_search_base</td>
<td>search base</td>
<td>The search base (string) for LDAP</td>
</tr>
<tr>
<td>ldap_port</td>
<td>number</td>
<td>The port number for the LDAP server.</td>
</tr>
</tbody>
</table>

#### DHCP relay

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay_gateway</td>
<td>ipaddress</td>
<td>Set DHCP relay gateway server.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> net dmz ipv4 configure
net-config[dmz-ipv4]> enable_dmz
```
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

```
net-config[dmz-ipv4]> ip_address 10.126.32.59
net-config[dmz-ipv4]> subnet_mask 2525.255.255.0
net-config[dmz-ipv4]> dhcp_mode None
net-config[dmz-ipv4]> dns_proxy_enable Y
net-config[dmz-ipv4]> save
```

Related show command: `show net dmz ipv4 setup`

---

IPv6 DMZ Setup Commands

```
net dmz ipv6 configure
```

This command enables, configures, or disables the IPv6 DMZ. After you have issued the `net dmz ipv6 configure` command, you enter the net-config [dmz-ipv6] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format
```
net dmz ipv6 configure
```

**Mode** net

**Step 2** Format
```
enable_dmz {Y | N}
ip_address <ipv6-address>
prefix_length <prefix length>

dhcp_enable {N | Y {dhcp_mode {Stateless | Stateful}}}
domain name <domain-name>
server_preference <number>
dns_server_option {useDnsProxy | useDnsFromISP | useEnteredDns
 {primary_dns_server <ipv6-address> [secondary_dns_server <ipv6-address>]}]
lease_time <seconds>
```

**Mode** net-config [dmz-ipv6]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_dmz</td>
<td>Y or N</td>
<td>Enables or disables the DMZ.</td>
</tr>
<tr>
<td>ip_address</td>
<td>ipv6-address</td>
<td>The IPv6 address of the DMZ port.</td>
</tr>
<tr>
<td>prefix_length</td>
<td>prefix length</td>
<td>The prefix length (integer) for the DMZ port.</td>
</tr>
</tbody>
</table>

---

Net Mode Configuration Commands

76
### Net Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

#### Net Mode Configuration Commands

**Command example:**

```
SRX5308> net dmz ipv6 configure
net-config[dmz-ipv6]> enable_dmz Y
net-config[dmz-ipv6]> ip_address 2001:176::1
net-config[dmz-ipv6]> prefix_length 64
net-config[dmz-ipv6]> dhcp_enable Y
net-config[dmz-ipv6]> dhcp_mode Stateful
net-config[dmz-ipv6]> domain_name netgear.com
net-config[dmz-ipv6]> server_preference 210
net-config[dmz-ipv6]> dns_server_option useDnsProxy
net-config[dmz-ipv6]> primary_dns_server ipv6-address
net-config[dmz-ipv6]> secondary_dns_server ipv6-address
net-config[dmz-ipv6]> lease_time 43200
net-config[dmz-ipv6]> save
```

**Related show command:** `show net dmz ipv6 setup`

---

### net dmz ipv6 pool configure <ipv6 address>

This command configures a new or existing IPv6 DHCP address pool for the DMZ. After you have issued the `net dmz ipv6 pool configure` command to specify the IPv6 start address of the IPv6 pool, you enter the `net-config [dmz-ipv6-pool]` mode, and then you can...
configure the IPv6 end address and the IPv6 prefix length for the IPv6 pool in the order that
you prefer.

Step 1 Format net dmz ipv6 pool configure <ipv6-address>
    Mode net

Step 2 Format ending_ip_address <ipv6-address>
    prefix_value <prefix length>
    Mode net-config [dmz-ipv6-pool]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ending_ip_address</td>
<td>ipv6-address</td>
<td>The end address of the IPv6 address pool.</td>
</tr>
<tr>
<td>prefix_value</td>
<td>prefix length</td>
<td>The prefix length for the IPv6 address pool.</td>
</tr>
</tbody>
</table>

Command example:
SRX5308> net dmz ipv6 pool configure 2001::1100
net-config[dmz-ipv6-pool]> ending_ip_address 2001::1120
net-config[dmz-ipv6-pool]> prefix_value 56
net-config[dmz-ipv6-pool]> save

Related show command: show net dmz ipv6 setup

net dmz pool ipv6 delete < ipv6 address>
This command deletes an IPv6 DHCP address pool for the DMZ by deleting the start address
of the pool.

Format net radvd pool dmz delete <ipv6-address>
    Mode net

Related show command: show net dmz ipv6 setup

net radvd configure dmz
This command configures the Router Advertisement Daemon (RADVD) process for the
link-local advertisements of IPv6 router addresses and prefixes in the DMZ. After you have
issued the net radvd configure dmz command, you enter the net-config [radvd-dmz]
mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**  
Format:  
```
net radvd configure dmz
```
Mode: net

**Step 2**  
Format:  
```
enable {Y | N}
mode {Unsolicited-Multicast | Unicast-Only}
interval <seconds>
flags {Managed | Other}
preference {Low | Medium | High}
mtu <number>
life_time <seconds>
```
Mode: net-config [radvd-dmz]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables the RADVD process to allow stateless autoconfiguration of the IPv6 DMZ or disables the RADVD process.</td>
</tr>
</tbody>
</table>
| mode                                        | Unsolicited-Multicast or Unicast-Only          | Specifies the advertisement mode:  
  - Unsolicited-Multicast. Allows unsolicited multicast and unicast communication with the hosts. Router advertisements (RAs) are sent to all interfaces at the rate that is defined by the interval keyword and associated parameter.  
  - Unicast-Only. Responds to unicast packet requests only. No unsolicited packets are advertised. |
| interval                                    | seconds                                        | The interval in seconds (integer) between unsolicited multicast RAs. Enter a period from 10 to 1800 seconds. The default is 30 seconds. |
| flags                                       | Managed or Other                               | Specifies the flag:  
  - Managed. Specifies that the DHCPv6 stateful protocol is used for autoconfiguration of the address.  
  - Other. Specifies that the DHCPv6 stateful protocol is used for autoconfiguration of other (that is, nonaddress) information. |
| preference                                  | Low, Medium, or High                           | Specifies the VPN firewall’s preference in relation to other hosts and routers in the DMZ. |
| mtu                                         | number                                         | The MTU size (integer) that is used in the RAs to ensure that all nodes in the network use the same MTU size. The default is 1500 seconds. |
| life_time                                   | seconds                                        | The advertisement lifetime in seconds (integer) of the route. The default is 3600 seconds. |
Command example:

SRX5308> net radvd configure dmz
net-config[radvd-dmz]> enable Y
net-config[radvd-dmz]> mode Unicast-Only
net-config[radvd-dmz]> flags Managed
net-config[radvd-dmz]> preference High
net-config[radvd-dmz]> mtu 1500
net-config[radvd-dmz]> life_time 7200
net-config[radvd-dmz]> save

Related show command: show net radvd dmz setup

WAN QoS Commands

net qos configure

This command configures the QoS mode for the WAN interfaces. After you have issued the net qos configure command, you enter the net-config [network-qos] mode, and then you can enable QoS and set the QoS mode to rate control or priority.

The configured QoS mode determines which WAN QoS profiles can be active, that is, you can add both rate control or priority WAN QoS profiles (see the net qos profile add command), but only the profiles for the configured QoS mode can be active. For example, if you set the QoS mode to priority, then only the profiles with a priority configuration can be active.

Step 1 Format  net qos configure
Mode  net

Step 2 Format  enable {Y | N}  
  qos_type {Rate-Control | Priority}
Mode  net-config [network-qos]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables QoS for all WAN interfaces.</td>
</tr>
<tr>
<td>qos_type</td>
<td>Rate-Control or Priority</td>
<td>Specifies whether QoS uses rate control or priority profiles.</td>
</tr>
</tbody>
</table>

Related show command: show net qos setup
**net qos profile add**

This command configures a new WAN QoS profile. After you have issued the `net qos profile add` command, you enter the net-config [network-qos-profile] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
Mode net qos profile add
```

**Step 2 Format**

The following settings apply to both rate control profiles and priority profiles:

```
qos_type {Rate-Control | Priority}
interface {WAN1 | WAN2 | WAN3 | WAN4}
service_name {default_services <default service name> | custom_services <custom service name>}
diffserv_qos_match <number>
diffserv_qos_remark <number>
```

The following settings apply only to rate control profiles:

```
direction_for_rate_control {Inbound | Outbound | Both}
congestion_priority {Default | High | Medium-high | Medium | Low}
hosts {Single-IP-Address <hosts_start_ip <ipaddress> | IP-Address-Range <hosts_start_ip <ipaddress> | hosts_end_ip <ipaddress>} | Group <hosts_group {Group1 | Group2 | Group3 | Group4 | Group5 | Group6 | Group7 | Group8}>
bandwidth_allocation {Shared | Individual}
outbound_min_bandwidth <bandwidth>
outbound_max_bandwidth <bandwidth>
inbound_min_bandwidth <bandwidth>
inbound_max_bandwidth <bandwidth>
```

The following settings apply only to priority profiles:

```
direction_for_priority {Inbound-Traffic | Outbound-Traffic}
priority {Low | High}
```

**Mode**

```
et-config [network-qos-profile]
```
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>qos_type</td>
<td>Rate-Control or Priority</td>
<td>Specifies the type of profile:</td>
</tr>
<tr>
<td></td>
<td>• Rate-Control. Configure the keywords and parameters in the Common settings section and Rate control profile settings section of this table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority. Configure the keywords and parameters in the Common settings section and Priority profile settings section of this table.</td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the interface to which the profile applies.</td>
</tr>
<tr>
<td>default_services</td>
<td></td>
<td>Specifies the default service and protocol to which the profile applies.</td>
</tr>
<tr>
<td>service_name</td>
<td>custom service name</td>
<td>The custom service that you have configured with the <code>security services add</code> command and to which the profile applies</td>
</tr>
</tbody>
</table>
### Keywords (might consist of two separate words)

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>differential_qos_match</code></td>
<td><code>number</code></td>
<td>(Optional) The DSCP value, from 0 through 63. Packets are classified against this value.</td>
</tr>
<tr>
<td><code>differential_qos_remark</code></td>
<td><code>number</code></td>
<td>(Optional) The DSCP value, from 0 through 63. Packets are marked with this value.</td>
</tr>
</tbody>
</table>

### Rate control profile settings

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| `direction_for_rate_control`                  | `Inbound, Outbound, or Both`                    | Specifies the direction to which rate control is applied:  
  - **Inbound.** Rate control is applied to inbound packets only. You need to issue the `inbound_min_bandwidth` and `inbound_max_bandwidth` keywords and specify the bandwidth that is allocated.  
  - **Outbound.** Rate control is applied to outbound packets only. You need to issue the `outbound_min_bandwidth` and `outbound_max_bandwidth` keywords and specify the bandwidth that is allocated.  
  - **Both.** Rate control is applied to both inbound and outbound packets. You need to issue the `inbound_min_bandwidth`, `inbound_max_bandwidth`, `outbound_min_bandwidth`, and `outbound_max_bandwidth` keywords and specify the bandwidth that is allocated. |
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| congestion_priority                          | Default, High, Medium-high, Medium, or Low     | Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall:  
  • Default. Traffic is mapped based on the ToS field in the packet’s IP header.  
  • High. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4.  
  • Medium-high. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3.  
  • Medium. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2.  
  • Low. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values. |
| hosts                                         | Single-IP-Address, IP-Address-Range, or Group | Specifies the IP address, range of IP addresses, or group to which the profile is applied:  
  • Single-IP-Address. The profile is applied to a single IP address. Issue the hosts_start_ip keyword to specify the IP address.  
  • IP-Address-Range. The profile is applied to an IP address range. Issue the hosts_start_ip and hosts_end_ip keywords to specify the start and end IP addresses of the range. In addition, issue the bandwidth_allocation keyword to specify if bandwidth is shared between all IP addresses in the range or is allocated to each IP address in the range.  
  • Group. The profile is applied to a group. Issue the hosts_group to specify the group. In addition, issue the bandwidth_allocation keyword to specify if bandwidth is shared between all members of the group or is allocated to each member in the group. |
| hosts_start_ip                                | ipaddress                                      | There are two options:  
  • The IP address if the hosts keyword is set to Single-IP-Address.  
  • The start IP address if the hosts keyword is set to IP-Address-Range. |
### Net Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the hosts keyword is set to IP-Address-Range.</td>
</tr>
</tbody>
</table>
| hosts_group                                  | Group1, Group2, Group3, Group4, Group5, Group6, Group7, or Group8 | Specifies the group if the hosts keyword is set to Group.  
**Note:** You cannot enter group names that you have specified with the `net lan lan_groups edit <row id> <new group name>` command. |
| bandwidth_allocation                         | Shared or Individual                             | Specifies how bandwidth is allocated. These options apply when the hosts keyword is set to IP-Address-Range or to group.  
- **Shared.** The bandwidth is shared among all IP addresses in a range or all members of a group.  
- **Individual.** The bandwidth is allocated to each IP address in the range or each member of a group. |
| outbound_min_bandwidth                       | bandwidth                                       | The outbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to outbound or both. |
| outbound_max_bandwidth                       | bandwidth                                       | The outbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to outbound or both. |
| inbound_min_bandwidth                        | bandwidth                                       | The inbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to inbound or both. |
| inbound_max_bandwidth                        | bandwidth                                       | The inbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to inbound or both. |
### Priority profile settings

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| direction_for_priority                        | Inbound-Traffic or Outbound-Traffic              | Specifies the direction to which the priority queue is applied:  
- **Inbound-Traffic.** The priority queue is applied to inbound traffic only.  
- **Outbound-Traffic.** The priority queue is applied to outbound traffic only. |
| priority                                      | Low or High                                      | Specifies the priority queue that determines the allocation of bandwidth:  
- **Low.** All services that are assigned a low-priority queue share 10 percent of interface bandwidth.  
- **High.** All services that are assigned a high-priority queue share 60 percent of interface bandwidth.  
**Note:** By default, all services are assigned the medium-priority queue in which they share 30 percent of the interface bandwidth. |

**Command example:**

```bash
SRX5308> net qos profile add
net-config[network-qos-profile]> qos_type Rate-Control
net-config[network-qos-profile]> interface WAN2
net-config[network-qos-profile]> service_name default_services http
net-config[network-qos-profile]> direction_for_rate_control Inbound
net-config[network-qos-profile]> congestion_priority High
net-config[network-qos-profile]> hosts IP-Address-Range
net-config[network-qos-profile]> hosts_start_ip 192.168.110.2
net-config[network-qos-profile]> hosts_end_ip 192.168.110.199
net-config[network-qos-profile]> bandwidth_allocation Shared
net-config[network-qos-profile]> inbound_min_bandwidth 7500
net-config[network-qos-profile]> inbound_max_bandwidth 15000
net-config[network-qos-profile]> diffserv_qos_match 5
net-config[network-qos-profile]> diffserv_qos_remark 12
net-config[network-qos-profile]> save
```

**Related show command:** `show net qos setup`

**net qos profile edit <row id>**

This command configures an existing WAN QoS profile. After you have issued the `net qos profile edit` command to specify the row to be edited, you enter the net-config
[network-qos-profile] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**
```
net qos profile edit <row id>
```

**Mode**
```
net
```

**Step 2 Format**
The following settings apply to both rate control profiles and priority profiles:
```
qos_type {Rate-Control | Priority}
interface {WAN1 | WAN2 | WAN3 | WAN4}
service_name {default_services <default service name> |
{custom_services <custom service name>}
diffserv_qos_match <number>
diffserv_qos_remark <number>
```

The following settings apply only to rate control profiles:
```
direction_for_rate_control {Inbound | Outbound | Both}
congestion_priority {Default | High | Medium-high | Medium | Low}
hosts {Single-IP-Address {hosts_start_ip <ipaddress>} |
IP-Address-Range {hosts_start_ip <ipaddress>} {hosts_end_ip 
<ipaddress>)} | Group {hosts_group {Group1 | Group2 | Group3| 
Group4 | Group5 | Group6 | Group7 | Group8}}}
bandwidth_allocation {Shared | Individual}
outbound_min_bandwidth <bandwidth>
outbound_max_bandwidth <bandwidth>
inbound_min_bandwidth <bandwidth>
inbound_max_bandwidth <bandwidth>
```

The following settings apply only to priority profiles:
```
direction_for_priority {Inbound-Traffic | Outbound-Traffic}
priority {Low | High}
```

**Mode**
```
net-config [network-qos-profile]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>qos_type</td>
<td>Rate-Control or Priority</td>
<td>Specifies the type of profile:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rate-Control. Configure the keywords and parameters in the Common settings section and Rate control profile settings section of this table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Priority. Configure the keywords and parameters in the Common settings section and Priority profile settings section of this table.</td>
</tr>
<tr>
<td>interface</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the interface to which the profile applies.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>default_services</td>
<td>custom_services</td>
<td>The custom service that you have configured with the <code>security services add</code> command and to which the profile applies.</td>
</tr>
<tr>
<td>diffserv_qos_match</td>
<td>number</td>
<td>(Optional) The DSCP value, from 0 through 63. Packets are classified against this value.</td>
</tr>
<tr>
<td>diffserv_qos_remark</td>
<td>number</td>
<td>(Optional) The DSCP value, from 0 through 63. Packets are marked with this value.</td>
</tr>
</tbody>
</table>
### Rate control profile settings

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| direction_for_rate_control                            | Inbound, Outbound, or Both                        | Specifies the direction to which rate control is applied:  
  - **Inbound**. Rate control is applied to inbound packets only. You need to issue the `inbound_min_bandwidth` and `inbound_max_bandwidth` keywords and specify the bandwidth that is allocated.  
  - **Outbound**. Rate control is applied to outbound packets only. You need to issue the `outbound_min_bandwidth` and `outbound_max_bandwidth` keywords and specify the bandwidth that is allocated.  
  - **Both**. Rate control is applied to both inbound and outbound packets. You need to issue the `inbound_min_bandwidth`, `inbound_max_bandwidth`, `outbound_min_bandwidth`, and `outbound_max_bandwidth` keywords and specify the bandwidth that is allocated. |
| congestion_priority                                   | Default, High, Medium-high, Medium, or Low        | Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall:  
  - **Default**. Traffic is mapped based on the ToS field in the packet’s IP header.  
  - **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4.  
  - **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3.  
  - **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2.  
  - **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values. |
### Net Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| hosts                                         | Single-IP-Address, IP-Address-Range, or Group   | Specifies the IP address, range of IP addresses, or group to which the profile is applied:  
- **Single-IP-Address.** The profile is applied to a single IP address. Issue the `hosts_start_ip` keyword to specify the IP address.  
- **IP-Address-Range.** The profile is applied to an IP address range. Issue the `hosts_start_ip` and `hosts_end_ip` keywords to specify the start and end IP addresses of the range. In addition, issue the `bandwidth_allocation` keyword to specify if bandwidth is shared between all IP addresses in the range or is allocated to each IP address in the range.  
- **Group.** The profile is applied to a group. Issue the `hosts_group` to specify the group. In addition, issue the `bandwidth_allocation` keyword to specify if bandwidth is shared between all members of the group or is allocated to each member in the group. |
| hosts_start_ip                                | ipaddress                                      | There are two options:  
- The IP address if the `hosts` keyword is set to **Single-IP-Address.**  
- The start IP address if the `hosts` keyword is set to **IP-Address-Range.** |
| hosts_end_ip                                  | ipaddress                                      | The end IP address if the if the `hosts` keyword is set to **IP-Address-Range.** |
| hosts_group                                   | Group1, Group2, Group3, Group4, Group5, Group6, Group7, or Group8 | Specifies the group if the `hosts` keyword is set to **Group.**  
**Note:** You cannot enter group names that you have specified with the `net lan lan_groups edit <row id><new group name>` command. |
### Net Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| `bandwidth_allocation`                        | Shared or Individual                              | Specifies how bandwidth is allocated. These options apply when the `hosts` keyword is set to `IP-Address-Range` or to `group`.  
* **Shared**: The bandwidth is shared among all IP addresses in a range or all members of a group.  
* **Individual**: The bandwidth is allocated to each IP address in the range or each member of a group. |
| `outbound_min_bandwidth`                     | `bandwidth`                                       | The outbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to `outbound` or `both`. |
| `outbound_max_bandwidth`                     | `bandwidth`                                       | The outbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to `outbound` or `both`. |
| `inbound_min_bandwidth`                      | `bandwidth`                                       | The inbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to `inbound` or `both`. |
| `inbound_max_bandwidth`                      | `bandwidth`                                       | The inbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies when the `direction_for_rate_control` keyword is set to `inbound` or `both`. |
| **Priority profile settings**                |                                                   |             |
| `direction_for_priority`                     | Inbound-Traffic or Outbound-Traffic              | Specifies the direction to which the priority queue is applied:  
* **Inbound-Traffic**: The priority queue is applied to inbound traffic only.  
* **Outbound-Traffic**: The priority queue is applied to outbound traffic only. |
### Net Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| priority                                      | Low or High                                      | Specifies the priority queue that determines the allocation of bandwidth:  
  - **Low**. All services that are assigned a low-priority queue share 10 percent of interface bandwidth.  
  - **High**. All services that are assigned a high-priority queue share 60 percent of interface bandwidth.  
  **Note**: By default, all services are assigned the medium-priority queue in which they share 30 percent of the interface bandwidth. |

**Related show command:** `show net qos setup`

---

**net qos profile delete <row id>**  
This command deletes a WAN QoS profile by deleting its row ID.

**Format**  
`net qos profile delete <row id>`

**Mode**  
net

**Related show command:** `show net qos setup`

---

**net qos profile disable <row id>**  
This command disables a WAN QoS profile by specifying its row ID.

**Format**  
`net qos profile disable <row id>`

**Mode**  
net

**Related show command:** `show net qos setup`
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

net qos profile enable <row id>

This command enables a WAN QoS profile by specifying its row ID.

Format  net qos profile enable <row id>
Mode      net

Related show command: show net qos setup

IPv4 Routing Commands

net routing static ipv4 configure <route name>

This command configures an IPv4 static route. After you have issued the net routing static ipv4 configure command to specify the name of the new route, you enter the net-config [static-routing-ipv4] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1  Format  net routing static ipv4 configure <route name>
         Mode      net

Step 2  Format  active_flag {Y | N}
         private_flag {Y | N}
         destination_address <ipaddress>
         subnet_mask <subnet mask>
         interface {custom_vlan <VLAN name> | dmz | lan | wan {WAN1 | WAN2 | WAN3 | WAN4}}
         gateway_address <ipaddress>
         metric <number>
         Mode      net-config [static-routing-ipv4]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_flag</td>
<td>Y or N</td>
<td>Specifies whether or not the route is an active route.</td>
</tr>
<tr>
<td>private_flag</td>
<td>Y or N</td>
<td>Specifies whether or not the route can be shared with other gateways when RIP is enabled.</td>
</tr>
<tr>
<td>destination_address</td>
<td>ipaddress</td>
<td>The destination IP address.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>subnet mask</td>
<td>The destination subnet mask.</td>
</tr>
</tbody>
</table>
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| interface        | custom_vlan <VLAN name>, dmz, lan, or wan (WAN1, WAN2, WAN3, WAN4) | Specifies the interface for which the route is applied. The dmz and lan keywords do not require additional selections. The custom_vlan and wan keywords require additional selections:  
  • If you issue the custom_vlan keyword, you also need to specify the VLAN name.  
  • If you issue the wan keyword, you also need to specify the WAN interface (WAN1, WAN2, WAN3, or WAN4). |

| gateway_address  | ipaddress                                        | The gateway IP address.                                                   |
| metric           | number                                           | The metric (integer) for this route. The number can be from 2 to 15. |

Command example:

SRX5308> net routing static ipv4 configure Orly
net-config[static-routing-ipv4]> active_flag Y
net-config[static-routing-ipv4]> private_flag Y
net-config[static-routing-ipv4]> subnet_mask 255.255.255.0
net-config[static-routing-ipv4]> interface wan WAN1
net-config[static-routing-ipv4]> gateway_address 10.192.44.13
net-config[static-routing-ipv4]> metric 7
net-config[static-routing-ipv4]> save

Related show command: show net routing static ipv4 setup

net routing static ipv4 delete <route name>

This command deletes a static IPv4 route by deleting its name.

Format     net routing static ipv4 delete <route name>
Mode       net

Related show command: show net routing static ipv4 setup
**Net Mode Configuration Commands**

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**net routing static ipv4 delete_all**

This command deletes all static IPv4 routes.

**Format**
```
net routing static ipv4 delete_all
```

**Mode**
```
net
```

**Related show command:** *show net routing static ipv4 setup*

---

**net routing dynamic configure**

This command configures RIP and the associated MD5 key information. After you have issued the `net routing dynamic configure` command, you enter the `net-config [dynamic-routing]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**
```
Format
net routing dynamic configure
```

**Mode**
```
net
```

**Step 2**
```
Format
authentication_enable {Y \mid N}
direction {None \mid In-only \mid Out-only \mid Both}
version {Disabled \mid Rip1 \mid Rip2B \mid Rip2M}
```

```
first_key authentication_id <authentication key>
first_key id_number <number>
first_key valid_from {day <day>}  
first_key valid_from {month <month>}  
first_key valid_from {year <year>}
first_key valid_from {hour <hour>}  
first_key valid_from {minute <minute>}  
first_key valid_from {second <second>}
first_key valid_to {day <day>}  
first_key valid_to {month <month>}  
first_key valid_to {year <year>}
first_key valid_to {hour <hour>}  
first_key valid_to {minute <minute>}  
first_key valid_to {second <second>}
```
```
second_key authentication_id <authentication key>
second_key id_number <number>
second_key valid_from {day <day>}
second_key valid_from {month <month>}
second_key valid_from {year <year>}}
second_key valid_from {hour <hour> |
second_key valid_from {minute <minute>}
second_key valid_from {second <second>}
second_key valid_to {day <day>}
second_key valid_to {month <month>}
second_key valid_to {year <year>}}
second_key valid_to {hour <hour> |
second_key valid_to {minute <minute>}
second_key valid_to {second <second>}
```

Mode
net-config [dynamic-routing]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication_enable</td>
<td>Y or N</td>
<td>Enables or disables authentication for RIP-2B or RIP-2M.</td>
</tr>
<tr>
<td>direction</td>
<td>None, In-only, Out-only, or Both.</td>
<td>Specifies the RIP direction.</td>
</tr>
<tr>
<td>version</td>
<td>Disabled, Rip1, Rip2B, or Rip2M</td>
<td>Specifies the RIP version.</td>
</tr>
<tr>
<td>First key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>first_key authentication_id</td>
<td>authentication key</td>
<td>The first MD5 authentication key (alphanumeric string).</td>
</tr>
<tr>
<td>first_key id_number</td>
<td>number</td>
<td>The first MD5 key ID (integer).</td>
</tr>
</tbody>
</table>
### Net Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Command example:**

```
SRX5308> net routing dynamic configure
net-config[dynamic-routing]> authentication_enable Y
net-config[dynamic-routing]> direction Both
net-config[dynamic-routing]> version Rip2M
net-config[dynamic-routing]> first_key authentication_id 2rt!00jkl26ll7Oo0
net-config[dynamic-routing]> first_key id_number 1
net-config[dynamic-routing]> first_key valid_from day 01
net-config[dynamic-routing]> first_key valid_from month 12
net-config[dynamic-routing]> first_key valid_from year 2011
net-config[dynamic-routing]> first_key valid_from hour 07
net-config[dynamic-routing]> first_key valid_from minute 00
net-config[dynamic-routing]> first_key valid_from second 00
net-config[dynamic-routing]> first_key valid_to day 31
```

---

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>first_key valid_from day</td>
<td>day</td>
<td>The day in the format DD (01 to 31).</td>
</tr>
<tr>
<td>first_key valid_from month</td>
<td>month</td>
<td>The month in the format MM (01 to 12).</td>
</tr>
<tr>
<td>first_key valid_from year</td>
<td>year</td>
<td>The year in the format YYYY (1970 to 2037).</td>
</tr>
<tr>
<td>first_key valid_from hour</td>
<td>hour</td>
<td>The hour in the 24-hour format HH (00 to 23).</td>
</tr>
<tr>
<td>first_key valid_from minute</td>
<td>minute</td>
<td>The minute in the format MM (00 to 59).</td>
</tr>
<tr>
<td>first_key valid_from second</td>
<td>second</td>
<td>The second in the format SS (00 to 59).</td>
</tr>
<tr>
<td>first_key valid_to day</td>
<td>day</td>
<td>The day in the format DD (01 to 31).</td>
</tr>
<tr>
<td>first_key valid_to month</td>
<td>month</td>
<td>The month in the format MM (01 to 12).</td>
</tr>
<tr>
<td>first_key valid_to year</td>
<td>year</td>
<td>The year in the format YYYY (1970 to 2037).</td>
</tr>
<tr>
<td>first_key valid_to hour</td>
<td>hour</td>
<td>The hour in the 24-hour format HH (00 to 23).</td>
</tr>
<tr>
<td>first_key valid_to minute</td>
<td>minute</td>
<td>The minute in the format MM (00 to 59).</td>
</tr>
<tr>
<td>first_key valid_to second</td>
<td>second</td>
<td>The second in the format SS (00 to 59).</td>
</tr>
</tbody>
</table>

**Second key**

*Note:* The keywords and parameters for the second key follow the same format as those for the first key.
Related show command: `show net routing dynamic setup`

---

**IPv6 Routing Commands**

`net routing static ipv6 configure <route name>`

This command configures an IPv6 static route. After you have issued the `net routing static ipv6 configure` command to specify the name of the new route, you enter the net-config [static-routing-ipv6] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**  
Format: `net routing static ipv6 configure <route name>`  
Mode: `net`

**Step 2**  
Format:  
- `active_flag {Y | N}`  
- `destination_address <ipv6-address>`  
- `prefix <prefix length>`  
- `gateway_address {6to4_gateway <ipv6-address> | ipv6_gateway <ipv6-address>}`  
- `interface [WAN1 | WAN2 | WAN3 | WAN4 | Sit0-WAN | LAN | DMZ]`  
- `metric <number>`

Mode: `net-config [static-routing-ipv6]`
Net Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_flag</td>
<td>Y or N</td>
<td>Specifies whether or not the route is an active route.</td>
</tr>
<tr>
<td>destination_address</td>
<td>ipv6-address</td>
<td>The destination IP address.</td>
</tr>
<tr>
<td>prefix</td>
<td>prefix length</td>
<td>The IPv6 prefix length (integer). This is a decimal value that indicates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the number of contiguous, higher-order bits of the address that make up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the network portion of the address.</td>
</tr>
<tr>
<td>interface</td>
<td>WAN1, WAN2, WAN3, WAN4, Sit0-WAN, LAN, or DMZ</td>
<td>Specifies the physical or virtual network interface through which the route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is accessible:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAN1. The selected WAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAN2. The selected WAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAN3. The selected WAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAN4. The selected WAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sit0-WAN1. The 6to4-WAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• LAN. The LAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DMZ. The LAN interface.</td>
</tr>
<tr>
<td>gateway_address</td>
<td>ipv6-address</td>
<td>The gateway IP address for a route that uses a 6to4 tunnel. The 6to4_gateway</td>
</tr>
<tr>
<td>6to4_gateway</td>
<td></td>
<td>and ipv6_gateway keywords are mutually exclusive.</td>
</tr>
<tr>
<td>gateway_address</td>
<td>ipv6-address</td>
<td>The gateway IP address for a route in an IPv6 to IPv6 network. The 6to4_gateway</td>
</tr>
<tr>
<td>ipv6_gateway</td>
<td></td>
<td>and ipv6_gateway keywords are mutually exclusive.</td>
</tr>
<tr>
<td>metric</td>
<td>number</td>
<td>The metric (integer) for this route. The number can be from 2 to 15.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> net routing static ipv6 configure SFO2
net-config[static-routing-ipv6]> active_flag Y
net-config[static-routing-ipv6]> destination_address 2002:201b:24e2::1001
net-config[static-routing-ipv6]> prefix 64
net-config[static-routing-ipv6]> interface WAN1
net-config[static-routing-ipv6]> gateway_address ipv6_gateway FE80::2001:5efe:ab23
net-config[static-routing-ipv6]> metric 2
net-config[static-routing-ipv6]> save

Related show command: show net routing static ipv6 setup

---

**net routing static ipv6 delete <route name>**

This command deletes a static IPv6 route by deleting its name.

**Format**    net routing static ipv6 delete <route name>

**Mode**      net
Related show command: `show net routing static ipv6 setup`

---

**net routing static ipv6 delete_all**

This command deletes all static IPv6 routes.

**Format**

`net routing static ipv6 delete_all`

**Mode**

`net`

---

Related show command: `show net routing static ipv6 setup`
Security Mode Configuration Commands

This chapter explains the configuration commands, keywords, and associated parameters in the security mode. The chapter includes the following sections:

- **Security Services Commands**
- **Security Schedules Commands**
- **IPv4 Add Firewall Rule and Edit Firewall Rule Commands**
- **IPv4 General Firewall Commands**
- **IPv6 Firewall Commands**
- **Attack Check Commands**
- **Session Limit, Time-Out, and Advanced Commands**
- **Address Filter and IP/MAC Binding Commands**
- **Port Triggering Commands**
- **UPnP Command**
- **Bandwidth Profile Commands**
- **Content Filtering Commands**

**IMPORTANT:**

After you have issued a command that includes the word configure, add, or edit, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 12.

### Security Services Commands

**security services add**

This command configures a new firewall custom service. After you have issued the *security services add* command, you enter the security-config [custom-service] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.
**Security Mode Configuration Commands**

**Security Mode Configuration Commands**

**Step 1** Format: `security services add`  
Mode: `security`

**Step 2** Format:  
- `name <service name>`  
- `protocol {TCP {start_port <number>} {finish_port <number>}} | UDP {start_port <number>} {finish_port <number>} | ICMP {icmp_type <number>} | ICMPv6 {icmp_type <number>}`

Mode: `security-config [custom-service]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>service name</td>
<td>The name (alphanumeric string) of the service.</td>
</tr>
<tr>
<td>protocol</td>
<td>TCP, UDP, ICMP, or ICMPv6</td>
<td>Specifies the protocol type that applies to the service.</td>
</tr>
<tr>
<td>start_port</td>
<td>number</td>
<td>For TCP and UDP, the start port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65535.</td>
</tr>
<tr>
<td>finish_port</td>
<td>number</td>
<td>For TCP and UDP, the end port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65535.</td>
</tr>
<tr>
<td>icmp_type</td>
<td>number</td>
<td>The ICMP type (integer) used by the destination user.</td>
</tr>
</tbody>
</table>

**Command example:**
```
SRX5308> security services add
security-config[custom-service]> name Traceroute
security-config[custom-service]> protocol ICMP
security-config[custom-service]> icmp_type 20
security-config[custom-service]> save
```

**Related show command:** `show security services setup`

---

**security services edit <row id>**

This command configures an existing firewall custom service. After you have issued the `security services edit` command to specify the row to be edited, you enter the `security-config [custom-service]` mode, and then you can edit the service. You cannot change the service name.

Step 1 Format: `security services edit <row id>`  
Mode: `security`
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Security Mode Configuration Commands

Step 2 Format

```
protocol {TCP {start_port <number>} {finish_port <number>} | UDP {start_port <number>} {finish_port <number}> | ICMP {icmp_type <number> | ICMPv6 {icmp_type <number>}}
```

Mode

```
security-config [custom-service]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>TCP, UDP, ICMP, or ICMPv6</td>
<td>Specifies the protocol type that applies to the service.</td>
</tr>
<tr>
<td>start_port</td>
<td>number</td>
<td>For TCP and UDP, the start port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65535.</td>
</tr>
<tr>
<td>finish_port</td>
<td>number</td>
<td>For TCP and UDP, the end port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65535.</td>
</tr>
<tr>
<td>icmp_type</td>
<td>number</td>
<td>The ICMP type (integer) used by the destination user.</td>
</tr>
</tbody>
</table>

Related show command: `show security services setup`

security services delete <row id>

This command deletes a custom security service by deleting its row ID.

```
Format     security services delete <row id>
Mode       security
```

Related show command: `show security services setup`

security services qos_profile add

This command configures a new Quality of Service (QoS) profile that you can associate with a nonblocking inbound or outbound IPv4 firewall rule. After you have issued the `security services qos_profile add` command, you enter the security-config [qosProfile] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 Format

```
Format     security services qos_profile add
Mode       security
```

103
**Step 2 Format**  
```
profile_name <profile name>
remark {N | Y} {qos_type | IP-Precedence | DSCP} {qos_value <number>}
qos_priority {Default | High | Medium-high | Medium | Low}
```

**Mode**  
```
security-config [qosProfile]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>profile name</td>
<td>The name (alphanumeric string) of the profile.</td>
</tr>
<tr>
<td>remark</td>
<td>Y or N</td>
<td>Specifies whether or not packets are remarked. If you select Y, you also need to issue the qos_type keyword to specify the traffic classification method and the qos_value keyword to specify the associated value.</td>
</tr>
</tbody>
</table>
| qos_type                                     | IP-Precedence or DSCP                          | Specifies the traffic classification method:  
  • **IP-Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. You need to issue the qos_value keyword to specify the IP precedence value.  
  • **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header. You need to issue the qos_value keyword to specify the DSCP value. |
| qos_value                                    | number                                         | There are two options:  
  • If the qos_type keyword is set to IP-Precedence, the IP precedence value, from 0 through 7. Packets are remarked with this value.  
  • If the qos_type keyword is set to DSCP, the DSCP value, from 1 through 63. Packets are remarked with this value. |
**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**Security Mode Configuration Commands**

### Command example:

```
SRX5308> security services qos_profile add
security-config[qosProfile]> profile name Voice
security-config[qosProfile]> remark Y
security-config[qosProfile]> qos_type DSCP
security-config[qosProfile]> qos_value 24
security-config[qosProfile]> qos_priority High
security-config[qosProfile]> save
```

**Related show command:** `show security services qos_profile setup`

### security services qos_profile edit <row id>

This command configures an existing Quality of Service (QoS) profile that you can associate with a nonblocking inbound or outbound IPv4 firewall rule. After you have issued the `security services qos_profile edit` command to specify the row to be edited, you enter the security-config [qosProfile] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the profile.

**Step 1** Format **security services qos_profile edit <row id>**

**Mode** security

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| qos_priority                                | Default, High, Medium-high, Medium, or Low       | Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall:  
- **Default.** Traffic is mapped based on the ToS field in the packet's IP header.  
- **High.** This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4.  
- **Medium-high.** This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3.  
- **Medium.** This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2.  
- **Low.** This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values. |
### Security Mode Configuration Commands

**Step 2 Format**

```plaintext
remark \{N | Y \[qos_type \{IP-Precedence | DSCP\} \{qos_value <number>\}\}\}
qos_priority \{Default | High | Medium-high | Medium | Low\}
```

**Mode**

`security-config [qosProfile]`

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remark</td>
<td>Y or N</td>
<td>Specifies whether or not packets are remarked. If you select Y, you also need to issue the <code>qos_type</code> keyword to specify the traffic classification method and the <code>qos_value</code> keyword to specify the associated value.</td>
</tr>
</tbody>
</table>
| qos_type                                     | IP-Precedence or DSCP                         | Specifies the traffic classification method:  
  - **IP-Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. You need to issue the `qos_value` keyword to specify the IP precedence value.  
  - **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header. You need to issue the `qos_value` keyword to specify the DSCP value. |
| qos_value                                   | number                                        | There are two options:  
  - If the `qos_type` keyword is set to **IP-Precedence**, the IP precedence value, from 0 through 7. Packets are remarked with this value.  
  - If the `qos_type` keyword is set to **DSCP**, the DSCP value, from 1 through 63. Packets are remarked with this value. |
### Keywords and Descriptions

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| qos_priority                                 | Default, High, Medium-high, Medium, or Low       | Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall:  
• Default. Traffic is mapped based on the ToS field in the packet's IP header.  
• High. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4.  
• Medium-high. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3.  
• Medium. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2.  
• Low. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values. |

#### Related show command:

`show security services qos_profile setup`

---

### security services qos_profile delete <row id>

This command deletes a QoS profile by deleting its row ID.

**Format**

```
security services qos_profile delete <row id>
```

**Mode**

`security`

#### Related show command:

`show security services qos_profile setup`

---

### security services ip_group add

This command configures a new LAN or WAN IP group. After you have issued the `security services ip_group add` command, you enter the security-config [ipGroup] mode, and then you can configure the group type and name in the order that you prefer.

**Step 1**

**Format**

```
security services ip_group add
```

**Mode**

`security`
## Security Mode Configuration Commands

### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Step 2 Format**

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip_group_type                                | LAN-Group or WAN-Group                           | Specifies the type of IP group:  
  - **LAN-Group**: The group can be used as a firewall object in an IPv4 LAN firewall rule.  
  - **WAN-Group**: The group can be used as a firewall object in an IPv4 WAN firewall rule. |
| ip_group_name                                | group name                                       | The name (alphanumeric string) of the group. |

**Command example:**

```
SRX5308> security services ip_group add
security-config[ipGroup]> ip_group_type LAN-Group
security-config[ipGroup]> ip_group_name TechSupport
security-config[ipGroup]> save
```

**Related show command:** `show security services ip_group ip_setup`

---

**security services ip_group edit <row id>**

This command configures an existing LAN or WAN IP group. After you have issued the `security services ip_group edit` command to specify the row to be edited, you enter the `security-config [ipGroup]` mode, and then you can configure the group type and name in the order that you prefer.

**Step 1 Format**

<table>
<thead>
<tr>
<th>Format</th>
<th>security services ip_group edit &lt;row id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>security</td>
</tr>
</tbody>
</table>

**Step 2 Format**

| Format | ip_group_type (LAN-Group | WAN-Group) |
|--------|--------------------------|
|        | ip_group_name <group name> |
| Mode   | security-config [ipGroup] |
### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Security Mode Configuration Commands**

**Related show command:** `show security services ip_group ip_setup`

### security services ip_group add_ip_to <group name>

This command adds an IPv4 address to a LAN or WAN IP group. After you have issued the `security services ip_group add_ip_to` command to specify the LAN IP or WAN IP group name to which an IP address is to be added, you enter the `security-config [ipGroup-Ip]` mode, and then you can add the IP address.

**Command example:**

```
SRX5308> security services ip_group add_ip_to TechSupport
security-config[ipGroup-Ip]> ip_address 10.55.3.201
security-config[ipGroup-Ip]> save
```

**Related show command:** `show security services ip_group ip_setup`
security services ip_group delete <row id>

This command deletes a LAN or WAN IP group by deleting its row ID.

Format  
security services ip_group delete <row id>

Mode  
security

Related show command: show security services ip_group ip_setup

security services ip_group delete_ip <row id>

This command removes an IP address from a LAN or WAN IP group by deleting the row ID of the IP address.

Format  
security services ip_group delete_ip <row id>

Mode  
security

Related show command: show security services ip_group ip_setup

Security Schedules Commands

security schedules edit {1 | 2 | 3}

This command configures one of the three security schedules. After you have issued the security schedule edit command to specify the row (that is, the schedule: 1, 2, or 3) to be edited, you enter the security-config [schedules] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 Format  
security schedules edit {1 | 2 | 3}

Mode  
security

Step 2 Format  

days {all [Y | N] ([days sunday [Y | N]] [days monday [Y | N]] [days tuesday [Y | N]] [days wednesday [Y | N]] [days thursday [Y | N]] [days friday [Y | N]] [days saturday [Y | N]])}

time_of_day {all_enable [Y | N] [time_of_day start hours <hour>] [time_of_day start minutes <minute>] [time_of_day start meridiem [AM | PM]] [time_of_day end hours <hour>] [time_of_day end minutes <minute>] [time_of_day end meridiem [AM | PM]]}

Mode  
security-config [schedules]
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (consists of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>days all</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on all days.</td>
</tr>
<tr>
<td>days sunday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Sundays.</td>
</tr>
<tr>
<td>days monday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Mondays.</td>
</tr>
<tr>
<td>days tuesday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Tuesdays.</td>
</tr>
<tr>
<td>days wednesday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Wednesdays.</td>
</tr>
<tr>
<td>days thursday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Thursdays.</td>
</tr>
<tr>
<td>days friday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Fridays.</td>
</tr>
<tr>
<td>days saturday</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active on Saturdays.</td>
</tr>
<tr>
<td>time_of_day all_enable</td>
<td>Y or N</td>
<td>Specifies whether or not the schedule is active all day.</td>
</tr>
<tr>
<td>time_of_day start hours</td>
<td>hour</td>
<td>The schedule starts at the specified hour in the 12-hour format HH (00 to 12).</td>
</tr>
<tr>
<td>time_of_day start mins</td>
<td>minute</td>
<td>The schedule starts at the specified minute in the format MM (00 to 59).</td>
</tr>
<tr>
<td>time_of_day start meridiem</td>
<td>AM or PM</td>
<td>Specifies the meridiem for the start time.</td>
</tr>
<tr>
<td>time_of_day end hours</td>
<td>hour</td>
<td>The schedule ends at the specified hour in the 12-hour format HH (00 to 12).</td>
</tr>
<tr>
<td>time_of_day end mins</td>
<td>minute</td>
<td>The schedule ends at the specified minute in the format MM (00 to 59).</td>
</tr>
<tr>
<td>time_of_day end meridiem</td>
<td>AM or PM</td>
<td>Specifies the meridiem for the end time.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> security schedule edit 1
security-config[schedules]> days monday Y
security-config[schedules]> days tuesday Y
security-config[schedules]> days wednesday Y
security-config[schedules]> days thursday Y
security-config[schedules]> days friday Y
security-config[schedules]> time_of_day start hours 07
security-config[schedules]> time_of_day start mins 30
security-config[schedules]> time_of_day start meridiem AM
security-config[schedules]> time_of_day end hours 08
IPv4 Add Firewall Rule and Edit Firewall Rule Commands

```
security firewall ipv4 add_rule lan_wan outbound
```

This command configures a new IPv4 LAN WAN outbound firewall rule. After you have issued the `security firewall ipv4 add_rule lan_wan outbound` command, you enter the security-config [firewall-ipv4-lan-wan-outbound] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters can you can apply to a rule.

**Step 1** Format
```
security firewall ipv4 add_rule lan_wan outbound
```

**Mode** security

**Step 2** Format
```
Mode security-config [firewall-ipv4-lan-wan-outbound]
```

**Format**
```
service_name {default_services <default service name> | {custom_services <custom service name>})
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
```

**lan_users** {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>} {lan_user_end_ip <ipaddress>}) | group_wise <group name>}

**wan_users** {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>} {wan_user_end_ip <ipaddress>}) | group_wise <group name>}

```
qos_profile <profile name>
log {NEVER | ALWAYS}
```

**bandwidth_profile** <profile name>
```
|nat_ip type Auto | WAN1 | WAN2 | WAN3 | WAN4| address <ipaddress>}
```

**Mode** security-config [firewall-ipv4-lan-wan-outbound]
## Security Mode Configuration Commands

### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service name, action, and schedule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>service_name</td>
<td>custom service name</td>
<td></td>
</tr>
<tr>
<td>custom_services</td>
<td></td>
<td>The custom service that you have configured with the <code>security services add</code> command and to which the firewall rule applies.</td>
</tr>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
</tbody>
</table>

### LAN user addresses or LAN group and WAN user addresses

<table>
<thead>
<tr>
<th>lan_users address-wise</th>
<th>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</th>
<th>Specifies the type of LAN address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</th>
</tr>
</thead>
</table>
| lan_user_start_ip                            | ipaddress                                        | There are two options:  

- The IP address if the `lan_users address_wise` keywords are set to `SINGLE_ADDRESS`.  
- The start IP address if the `lan_users address_wise` keywords are set to `ADDRESS_RANGE`. |
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_users group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command. The LAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>wan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
| wan_user_start_ip                             | ipaddress                                       | There are two options:  
* The IP address if the wan_users keyword is set to SINGLE_ADDRESS.  
* The start IP address if the wan_users keyword is set to ADDRESS_RANGE. |
<p>| wan_user_end_ip                               | ipaddress                                       | The end IP address if the wan_users keyword is set to ADDRESS_RANGE. |
| wan_users group_wise                          | group name                                      | The name of the WAN IP group. The WAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive. |
| <strong>QoS profile, logging, bandwidth profile, and NAT IP address</strong> | | |
| qos_profile                                   | profile name                                    | The name of the QoS profile that you have specified with the security services qos_profile add command. |</p>
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>NEVER or ALWAYS</td>
<td>Specifies whether logging is disabled or enabled.</td>
</tr>
<tr>
<td>bandwidth_profile</td>
<td>profile name</td>
<td>The name of the bandwidth profile that you have specified with the <code>security bandwidth profile add</code> command.</td>
</tr>
</tbody>
</table>
| nat_ip type                                 | Auto, WAN1, WAN2, WAN3, or WAN4                  | Specifies the type of NAT IP address for a nonblocking rule:  
• Auto. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules.  
• WAN1, WAN2, WAN3, or WAN4. The IP address of the selected WAN interface.  
  **Note:** The `nat_ip type` and `nat_ip address` keywords are mutually exclusive. |
| nat_ip address                              | ipaddress                                       | The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address.  
  **Note:** The `nat_ip type` and `nat_ip address` keywords are mutually exclusive. |

**Command example:**

SRX5308> `security firewall ipv4 add_rule lan_wan outbound`  
security-config[firewall-ipv4-lan-wan-outbound]> `service_name default_services HTTP`  
security-config[firewall-ipv4-lan-wan-outbound]> `action ALWAYS_ALLOW`  
security-config[firewall-ipv4-lan-wan-outbound]> `lan_users group_wise SalesAmericas`  
security-config[firewall-ipv4-lan-wan-outbound]> `wan_users address_wise ANY`  
security-config[firewall-ipv4-lan-wan-outbound]> `bandwidth_profile PriorityQueue`  
security-config[firewall-ipv4-lan-wan-outbound]> `nat_ip type Auto`  
security-config[firewall-ipv4-lan-wan-outbound]> `log NEVER`  
security-config[firewall-ipv4-lan-wan-outbound]> `save`  

**Related show command:** `show security firewall ipv4 setup lan_wan`
security firewall ipv4 edit_rule lan_wan outbound <row id>

This command configures an existing IPv4 LAN WAN outbound firewall rule. After you have issued the `security firewall ipv4 edit_rule lan_wan outbound` command to specify the row to be edited (for row information, see the output of the `show security firewall ipv4 setup lan_wan` command), you enter the security-config [firewall-ipv4-lan-wan-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters you can apply to a rule.

**Step 1 Format**
```
security firewall ipv4 edit_rule lan_wan outbound <row id>
```
**Mode**
`security`

**Step 2 Format**
```
service_name {default_services <default service name> | {custom_services <custom service name>}}
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
lan_users {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip <ipaddress>}} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}} | group_wise <group name>)
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>}} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}} | group_wise <group name>)
qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
{nat_ip_type {Auto | WAN1 | WAN2 | WAN3 | WAN4} | address <ipaddress>}
```
**Mode**
`security-config [firewall-ipv4-lan-wan-outbound]`
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default_services</strong></td>
<td>custom service name</td>
<td>The custom service that you have configured with the <code>security services add</code> command and to which the firewall rule applies.</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td><strong>schedule</strong></td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td><strong>LAN user addresses or LAN group and WAN user addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>lan_users address_wise</strong></td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><strong>lan_user_start_ip</strong></td>
<td>ipaddress</td>
<td>There are two options: *The IP address if the <code>lan_users address_wise</code> keywords are set to <code>SINGLE_ADDRESS</code>. *The start IP address if the <code>lan_users address_wise</code> keywords are set to <code>ADDRESS_RANGE</code>.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_users group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command. The LAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>wan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
| wan_user_start_ip                           | ipaddress                                      | There are two options:  
  • The IP address if the wan_users keyword is set to SINGLE_ADDRESS.  
  • The start IP address if the wan_users keyword is set to ADDRESS_RANGE. |
<p>| wan_user_end_ip                             | ipaddress                                      | The end IP address if the wan_users keyword is set to ADDRESS_RANGE. |
| wan_users group_wise                        | group name                                     | The name of the WAN IP group. The WAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive. |
| QoS profile, logging, bandwidth profile, and NAT IP address | | |
| qos_profile                                 | profile name                                   | The name of the QoS profile that you have specified with the security services qos_profile add command. |</p>
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>NEVER or ALWAYS</td>
<td>Specifies whether logging is disabled or enabled.</td>
</tr>
<tr>
<td>bandwidth_profile</td>
<td>profile name</td>
<td>The name of the bandwidth profile that you have specified with the <code>security bandwidth profile add</code> command.</td>
</tr>
</tbody>
</table>
| nat_ip type                                  | Auto, WAN1, WAN2, WAN3, or WAN4                 | Specifies the type of NAT IP address for a nonblocking rule:  
  • Auto. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules.  
  • WAN1, WAN2, WAN3, or WAN4. The IP address of the selected WAN interface.  
  **Note:** The `nat_ip type` and `nat_ip address` keywords are mutually exclusive. |
| nat_ip address                               | ipaddress                                       | The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address.  
  **Note:** The `nat_ip type` and `nat_ip address` keywords are mutually exclusive. |

**Command example:** See the command example for the `security firewall ipv4 add_rule lan_wan outbound` command.

**Related show command:** `show security firewall ipv4 setup lan_wan`
security firewall ipv4 add_rule lan_wan inbound

This command configures a new IPv4 LAN WAN outbound firewall rule. After you have issued the `security firewall ipv4 add_rule lan_wan inbound` command, you enter the security-config [firewall-ipv4-lan-wan-inbound] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters can you can apply to a rule.

**Step 1 Format**
```
security firewall ipv4 add_rule lan_wan inbound
```

**Mode**
```
security
```

**Step 2 Format**
```
service_name {default_services <default service name> | 
{custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
  BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
  Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK 
{schedule {Schedule1 | Schedule2 | Schedule3}}}
send_to_lan_server {SINGLE_ADDRESS {send_to_lan_server_start_ip <ipaddress>} | ADDRESS_RANGE {send_to_lan_server_start_ip <ipaddress>} {send_to_lan_server_end_ip <ipadress>}}
translate_to_port_number enable {N | Y} 
{translate_to_port_number port <number>}
wan_destination_ip_address {WAN1 | WAN2 | WAN3 | WAN4} | RANGE 
{wan_destination_ip_address_start <ipaddress>}
{wan_destination_ip_address_end <ipaddress>}
lan_user {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip <ipaddress>} 
{lan_user_end_ip <ipaddress>}} | group_wise <group name>}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip 
<iipaddress>}} | ADDRESS_RANGE {wan_user_start_ip <iipaddress>} 
{wan_user_end_ip <iipaddress>}} | group_wise <group name>}
qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
```
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service name, action, and schedule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default_services</td>
<td>custom service name</td>
<td>The custom service that you have configured with the <strong>security services add</strong> command and to which the firewall rule applies.</td>
</tr>
<tr>
<td><strong>LAN server addresses, port number translation, and WAN destination addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>send_to_lan_server</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address.</td>
</tr>
</tbody>
</table>
| send_to_lan_server_start_ip                  | ipaddress                                        | There are two options:  
• The IP address if the **send_to_lan_server** keyword is to **SINGLE_ADDRESS**.  
• The start IP address if the **send_to_lan_server** keyword is set to **ADDRESS_RANGE**. |
<p>| send_to_lan_server_end_ip                    | ipaddress                                        | The end IP address if the <strong>send_to_lan_server</strong> keyword is set to <strong>ADDRESS_RANGE</strong>. |</p>
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>translate_to_port_number enable</td>
<td>Y or N</td>
<td>Enables or disables port forwarding.</td>
</tr>
<tr>
<td>translate_to_port_number port</td>
<td>number</td>
<td>The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65535.</td>
</tr>
</tbody>
</table>
| wan_destination_ip_address                 | WAN1, WAN2, WAN3, WAN4, or RANGE               | Specifies the type of destination WAN address for an inbound rule:  
  • WAN1, WAN2, WAN3, or WAN4. The IP address of the selected WAN interface.  
  • RANGE. A range of public IP addresses, which you need to configure by issuing the wan_destination_ip_address_start and wan_destination_ip_address_end keywords and specifying IPv4 addresses. |
| wan_destination_ip_address_start           | ipaddress                                     | The start IP address if the wan_destination_ip_address keyword is set to RANGE. |
| wan_destination_ip_address_end             | ipaddress                                     | The end IP address if the wan_destination_ip_address keyword is set to RANGE. |

**LAN user addresses or LAN group and WAN user addresses**

| lan_user_address_wise                     | ANY, SINGLE_ADDRESS, or ADDRESS_RANGE         | Specifies the type of LAN address. The address_wise and group_wise keywords are mutually exclusive.  
  For an inbound rule, this option is available only when the WAN mode is Classical Routing. |
| lan_user_start_ip                         | ipaddress                                     | There are two options:  
  • The IP address if the lan_user_address_wise keywords are set to SINGLE_ADDRESS.  
  • The start IP address if the lan_user_address_wise keywords are set to ADDRESS_RANGE. |
<p>| lan_user_end_ip                           | ipaddress                                     | The end IP address if the lan_user_address_wise keywords are set to ADDRESS_RANGE. |</p>
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan_user group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the <code>net lan lan_groups edit &lt;row_id&gt; &lt;new group name&gt;</code> command. The LAN IP group name is a name that you have specified with the <code>security services ip_group add</code> command. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.</td>
</tr>
<tr>
<td>wan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
| wan_user_start_ip                             | ipaddress                                     | There are two options:  
  • The IP address if the `wan_user` keyword is set to SINGLE_ADDRESS.  
  • The start IP address if the `wan_user` keyword is set to ADDRESS_RANGE. |
| wan_user_end_ip                               | ipaddress                                     | The end IP address if the `wan_user` keyword is set to ADDRESS_RANGE. |
| wan_users group_wise                          | group name                                    | The name of the WAN IP group. The WAN IP group name is a name that you have specified with the `security services ip_group add` command. The `address_wise` and `group_wise` keywords are mutually exclusive. |

**QoS profile, logging, and bandwidth profile**

| qos_profile | profile name | The name of the QoS profile that you have specified with the `security services qos_profile add` command. |
Command example:

SRX5308> security firewall ipv4 add_rule lan_wan inbound
security-config[firewall-ipv4-lan-wan-inbound]> service_name default_services FTP
security-config[firewall-ipv4-lan-wan-inbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-lan-wan-inbound]> send_to_lan_server SINGLE_ADDRESS
security-config[firewall-ipv4-lan-wan-inbound]> send_to_lan_server_start_ip 192.168.5.71
security-config[firewall-ipv4-lan-wan-inbound]> wan_destination_ip_address_start 10.168.50.1
security-config[firewall-ipv4-lan-wan-inbound]> wan_user ANY
security-config[firewall-ipv4-lan-wan-inbound]> qos_profile Standard
security-config[firewall-ipv4-lan-wan-inbound]> log NEVER
security-config[firewall-ipv4-lan-wan-inbound]> save

Related show command: show security firewall ipv4 setup lan_wan

security firewall ipv4 edit_rule lan_wan inbound <row id>

This command configures an existing IPv4 LAN WAN inbound firewall rule. After you have issued the security firewall ipv4 edit_rule lan_wan inbound command to specify the row to be edited (for row information, see the output of the show security firewall ipv4 setup lan_wan command), you enter the security-config [firewall-ipv4-lan-wan-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the action keyword determines which other keywords and parameters you can apply to a rule.

Step 1 Format security firewall ipv4 edit_rule lan_wan inbound <row id>
Step 2 Format service_name {default_services <default service name> | 
{custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK |
schedule {Schedule1 | Schedule2 | Schedule3}}

Security Mode Configuration Commands
send_to_lan_server {SINGLE_ADDRESS {send_to_lan_server_start_ip <ipaddress>}} | ADDRESS_RANGE {send_to_lan_server_start_ip <ipaddress>} | ADDRESS_RANGE {send_to_lan_server_end_ip <ipaddress>}])
translate_to_port_number enable {N | Y} [translate_to_port_number <number>]
wan_destination_ip_address {[WAN1 | WAN2 | WAN3 | WAN4] | RANGE {wan_destination_ip_address_start <ipaddress>}} {wan_destination_ip_address_end <ipaddress>})

lan_user {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip <ipaddress>}} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}} | group_wise <group name>}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>}} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}} | group_wise <group name>}

qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>

Mode security-config [firewall-ipv4-lan-wan-inbound]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>service_name custom_services</td>
<td>custom service name</td>
<td>The custom service that you have configured with the <code>security services add</code> command and to which the firewall rule applies.</td>
</tr>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td>LAN server addresses, port number translation, and WAN destination addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>send_to_lan_server</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address.</td>
</tr>
</tbody>
</table>
| send_to_lan_server_start_ip                 | ipaddress                                      | There are two options:  
- The IP address if the `send_to_lan_server` keyword is to SINGLE_ADDRESS.  
- The start IP address if the `send_to_lan_server` keyword is set to ADDRESS_RANGE. |
| send_to_lan_server_end_ip                   | ipaddress                                      | The end IP address if the `send_to_lan_server` keyword is set to ADDRESS_RANGE. |
| translate_to_port_number enable             | Y or N                                          | Enables or disables port forwarding. |
| translate_to_port_number port               | number                                          | The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65535. |
| wan_destination_ip_address                  | WAN1, WAN2, WAN3, WAN4, or RANGE                | Specifies the type of destination WAN address for an inbound rule:  
- WAN1, WAN2, WAN3, or WAN4. The IP address of the selected WAN interface.  
- RANGE. A range of public IP addresses, which you need to configure by issuing the `wan_destination_ip_address_start` and `wan_destination_ip_address_end` keywords and specifying IPv4 addresses. |
<p>| wan_destination_ip_address_start            | ipaddress                                      | The start IP address if the <code>wan_destination_ip_address</code> keyword is set to RANGE. |</p>
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan_destination_ip_address_end</td>
<td>ipaddress</td>
<td>The end IP address if the wan_destination_ip_address keyword is set to RANGE.</td>
</tr>
<tr>
<td><strong>LAN user addresses or LAN group and WAN user addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lan_user_address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address. The address_wise and group_wise keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.</td>
</tr>
<tr>
<td>lan_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the lan_user_address_wise keywords are set to SINGLE_ADDRESS. • The start IP address if the lan_user_address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_user_address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_user_group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the <code>net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt;</code> command. The LAN IP group name is a name that you have specified with the <code>security services ip_group add</code> command. The address_wise and group_wise keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.</td>
</tr>
<tr>
<td>wan_users_address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
Security Mode Configuration Commands

### Command example:
See the command example for the `security firewall ipv4 add_rule lan_wan inbound` command.

### Related show command:
`show security firewall ipv4 setup lan_wan`

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| wan_user_start_ip                            | ipaddress                                     | There are two options:  
  - The IP address if the `wan_user` keyword is set to `SINGLE_ADDRESS`.  
  - The start IP address if the `wan_user` keyword is set to `ADDRESS_RANGE`. |
| wan_user_end_ip                               | ipaddress                                     | The end IP address if the `wan_user` keyword is set to `ADDRESS_RANGE`. |
| wan_users group_wise                          | group name                                     | The name of the WAN IP group.  
  The WAN IP group name is a name that you have specified with the `security services ip_group add` command.  
  The `address_wise` and `group_wise` keywords are mutually exclusive. |

**QoS profile, logging, and bandwidth profile**

| qos_profile                                   | profile name                                  | The name of the QoS profile that you have specified with the `security services qos_profile add` command. |
| log                                          | NEVER or ALWAYS                               | Specifies whether logging is disabled or enabled. |
| bandwidth_profile                            | profile name                                  | The name of the bandwidth profile that you have specified with the `security bandwidth_profile add` command. |
Security Mode Configuration Commands

security firewall ipv4 add_rule dmz_wan outbound

This command configures a new IPv4 DMZ WAN outbound firewall rule. After you have issued the `security firewall ipv4 add_rule dmz_wan outbound` command, you enter the security-config [firewall-ipv4-dmz-wan-outbound] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters you can apply to a rule.

Step 1 Format
security firewall ipv4 add_rule dmz_wan outbound
Mode
security

Step 2 Format
service_name {default_services <default service name> | [custom_services <custom service name>]
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>} | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}} | group_wise <group name>}
qos_profile <profile name>
log {NEVER | ALWAYS}
{nat_ip_type {Auto | WAN1 | WAN2 | WAN3 | WAN4} | address <ipaddress>}

Mode
security-config [firewall-ipv4-dmz-wan-outbound]
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service name, action, and schedule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom_services</td>
<td>custom service name</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>DMZ user addresses and WAN user addresses</td>
</tr>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address.</td>
</tr>
<tr>
<td>dmz_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The IP address if the <code>dmz_users</code> keyword is set to SINGLE_ADDRESS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The start IP address if the <code>dmz_users</code> keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>dmz_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the <code>dmz_users</code> keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><code>wan_users address_wise</code></td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><code>wan_user_start_ip</code></td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the <code>wan_user</code> keyword is set to SINGLE_ADDRESS. • The start IP address if the <code>wan_user</code> keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td><code>wan_user_end_ip</code></td>
<td>ipaddress</td>
<td>The end IP address if the <code>wan_user</code> keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td><code>wan_users group_wise</code></td>
<td>group name</td>
<td>The name of the WAN IP group. The WAN IP group name is a name that you have specified with the <code>security services ip_group add</code> command. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>

### QoS profile, logging, and NAT IP address

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>qos_profile</code></td>
<td>profile name</td>
<td>The name of the QoS profile that you have specified with the <code>security services qos_profile add</code> command.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>NEVER or ALWAYS</td>
<td>Specifies whether logging is disabled or enabled.</td>
</tr>
<tr>
<td><code>nat_ip type</code></td>
<td>Auto, WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the type of NAT IP address for a nonblocking rule: • Auto. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • WAN1, WAN2, WAN3, or WAN4. The IP address of the selected WAN interface. <strong>Note:</strong> The <code>nat_ip type</code> and <code>nat_ip address</code> keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
## Command example:

SRX5308> security firewall ipv4 add_rule dmz_wan outbound
security-config[firewall-ipv4-dmz-wan-outbound]> service_name default_services CU-SEEME:TCP
security-config[firewall-ipv4-dmz-wan-outbound]> action BLOCK_BY_SCHEDULE_ELSE_BLOCK
security-config[firewall-ipv4-dmz-wan-outbound]> schedule Schedule2
security-config[firewall-ipv4-dmz-wan-outbound]> dmz_users ANY
security-config[firewall-ipv4-dmz-wan-outbound]> wan_users ANY
security-config[firewall-ipv4-dmz-wan-outbound]> qos_profile Video
security-config[firewall-ipv4-dmz-wan-outbound]> log Never
security-config[firewall-ipv4-dmz-wan-outbound]> nat_ip_type WAN1
security-config[firewall-ipv4-dmz-wan-outbound]> save

Related show command: `show security firewall ipv4 setup dmz_wan`

---

### security firewall ipv4 edit_rule dmz_wan outbound `<row id>`

This command configures an existing IPv4 DMZ WAN outbound firewall rule. After you have issued the `security firewall ipv4 DMZ WAN outbound firewall` command to specify the row to be edited (for row information, see the output of the `show security firewall ipv4 setup dmz_wan` command), you enter the security-config [firewall-ipv4-dmz-wan-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters you can apply to a rule.

**Step 1**

Format: `security firewall ipv4 edit_rule dmz_wan outbound <row id>`

Mode: `security`

**Step 2**

Format:

```
security_name {default_services <default service name> | {custom_services <custom service name>}}
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
```

---

## Table: nat_ip address

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat_ip address</td>
<td>ipaddress</td>
<td>The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address. <strong>Note:</strong> The <code>nat_ip_type</code> and <code>nat_ip_address</code> keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
**dmz_users** [ANY | SINGLE_ADDRESS (dmz_user_start_ip <ipaddress>) | ADDRESS_RANGE (dmz_user_start_ip <ipaddress>) | Address_RANGE (dmz_user_start_ip <ipaddress>) | Address_RANGE (dmz_user_start_ip <ipaddress>)]

**wan_users** [address_wise [ANY | SINGLE_ADDRESS (wan_user_start_ip <ipaddress>) | ADDRESS_RANGE (wan_user_start_ip <ipaddress>) | ADDRESS_RANGE (wan_user_start_ip <ipaddress>) | Address_RANGE (wan_user_start_ip <ipaddress>) | Address_RANGE (wan_user_start_ip <ipaddress>) | Address_RANGE (wan_user_start_ip <ipaddress>) | Address_RANGE (wan_user_start_ip <ipaddress>)]

**qos_profile** <profile name>

**log** {NEVER | ALWAYS}

{nat_ip type {Auto | WAN1 | WAN2 | WAN3 | WAN4} | address <ipaddress>}

**Mode** security-config [firewall-ipv4-dmz-wan-outbound]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_name action schedule</td>
<td>service_name default_services</td>
<td></td>
</tr>
<tr>
<td>service_name custom_services</td>
<td>custom service name</td>
<td>The custom service that you have configured with the <strong>security services add</strong> command and to which the firewall rule applies.</td>
</tr>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DMZ user addresses and WAN user addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address.</td>
</tr>
</tbody>
</table>
| dmz_user_start_ip                             | ipaddress                                       | There are two options:  
  • The IP address if the dmz_users keyword is set to SINGLE_ADDRESS.  
  • The start IP address if the dmz_users keyword is set to ADDRESS_RANGE. |
| dmz_user_end_ip                               | ipaddress                                       | The end IP address if the dmz_users keyword is set to ADDRESS_RANGE. |
| wan_users address_wise                        | ANY, SINGLE_ADDRESS, or ADDRESS_RANGE           | Specifies the type of WAN address.  
  The address_wise and group_wise keywords are mutually exclusive. |
| wan_user_start_ip                             | ipaddress                                       | There are two options:  
  • The IP address if the wan_user keyword is set to SINGLE_ADDRESS.  
  • The start IP address if the wan_user keyword is set to ADDRESS_RANGE. |
| wan_user_end_ip                               | ipaddress                                       | The end IP address if the wan_user keyword is set to ADDRESS_RANGE. |
| wan_users group_wise                          | group name                                       | The name of the WAN IP group.  
  The WAN IP group name is a name that you have specified with the security services ip_group add command.  
  The address_wise and group_wise keywords are mutually exclusive. |
| QoS profile, logging, and NAT IP address      |                                                 |             |
| qos_profile                                   | profile name                                    | The name of the QoS profile that you have specified with the security services qos_profile add command. |
| log                                          | NEVER or ALWAYS                                  | Specifies whether logging is disabled or enabled. |


### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Security Mode Configuration Commands**

#### Command example:

See the command example for the `security firewall ipv4 add_rule dmz_wan outbound` command.

**Related show command:** `show security firewall ipv4 setup dmz_wan`

---

### security firewall ipv4 add_rule dmz_wan inbound

This command configures a new IPv4 DMZ WAN inbound firewall rule. After you have issued the `security firewall ipv4 add_rule dmz_wan inbound` command, you enter the security-config [firewall-ipv4-dmz-wan-inbound] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters can you can apply to a rule.

**Step 1** Format  
Mode  

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat_ip type                                  | Auto, WAN1, WAN2, WAN3, or WAN4                  | Specifies the type of NAT IP address for a nonblocking rule:  
  • **Auto.** The source address of the outgoing packets is autodetected through the configured routing and load balancing rules.  
  • **WAN1, WAN2, WAN3, or WAN4.** The IP address of the selected WAN interface.  
  
  **Note:** The `nat_ip type` and `nat_ip address` keywords are mutually exclusive. |
| nat_ip address                               | ipaddress                                       | The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address.  
  
  **Note:** The `nat_ip type` and `nat_ip address` keywords are mutually exclusive. |

---

<table>
<thead>
<tr>
<th>Security Mode Configuration Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>135</td>
</tr>
</tbody>
</table>
Step 2 Format

```
service_name {default_services <default service name> | {custom_services <custom service name>})
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
    BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3})} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3})}
```

send_to_dmz_server_ip <ipaddress>
translate_to_port_number enable {N | Y}
{translate_to_port_number port <number>}}
{wan_destination_ip_address {WAN1 | WAN2 | WAN3 | WAN4}
wan_destination_ip_address_start <ipaddress>}

dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
| ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}}
{dmz_user_end_ip <ipaddress>}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>}
| ADDRESS_RANGE {wan_user_start_ip <ipaddress>}}
| group_wise <group name>}
{wan_user_end_ip <ipaddress>}}
qos_profile <profile name>
log {NEVER | ALWAYS}

Mode

security-config [firewall-ipv4-dmz-wan-inbound]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
### Security Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_name</td>
<td>custom service name</td>
<td>The custom service that you have configured with the security services add command and to which the firewall rule applies.</td>
</tr>
<tr>
<td>custom_services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
</tbody>
</table>

**DMZ server address, port number translation, and WAN destination address**

<table>
<thead>
<tr>
<th>send_to_dmz_server_ip</th>
<th>ipaddress</th>
<th>The IP address of the DMZ server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>translate_to_port_number</td>
<td>enable Y or N</td>
<td>Enables or disables port forwarding.</td>
</tr>
<tr>
<td>translate_to_port_number port</td>
<td>number</td>
<td>The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65535.</td>
</tr>
<tr>
<td>wan_destination_ip_address</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the IP address of the selected WAN interface as the destination address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The wan_destination_ip_address and wan_destination_ip_address_start keywords are mutually exclusive.</td>
</tr>
<tr>
<td>wan_destination_ip_address_start</td>
<td>ipaddress</td>
<td>The WAN IP address, if the destination address is different from the IP address of a WAN interface, for example, a secondary WAN IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The wan_destination_ip_address and wan_destination_ip_address_start keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>

**DMZ user addresses and WAN user addresses**

| dmz_users                                    | ANY, SINGLE_ADDRESS, or ADDRESS_RANGE          | Specifies the type of DMZ address. For an inbound rule, this option is available only when the WAN mode is Classical Routing. |
### Security Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| `dmz_user_start_ip`                         | `ipaddress`                                      | There are two options:  
  • The IP address if the `dmz_users` keyword is set to `SINGLE_ADDRESS`.  
  • The start IP address if the `dmz_users` keyword is set to `ADDRESS_RANGE`. |
| `dmz_user_end_ip`                           | `ipaddress`                                      | The end IP address if the `dmz_users` keyword is set to `ADDRESS_RANGE`. |
| `wan_users address_wise`                    | ANY SINGLE ADDRESS, or ADDRESS_RANGE             | Specifies the type of WAN address.  
  The `address_wise` and `group_wise` keywords are mutually exclusive. |
| `wan_user_start_ip`                         | `ipaddress`                                      | There are two options:  
  • The IP address if the `wan_user` keyword is set to `SINGLE_ADDRESS`.  
  • The start IP address if the `wan_user` keyword is set to `ADDRESS_RANGE`. |
| `wan_user_end_ip`                           | `ipaddress`                                      | The end IP address if the `wan_user` keyword is set to `ADDRESS_RANGE`. |
| `wan_users group_wise`                      | `group name`                                     | The name of the WAN IP group.  
  The WAN IP group name is a name that you have specified with the `security services ip_group add` command.  
  The `address_wise` and `group_wise` keywords are mutually exclusive. |

#### QoS profile and logging

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>qos_profile</code></td>
<td><code>profile name</code></td>
<td>The name of the QoS profile that you have specified with the <code>security services qos_profile add</code> command.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>NEVER or ALWAYS</td>
<td>Specifies whether logging is disabled or enabled.</td>
</tr>
</tbody>
</table>

#### Command example:

```
SRX5308> security firewall ipv4 add_rule dmz_wan inbound
security-config[firewall-ipv4-dmz-wan-inbound]> service_name custom_services BOOTP_CLIENT
security-config[firewall-ipv4-dmz-wan-inbound]> action ALWAYS ALLOW
security-config[firewall-ipv4-dmz-wan-inbound]> send_to_dmz_server_ip 192.168.24.112
security-config[firewall-ipv4-dmz-wan-inbound]> translate_to_port_number enable Y
```
security-config[firewall-ipv4-dmz-wan-inbound]>

```
translate_to_port_number port 6700
wan_destination_ip_address_start 10.168.50.1
wan_users Single_Address
wan_user_start_ip 10.132.215.4
log Always
save
```

**Related show command:** show security firewall ipv4 setup dmz_wan

---

**security firewall ipv4 edit_rule dmz_wan inbound <row id>**

This command configures an existing IPv4 DMZ WAN inbound firewall rule. After you have issued the `security firewall ipv4 edit_rule dmz_wan inbound` command to specify the row to be edited (for row information, see the output of the `show security firewall ipv4 setup dmz_wan` command), you enter the security-config [firewall-ipv4-dmz-wan-inbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the *action* keyword determines which other keywords and parameters you can apply to a rule.

**Step 1 Format**

```
security firewall ipv4 edit_rule dmz_wan inbound <row id>
```

**Mode**

security

**Step 2 Format**

```
service_name {default_services <default service name> | [custom_services <custom service name>]}
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
send_to_dmz_server_ip <ipaddress>
translate_to_port_number enable {N | Y | [translate_to_port_number port <number>]}
{wan_destination_ip_address_start {WAN1 | WAN2 | WAN3 | WAN4}
wan_destination_ip_address_start <ipaddress>}
dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress> | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
{dmz_user_end_ip <ipaddress>}}}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress> | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
{wan_user_end_ip <ipaddress>}} | group_wise <group name>}
log {NEVER | ALWAYS}
```

**Mode**

security-config [firewall-ipv4-dmz-wan-inbound]
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service name, action, and schedule</td>
<td>custom_services custom service name</td>
<td>The custom service that you have configured with the security services add command and to which the firewall rule applies.</td>
</tr>
<tr>
<td>Action</td>
<td>action ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>schedule Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td>DMZ server address, port number translation, and WAN destination address</td>
<td>send_to_dmz_server_ip ipaddress</td>
<td>The IP address of the DMZ server.</td>
</tr>
<tr>
<td></td>
<td>translate_to_port_number enable Y or N</td>
<td>Enables or disables port forwarding.</td>
</tr>
<tr>
<td></td>
<td>translate_to_port_number port number</td>
<td>The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65535.</td>
</tr>
</tbody>
</table>
### Security Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan_destination_ip_address</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the IP address of the selected WAN interface as the destination address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The wan_destination_ip_address and wan_destination_ip_address_start keywords are mutually exclusive.</td>
</tr>
<tr>
<td>wan_destination_ip_address_start</td>
<td>ipaddress</td>
<td>The WAN IP address, if the destination address is different from the IP address of a WAN interface, for example, a secondary WAN IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The wan_destination_ip_address and wan_destination_ip_address_start keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>

#### DMZ user addresses and WAN user addresses

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address. For an inbound rule, this option is available only when the WAN mode is Classical Routing.</td>
</tr>
<tr>
<td>dmz_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The IP address if the dmz_users keyword is set to SINGLE_ADDRESS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The start IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>dmz_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>wan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of WAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>wan_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The IP address if the wan_user keyword is set to SINGLE_ADDRESS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The start IP address if the wan_user keyword is set to ADDRESS_RANGE.</td>
</tr>
</tbody>
</table>
Security Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the wan_user keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>wan_users group_wise</td>
<td>group name</td>
<td>The name of the WAN IP group. The WAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>

QoS profile and logging

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos_profile</td>
<td>profile name</td>
<td>The name of the QoS profile that you have specified with the security services qos_profile add command.</td>
</tr>
<tr>
<td>log</td>
<td>NEVER or ALWAYS</td>
<td>Specifies whether logging is disabled or enabled.</td>
</tr>
</tbody>
</table>

**Command example:** See the command example for the **security firewall ipv4 add_rule dmz_wan inbound** command.

**Related show command:** **show security firewall ipv4 setup dmz_wan**

---

**security firewall ipv4 add_rule lan_dmz outbound**

This command configures a new IPv4 LAN DMZ outbound firewall rule. After you have issued the **security firewall ipv4 add_rule lan_dmz outbound** command, you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the action keyword determines which other keywords and parameters can you can apply to a rule.

**Step 1 Format**

```
security firewall ipv4 add_rule lan_dmz outbound
Mode security
```

**Step 2 Format**

```
service_name {default_services <default service name> | {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
```
**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

```
lan_users {address_wise | ANY | SINGLE_ADDRESS | ADDRESS_RANGE} 
     [lan_user_start_ip <ipaddress>] | [lan_user_end_ip <ipaddress>] 
     [group_wise <group name>] 

dmz_users {ANY | SINGLE_ADDRESS | ADDRESS_RANGE} 
     [dmz_user_start_ip <ipaddress>] | [dmz_user_end_ip <ipaddress>] 

log {NEVER | ALWAYS}
```

**Mode**

```
security-config [firewall-ipv4-lan-dmz-outbound]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>custom_services</strong></td>
<td>custom service name</td>
<td>The custom service that you have configured with the security services add command and to which the firewall rule applies.</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td><strong>schedule</strong></td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>LAN user addresses or LAN group and DMZ user addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>lan_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the lan_users address_wise keywords are set to SINGLE_ADDRESS. • The start IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_users group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command. The LAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address.</td>
</tr>
<tr>
<td>dmz_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the dmz_users keyword is set to SINGLE_ADDRESS. • The start IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>dmz_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
</tbody>
</table>
Security Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Command example:

SRX5308> security firewall ipv4 add_rule lan_dmz outbound
security-config[firewall-ipv4-lan-dmz-outbound]> service_name default_services FTP
security-config[firewall-ipv4-lan-dmz-outbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-lan-dmz-outbound]> lan_users group_wise GROUP4
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_users ADDRESS_RANGE
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_user_start_ip 176.14.2.30
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_user_end_ip 176.14.2.79
security-config[firewall-ipv4-lan-dmz-outbound]> log Never
security-config[firewall-ipv4-lan-dmz-outbound]> save

Related show command: show security firewall ipv4 setup lan_dmz

security firewall ipv4 edit_rule lan_dmz outbound <row id>

This command configures an existing IPv4 LAN DMZ outbound firewall rule. After you have issued the `security firewall ipv4 edit_rule lan_dmz outbound` command to specify the row to be edited (for row information, see the output of the `show security firewall ipv4 setup lan_dmz` command), you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters you can apply to a rule.

<table>
<thead>
<tr>
<th>Step 1 Format</th>
<th>security firewall ipv4 edit_rule lan_dmz outbound &lt;row id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>security</td>
</tr>
</tbody>
</table>

| Step 2 Format | service_name {default_services <default service name> | [custom_services <custom service name>] | action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3)}} |

---

**Keyword (might consist of two separate words)** | **Associated Keyword to Select or Parameter to Type** | **Description**
---|---|---
**Logging** | | |
log | NEVER or ALWAYS | Specifies whether logging is disabled or enabled.

---

**Security Mode Configuration Commands**

145
lan_users {address_wise | ANY | SINGLE_ADDRESS {lan_user_start_ip <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>} {lan_user_end_ip <ipaddress>} | group_wise <group name>}

dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>} | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>} {dmz_user_end_ip <ipaddress>}}

log {NEVER | ALWAYS}

Mode security-config [firewall-ipv4-lan-dmz-outbound]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_name</td>
<td>custom_services custom service name</td>
<td>The custom service that you have configured with the security services add command and to which the firewall rule applies.</td>
</tr>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>LAN user addresses or LAN group and DMZ user addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>lan_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the lan_users address_wise keywords are set to SINGLE_ADDRESS. • The start IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_users group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command. The LAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address.</td>
</tr>
<tr>
<td>dmz_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the dmz_users keyword is set to SINGLE_ADDRESS. • The start IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>dmz_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
</tbody>
</table>
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>log</td>
<td>NEVER or ALWAYS Specifies whether logging is disabled or enabled.</td>
</tr>
</tbody>
</table>

**Command example:** See the command example for the `security firewall ipv4 add_rule lan_dmz outbound` command.

**Related show command:** `show security firewall ipv4 setup lan_dmz`

---

**security firewall ipv4 add_rule lan_dmz inbound**

This command configures a new IPv4 LAN DMZ inbound firewall rule. After you have issued the `security firewall ipv4 add_rule lan_dmz inbound` command, you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters can you can apply to a rule.

**Step 1** Format

| Mode | security firewall ipv4 add_rule lan_dmz inbound |

**Step 2** Format

| Format | service_name {default_services <default service name> | {custom_services <custom service name>}
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>ALWAYS_BLOCK</td>
</tr>
<tr>
<td></td>
<td>schedule</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lan_users</th>
<th>address_wise</th>
<th>ANY</th>
<th>SINGLE_ADDRESS</th>
<th>lan_user_start_ip &lt;ipaddress&gt;</th>
<th>lan_user_end_ip &lt;ipaddress&gt;</th>
<th>ADDRESS_RANGE</th>
<th>lan_user_start_ip &lt;ipaddress&gt;</th>
<th>lan_user_end_ip &lt;ipaddress&gt;</th>
<th>group_wise</th>
<th>group name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dmz_users</td>
<td>ANY</td>
<td>SINGLE_ADDRESS</td>
<td>dmz_user_start_ip &lt;ipaddress&gt;</td>
<td>dmz_user_end_ip &lt;ipaddress&gt;</td>
<td>ADDRESS_RANGE</td>
<td>dmz_user_start_ip &lt;ipaddress&gt;</td>
<td>dmz_user_end_ip &lt;ipaddress&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| log | NEVER | ALWAYS |

| Mode | security-config [firewall-ipv4-lan-dmz-inbound] |

---

Security Mode Configuration Commands

148
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service name, action, and schedule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>service_name</td>
<td>default_services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>custom_services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>custom service name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td><strong>schedule</strong></td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td><strong>LAN user addresses or LAN group and DMZ user addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lan_users address_wise</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
</tbody>
</table>
| lan_user_start_ip                          | ipaddress                                       | There are two options:  
- The IP address if the lan_users address_wise keywords are set to SINGLE_ADDRESS.  
- The start IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE. |
### Command example:

```
SRX5308> security firewall ipv4 add_rule lan_dmz inbound
security-config[firewall-ipv4-lan-dmz-inbound]> service_name default_services SSH:UDP
security-config[firewall-ipv4-lan-dmz-inbound]> action BLOCK_BY_SCHEDULE_ELSE_ALLOW
security-config[firewall-ipv4-lan-dmz-inbound]> schedule Schedule1
security-config[firewall-ipv4-lan-dmz-inbound]> lan_users address_wise SINGLE_ADDRESS
security-config[firewall-ipv4-lan-dmz-inbound]> lan_user_start_ip 192.168.5.108
security-config[firewall-ipv4-lan-dmz-inbound]> dmz_users ANY
security-config[firewall-ipv4-lan-dmz-inbound]> dmz_user_start_ip 176.16.2.101
security-config[firewall-ipv4-lan-dmz-inbound]> log Always
security-config[firewall-ipv4-lan-dmz-inbound]> save
```

---

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_users group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command. The LAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address.</td>
</tr>
</tbody>
</table>
| dmz_user_start_ip                           | ipaddress                                       | There are two options:  
- The IP address if the dmz_users keyword is set to SINGLE_ADDRESS.  
- The start IP address if the dmz_users keyword is set to ADDRESS_RANGE. |
| dmz_user_end_ip                             | ipaddress                                       | The end IP address if the dmz_users keyword is set to ADDRESS_RANGE. |

**Logging**

| log                                         | NEVER or ALWAYS                                 | Specifies whether logging is disabled or enabled. |
Related show command: `show security firewall ipv4 setup lan_dmz`

security firewall ipv4 edit_rule lan_dmz inbound <row id>

This command configures an existing IPv4 LAN DMZ inbound firewall rule. After you have issued the `security firewall ipv4 edit_rule lan_dmz inbound` command to specify the row to be edited (for row information, see the output of the `show security firewall ipv4 setup lan_dmz` command), you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the action keyword determines which other keywords and parameters you can apply to a rule.

Step 1 Format
security firewall ipv4 edit_rule lan_dmz inbound <row id>

Mode security

Step 2 Format
  service_name {default_services <default service name> | custom_services <custom service name} action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}

  lan_users {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip <ipaddress> | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}} | lan_user_end_ip <ipaddress>}} | group_wise <group name>}

  dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress> | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}} | dmz_user_end_ip <ipaddress>}

  log {NEVER | ALWAYS}

Mode security-config [firewall-ipv4-lan-dmz-inbound]
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service name, action, and schedule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>service_name</code></td>
<td>ANY, AIM, BGP, BOOTP_CLIENT,</td>
<td>Specifies the default service and protocol to which the firewall rule applies.</td>
</tr>
<tr>
<td><code>default_services</code></td>
<td>BOOTP_SERVER, CU-SEEEME:UDP,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CU-SEEEME:TCP, DNS:UDP, DNS:TCP, FINGER,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTP, HTTP, HTTPS, ICMP-TYPE-3, ICMP-TYPE-4,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICMP-TYPE-5, ICMP-TYPE-6, ICMP-TYPE-7, ICMP-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TYPE-8, ICMP-TYPE-9, ICMP-TYPE-10, ICMP-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TYPE-11, ICMP-TYPE-13, ICQ, IMAP2, IMAP3, IRC,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NEWS, NFS, NNTP, PING, POP3, PPTP, RCMD, REAL-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUDIO, REXEC, RLOGIN, RTELNET, RTSP:TCP, RTSP:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP, SFTP, SMTP, SNMP:TCP, SNMP:UDP, SNMP-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TRAPS:TCP, SNMP-TRAPS:UDP, SQL-NET, SSH:TCP,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSH:UDP, STREAMWORKS, TACACS, TELNET, TFTP,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RIP, IKE, SSH-TTPL, IPSEC-UDP-ENCAP, IDENT,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VDOLIVE, SSH, SIP-TCP, SIP-UDP, NFS-TCP, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RPC-TCP.</td>
<td></td>
</tr>
<tr>
<td><code>custom_services</code></td>
<td>custom service name</td>
<td>The custom service that you have configured with the <code>security services add</code> command and to which the firewall rule applies.</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_</td>
<td>Specifies the type of action to be enforced by the rule.</td>
</tr>
<tr>
<td></td>
<td>ELSE_ALLOW, ALLOW_BY_SCHEDULE_ELSE_BLOCK</td>
<td></td>
</tr>
<tr>
<td><strong>schedule</strong></td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
<tr>
<td><strong>LAN user addresses or LAN group and DMZ user addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>lan_users address_wise</code></td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of LAN address. The <code>address_wise</code> and <code>group_wise</code> keywords are mutually exclusive.</td>
</tr>
<tr>
<td><code>lan_user_start_ip</code></td>
<td>ipaddress</td>
<td>There are two options:</td>
</tr>
<tr>
<td></td>
<td>• The IP address if the <code>lan_users address_wise</code> keywords are set to <code>SINGLE_ADDRESS</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The start IP address if the <code>lan_users address_wise</code> keywords are set to <code>ADDRESS_RANGE</code>.</td>
<td></td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>lan_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the lan_users address_wise keywords are set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>lan_users group_wise</td>
<td>group name</td>
<td>The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you have specified with the net lan lan_groups edit &lt;row id&gt; &lt;new group name&gt; command. The LAN IP group name is a name that you have specified with the security services ip_group add command. The address_wise and group_wise keywords are mutually exclusive.</td>
</tr>
<tr>
<td>dmz_users</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of DMZ address.</td>
</tr>
<tr>
<td>dmz_user_start_ip</td>
<td>ipaddress</td>
<td>There are two options: • The IP address if the dmz_users keyword is set to SINGLE_ADDRESS. • The start IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td>dmz_user_end_ip</td>
<td>ipaddress</td>
<td>The end IP address if the dmz_users keyword is set to ADDRESS_RANGE.</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td></td>
<td><strong>NEVER or ALWAYS</strong> Specifies whether logging is disabled or enabled.</td>
</tr>
</tbody>
</table>

**Command example:** See the command example for the security firewall ipv4 add_rule lan_dmz inbound command.

**Related show command:** show security firewall ipv4 setup lan_dmz
IPv4 General Firewall Commands

security firewall ipv4 default_outbound_policy {Allow | Block}

This command allows or blocks the IPv4 firewall default outbound policy.

Format    security firewall ipv4 default_outbound_policy {Allow | Block}
Mode      security

Related show command: show security firewall ipv4 setup lan_wan, show security firewall ipv4 setup dmz_wan, and show security firewall ipv4 setup lan_dmz

security firewall ipv4 delete <row id>

This command deletes an IPv4 firewall rule by deleting its row ID.

Format    security firewall ipv4 delete <row id>
Mode      security

Related show command: show security firewall ipv4 setup lan_wan, show security firewall ipv4 setup dmz_wan, and show security firewall ipv4 setup lan_dmz

security firewall ipv4 disable <row id>

This command disables an IPv4 firewall rule by specifying its row ID.

Format    security firewall ipv4 disable <row id>
Mode      security

Related show command: show security firewall ipv4 setup lan_wan, show security firewall ipv4 setup dmz_wan, and show security firewall ipv4 setup lan_dmz

security firewall ipv4 enable <row id>

This command enables an IPv4 firewall rule by specifying its row ID.

Format    security firewall ipv4 enable <row id>
Mode      security
Related show command: `show security firewall ipv4 setup lan_wan`, `show security firewall ipv4 setup dmz_wan`, and `show security firewall ipv4 setup lan_dmz`

---

IPv6 Firewall Commands

`security firewall ipv6 default_outbound_policy {Allow | Block}`

This command allows or blocks the IPv6 firewall default outbound policy.

**Format**
```
security firewall ipv6 default_outbound_policy {Allow | Block}
```

**Mode**
```
security
```

Related show command: `show security firewall ipv6 setup`

---

`security firewall ipv6 configure`

This command configures a new IPv6 firewall rule. After you have issued the `security firewall ipv6 configure` command, you enter the security-config [firewall-ipv6] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters you can apply to a rule.

**Step 1**
```
Format
security firewall ipv6 configure
```

**Mode**
```
security
```

**Step 2**
```
Format
from_zone {LAN | WAN | DMZ}
to_zone {LAN | WAN | DMZ}
service_name {default_services <default service name> | custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}}
source_address_type {ANY | SINGLE_ADDRESS {source_start_address <ipv6-address> | ADDRESS_RANGE {source_start_address <ipv6-address> | source_end_address <ipv6-address>}}}
destination_address_type {ANY | SINGLE_ADDRESS {destination_start_address <ipv6-address> | ADDRESS_RANGE {destination_start_address <ipv6-address> | destination_end_address <ipv6-address>}}}
```
### Security Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

```
qos_priority {Normal-Service | Minimize-Cost | Maximize-Reliability | Maximize-Throughput | Minimize-Delay}
log {NEVER | ALWAYS}
```

**Mode** security-config [firewall-ipv6]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction of service, service name, action, and schedule</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| from_zone | LAN, WAN, or DMZ | Specifies the outbound direction:  
- LAN. From the LAN.  
- WAN. From the WAN.  
- DMZ. From the DMZ. |
| to_zone | LAN, WAN, or DMZ | Specifies the inbound direction:  
- LAN. To the LAN.  
- WAN. To the WAN.  
- DMZ. To the DMZ. |
| service_name custom_Services | custom service name | The custom service that you have configured with the `security services add` command and to which the firewall rule applies. |
| action | ALWAYS_BLOCK, ALWAYS_ALLOW, BLOCK_BY_SCHEDULE_ELSE_ALLOW, or ALLOW_BY_SCHEDULE_ELSE_BLOCK | Specifies the type of action to be taken by the rule. |
## Security Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
<td>Specifies the schedule, if any, that is applicable to the rule.</td>
</tr>
</tbody>
</table>

### LAN, WAN, and DMZ source and destination IP addresses

<table>
<thead>
<tr>
<th>source_address_type</th>
<th>source_start_address</th>
<th>source_end_address</th>
<th>destination_address_type</th>
<th>destination_start_address</th>
<th>destination_end_address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>ipv6-address</td>
<td></td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>ipv6-address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are two options:
- The IPv6 address if the `source_address_type` keyword is set to SINGLE_ADDRESS.
- The start IPv6 address if the `source_address_type` keyword is set to ADDRESS_RANGE.

There are two options:
- The IPv6 address if the `destination_address_type` keyword is set to SINGLE_ADDRESS.
- The start IPv6 address if the `destination_address_type` keyword is set to ADDRESS_RANGE.

<table>
<thead>
<tr>
<th>QoS priority and logging</th>
<th>qos_priority</th>
<th>log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal-Service, Minimize-Cost, Maximize-Reliability, Maximize-Throughput, or Minimize-Delay</td>
<td>NEVER or ALWAYS</td>
<td>Specifies the type of QoS that applies to the rule. You can apply QoS to LAN WAN and DMZ WAN outbound rules only. Specifies whether logging is disabled or enabled.</td>
</tr>
</tbody>
</table>
Command example:

```
SRX5308> security firewall ipv6 configure
security-config[firewall-ipv6]> from_zone WAN
security-config[firewall-ipv6]> to_zone LAN
security-config[firewall-ipv6]> service_name default_services RTELNET
security-config[firewall-ipv6]> action ALWAYS_ALLOW
security-config[firewall-ipv6]> source_address_type SINGLE_ADDRESS
security-config[firewall-ipv6]> source_start_address 2002::B32:AAB1::fD41
security-config[firewall-ipv6]> destination_address_type SINGLE_ADDRESS
security-config[firewall-ipv6]> destination_start_address FEC0::db8:145
security-config[firewall-ipv6]> log ALWAYS
security-config[firewall-ipv6]> save
```

Related show command: `show security firewall ipv6 setup`

**security firewall ipv6 edit <row id>**

This command configures an existing IPv6 firewall rule. After you have issued the `security firewall ipv6 edit` command to specify the row to be edited (for row information, see the output of the `show security firewall ipv6 setup` command), you enter the security-config [firewall-ipv6] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the `action` keyword determines which other keywords and parameters you can apply to a rule.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Format</th>
<th>security firewall ipv6 edit &lt;row id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td></td>
<td>security</td>
</tr>
</tbody>
</table>

| Step 2 | Format | from_zone [LAN | WAN | DMZ] |
|--------|--------|--------------------------------------|
|        | to_zone [LAN | WAN | DMZ] |
|        | service_name [default_services <default service name> | custom_services <custom service name>] |
|        | action [ALWAYS_BLOCK | ALWAYS_ALLOW | BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 | Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK {schedule {Schedule1 | Schedule2 | Schedule3}}] |

|        | source_address_type [ANY | SINGLE_ADDRESS [source_start_address <ipv6-address>] | ADDRESS_RANGE [source_start_address <ipv6-address>] [source_end_address <ipv6-address>]] |
|        | destination_address_type [ANY | SINGLE_ADDRESS [destination_start_address <ipv6-address>] | ADDRESS_RANGE [destination_start_address <ipv6-address>] [destination_end_address <ipv6-address>]] |
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

qos_priority {Normal-Service | Minimize-Cost | Maximize-Reliability | Maximize-Throughput | Minimize-Delay}

log {NEVER | ALWAYS}

Mode security-config [firewall-ipv6]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction of service, service name, action, and schedule</td>
<td>from_zone</td>
<td>LAN, WAN, or DMZ</td>
</tr>
<tr>
<td></td>
<td>to_zone</td>
<td>LAN, WAN, or DMZ</td>
</tr>
<tr>
<td></td>
<td>default_services</td>
<td>custom service name</td>
</tr>
<tr>
<td></td>
<td>service_name</td>
<td>custom_services</td>
</tr>
<tr>
<td></td>
<td>schedule</td>
<td>Schedule1, Schedule2, or Schedule3</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>LAN, WAN, and DMZ source and destination IP addresses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source_address_type</td>
<td>ANY, SINGLE_ADDRESS, or ADDRESS_RANGE</td>
<td>Specifies the type of source address.</td>
</tr>
</tbody>
</table>
| source_start_address | ipv6-address | There are two options:  
• The IPv6 address if the source_address_type keyword is set to SINGLE_ADDRESS.  
• The start IPv6 address if the source_address_type keyword is set to ADDRESS_RANGE. |
| source_end_address | ipv6-address | The end IPv6 address if the source_address_type keyword is set to ADDRESS_RANGE. |
| destination_address_type | ANY, SINGLE_ADDRESS, or ADDRESS_RANGE | Specifies the type of destination address. |
| destination_start_address | ipv6-address | There are two options:  
• The IPv6 address if the destination_address_type keyword is set to SINGLE_ADDRESS.  
• The start IPv6 address if the destination_address_type keyword is set to ADDRESS_RANGE. |
| destination_end_address | ipv6-address | The end IPv6 address if the destination_address_type keyword is set to ADDRESS_RANGE. |
| **QoS profile and logging** | | |
| qos_priority | Normal-Service, Minimize-Cost, Maximize-Reliability, Maximize-Throughput, or Minimize-Delay | Specifies the type of QoS that applies to the rule. You can apply QoS to LAN WAN and DMZ WAN outbound rules only. |
| log | NEVER or ALWAYS | Specifies whether logging is disabled or enabled. |
Command example: See the command example for the `security firewall ipv6 configure` command.

Related show command: `show security firewall ipv6 setup`

---

**security firewall ipv6 delete <row id>**

This command deletes an IPv6 firewall rule by deleting its row ID.

**Format**

```
security firewall ipv6 delete <row id>
```

**Mode**

`security`

Related show command: `show security firewall ipv6 setup`

---

**security firewall ipv6 disable <row id>**

This command disables an IPv6 firewall rule by specifying its row ID.

**Format**

```
security firewall ipv6 disable <row id>
```

**Mode**

`security`

Related show command: `show security firewall ipv6 setup`

---

**security firewall ipv6 enable <row id>**

This command enables an IPv6 firewall rule by specifying its row ID.

**Format**

```
security firewall ipv6 enable <row id>
```

**Mode**

`security`

Related show command: `show security firewall ipv6 setup`
Attack Check Commands

security firewall attack_checks configure ipv4

This command configures ipv4 WAN and LAN security attack checks. After you have issued the `security firewall attack_checks configure ipv4` command, you enter the `security-config [attack-checks-ipv4]` mode, and then you can edit one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format:  
```
security firewall attack_checks configure ipv4
```

**Mode**: `security`

**Step 2** Format:  
```
respond_to_ping_on_internet_ports { Y | N }
enable_stealth_mode { Y | N }
block_tcp_flood { Y | N }
block_udp_flood { Y | N }
disable_ping_reply_on_lan { Y | N }
```

**Mode**: `security-config [attack-checks-ipv4]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>respond_to_ping_on_internet_ports</td>
<td>Y or N</td>
<td>Enables or disables the response to a ping from the WAN port.</td>
</tr>
<tr>
<td>enable_stealth_mode</td>
<td>Y or N</td>
<td>Enables or disables stealth mode.</td>
</tr>
<tr>
<td>block_tcp_flood</td>
<td>Y or N</td>
<td>Blocks or allows TCP floods on the WAN port.</td>
</tr>
<tr>
<td>block_udp_flood</td>
<td>Y or N</td>
<td>Blocks or allows UDP floods on LAN ports.</td>
</tr>
<tr>
<td>disable_ping_reply_on_lan</td>
<td>Y or N</td>
<td>Enables or disables ping replies from LAN ports.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> security firewall attack_checks configure ipv4
security-config[attack-checks-ipv4]> respond_to_ping_on_internet_ports N
security-config[attack-checks-ipv4]> enable_stealth_mode Y
security-config[attack-checks-ipv4]> block_tcp_flood Y
security-config[attack-checks-ipv4]> block_udp_flood N
security-config[attack-checks-ipv4]> disable_ping_reply_on_lan Y
security-config[attack-checks-ipv4]> save
```
Related show command: `show security firewall attack_checks setup ipv4`

**security firewall attack_checks igmp configure**

This command enables or disables multicast pass-through by enabling or disabling the IGMP proxy for IPv4 traffic. After you have issued the `security firewall attack_checks igmp configure` command, you enter the security-config [igmp] mode, and then you can enable or disable the IGMP proxy.

**Step 1** Format: `security firewall attack_checks igmp configure`  
  Mode: `security`

**Step 2** Format: `enable_igmp_proxy {Y | N}`  
  Mode: `security-config [igmp]`

Related show command: `show security firewall attack_checks igmp`

**security firewall attack_checks vpn_passthrough configure**

This command configures VPN pass-through for IPv4 traffic. After you have issued the `security firewall attack_checks vpn_passthrough configure` command, you enter the security-config [vpn-passthrough] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format: `security firewall attack_checks vpn_passthrough configure`  
  Mode: `security`

**Step 2** Format:  
  **ipsec_enable** `{Y | N}`  
  **l2tp_enable** `{Y | N}`  
  **pptp_enable** `{Y | N}`  
  Mode: `security-config [vpn-passthrough]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec_enable</td>
<td>Y or N</td>
<td>Enables or disables IPSec pass-through.</td>
</tr>
<tr>
<td>l2tp_enable</td>
<td>Y or N</td>
<td>Enables or disables L2TP pass-through.</td>
</tr>
<tr>
<td>pptp_enable</td>
<td>Y or N</td>
<td>Enables or disables PPTP pass-through.</td>
</tr>
</tbody>
</table>

Command example:  

SRX5308> `security firewall attack_checks vpn_passthrough configure`  
security-config[vpn-passthrough]> `ipsec_enable Y`
security-config[vpn-passthrough] > l2tp_enable Y
security-config[vpn-passthrough] > pptp_enable N
security-config[vpn-passthrough] > save

Related show command: show security firewall attack_checks vpn_passthrough setup

security firewall attack_checks configure ipv6

This command configures ipv6 WAN security attack checks. After you have issued the security firewall attack_checks configure ipv6 command, you enter the security-config[attack-checks-ipv6] mode, and then you can edit one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 Format  security firewall attack_checks configure ipv6
Mode      security
Step 2 Format  respond_to_ping_on_internet_ports {Y | N}
             vpn_ipsec_passthrough {Y | N}
Mode      security-config[attack-checks-ipv6]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>respond_to_ping_on_internet_ports</td>
<td>Y or N</td>
<td>Enables or disables the response to a ping from the WAN port.</td>
</tr>
<tr>
<td>vpn_ipsec_passthrough</td>
<td>Y or N</td>
<td>Enables or disables IPSec VPN traffic that is initiated from the LAN to reach the WAN, irrespective of the default firewall outbound policy and custom firewall rules.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> security firewall attack_checks configure ipv6
security-config[attack-checks-ipv6]> respond_to_ping_on_internet_ports N
security-config[attack-checks-ipv6]> vpn_ipsec_passthrough Y
security-config[attack-checks-ipv6]> save

Related show command: show security firewall attack_checks setup ipv6

Security Mode Configuration Commands

164
Session Limit, Time-Out, and Advanced Commands

security firewall session_limit configure

This command configures global session limits. After you have issued the `security firewall session_limit configure` command, you enter the security-config [session-limit] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

<table>
<thead>
<tr>
<th>Step 1 Format</th>
<th>security firewall session_limit configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>security</td>
</tr>
</tbody>
</table>

| Step 2 Format | enable {Y | N}                             |
|---------------|------------------------------------------|
|               | session_limit_control {Single_IP_cannot_Exceed | |
|               | When_Single_IP_Exceed}                   |
|               | conn_limit_type {Percentage_Of_MaxSessions | Number_Of_Sessions}                   |
|               | user_limit <number>                     |
|               | block_new_session {Block_IP_to_add_new_session |
|               | block_IP_to_add_new_session_for_time <seconds> | } | |
|               | Block_IPs_all_connections {block_IPs_all_connections_for_time |
|               | block_IPs_all_connections_for_time <seconds>}} |
| Mode          | security-config [session-limit]           |

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables session limits.</td>
</tr>
<tr>
<td>session_limit_control</td>
<td>When_Single_IP_Exceed or Single_IP_cannot_Exceed</td>
<td>Specifies how limit control is implemented:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>When_Single_IP_Exceed.</strong> When the limit is reached, no new session is allowed from the IP address for a specified period, or all sessions from the IP address are terminated and new sessions are blocked for a specified period. Issue the <code>conn_limit_type</code> keyword to specify the type of session limit and issue the <code>block_new_session</code> keyword to specify the type of blockage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Single_IP_cannot_Exceed.</strong> When the limit is reached, no new session is allowed from the IP address. A new session is allowed only when an existing session is terminated or times out. Issue the <code>conn_limit_type</code> keyword to specify the type of session limit.</td>
</tr>
</tbody>
</table>
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conn_limit_type</td>
<td>Percentage_Of_MaxSessions or Number_Of_Sessions</td>
<td>Specifies the type of session limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percentage_Of_MaxSessions. Specifies a percentage of the total session-connection capacity on the VPN firewall. Issue the user_limit keyword to specify a percentage of the total session connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Number_Of_Sessions. Specifies an absolute number of maximum sessions. Issue the user_limit keyword to specify an absolute number of maximum sessions.</td>
</tr>
<tr>
<td>user_limit</td>
<td>number</td>
<td>The percentage of the total session-connection capacity on the VPN firewall or an absolute number of maximum sessions.</td>
</tr>
<tr>
<td>block_new_session</td>
<td>Block_IP_to_add_new_session or Block_IPs_all_connections</td>
<td>Specifies the type of blockage:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Block_IP_to_add_new_session. No new session is allowed from the IP address for a period. Issue the block_IP_to_add_new_session_for_time keyword to specify the period in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Block_IPs_all_connections. All sessions from the IP address are terminated, and new sessions are blocked for a period. Issue the block_IPs_all_connections_for_time keyword to specify the period in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These options are available only if the session_limit_control keyword is set to When_Single_IP_Exceed.</td>
</tr>
<tr>
<td>block_IP_to_add_new_session_for_time</td>
<td>seconds</td>
<td>The period during which no new session is allowed from the IP address.</td>
</tr>
<tr>
<td>block_IPs_all_connections_for_time</td>
<td>seconds</td>
<td>The period during which all sessions are blocked from the IP address.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> security firewall session_limit configure
security-config[session-limit]> enable Y
security-config[session-limit]> session_limit_control When_Single_IP_Exceed
security-config[session-limit]>
conn_limit_type Percentage_Of_MaxSessions
security-config[session-limit]>
user_limit 80
security-config[session-limit]>
block_new_session Block_IP_to_add_new_session
security-config[session-limit]>
block_IP_to_add_new_session_for_time 60
security-config[session-limit]>
save

Related show command: show security firewall session_limit

---

**security firewall session_settings configure**

This command configures global session time-outs. After you have issued the `security firewall session_settings configure` command, you enter the security-config [session-settings] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
security firewall session_settings configure
```

**Mode**

security

**Step 2 Format**

```
tcp_session_timeout <seconds>
udp_session_timeout <seconds>
icmp_session_timeout <seconds>
```

**Mode**

security-config [session-settings]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp_session_timeout</td>
<td>seconds</td>
<td>Specifies the TCP session timeout period (integer) in seconds.</td>
</tr>
<tr>
<td>udp_session_timeout</td>
<td>seconds</td>
<td>Specifies the UDP session timeout period (integer) in seconds.</td>
</tr>
<tr>
<td>icmp_session_timeout</td>
<td>seconds</td>
<td>Specifies the ICMP session timeout period (integer) in seconds.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> security firewall session_settings configure
security-config[session-settings]> tcp_session_timeout 3600
security-config[session-settings]> udp_session_timeout 180
security-config[session-settings]> icmp_session_timeout 120
security-config[session-settings]> save
```

Related show command: show security firewall session_settings

---

Security Mode Configuration Commands

167
**security firewall advanced algs**

This command configures Session Initiation Protocol (SIP) support for the application level gateway (ALG). After you have issued the `security firewall advanced algs` command, you enter the security-config [firewall-alg] mode, and then you can enable or disable SIP support.

**Command example:**

```
FVS318N> security firewall advanced algs
security-config[firewall-alg]> sip Y
security-config[firewall-alg]> save
```

**Related show command:** `show security firewall advanced algs`

---

**Address Filter and IP/MAC Binding Commands**

**security address_filter mac_filter configure**

This command configures the source MAC address filter. After you have issued the `security address_filter mac_filter configure` command, you enter the security-config [mac-filter] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Command example:**

```
FVS318N> security address_filter mac_filter configure
security-config[mac-filter]> enable Y
security-config[mac-filter]> save
```
Security Mode Configuration Commands

### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

#### Security Mode Configuration Commands

**security address_filter mac_filter configure**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables the source MAC address filter.</td>
</tr>
<tr>
<td>policy</td>
<td>Permit-And-Block-Rest or Block-And-Permit-Rest</td>
<td>Specifies the policy of the source MAC address filter.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> security address_filter mac_filter configure
security-config[mac-filter]> enable Y
security-config[mac-filter]> policy Block-And-Permit-Rest
security-config[mac-filter]> save
```

Related show command: *show security address_filter mac_filter setup*

---

**security address_filter mac_filter source add**

This command adds a new MAC address to the MAC address table for the source MAC address filter. After you have issued the `security address_filter mac_filter source add` command, you enter the security-config [mac-filter-source] mode, and then you can add a MAC address.

**Step 1**

**Format**

```
security address_filter mac_filter source add
```

**Mode**

```
security
```

**Step 2**

**Format**

```
address <mac address>
```

**Mode**

```
security-config [mac-filter-source]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>mac address</td>
<td>The MAC address that needs to be added to the MAC address table for the source MAC address filter.</td>
</tr>
</tbody>
</table>

**Command example:**

```
FVS318N> security address_filter mac_filter source add
security-config[mac-filter-source]> address a1:b2:c3:de:11:22
security-config[mac-filter-source]> save
security-config[mac-filter-source]> address a1:b2:c3:de:11:25
security-config[mac-filter-source]> save
```

Related show command: *show security address_filter mac_filter setup*
Security Mode Configuration Commands

security address_filter mac_filter source delete <row id>

This command deletes a MAC address from the MAC address table by deleting its row ID.

Format    security address_filter mac_filter source delete <row id>
Mode      security

Related show command: show security address_filter mac_filter setup

security address_filter ip_or_mac_binding add

This command configures a new IP/MAC binding rule. After you have issued the security address_filter ip_or_mac_binding add command, you enter the security-config [ip-or-mac-binding] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1
Format      security address_filter ip_or_mac_binding add
Mode        security

Step 2
Format      name <rule name>
            mac_address <mac address>
            ip_version {IPv4 {ip_address <ipaddress>} | IPv6 {ip_address6 <ipv6-address>}}
            log_dropped_packets {Y | N}
Mode        security-config [ip-or-mac-binding]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>rule name</td>
<td>The name (alphanumeric string) of the IP/MAC binding rule.</td>
</tr>
<tr>
<td>mac_address</td>
<td>mac address</td>
<td>The MAC address to which the IP/MAC binding rule is applied.</td>
</tr>
<tr>
<td>ip_version</td>
<td>IPv4 or IPv6</td>
<td>Specifies the type of IP address to which the IP/MAC binding rule is applied:</td>
</tr>
<tr>
<td></td>
<td>• IPv4. You need to issue the ip_address keyword and specify an IPv4 address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IPv6. You need to issue the ip_address6 keyword and specify an IPv6 address.</td>
<td></td>
</tr>
<tr>
<td>ip_address</td>
<td>ipaddress</td>
<td>The IPv4 address to which the IP/MAC binding rule is applied.</td>
</tr>
</tbody>
</table>
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Command example:**

SRX5308> security address_filter ip_or_mac_binding add
security-config[ip-or-mac-binding]> name PhoneConfRoom52
security-config[ip-or-mac-binding]> mac_address d1:e1:55:54:8e:7f
security-config[ip-or-mac-binding]> ip_version IPv4
security-config[ip-or-mac-binding]> ip_address 192.151.1.107
security-config[ip-or-mac-binding]> log_dropped_packets N
security-config[ip-or-mac-binding]> save

**Related show command:** show security address_filter ip_or_mac_binding setup

---

**security address_filter ip_or_mac_binding edit <row id>**

This command configures an existing IP/MAC binding rule. After you have issued the `security address_filter ip_or_mac_binding edit` command to specify the row to be edited, you enter the `security-config [ip-or-mac-binding]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the rule.

**Step 1 Format**

security address_filter ip_or_mac_binding edit <row id>

**Mode**

security

**Step 2 Format**

mac_address <mac address>

ip_version {IPv4 {ip_address <ipaddress>} | IPv6 {ip_address6 <ipv6-address>}}

log_dropped_packets {Y | N}

**Mode**

security-config [ip-or-mac-binding]

---

**Keyword** | **Associated Keyword to Select or Parameter to Type** | **Description**
---|---|---
ip_address6 | ipv6-address | The IPv6 address to which the IP/MAC binding rule is applied.
log_dropped_packets | Y or N | Enables or disables logging for the IP/MAC binding rule.

---

**Keyword** | **Associated Keyword to Select or Parameter to Type** | **Description**
---|---|---
mac_address | mac address | The MAC address to which the IP/MAC binding rule is applied.
**Security Mode Configuration Commands**

The document provides configuration commands for ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308, focusing on the security mode and configuring IP/MAC address filtering.

### security address_filter ip_or_mac_binding delete <row id>

This command deletes an IP/MAC binding rule by deleting its row ID.

- **Format**: `security address_filter ip_or_mac_binding delete <row id>`
- **Mode**: security

### security address_filter ip_or_mac_binding enable_email_log <ip version>

This command configures the email log for IP/MAC binding violations. After you have issued the `security address_filter ip_or_mac_binding enable_email_log` command to specify the IP version, you enter the security-config [ip-or-mac-binding] mode, and then you can configure the email log setting.

- **Step 1 Format**: `security address_filter ip_or_mac_binding enable_email_log {IPv4 | IPv6}`
  - **Mode**: security
- **Step 2 Format**: `enable_email_logs {Y | N}`
  - **Mode**: security-config [ip-or-mac-binding]
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Security Mode Configuration Commands

**Command example:**

```
FVS318N> security address_filter ip_or_mac_binding enable_email_log IPv4
security-config[ip-or-mac-binding]> enable_email_logs Y
security-config[ip-or-mac-binding]> save
```

**Related show command:** `show security address_filter enable_email_log`

---

### Port Triggering Commands

**security porttriggering_rules add**

This command configures a new port triggering rule. After you have issued the `security porttriggering_rules add` command, you enter the security-config [porttriggering-rules] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

<table>
<thead>
<tr>
<th>Step 1 Format</th>
<th>Mode</th>
<th>security porttriggering_rules add</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2 Format</th>
<th>Mode</th>
<th>security-config [porttriggering-rules]</th>
</tr>
</thead>
<tbody>
<tr>
<td>name &lt;rule name&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable_rule {Y</td>
<td>N}</td>
<td></td>
</tr>
<tr>
<td>protocol {TCP</td>
<td>UDP}</td>
<td></td>
</tr>
<tr>
<td>outgoing_start_port &lt;number&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>outgoing_end_port &lt;number&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incoming_start_port &lt;number&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incoming_end_port &lt;number&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>rule name</td>
<td>The name (alphanumeric string) of the port triggering rule.</td>
</tr>
<tr>
<td>enable_rule</td>
<td>Y or N</td>
<td>Enables or disables the port triggering rule.</td>
</tr>
<tr>
<td>protocol</td>
<td>TCP or UDP</td>
<td>Specifies whether the port uses the TCP or UDP protocol.</td>
</tr>
</tbody>
</table>
Security Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Command example:

SRX5308> security porttriggering_rules add
security-config[porttriggering-rules]> name Skype
security-config[porttriggering-rules]> enable_rule Y
security-config[porttriggering-rules]> protocol TCP
security-config[porttriggering-rules]> outgoing_start_port 61196
security-config[porttriggering-rules]> outgoing_end_port 61196
security-config[porttriggering-rules]> incoming_start_port 61197
security-config[porttriggering-rules]> incoming_end_port 61197
security-config[porttriggering-rules]> save

Related show command: show security porttriggering_rules setup and show security porttriggering_rules status

security porttriggering_rules edit <row id>

This command configures an existing port triggering rule. After you have issued the security porttriggering_rules edit command to specify the row to be edited, you enter the security-config [porttriggering-rules] mode, and then you can configure one keyword and associated parameter or associated keyword mode at a time in the order that you prefer. You cannot change the name of the rule.

Step 1 Format security porttriggering_rules edit <row id>
Mode security

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outgoing_start_port</td>
<td>number</td>
<td>The start port number (integer) of the outgoing traffic range. Valid numbers are from 1025 to 65535.</td>
</tr>
<tr>
<td>outgoing_end_port</td>
<td>number</td>
<td>The end port number (integer) of the outgoing traffic range. Valid numbers are from 1025 to 65535.</td>
</tr>
<tr>
<td>incoming_start_port</td>
<td>number</td>
<td>The start port number (integer) of the incoming traffic range. Valid numbers are from 1025 to 65535.</td>
</tr>
<tr>
<td>incoming_end_port</td>
<td>number</td>
<td>The end port number (integer) of the incoming traffic range. Valid numbers are from 1025 to 65535.</td>
</tr>
</tbody>
</table>
Step 2  Format  

```
enable_rule {Y | N}
protocol {TCP | UDP}
ongoing_start_port <number>
ongoing_end_port <number>
incoming_start_port <number>
incoming_end_port <number>
```

Mode  
security-config [porttriggering-rules]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_rule</td>
<td>Y or N</td>
<td>Enables or disables the port triggering rule.</td>
</tr>
<tr>
<td>protocol</td>
<td>TCP or UDP</td>
<td>Specifies whether the port uses the TCP or UDP</td>
</tr>
<tr>
<td>outgoing_start_port</td>
<td>number</td>
<td>The start port number (integer) of the outgoing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traffic range. Valid numbers are from 1025 to 65535.</td>
</tr>
<tr>
<td>outgoing_end_port</td>
<td>number</td>
<td>The end port number (integer) of the outgoing traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>range. Valid numbers are from 1025 to 65535.</td>
</tr>
<tr>
<td>incoming_start_port</td>
<td>number</td>
<td>The start port number (integer) of the incoming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traffic range. Valid numbers are from 1025 to 65535.</td>
</tr>
<tr>
<td>incoming_end_port</td>
<td>number</td>
<td>The end port number (integer) of the incoming traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>range. Valid numbers are from 1025 to 65535.</td>
</tr>
</tbody>
</table>

Related show command: show security porttriggering_rules setup and show security porttriggering_rules status

security porttriggering_rules delete <row id>

This command deletes a port triggering rule by deleting its row.

Format  
security porttriggering_rules delete <row id>

Mode  
security

Related show command: show security porttriggering_rules setup and show security porttriggering_rules status
UPnP Command

**security upnp configure**

This command configures Universal Plug and Play (UPnP). After you have issued the `security upnp configure` command, you enter the security-config [upnp] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
security upnp configure
```

**Mode**

```
security
```

**Step 2 Format**

```
enable {Y | N}
advertisement period <seconds>
advertisement time_to_live <number>
```

**Mode**

```
security-config [upnp]
```

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables UPnP.</td>
</tr>
<tr>
<td>advertisement period</td>
<td>seconds</td>
<td>The advertisement period in seconds, from 1 to 1440 seconds.</td>
</tr>
<tr>
<td>advertisement time_to_live</td>
<td>number</td>
<td>The advertisement time-to-live period in hops, from 1 to 255 hops.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> security upnp configure
security-config[upnp]> enable Y
security-config[upnp]> advertisement period 60
security-config[upnp]> advertisement time_to_live 6
security-config[upnp]> save
```

**Related show command:** *show security upnp setup and show security upnp portmap*
Bandwidth Profile Commands

security bandwidth enable_bandwidth_profiles \{Y | N\}

This command enables or disables bandwidth profiles globally. Select Y to enable bandwidth profiles globally or N to disable bandwidth profiles globally.

**Format**  
security bandwidth enable_bandwidth_profiles \{Y | N\}

**Mode**  
security

**Related show command:**  
`show security bandwidth profile setup`

---

security bandwidth profile add

This command configures a new bandwidth profile. After you have issued the `security bandwidth profile add` command, you enter the `security-config [bandwidth-profile]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**  
**Format**  
security bandwidth profile add

**Mode**  
security

**Step 2**  
**Format**  
name <profile name>

direction {Inbound | Outbound | Both_Directions}

inbound_minimum_rate <kbps>

inbound_maximum_rate <kbps>

outbound_minimum_rate <kbps>

outbound_maximum_rate <kbps>

is_group {Individual | Group}

max_instances <number>

**Mode**  
security-config [bandwidth-profile]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>profile name</td>
<td>The profile name (alphanumeric string).</td>
</tr>
<tr>
<td>direction</td>
<td>Inbound, Outbound, or Both_Directions</td>
<td>Specifies the direction to which the bandwidth profile applies.</td>
</tr>
<tr>
<td>inbound_minimum_rate</td>
<td>kbps</td>
<td>The minimum inbound bandwidth in kbps (0 to 100000) provided to the group or individual user.</td>
</tr>
<tr>
<td>inbound_maximum_rate</td>
<td>kbps</td>
<td>The maximum inbound bandwidth in kbps (100 to 100000) provided to the group or individual user.</td>
</tr>
</tbody>
</table>
**Keyword** | **Associated Keyword to Select or Parameter to Type** | **Description**
---|---|---
outbound_minimum_rate | kbps | The minimum outbound bandwidth in kbps (0 to 100000) provided to the group or individual user.
outbound_maximum_rate | kbps | The maximum outbound bandwidth in kbps (100 to 100000) provided to the group or individual user.
is_group | Individual or Group | Specifies the type for the bandwidth profile:
• Individual. The profile applies to an individual user. Issue the max_instances keyword to specify the maximum number of users.
• Group. The profile applies to a group.
max_instances | number | If the is_group keyword is set to Individual, specify the maximum number of class instances that can be created by the individual bandwidth profile.

**Command example:**

SRX5308> security bandwidth profile add
security-config[brightness-profile] > name BusinessLevelI
security-config[brightness-profile] > direction Both _Directions
security-config[brightness-profile] > inbound_minimum_rate 7500
security-config[brightness-profile] > inbound_maximum_rate 25000
security-config[brightness-profile] > outbound_minimum_rate 5000
security-config[brightness-profile] > outbound_maximum_rate 10000
security-config[brightness-profile] > is_group Group
security-config[brightness-profile] > save

Related show command: `show security bandwidth profile setup`

---

**security bandwidth profile edit <row id>**

This command configures an existing bandwidth profile. After you have issued the security bandwidth profile edit command to specify the row to be edited, you enter the security-config [brightness-profile] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the profile.

**Step 1 Format**

- **Mode** security

---

**Security Mode Configuration Commands**

178
Step 2 Format direction {Inbound | Outbound | Both_Directions}
inbound_minimum_rate <kbps>
inbound_maximum_rate <kbps>
outbound_minimum_rate <kbps>
outbound_maximum_rate <kbps>
is_group {Individual | Group}
max_instances <number>

Mode security-config [bandwidth-profile]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direction</td>
<td>Inbound, Outbound, or Both_Directions</td>
<td>Specifies the direction to which the bandwidth profile applies.</td>
</tr>
<tr>
<td>inbound_minimum_rate</td>
<td>kbps</td>
<td>The minimum inbound bandwidth in kbps (0 to 100000) provided to the group or individual user.</td>
</tr>
<tr>
<td>inbound_maximum_rate</td>
<td>kbps</td>
<td>The maximum inbound bandwidth in kbps (100 to 100000) provided to the group or individual user.</td>
</tr>
<tr>
<td>outbound_minimum_rate</td>
<td>kbps</td>
<td>The minimum outbound bandwidth in kbps (0 to 100000) provided to the group or individual user.</td>
</tr>
<tr>
<td>outbound_maximum_rate</td>
<td>kbps</td>
<td>The maximum outbound bandwidth in kbps (100 to 100000) provided to the group or individual user.</td>
</tr>
<tr>
<td>is_group</td>
<td>Individual or Group</td>
<td>Specifies the type for the bandwidth profile:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Individual. The profile applies to an individual user. Issue the max_instances keyword to specify the maximum number of users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Group. The profile applies to a group.</td>
</tr>
<tr>
<td>max_instances</td>
<td>number</td>
<td>If the is_group keyword is set to Individual, specify the maximum number of class instances that can be created by the individual bandwidth profile.</td>
</tr>
</tbody>
</table>

Related show command: show security bandwidth profile setup

security bandwidth profile delete <row id>

This command deletes a bandwidth profile by deleting its row ID.

Format net bandwidth profile delete <row id>

Mode security
Content Filtering Commands

security content_filter content_filtering configure

This command globally enables or disables content filtering and configures web components. After you have issued the security content_filter content_filtering configure command, you enter the security-config [content-filtering] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format
security content_filter content_filtering configure

Mode
security

**Step 2** Format
content_filtering {Y | N}
activex_enable {Y | N}
cookies_enable {Y | N}
java_enable {Y | N}
proxy_enable {Y | N}

Mode
security-config [content-filtering]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content_filtering</td>
<td>Y or N</td>
<td>Enables or disables content filtering globally.</td>
</tr>
<tr>
<td>activex_enable</td>
<td>Y or N</td>
<td>Enables or disables ActiveX.</td>
</tr>
<tr>
<td>cookies_enable</td>
<td>Y or N</td>
<td>Enables or disables cookies.</td>
</tr>
<tr>
<td>java_enable</td>
<td>Y or N</td>
<td>Enables or disables Java.</td>
</tr>
<tr>
<td>proxy_enable</td>
<td>Y or N</td>
<td>Enables or disables the proxy server.</td>
</tr>
</tbody>
</table>

Command example:
SRX5308> security content_filter content_filtering configure
security-config[content-filtering]> content_filtering Y
security-config[content-filtering]> activex_enable Y
security-config[content-filtering]> cookies_enable Y
security-config[content-filtering]> java_enable Y
security-config[content-filtering]> proxy_enable N
security-config[content-filtering]> save

Related show command: show security content_filter content_filtering
**security content_filter block_group enable**

This command applies content filtering to selected groups or to all groups. After you have issued the `security content_filter block_group enable` command, you enter the security-config [block-group-enable] mode, and then you can select a group, several groups, or all groups.

### Step 1

**Format**

```
security content_filter block_group enable
```

**Mode**

```
security
```

### Step 2

**Format**

```
group all
```

```
group group1
```

```
group group2
```

```
group group3
```

```
group group4
```

```
group group5
```

```
group group6
```

```
group group7
```

```
group group8
```

**Mode**

```
security-config [block-group-enable]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group all</td>
<td>Y</td>
<td>Enables content filtering for all groups.</td>
</tr>
<tr>
<td>group group1</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group2</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group3</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group4</td>
<td>Y</td>
<td>Enables content filtering for the selected group.</td>
</tr>
<tr>
<td>group group5</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group6</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group7</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group8</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> security content_filter blocked_group enable
security-config[block-group-enable]> group group1 Y
security-config[block-group-enable]> group group2 Y
security-config[block-group-enable]> group group3 Y
security-config[block-group-enable]> group group8 Y
security-config[block-group-enable]> save
```
**security content_filter block_group disable**

This command removes content filtering from selected groups or from all groups. After you have issued the `security content_filter block_group disable` command, you enter the security-config [block-group-disable] mode, and then you can select a group, several groups, or all groups.

**Step 1** Format
security content_filter block_group disable

Mode security

**Step 2** Format

group all {Y}
group group1 {Y}
group group2 {Y}
group group3 {Y}
group group4 {Y}
group group5 {Y}
group group6 {Y}
group group7 {Y}
group group8 {Y}

Mode security-config [block-group-disable]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group all</td>
<td>Y</td>
<td>Disables content filtering for all groups.</td>
</tr>
<tr>
<td>group group1</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group2</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group3</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group4</td>
<td>Y</td>
<td>Disables content filtering for the selected group.</td>
</tr>
<tr>
<td>group group5</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group6</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group7</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>group group8</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

**Command example:**

SRX5308> **security content_filter blocked_group disable**
security-config[block-group-disable]> group group3 Y
security-config[block-group-disable]> group group8 Y
security-config[block-group-disable]> save

---

Security Mode Configuration Commands

182
Related show command: `show security content_filter block_group`

---

**security content_filter blocked_keywords add**

This command configures a new blocked keyword for content filtering. After you have issued the `security content_filter blocked_keywords add` command, you enter the security-config [blocked-keywords] mode, and then you can configure one keyword a time.

**Step 1** Format  
security content_filter blocked_keywords add  
Mode  
security  

**Step 2** Format  
blocked_keyword <keyword>  
Mode  
security-config [blocked-keywords]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocked_keyword</td>
<td>keyword</td>
<td>The keyword (string) that needs to be blocked.</td>
</tr>
</tbody>
</table>

Command example:

```plaintext
FVS318N> security content_filter blocked_keywords add
security-config[blocked-keywords]> blocked_keyword casino
security-config[blocked-keywords]> save
security-config[blocked-keywords]> blocked_keyword gambl*
security-config[blocked-keywords]> save
```

Related show command: `show security content_filter blocked_keywords`

---

**security content_filter blocked_keywords edit <row id>**

This command configures an existing blocked keyword for content filtering. After you have issued the `security content_filter blocked_keywords edit` command to specify the row to be edited, you enter the security-config [blocked-keywords] mode, and then you can edit the keyword.

**Step 1** Format  
security content_filter blocked_keywords edit  
Mode  
security  

**Step 2** Format  
blocked_keyword <keyword>  
Mode  
security-config [blocked-keywords]
**Security Mode Configuration Commands**

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocked_keyword</td>
<td>keyword</td>
<td>The keyword (string) that needs to be blocked.</td>
</tr>
</tbody>
</table>

**Related show command:** `show security content_filter blocked_keywords`

---

**security content_filter blocked_keywords delete <row id>**

This command deletes a blocked keyword by deleting its row ID.

**Format**  
`security content_filter blocked_keywords delete <row id>`

**Mode**  
security

**Related show command:** `show security content_filter blocked_keywords`

---

**security content_filter trusted_domain add**

This command configures a new trusted domain for content filtering. After you have issued the `security content_filter trusted_domain add` command, you enter the `security-config [approved-urls]` mode, and then you can add a URL or domain name.

**Step 1**  
**Format**  
`security content_filter trusted_domain add`

**Mode**  
security

**Step 2**  
**Format**  
`url <url>`

**Mode**  
security-config [approved-urls]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>url</td>
<td>The URL or domain name that needs to be blocked.</td>
</tr>
</tbody>
</table>

**Command example:**

```
FVS318N> security content_filter trusted_domain add
security-config[approved-urls]> url netgear
security-config[approved-urls]> save
security-config[approved-urls]> url google.com
security-config[approved-urls]> save
security-config[approved-urls]> save
```
security content_filter trusted_domain edit <row id>

This command configures an existing trusted domain for content filtering. After you have issued the `security content_filter trusted_domain edit` command to specify the row to be edited, you enter the security-config [approved-urls] mode, and then you can edit the URL or domain name.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td><code>security content_filter trusted_domain edit &lt;row id&gt;</code></td>
<td>security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td><code>url &lt;url&gt;</code></td>
<td>security-config [approved-urls]</td>
</tr>
<tr>
<td>Mode</td>
<td>security-config [approved-urls]</td>
<td>security</td>
</tr>
</tbody>
</table>

**Keyword** | **Associated Parameter to Type** | **Description**
---|---|---
url | url | The URL or domain name that needs to be blocked.

Related show command: `show security content_filter trusted_domains`

security content_filter trusted_domain delete <row id>

This command deletes a trusted domain by deleting its row ID.

**Format** | `security content_filter trusted_domain delete <row id>` |
**Mode** | security |

Related show command: `show security content_filter trusted_domains`
This chapter explains the configuration commands, keywords, and associated parameters in the system mode. The chapter includes the following sections:

- Remote Management Commands
- SNMP Commands
- Time Zone Command
- WAN Traffic Meter Command
- Firewall Logs and Email Alerts Commands

**IMPORTANT:**

After you have issued a command that includes the word configure, add, or edit, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 12.

**Remote Management Commands**

```
system remote_management https configure
```

This command configures remote management over HTTPS. After you have issued the `system remote_management https configure` command, you enter the system-config [https] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Note:** You can configure remote management over HTTPS for both IPv4 and IPv6 connections because these connections are not mutually exclusive.

**Step 1  Format**  `system remote_management https configure`

**Mode**  `system`
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Step 2  Format  \texttt{ip\_version} \{IPv4 \mid IPv6\}

\begin{verbatim}
enable_ipv4 \{Y \mid N\}
access_type \{Everyone \mid IP\_Range \{from\_address <ipaddress>\}
{end\_address <ipaddress>} \mid To\_this\_PC\_only \{only\_this\_pc\_ip
<ipaddress>\}}
port <number>
\end{verbatim}

\begin{verbatim}
enable_ipv6 \{Y \mid N\}
access_type6 \{Everyone \mid IP\_Range \{from\_address6
<ipv6-address>\} {end\_address6 <ipv6-address>} \mid
To\_this\_PC\_only \{only\_this\_pc\_ipv6 <ipv6-address>\}}
port <number>
\end{verbatim}

Mode  system-config [https]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_version</td>
<td>IPv4 or IPv6</td>
<td>Specifies the configuration of IPv4 or IPv6.</td>
</tr>
<tr>
<td>enable_ipv4</td>
<td>Y or N</td>
<td>Enables or disables remote management over HTTPS for an IPv4 connection.</td>
</tr>
<tr>
<td>access_type</td>
<td>Everyone, IP_Range, or To_this_PC_only</td>
<td>Specifies the type of access:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• \textit{Everyone}. Enables access to all IP addresses. You do not need to configure any IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• \textit{IP_Range}. Enables access to a range of IP addresses. You also need to configure the \textit{from_address} and \textit{end_address} keywords and associated parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• \textit{To_this_PC_only}. Enables access to a single IP address. You also need to configure the \textit{only_this_pc_ip} keyword and associated parameter.</td>
</tr>
<tr>
<td>from_address</td>
<td>ipaddress</td>
<td>The start IP address if you have set the \textit{access_type} keyword to \textit{IP_Range}.</td>
</tr>
<tr>
<td>end_address</td>
<td>ipaddress</td>
<td>The end IP address if you have set the \textit{access_type} keyword to \textit{IP_Range}.</td>
</tr>
<tr>
<td>only_this_pc_ip</td>
<td>ipaddress</td>
<td>The single IP address if you have set the \textit{access_type} keyword to \textit{To_this_PC_only}.</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>The number of the port through which access is allowed.</td>
</tr>
</tbody>
</table>

HTTPS over an IPv6 connection

| enable_ipv6    | Y or N                                             | Enables or disables remote management over HTTPS for an IPv6 connection. |
## System Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

### Command example:

SRX5308> system remote_management https configure
system-config[https]> ip_version IPv4
system-config[https]> enable_ipv4 Y
system-config[https]> access_type6 Everyone
system-config[https]> port 445
system-config[https]> save

**Related show command:** show system remote_management setup

### system remote_management telnet configure

This command configures remote management over Telnet. After you have issued the system remote_management telnet configure command, you enter the system-config[telnet] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Note:** You can configure remote management over Telnet for both IPv4 and IPv6 connections because these connections are not mutually exclusive.
### Step 1: Format

- `system remote_management telnet configure`
- **Mode**: `system`

### Step 2: Format

- `ip_version {IPv4 | IPv6}`
- `enable_ipv4 {Y | N}`
- `access_type {Everyone | IP_Range {from_address <ipaddress> | to_address <ipaddress>} | To_this_PC_only {only_this_pc_ip <ipaddress>}}`
- `enable_ipv6 {Y | N}`
- `access_type6 {Everyone | IP_Range {from_address6 <ipv6-address> | to_address6 <ipv6-address>} | To_this_PC_only {only_this_pc_ip6 <ipv6-address>}}`

**Mode**: `system-config [telnet]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip_version</strong></td>
<td>IPv4 or IPv6</td>
<td>Specifies the configuration of IPv4 or IPv6.</td>
</tr>
<tr>
<td><strong>enable_ipv4</strong></td>
<td>Y or N</td>
<td>Enables or disables remote management over Telnet for an IPv4 connection.</td>
</tr>
<tr>
<td><strong>access_type</strong></td>
<td>Everyone, IP_Range, or To_this_PC_only</td>
<td>Specifies the type of access:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Everyone</strong> Enables access to all IP addresses. You do not need to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configure any IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>IP_Range</strong> Enables access to a range of IP addresses. You also need</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to configure the <strong>from_address</strong> and <strong>to_address</strong> keywords and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>associated parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>To_this_PC_only</strong> Enables access to a single IP address. You also</td>
</tr>
<tr>
<td></td>
<td></td>
<td>need to configure the <strong>only_this_pc_ip</strong> keyword and associated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>parameter.</td>
</tr>
<tr>
<td><strong>from_address</strong></td>
<td>ipaddress</td>
<td>The start IP address if you have set the <strong>access_type</strong> keyword to <strong>IP_Range</strong>.</td>
</tr>
<tr>
<td><strong>to_address</strong></td>
<td>ipaddress</td>
<td>The end IP address if you have set the <strong>access_type</strong> keyword to <strong>IP_Range</strong>.</td>
</tr>
<tr>
<td><strong>only_this_pc_ip</strong></td>
<td>ipaddress</td>
<td>The single IP address if you have set the <strong>access_type</strong> keyword to <strong>To_this_PC_only</strong>.</td>
</tr>
</tbody>
</table>

**Telnet over an IPv6 connection**

- `enable_ipv6 Y or N` Enables or disables remote management over Telnet for an IPv6 connection.
System Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access_type6</td>
<td>Everyone, IP_Range, or To_this_PC_only</td>
<td>Specifies the type of access:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Everyone</strong>. Enables access to all IP addresses. You do not need to configure any IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>IP_Range</strong>. Enables access to a range of IP addresses. You also need to configure the from_address6 and to_address6 keywords and associated parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>To_this_PC_only</strong>. Enables access to a single IP address. You also need to configure the only_this_pc_ip6 keyword and associated parameter.</td>
</tr>
<tr>
<td>from_address6</td>
<td>ipv6-address</td>
<td>The start IP address if you have set the access_type6 keyword to IP_Range.</td>
</tr>
<tr>
<td>to_address6</td>
<td>ipv6-address</td>
<td>The end IP address if you have set the access_type6 keyword to IP_Range.</td>
</tr>
<tr>
<td>only_this_pc_ip6</td>
<td>ipaddress</td>
<td>The single IP address if you have set the access_type6 keyword to To_this_PC_only.</td>
</tr>
</tbody>
</table>

**Command example:**

SRX5308> **system remote_management telnet configure**
system-config[telnet]> ip_version IPv6
system-config[telnet]> enable_ipv6 Y
system-config[telnet]> **access_type6 IP_Range**
system-config[telnet]> from_address6 FEC0::3001
system-config[telnet]> end_address6 FEC0::3100
system-config[telnet]> save

**Related show command:** **show system remote_management setup**
SNMP Commands

`system snmp sys configure`

This command configures the SNMP system information. After you have issued the `system snmp sys configure` command, you enter the system-config [snmp-system] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**
```
system snmp sys configure
```
**Mode**
`system`

**Step 2 Format**
```
  sys_contact <contact name>
  sys_location <location name>
  sys_name <system name>
```
**Mode**
`system-config [snmp-system]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_contact</td>
<td>contact name</td>
<td>The system contact name (alphanumeric string).</td>
</tr>
<tr>
<td>sys_location</td>
<td>location name</td>
<td>The system location name (alphanumeric string).</td>
</tr>
<tr>
<td>sys_name</td>
<td>system name</td>
<td>The system name (alphanumeric string).</td>
</tr>
</tbody>
</table>

**Command example:**
```
SRX5308> system snmp sys configure
system-config[snmp-system]> sys_contact AdminSRX@netgear.com
system-config[snmp-system]> sys_location San Jose
system-config[snmp-system]> sys_name SRX5308-Bld3
system-config[snmp-system]> save
```

**Related show command:** `show system snmp sys`
Time Zone Command

**system time configure**

This command configures the system time, date, and NTP servers. After you have issued the `system time configure` command, you enter the system-config [time] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format  
`system time configure`

Mode  
`system`

**Step 2** Format  
```
timezone <timezone>
auto_daylight {Y | N}
resolv_ipv6_address {Y | N}
ntp_mode {Authoritative_Mode {stratum <number>} | Sync_to_NTP_Servers_on_Internet | Sync_to_NTP_Servers_on_VPN {vpn_policy <vpn policy name>}}
set_date_time_manually {N | Y {ntp_hour <hour> | ntp_minutes <minutes> | ntp_seconds <seconds> | ntp_day <day> | ntp_month <month> | ntp_year <year>}}
use_default_servers {Y | N}
configure_ntp_servers {Y | N {ntp_server1 {<ipaddress> | <domain name>}} {ntp_server2 {<ipaddress> | <domain name>}}}
```

Mode  
`system-config [time]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timezone</td>
<td>timezone keyword</td>
<td>For a list of time zones that you can enter, see Table 11.</td>
</tr>
<tr>
<td>auto_daylight</td>
<td>Y or N</td>
<td>Enables or disables automatic adjustment for daylight savings time.</td>
</tr>
</tbody>
</table>
| resolv_ipv6_address          | Y or N                                           | Specifies whether or not the VPN firewall automatically resolves a domain name for an NTP server to an IPv6 address:  
• Y. A domain name is resolved to an IPv6 address.  
• N. A domain name is resolved to an IPv4 address. |
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| ntp_mode              | Authoritative_Mode, Sync_to_NTP_Servers_on_ Internet, or Sync_to_NTP_Servers_on_VPN | Specifies the NTP mode:  
- **Authoritative_Mode**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall’s real-time clock (RTC) provides time service to clients. Issue the `stratum` keyword to specify the stratum value. As an option, issue the `set_date_time_manually` value keyword to enable manual configuration of the date and time.  
- **Sync_to_NTP_Servers_on_Internet**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall does not use its RTC.  
- **Sync_to_NTP_Servers_on_VPN**. The VPN firewall synchronizes its clock with the specified NTP server on the VPN. If the server is unreachable, the VPN firewall does not use its RTC. Issue the `vpn_policy` keyword to specify a VPN policy that enables the VPN firewall to contact the NTP server on the VPN. |
| stratum               | number                                           | If the `ntp_mode` keyword is set to `Authoritative_Mode`, the stratum value. This value indicates the distance between the RTC of the VPN firewall and a reference clock.                                                   |
| set_date_time_manually | Y or N                                            | Enables or disables manual configuration of the date and time. If you enable manual configuration, issue the `ntp_hour`, `ntp_minutes`, `ntp_seconds`, `ntp_day`, `ntp_month`, and `ntp_year` keywords to specify the date and time manually.  |
| ntp_hour              | hour                                             | The hour in the format HH (00 to 24) for manual configuration.                                                                                                                                               |
| ntp_minutes           | minutes                                          | The minutes in the format MM (00 to 59) for manual configuration.                                                                                                                                              |
| ntp_seconds           | seconds                                          | The seconds in the format SS (00 to 59) for manual configuration.                                                                                                                                              |
| ntp_day               | day                                              | The day in the format DD (00 to 31) for manual configuration.                                                                                                                                                  |
| ntp_month             | month                                            | The month in the format MM (01 to 12) for manual configuration.                                                                                                                                                 |
| ntp_year              | year                                             | The year in the format YYYY for manual configuration.                                                                                                                                                          |
If the `ntp_mode` keyword is set to `Sync_to_NTP_Servers_on_VPN`, the name of the VPN policy that enables the VPN firewall to contact the NTP server on the VPN.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpn_policy</code></td>
<td><code>vpn policy name</code></td>
<td>If the <code>ntp_mode</code> keyword is set to <code>Sync_to_NTP_Servers_on_VPN</code>, the name of the VPN policy that enables the VPN firewall to contact the NTP server on the VPN.</td>
</tr>
<tr>
<td><code>use_default_servers</code></td>
<td><code>Y</code> or <code>N</code></td>
<td>Enables or disables the use of default NTP servers.</td>
</tr>
<tr>
<td><code>configure_ntp_servers</code></td>
<td><code>Y</code> or <code>N</code></td>
<td>Enables or disables the use of custom NTP servers. If you enable the use of custom NTP servers, you need to specify the server IP addresses or domain names with the <code>ntp_server1</code> and <code>ntp_server2</code> keywords.</td>
</tr>
<tr>
<td><code>ntp_server1</code></td>
<td><code>ipaddress</code> or <code>domain name</code></td>
<td>The IP address of domain name of the first custom NTP server.</td>
</tr>
<tr>
<td><code>ntp_server2</code></td>
<td><code>ipaddress</code> or <code>domain name</code></td>
<td>The IP address of domain name of the second custom NTP server.</td>
</tr>
</tbody>
</table>

Table 11. Timezone keywords

**GMT time and location**

**Note:** Enter the keywords exactly as stated (you can use autocompletion keys). If there are two locations for the same time zone, enter the location exactly as stated. For example, either enter `GMT-11:00::Samoa` or enter `GMT-10:00::Hawaii`.

<table>
<thead>
<tr>
<th>GMT time and location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT:::Greenwich-Mean-Time::Edinburgh,London</td>
</tr>
<tr>
<td>GMT-12:00::Eniwetok</td>
</tr>
<tr>
<td>GMT-12:00::Kwajalein</td>
</tr>
<tr>
<td>GMT-11:00::Midway_Island</td>
</tr>
<tr>
<td>GMT-11:00::Samoa</td>
</tr>
<tr>
<td>GMT-10:00::Hawaii</td>
</tr>
<tr>
<td>GMT-09:30::Marquesas_Is</td>
</tr>
<tr>
<td>GMT-09:00::Alaska</td>
</tr>
<tr>
<td>GMT-08:30::Pitcairn_Is</td>
</tr>
<tr>
<td>GMT-08:00::Pacific_Time-Canada</td>
</tr>
<tr>
<td>GMT-08:00::Pacific_Time-US</td>
</tr>
<tr>
<td>GMT-08:00::Tijuana</td>
</tr>
<tr>
<td>GMT-07:00::Mountain_Time-Canada</td>
</tr>
<tr>
<td>GMT-07:00::Mountain_Time-US</td>
</tr>
</tbody>
</table>
Table 11. Timezone keywords (continued)

<table>
<thead>
<tr>
<th>GMT time and location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Enter the keywords exactly as stated (you can use autocompletion keys). If there are two locations for the same time zone, enter the location exactly as stated. For example, either enter GMT-11:00::Samoa or enter GMT-10:00::Hawaii.</td>
</tr>
<tr>
<td>GMT-06:00::Central_Time-Canada</td>
</tr>
<tr>
<td>GMT-06:00::Central_Time-US</td>
</tr>
<tr>
<td>GMT-05:00::Eastern_Time-Canada</td>
</tr>
<tr>
<td>GMT-05:00::Eastern_Time-Lima</td>
</tr>
<tr>
<td>GMT-05:00::Eastern_Time-US</td>
</tr>
<tr>
<td>GMT-04:30::Caracas</td>
</tr>
<tr>
<td>GMT-04:00::Atlantic_Time-Canada</td>
</tr>
<tr>
<td>GMT-03:30::Newfoundland</td>
</tr>
<tr>
<td>GMT-03:00::Brasilia,Buenos_Aires</td>
</tr>
<tr>
<td>GMT-02:00::Mid-Atlantic</td>
</tr>
<tr>
<td>GMT-01:00::Azores</td>
</tr>
<tr>
<td>GMT-01:00::Cape_Verde_Is</td>
</tr>
<tr>
<td>GMT+01:00::Europe</td>
</tr>
<tr>
<td>GMT+02:00::Athens</td>
</tr>
<tr>
<td>GMT+02:00::Istanbul</td>
</tr>
<tr>
<td>GMT+02:00::Minsk</td>
</tr>
<tr>
<td>GMT+02:00::Cairo</td>
</tr>
<tr>
<td>GMT+03:00::Baghdad</td>
</tr>
<tr>
<td>GMT+03:00::Kuwait</td>
</tr>
<tr>
<td>GMT+03:00::Moscow</td>
</tr>
<tr>
<td>GMT+03:30::Tehran</td>
</tr>
<tr>
<td>GMT+04:00::Abu-Dhabi</td>
</tr>
<tr>
<td>GMT+04:00::Muscat</td>
</tr>
<tr>
<td>GMT+04:00::Baku</td>
</tr>
<tr>
<td>GMT+04:30::Kabul</td>
</tr>
<tr>
<td>GMT+05:00::Ekaterinburg</td>
</tr>
<tr>
<td>GMT+05:00::Islamabad</td>
</tr>
</tbody>
</table>
Table 11. Timezone keywords (continued)

<table>
<thead>
<tr>
<th>GMT time and location</th>
<th>Note: Enter the keywords exactly as stated (you can use autocompletion keys). If there are two locations for the same time zone, enter the location exactly as stated. For example, either enter GMT-11:00::Samoa or enter GMT-10:00::Hawaii.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT+05:00::Karachi</td>
<td></td>
</tr>
<tr>
<td>GMT+05:30::Bombay,Calcutta,Madras,Delhi</td>
<td></td>
</tr>
<tr>
<td>GMT+05:30::Colombo</td>
<td></td>
</tr>
<tr>
<td>GMT+06:00::Almaty</td>
<td></td>
</tr>
<tr>
<td>GMT+06:00::Dhaka</td>
<td></td>
</tr>
<tr>
<td>GMT+06:30::Burma</td>
<td></td>
</tr>
<tr>
<td>GMT+07:00::Bangkok</td>
<td></td>
</tr>
<tr>
<td>GMT+07:00::Hanoi</td>
<td></td>
</tr>
<tr>
<td>GMT+07:00::Jakarta</td>
<td></td>
</tr>
<tr>
<td>GMT+08:00::Beijing,Chongqing,Hong_Kong</td>
<td></td>
</tr>
<tr>
<td>GMT+08:00::AWST-Perth</td>
<td></td>
</tr>
<tr>
<td>GMT+09:00::Osaka,Sapporo, Tokyo</td>
<td></td>
</tr>
<tr>
<td>GMT+09:00::Seoul</td>
<td></td>
</tr>
<tr>
<td>GMT+09:30::ACST-Adelaide</td>
<td></td>
</tr>
<tr>
<td>GMT+09:30::ACST-Darwin</td>
<td></td>
</tr>
<tr>
<td>GMT+09:30::ACST--Broken_Hill,NSW</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::AEST-Brisbane</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::Guam</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::Port_Moresby</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::AEST-Canberra</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::AEST-Melbourne</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::AEST-Sydney</td>
<td></td>
</tr>
<tr>
<td>GMT+10:00::AEST-Hobart</td>
<td></td>
</tr>
<tr>
<td>GMT+10:30::Lord_Howe_Is</td>
<td></td>
</tr>
<tr>
<td>GMT+11:00::Magadan</td>
<td></td>
</tr>
<tr>
<td>GMT+11:00::Solomon_Is</td>
<td></td>
</tr>
<tr>
<td>GMT+11:00::New_Caledonia</td>
<td></td>
</tr>
</tbody>
</table>
Table 11. Timezone keywords (continued)

<table>
<thead>
<tr>
<th>GMT time and location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Enter the keywords exactly as stated (you can use autocompletion keys). If there are two locations for the same time zone, enter the location exactly as stated. For example, either enter GMT-11:00::Samoa or enter GMT-10:00::Hawaii.</td>
</tr>
<tr>
<td>GMT+11:30::Norfolk_I</td>
</tr>
<tr>
<td>GMT+12:00::Auckland</td>
</tr>
<tr>
<td>GMT+12:00::Wellington</td>
</tr>
<tr>
<td>GMT+12:00::New_Zealand</td>
</tr>
<tr>
<td>GMT+12:00::Fiji</td>
</tr>
<tr>
<td>GMT+13:00::Tonga</td>
</tr>
<tr>
<td>GMT+14:00::Kiribati</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> **system time configure**
system-config[time]> **timezone GMT-08:00::Pacific_Time-US**
system-config[time]> **auto_daylight Y**
system-config[time]> **resolve_ipv6_address N**
system-config[time]> **ntp_mode Sync_to_NTP_Servers_on_Internet**
system-config[time]> **use_default_servers Y**
system-config[time]> **configure_ntp_servers N**
system-config[time]> **save**

Related show command: **show system time setup**
**WAN Traffic Meter Command**

system traffic_meter configure <wan interface>

This command configures the traffic meter. After you have issued the `system traffic_meter configure` command to specify one of the four WAN interfaces (that is, WAN1, WAN2, WAN3, or WAN4), you enter the system-config [traffic-meter] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
Step 1  Format  system traffic_meter configure {WAN1 | WAN2 | WAN3 | WAN4}
     Mode     system
```

**Step 2 Format**

```
Step 2  Format  enable {Y | N} 
             limit_type {Nolimit | Downloadonly | Directions} 
             monthly_limit <number> 
             increase_limit_enable {N | Y {increase_limit_by <number>}} 
             counter {RestartCounter | SpecificTime {day_of_month <day>} 
                       {time_hour <hour>} {time_meridian {AM | PM}} {time_minute 
                       <minute>}} 
             send_email_report {Y | N} 
             block_type {Block-all-traffic | Block-all-traffic-except-email}
             send_email_alert {Y | N}
     Mode     system-config [traffic-meter]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic meter configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables the traffic meter.</td>
</tr>
<tr>
<td>limit_type</td>
<td>Nolimit, Downloadonly, or Directions</td>
<td>Specifies the type of traffic limit, if any:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Nolimit. There is no traffic limit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Downloadonly. The traffic limit applies to downloaded traffic only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Directions. The traffic limit applies to both downloaded and uploaded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td>monthly_limit</td>
<td>number</td>
<td>The monthly limit for the traffic meter in MB.</td>
</tr>
</tbody>
</table>

System Mode Configuration Commands

198
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>increase_limit_enable</td>
<td>Y or N</td>
<td>Enables or disables automatic increase of the limit after the meter has exceeded the configured limit. If you enable an automatic increase, issue the increase_limit_by keyword to specify the number of MB.</td>
</tr>
<tr>
<td>increase_limit_by</td>
<td>number</td>
<td>The number in MB to increase the configured limit of the traffic meter.</td>
</tr>
<tr>
<td>Traffic counter configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>counter</td>
<td>SpecificTime or RestartCounter</td>
<td>Specifies how the traffic counter is restarted:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SpecificTime. Restarts the traffic counter on a specific day and time. You need to set the day_of_month, time_hour, time_meridian, and time_minute keywords and associated parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RestartCounter. Restarts the traffic counter after you have saved the command.</td>
</tr>
<tr>
<td>day_of_month</td>
<td>day</td>
<td>The day in the format DD (01 to 31) that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>time_hour</td>
<td>hour</td>
<td>The hour in the format HH (00 to 12) that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>time_meridian</td>
<td>AM or PM</td>
<td>Specifies the meridiem for the hour that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>time_minute</td>
<td>minutes</td>
<td>The minutes in the format MM (00 to 59) that the traffic counter restarts. This keyword applies only if you have set the counter keyword to SpecificTime.</td>
</tr>
<tr>
<td>send_email_report</td>
<td>Y or N</td>
<td>Specifies whether or not an email report is sent when the traffic counter restarts.</td>
</tr>
</tbody>
</table>
System Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action when limit is reached</td>
<td></td>
<td></td>
</tr>
<tr>
<td>block_type</td>
<td>Block-all-traffic, or Block-all-traffic-except-email</td>
<td>Specifies the type of traffic blocking after the meter has exceeded the configured limit.</td>
</tr>
<tr>
<td>send_email_alert</td>
<td>Y or N</td>
<td>Specifies whether or not an email alert is sent when the traffic limit is reached.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> system traffic_meter configure WAN1
system-config[traffic-meter]> enable Y
system-config[traffic-meter]> limit_type Downloadonly
system-config[traffic-meter]> monthly_limit 150000
system-config[traffic-meter]> increase_limit_enable Y
system-config[traffic-meter]> increase_limit_by 50000
system-config[traffic-meter]> counter SpecificTime
day_of_month 01
system-config[traffic-meter]> time_hour 00
time_meridian AM
system-config[traffic-meter]> time_minute 00
system-config[traffic-meter]> send_email_report Y
system-config[traffic-meter]> block_type Block-all-traffic-except-email
system-config[traffic-meter]> send_email_alert Y
system-config[traffic-meter]> save

Related show command: show system traffic_meter setup <wan interface>
Firewall Logs and Email Alerts Commands

**system logging configure**

This command configures routing logs for accepted and dropped IPv4 and IPv6 packets, selected system logs, and logs for other events. After you have issued the `system logging configure` command, you enter the `system-config [logging-ipv4-ipv6]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```plaintext
system logging configure
```

**Mode**

```plaintext
system
```

**Step 2 Format**

```plaintext
lan_wan_accept_packet_logs {Y | N}
lan_wan_drop_packet_logs {Y | N}
lan_dmz_accept_packet_logs {Y | N}
lan_dmz_drop_packet_logs {Y | N}
dmz_wan_accept_packet_logs {Y | N}
dmz_wan_drop_packet_logs {Y | N}
wlan_accept_packet_logs {Y | N}
wlan_drop_packet_logs {Y | N}
dmz_wlan_accept_packet_logs {Y | N}
dmz_wlan_drop_packet_logs {Y | N}
wlan_dmz_accept_packet_logs {Y | N}
wlan_dmz_drop_packet_logs {Y | N}
change_of_time_by_NTP_logs {Y | N}
login_attempts_logs {Y | N}
secure_login_attempts_logs {Y | N}
reboot_logs {Y | N}
unicast_traffic_logs {Y | N}
broadcast_or_multicast_traffic_logs {Y | N}
wlan_status_logs {Y | N}
resol_val_DNS_names_logs {Y | N}
vpn_logs {Y | N}
dhcp_server_logs {Y | N}
source_mac_filter_logs {Y | N}
session_limit_logs {Y | N}
bandwidth_limit_logs {Y | N}
```

**Mode**

```plaintext
system-config [logging-ipv4-ipv6]
```
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routing logs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lan_wan_accept_packet_logs</td>
<td>Y or N</td>
<td>Enables or disables packet logging for the traffic direction and type of packet (accepted or dropped) that is defined in the keyword.</td>
</tr>
<tr>
<td>lan_wan_drop_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>lan_dmz_accept_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>lan_dmz_drop_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>dmz_wan_accept_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>dmz_wan_drop_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>wan_lan_accept_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>wan_lan_drop_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>dmz_lan_accept_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>dmz_lan_drop_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>wan_dmz_accept_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td>wan_dmz_drop_packet_logs</td>
<td>Y or N</td>
<td></td>
</tr>
<tr>
<td><strong>System logs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>change_of_time_by_NTP_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of time changes of the VPN firewall.</td>
</tr>
<tr>
<td>login_attempts_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of login attempts.</td>
</tr>
<tr>
<td>secure_login_attempts_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of secure login attempts.</td>
</tr>
<tr>
<td>reboot_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of rebooting of the VPN firewall.</td>
</tr>
<tr>
<td>unicast_traffic_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of unicast traffic.</td>
</tr>
<tr>
<td>broadcast_or_multicast_traffic_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of broadcast and multicast traffic.</td>
</tr>
<tr>
<td>wan_status_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of WAN link–status-related events.</td>
</tr>
<tr>
<td>resolved_DNS_names_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of resolved DNS names.</td>
</tr>
<tr>
<td>vpn_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of VPN negotiation messages.</td>
</tr>
<tr>
<td>dhcp_server_logs</td>
<td>Y or N</td>
<td>Enables or disables logging of DHCP server events.</td>
</tr>
</tbody>
</table>
### System Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Command example:**

SRX5308> **system logging configure**

```bash
system-config[logging-ipv4-ipv6]> lan_wan_drop_packet_logs Y
system-config[logging-ipv4-ipv6]> wan_lan_drop_packet_logs Y
system-config[logging-ipv4-ipv6]> change_of_time_by_NTP_logs Y
system-config[logging-ipv4-ipv6]> secure_login_attempts_logs Y
system-config[logging-ipv4-ipv6]> reboot_logs Y
system-config[logging-ipv4-ipv6]> unicast_traffic_logs Y
system-config[logging-ipv4-ipv6]> bandwidth_limit_logs Y
system-config[logging-ipv4-ipv6]> save
```

**Related show command:** *show system logging setup* and *show system logs*

---

**system logging remote configure**

This command configures email logs and alerts, schedules email logs and alerts, and configures a syslog server. After you have issued the **system logging remote configure** command, you enter the system-config [logging-remote] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
Format: system logging remote configure
Mode: system
```

**Step 2 Format**

```
Format: log_identifier <identifier>
```
email_logs_enable \{Y \mid N\}
email_server \{ipaddress \mid domain name\}
return_email <email address>
send_to_email <email address>
smtp_custom_port <number>
smtp_auth type \{None \mid Plain \{smtp_auth username <user name>\} \mid CRAM-MD5 \{smtp_auth username <user name>\} \{smtp_auth password <password>\}\}
identd_from_smtp_server_enable \{Y \mid N\}
schedule unit \{Never \mid Hourly \mid Daily \{schedule time 0:00 \mid 1:00 \mid 2:00 \mid 3:00 \mid 4:00 \mid 5:00 \mid 6:00 \mid 7:00 \mid 8:00 \mid 9:00 \mid 10:00 \mid 11:00\} \{schedule meridiem \{AM \mid PM\}\} \mid Weekly \{schedule day \{Sunday \mid Monday \mid Tuesday \mid Wednesday \mid Thursday \mid Friday \mid Saturday\}\{schedule time 0:00 \mid 1:00 \mid 2:00 \mid 3:00 \mid 4:00 \mid 5:00 \mid 6:00 \mid 7:00 \mid 8:00 \mid 9:00 \mid 10:00 \mid 11:00\}\{schedule meridiem \{AM \mid PM\}\}\}
syslog_server \{ipaddress \mid domain name\}
syslog_severity \{LOG_EMERG \mid LOG_ALERT \mid LOG_CRITICAL \mid LOG_ERROR \mid LOG_WARNING \mid LOG_NOTICE \mid LOG_INFO \mid LOG_DEBUG\}

Mode
system-config [logging-remote]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log_identifier</td>
<td>identifier</td>
<td>The log identifier (alphanumeric string).</td>
</tr>
<tr>
<td>Email log configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>email_logs_enable</td>
<td>Y or N</td>
<td>Enables or disables emailing of logs.</td>
</tr>
<tr>
<td>email_server</td>
<td>ipaddress or domain name</td>
<td>The IP address or domain name of the SMTP server.</td>
</tr>
<tr>
<td>return_email</td>
<td>email address</td>
<td>The email address (alphanumeric string) to which the SMTP server replies are sent.</td>
</tr>
<tr>
<td>send_to_email</td>
<td>email address</td>
<td>The email address (alphanumeric string) to which the logs and alerts are sent.</td>
</tr>
<tr>
<td>smtp_custom_port</td>
<td>number</td>
<td>The port number of the SMTP server for the outgoing email. The default port number is 25.</td>
</tr>
<tr>
<td>Keyword (might consist of two separate words)</td>
<td>Associated Keyword to Select or Parameter to Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>smtp_auth type</td>
<td>None, Plain, or CRAM-MD5</td>
<td>Specifies the type of authentication for the SMTP server. If you select Plain or CRAM-MD5, you also need to configure the smtp_auth username and smtp_auth password keywords and associated parameters.</td>
</tr>
<tr>
<td>smtp_auth username</td>
<td>user name</td>
<td>The user name for SMTP authentication if you have set the smtp_auth type keyword type to Plain or CRAM-MD5.</td>
</tr>
<tr>
<td>smtp_auth password</td>
<td>password</td>
<td>The password for SMTP authentication if you have set smtp_auth type keyword to Plain or CRAM-MD5.</td>
</tr>
<tr>
<td>identd_from_smtp_server_enable</td>
<td>Y or N</td>
<td>Allows or rejects Identd protocol messages from the SMTP server.</td>
</tr>
</tbody>
</table>

**Email log schedule**

<table>
<thead>
<tr>
<th>Schedule unit</th>
<th>Never, Hourly, Daily, or Weekly</th>
<th>Specifies the type of schedule for emailing logs and alerts:</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedule day</td>
<td>Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday</td>
<td>Specifies the scheduled day if you have set the schedule unit keyword to Weekly.</td>
</tr>
<tr>
<td>schedule time</td>
<td>0:00, 1:00, 2:00, 3:00, 4:00, 5:00, 6:00, 7:00, 8:00, 9:00, 10:00, or 11:00</td>
<td>Specifies the scheduled time if you have set the schedule unit keyword to Daily or Weekly.</td>
</tr>
<tr>
<td>schedule meridiem</td>
<td>AM or PM</td>
<td>Specifies the meridiem for the start time if you have set the schedule unit keyword to Daily or Weekly.</td>
</tr>
</tbody>
</table>
### System Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

#### Command example:

```
SRX5308> system logging remote configure
system-config[logging-remote]> log_identifier SRX5308-Bld3
system-config[logging-remote]> email_logs_enable Y
system-config[logging-remote]> email_server SMTP.Netgear.com
system-config[logging-remote]> return_email SRX5308@netgear.com
system-config[logging-remote]> send_to_email admin2@netgear.com
system-config[logging-remote]> smtp_custom_port 2025
system-config[logging-remote]> smtp_auth type None
system-config[logging-remote]> schedule unit Weekly
system-config[logging-remote]> schedule day Sunday
system-config[logging-remote]> schedule time 00
system-config[logging-remote]> schedule meridiem AM
system-config[logging-remote]> syslog_server fe80::a0ca:f072:127f:b028\%21
system-config[logging-remote]> syslog_severity LOG_EMERG, LOG_ALERT,
               LOG_CRITICAL, LOG_ERROR, LOG_WARNING, LOG_NOTICE, LOG_INFO, or
               LOG_DEBUG
system-config[logging-remote]> save
```

**Related show command:** `show system logging remote setup`

---

### Syslog server

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog_server</td>
<td>ipaddress or domain name</td>
<td>The IP address or domain name of the syslog server.</td>
</tr>
<tr>
<td>syslog_severity</td>
<td>LOG_EMERG, LOG_ALERT, LOG_CRITICAL, LOG_ERROR, LOG_WARNING, LOG_NOTICE, LOG_INFO, or LOG_DEBUG</td>
<td>Specifies the syslog severity level. The keywords are self-explanatory.</td>
</tr>
</tbody>
</table>

**Note:** All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select LOG_CRITICAL as the severity, then the logs with the severities LOG_CRITICAL, LOG_ALERT, and LOG_EMERG are logged.
VPN Mode Configuration Commands

This chapter explains the configuration commands, keywords, and associated parameters in the vpn mode. The chapter includes the following sections:

- IPSec VPN Wizard Command
- IPSec IKE Policy Commands
- IPSec VPN Policy Commands
- IPSec VPN Mode Config Commands
- SSL VPN Portal Layout Commands
- SSL VPN Authentication Domain Commands
- SSL VPN Authentication Group Commands
- SSL VPN User Commands
- SSL VPN Port Forwarding Commands
- SSL VPN Client and Client Route Commands
- SSL VPN Resource Commands
- SSL VPN Policy Commands
- RADIUS Server Command
- PPTP Server Commands
- L2TP Server Commands

**IMPORTANT:**

After you have issued a command that includes the word configure, add, or edit, you need to save (or cancel) your changes. For more information, see Save Commands on page 12.
**IPSec VPN Wizard Command**

`vpn ipsec wizard configure <Gateway | VPN_Client>`

This command configures the IPSec VPN wizard for a gateway-to-gateway or gateway-to-VPN client connection. After you have issued the `vpn ipsec wizard configure` command to specify the type of peer for which you want to configure the wizard, you enter the `vpn-config [wizard]` mode, and then you can configure one keyword and associated parameter or associated keyword or associated keyword at a time in the order that you prefer.

**Step 1  Format**

| Mode             | `vpn ipsec wizard configure {Gateway | VPN_Client}` |
|------------------|-----------------------------------------------------|

**Step 2  Format**

| `ip_version {IPv4 | IPv6}` | `conn_name <name>` | `preshared_key <key>` | `local_wan_interface {WAN1 | WAN2 | WAN3 | WAN4}` | `enable_rollover {N | Y |rollover_gateway {WAN1 | WAN2 | WAN3 | WAN4}}` | `remote_wan_ipaddress {<ipaddress> | <ipv6-address> | <domain name>}` | `local_wan_ipaddress {<ipaddress> | <ipv6-address> | <domain name>}` |
|----------------------|-------------------|----------------------|---------------------------|---------------------------------|-------------------------------------------------|-------------------------------------------------|
| `remote_wan_ipaddress` | `<ipaddress>`     | `remote_wan_net_mask` | `<subnet mask>`              |                                      | `remote_lan_ipaddress` | `<ipv6-address>` |
| `remote_lan_ipv6address` | `<ipv6-address>` | `remote_lan_prefixLength` | `<prefix length>`              |                                      | `remote_lan_ipv6address` | `<prefix length>` |

<table>
<thead>
<tr>
<th>Mode</th>
<th><code>vpn-config [wizard]</code></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| `ip_version`             | IPv4 or IPv6                                       | Specifies the IP address version for both the local and remote endpoints:  
  • **IPv4**. Both endpoints use IPv4 addresses. For the remote LAN IP address, you need to issue the `remote_lan_ipaddress` and `remote_lan_net_mask` keywords and specify the associated parameters.  
  • **IPv6**. Both endpoints use IPv6 addresses. For the remote LAN IP address, you need to issue the `remote_lan_ipv6address` and `remote_lan_prefixLength` keywords and specify the associated parameters. |
### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

#### Command example:

```
SRX5308> vpn ipsec wizard configure Gateway
vpn-config[wizard]> ip_version IPv6
vpn-config[wizard]> conn_name SRX5308-to-Peer44
vpn-config[wizard]> preshared_key 2%sgd55%!@GH
vpn-config[wizard]> local_wan_interface WAN1
```

#### VPN Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conn_name</td>
<td>connection name</td>
<td>The unique connection name (alphanumeric string).</td>
</tr>
<tr>
<td>preshared_key</td>
<td>key</td>
<td>The key (alphanumeric string) that needs to be entered on both peers.</td>
</tr>
<tr>
<td>local_wan_interface</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>Specifies the local WAN interface that the VPN tunnel uses as the local endpoint.</td>
</tr>
<tr>
<td>enable_rollover</td>
<td>Y or N</td>
<td>Enables or disables VPN rollover mode. If VPN rollover mode is enabled, you need to issue the <code>rollover_gateway</code> keyword to specify the WAN interface to which the VPN rollover should occur. If VPN rollover mode is enabled, specifies the WAN interface to which the rollover should occur.</td>
</tr>
<tr>
<td>rollover_gateway</td>
<td>WAN1, WAN2, WAN3, or WAN4</td>
<td>If VPN rollover mode is enabled, specifies the WAN interface to which the rollover should occur.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Rollover mode functions only when the IP version is IPv4.</td>
</tr>
</tbody>
</table>

#### Remote WAN and local WAN address information

| remote_wan_ipaddress     | ipaddress, ipv6-address, or domain name          | Depending on the setting of the `ip_version` keyword, specifies an IPv4 or IPv6 local WAN address. You can also specify a domain name. |
| local_wan_ipaddress      | ipaddress, ipv6-address, or domain name          | Depending on the setting of the `ip_version` keyword, specifies an IPv4 or IPv6 local WAN address. You can also specify a domain name. |

#### Remote LAN IPv4 address information

| remote_lan_ipaddress     | ipaddress                                       | The IPv4 remote LAN address when the `ip_version` keyword is set to IPv4.   |
| remote_lan_net_mask      | subnet mask                                      | The IPv4 remote LAN subnet mask when the `ip_version` keyword is set to IPv4. |

#### Remote LAN IPv6 address information

| remote_lan_ipv6address   | ipv6-address                                    | The IPv6 remote LAN address when the `ip_version` keyword is set to IPv6.   |
| remote_lan_prefixLength  | prefix length                                    | The IPv6 remote LAN prefix length when the `ip_version` keyword is set to IPv6. |
**VPN Mode Configuration Commands**

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

```plaintext
vpn-config[wizard]> enable_rollover N
vpn-config[wizard]> remote_wan_ipaddress peer44.com
vpn-config[wizard]> local_wan_ipaddress fe80::a8ab:bbff:fe00:2
vpn-config[wizard]> remote_lan_ipv6address fe80::a4bb:ffdd:fe01:2
vpn-config[wizard]> remote_lan_prefixLength 64
vpn-config[wizard]> save
```

**Related show command:** `show vpn ipsec vpnpolicy setup`, `show vpn ipsec ikepolicy setup`, and `show vpn ipsec vpnpolicy status`

To display the VPN policy configuration that the wizard created through the `vpn ipsec wizard configure` command, issue the `show vpn ipsec vpnpolicy setup` command:

```
SRX5308> show vpn ipsec vpnpolicy setup
```

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Type</th>
<th>IPSec Mode</th>
<th>Local</th>
<th>Remote</th>
<th>Auth</th>
<th>Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>SRX5308-to-Peer44</td>
<td>Auto Policy</td>
<td>Tunnel Mode</td>
<td>2002:408b:36e4:a8ab:bbff:fe00:1 / 64</td>
<td>fe80::a4bb:ffdd:fe01:2 / 64</td>
<td>SHA-1</td>
<td>3DES</td>
</tr>
<tr>
<td>Enabled</td>
<td>SRX-to-Paris</td>
<td>Auto Policy</td>
<td>Tunnel Mode</td>
<td>192.168.1.0 / 255.255.255.0</td>
<td>192.168.50.0 / 255.255.255.255</td>
<td>SHA-1</td>
<td>3DES</td>
</tr>
</tbody>
</table>

To display the IKE policy configuration that the wizard created through the `vpn ipsec wizard configure` command, issue the `show vpn ipsec ikepolicy setup` command:

```
SRX5308> show vpn ipsec ikepolicy setup
```

**List of IKE Policies**

<table>
<thead>
<tr>
<th>Name</th>
<th>Mode</th>
<th>Local ID</th>
<th>Remote ID</th>
<th>Encryption</th>
<th>Authentication</th>
<th>DH Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRX5308-to-Peer44</td>
<td>main</td>
<td>fe80::a8ab:bbff:fe00:2</td>
<td>peer44.com</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Group 2 (1024 bit)</td>
</tr>
<tr>
<td>SRX-to-Paris</td>
<td>main</td>
<td>10.139.54.228</td>
<td>10.112.71.154</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Group 2 (1024 bit)</td>
</tr>
<tr>
<td>iphone</td>
<td>aggressive</td>
<td>10.139.54.228</td>
<td>0.0.0.0</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>Group 2 (1024 bit)</td>
</tr>
</tbody>
</table>

**IPSec IKE Policy Commands**

**vpn ipsec ikepolicy configure <ike policy name>**

This command configures a new or existing manual IPSec IKE policy. After you have issued the `vpn ipsec ikepolicy configure` command to specify the name of a new or existing IKE policy, you enter the vpn-config [ike-policy] mode, and then you can configure one keyword and associated parameter or associated keyword or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
Step 1 Format: vpn ipsec ikepolicy configure <ike policy name>
```

**VPN Mode Configuration Commands**

210
**Step 2 Format**

```plaintext
enable_mode_config {N | Y {mode_config_record <record name>}}
direction_type {Initiator | Responder | Both}
exchange_mode {Main | Aggressive}

ip_version {IPv4 | IPv6}
select_local_gateway {WAN1 | WAN2 | WAN3 | WAN4}
local_ident_type {Local_Wan_IP | FQDN | User-FQDN | DER_ASN1_DN}
  {local_identifier <identifier>}
remote_ident_type {Remote_Wan_IP | FQDN | User-FQDN | DER_ASN1_DN}{remote_identifier <identifier>}

encryption_algorithm {DES | 3DES | AES_128 | AES_192 | AES_256}
auth_algorithm {MD5 | SHA-1}
auth_method {Pre_shared_key {pre_shared_key <key>} | RSA_Signature}
dh_group {Group1_768_bit | Group2_1024_bit | Group5_1536_bit}
lifetime <seconds>
enable_dead_peer_detection {N | Y {detection_period <seconds>}
  {reconnect_failure_count <number>}}

extended_authentication {None | IPSecHost {xauth_username <user name> | xauth_password <password>} | EdgeDevice
  {extended_authentication_type (User-Database | RadiusPap | RadiusChap)}}
```

### ModeVPN config [ike-policy]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_mode_config</td>
<td>Y or N</td>
<td>Specifies whether or not the IKE policy uses a Mode Config record.</td>
</tr>
<tr>
<td>mode_config_record</td>
<td>record name</td>
<td>If the enable_mode_config keyword is set to Y, specifies the Mode Config record that should be used. For information about configuring Mode Config records, see the vpn ipsec mode_config configure &lt;record name&gt; command.</td>
</tr>
</tbody>
</table>
VPN Mode Configuration Commands

### Direction Type

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| direction_type     | Initiator, Responder, or Both                    | Specifies the IKE direction type:  
• **Initiator.** The VPN firewall initiates the connection to the remote endpoint.  
• **Responder.** The VPN firewall responds only to an IKE request from the remote endpoint.  
• **Both.** The VPN firewall can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint. |

### Exchange Mode

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| exchange_mode      | Main or Aggressive                               | Specifies the exchange mode:  
• **Main.** This mode is slower than the Aggressive mode but more secure.  
• **Aggressive.** This mode is faster than the Main mode but less secure. When the IKE policy uses a Mode Config record, the exchange mode needs to be set to Aggressive. |

### Local and Remote Identifiers

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip_version          | IPv4 or IPv6                                     | If the local_ident_type and remote_ident_type keywords are set to Local_Wan_IP, specifies the IP address version for both the local and remote endpoints:  
• **IPv4.** Both endpoints use IPv4 addresses. You need to specify IPv4 addresses for the local_identifier and remote_identifier keywords.  
• **IPv6.** Both endpoints use IPv6 addresses. You need to specify IPv6 addresses for the local_identifier and remote_identifier keywords. |
| select_local_gateway| WAN1, WAN2, WAN3, or WAN4                        | Specifies the WAN interface for the local gateway.                                                                                                                                                      |
### VPN Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_ident_type</td>
<td>Local_Wan_IP, FQDN, User-FQDN, or DER_ASN1_DN</td>
<td>Specifies the ISAKMP identifier to be used by the VPN firewall:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Local_Wan_IP</strong>. The WAN IP address of the VPN firewall. The setting of the ip_version keyword determines if you need to specify an IPv4 or IPv6 address for the local_identifier keyword.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>FQDN</strong>. The domain name for the VPN firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>User-FQDN</strong>. The email address for a local VPN client or the VPN firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>DER_ASN1_DN</strong>. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.</td>
</tr>
<tr>
<td>local_identifier</td>
<td>identifier</td>
<td>The identifier of the VPN firewall. The setting of the local_ident_type and ip_version keywords determines the type of identifier that you need to specify.</td>
</tr>
<tr>
<td>remote_ident_type</td>
<td>Remote_Wan_IP, FQDN, User-FQDN, or DER_ASN1_DN</td>
<td>Specifies the ISAKMP identifier to be used by the VPN firewall:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Remote_Wan_IP</strong>. The WAN IP address of the remote endpoint. The setting of the ip_version keyword determines if you need to specify an IPv4 or IPv6 address for the local_identifier keyword.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>FQDN</strong>. The domain name for the VPN firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>User-FQDN</strong>. The email address for a local VPN client or the VPN firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>DER_ASN1_DN</strong>. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.</td>
</tr>
<tr>
<td>remote_identifier</td>
<td>identifier</td>
<td>The identifier of the remote endpoint. The setting of the remote_ident_type and ip_version keywords determines the type of identifier that you need to specify.</td>
</tr>
<tr>
<td>IKE SA settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryption_algorithm</td>
<td>DES, 3DES, AES_128, AES_192, or AES_256</td>
<td>Specifies the algorithm to negotiate the security association (SA):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>DES</strong>. Data Encryption Standard (DES).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>3DES</strong>. Triple DES.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>AES_128</strong>. Advanced Encryption Standard (AES) with a 128-bit key size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>AES_192</strong>. AES with a 192-bit key size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>AES_256</strong>. AES with a 256-bit key size.</td>
</tr>
</tbody>
</table>
### VPN Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth_algorithm</td>
<td>MD5 or SHA-1</td>
<td>Specifies the algorithm to be used in the VPN header for the authentication process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SHA-1. Hash algorithm that produces a 160-bit digest.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MD5. Hash algorithm that produces a 128-bit digest.</td>
</tr>
<tr>
<td>auth_method</td>
<td>Pre_shared_key or RSA_Signature</td>
<td>Specifies the authentication method:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pre_shared_key. A secret that is shared between the VPN firewall and the remote endpoint. You also need to issue the pre_shared_key keyword and specify the key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RSA_Signature. Uses the active self-signed certificate that you uploaded on the Certificates screen of the web management interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You cannot upload certificates by using the CLI.</td>
</tr>
<tr>
<td>pre_shared_key</td>
<td>key</td>
<td>If the auth_method keyword is set to Pre_shared_key, specifies a key with a minimum length of 8 characters and no more than 49 characters.</td>
</tr>
<tr>
<td>dh_group</td>
<td>Group1_768_bit, Group2_1024_bit, or Group5_1536_bit</td>
<td>Specifies the Diffie-Hellman (DH) group, which sets the strength of the algorithm in bits. The higher the group, the more secure the exchange.</td>
</tr>
<tr>
<td>lifetime</td>
<td>seconds</td>
<td>The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs.</td>
</tr>
<tr>
<td>enable_dead_peer_detection</td>
<td>Y or N</td>
<td>Enables or disables dead peer detection (DPD). When DPD is enabled, you also need to issue the detection_period and reconnect_failure_count keywords and associated parameters.</td>
</tr>
<tr>
<td>detection_period</td>
<td>seconds</td>
<td>The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle.</td>
</tr>
<tr>
<td>reconnect_failure_count</td>
<td>number</td>
<td>The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer.</td>
</tr>
</tbody>
</table>
### Extended authentication settings

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>extended_authentication</td>
<td>None, IPSecHost, or EdgeDevice</td>
<td>Specifies whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• None. XAUTH is disabled. This the default setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPSecHost. The VPN firewall functions as a VPN client of the remote gateway. In this configuration the VPN firewall is authenticated by a remote</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gateway. You need to issue the xauth_username and xauth_password keywords and specify the associated parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EdgeDevice. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. You need to issue the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extended_authentication_type keyword and select an associated keyword.</td>
</tr>
<tr>
<td>extended_authentication_type</td>
<td>User-Database, RadiusPap, or RadiusChap</td>
<td>If the extended_authentication keyword is set to EdgeDevice, specifies the authentication type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User-Database. XAUTH occurs through the VPN firewall’s user database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RadiusPap. XAUTH occurs through RADIUS Password Authentication Protocol (PAP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RadiusChap. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> For information about how to configure a RADIUS server for authentication of VPN connections, see RADIUS Server Command.</td>
</tr>
<tr>
<td>xauth_username</td>
<td>user name</td>
<td>If the extended_authentication keyword is set to IPSecHost, specifies a user name.</td>
</tr>
<tr>
<td>xauth_password</td>
<td>password</td>
<td>If the extended_authentication keyword is set to IPSecHost, specifies a password.</td>
</tr>
</tbody>
</table>
Command example:

SRX5308> vpn ipsec ikepolicy configure SRX-to-Paris
vpn-config[ike-policy]> enable_mode_config N
vpn-config[ike-policy]> direction_type Both
vpn-config[ike-policy]> exchange_mode Main
vpn-config[ike-policy]> ip_version ipv4
vpn-config[ike-policy]> select_local_gateway WAN1
vpn-config[ike-policy]> local_ident_type Local_Wan_IP
vpn-config[ike-policy]> local_identifier 10.139.54.228
vpn-config[ike-policy]> remote_ident_type Remote_Wan_IP
vpn-config[ike-policy]> remote_identifier 10.112.71.154
vpn-config[ike-policy]> encryption_algorithm 3DES
vpn-config[ike-policy]> auth_algorithm SHA-1
vpn-config[ike-policy]> auth_method Pre_shared_key
vpn-config[ike-policy]> pre_shared_key 3Tg67!JXL0o?
vpn-config[ike-policy]> dh_group Group2_1024_bit
vpn-config[ike-policy]> lifetime 28800
vpn-config[ike-policy]> enable_dead_peer_detection Y
vpn-config[ike-policy]> detection_period 20
vpn-config[ike-policy]> reconnect_failure_count 3
vpn-config[ike-policy]> extended_authentication EdgeDevice
vpn-config[ike-policy]> extended_authentication_type RadiusChap
vpn-config[ike-policy]> save

Related show command: show vpn ipsec ikepolicy setup

---

**vpn ipsec ikepolicy delete <ike policy name>**

This command deletes an IKE policy by specifying the name of the IKE policy.

**Format**

```
vpn ipsec ikepolicy delete <ike policy name>
```

**Mode**

`vpn`

Related show command: show vpn ipsec ikepolicy setup

---

**IPSec VPN Policy Commands**

**vpn ipsec vpnpolicy configure <vpn policy name>**

This command configures a new or existing auto IPSec VPN policy or manual IPSec VPN policy. After you have issued the `vpn ipsec vpnpolicy configure` command to specify the name of a new or existing VPN policy, you enter the vpn-config [vpn-policy] mode, and then you can configure one keyword and associated parameter or associated keyword or
associated keyword at a time in the order that you prefer.

Step 1 Format

```
vpn ipsec vpnpolicy configure <vpn policy name>
```

Step 2 Format

```
general_policy_type {Auto-Policy | Manual-Policy}
general_ip_version {IPv4 | IPv6}
general_select_local_gateway {WAN1 | WAN2 | WAN3 | WAN4} 
general_remote_end_point_type {FQDN | IP-Address | IPv6-address}
general_enable_netbios {N | Y}
general_enable_rollover {N | Y | general_rollover_gateway {WAN1 | WAN2 | WAN3 | WAN4}}
general_enable_auto_initiate_policy {N | Y}
general_enable_keep_alive {N | Y | general_ping_ipaddress <ipaddress> | general_ping_ipaddress6 <ipv6-address>}
  [general_keep_alive_detection_period <seconds>]
  [general_keep_alive_failureCount <number>]
general_local_network_type {ANY | SINGLE
  [general_local_start_address <ipaddress> | general_local_start_address_ipv6 <ipv6-address>]
  [general_local_end_address <ipaddress> | general_local_end_address_ipv6 <ipv6-address>]
  [general_local_subnet_mask <subnet mask> | general_local_ipv6_prefix_length <prefix length>]
} | RANGE
  [{general_local_start_address <ipaddress> | general_local_start_address_ipv6 <ipv6-address>]
  [{general_local_end_address <ipaddress> | general_local_end_address_ipv6 <ipv6-address>]
  [{general_local_subnet_mask <subnet mask> | general_local_ipv6_prefix_length <prefix length>}] | SUBNET
  [{general_remote_start_address <ipaddress> | general_remote_start_address_ipv6 <ipv6-address>]
  [{general_remote_end_address <ipaddress> | general_remote_end_address_ipv6 <ipv6-address>]
  [{general_remote_subnet_mask <subnet mask> | general_remote_ipv6_prefix_length <prefix length>}] | SUBNET
  [{general_local_start_address <ipaddress> | general_local_start_address_ipv6 <ipv6-address>]
  [{general_local_end_address <ipaddress> | general_local_end_address_ipv6 <ipv6-address>]
  [{general_local_subnet_mask <subnet mask> | general_local_ipv6_prefix_length <prefix length>}] | RANGE
  [{general_remote_start_address <ipaddress> | general_remote_start_address_ipv6 <ipv6-address>]
  [{general_remote_end_address <ipaddress> | general_remote_end_address_ipv6 <ipv6-address>]
  [{general_remote_subnet_mask <subnet mask> | general_remote_ipv6_prefix_length <prefix length>}]}
```

```
manual_spi_in <number>
manual_encryption_algorithm {None | DES | 3DES | AES-128 | AES-192 | AES-256}
manual_encryption_key_in <key>
manual_encryption_key_out <key>
```
### VPN Mode Configuration Commands

**manual_spi_out** <number>

**manual_authentication_algorithm** {MD5 | SHA-1}

**manual_authentication_key_in** <key>

**manual_authentication_key_out** <key>

**auto_sa_lifetime** {Kbytes <number> | {seconds <seconds>}}

**auto_encryption_algorithm** {None | DES | 3DES | AES-128 | AES-192 | AES-256}

**auto_authentication_algorithm** {MD5 | SHA-1}

**auto_enable_pfskeygroup** {N | Y {auto_dh_group {Group1_768_bit | Group2_1024_bit | Group5_1536_bit}}}

**auto_select_ike_policy** <ike policy name>

---

**Mode** vpn-config [vpn-policy]

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **general_policy_type** | Auto-Policy or Manual-Policy | Species whether the policy type is an auto or manual VPN policy:
- **Auto-Policy.** The inbound and outbound policy settings for the VPN tunnel are automatically generated after you have issued the keywords and associated parameters that are listed in the Auto policy settings section of this table. All other VPN policy settings need to be specified manually.
- **Manual-Policy.** All settings need to be specified manually, excluding the ones in the Auto policy settings section of this table. |
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| general_ip_version | IPv4 or IPv6 | If the `general_remote_end_point_type` keyword is set to `IP-Address`, specifies the IP address version for the remote endpoint, local address information, and remote address information:  
  • **IPv4**. The IPv4 selection requires you to specify IPv4 addresses for the following keywords:  
    - `general_remote_end_point_ip_address`
    - `general_local_start_address`
    - `general_local_end_address`
    - `general_remote_start_address`
    - `general_remote_end_address`
  
  • **IPv6**. The IPv6 selection requires you to specify IPv6 addresses for the following keywords:  
    - `general_remote_end_point_ipv6_address`
    - `general_local_start_address_ipv6`
    - `general_local_end_address_ipv6`
    - `general_remote_start_address_ipv6`
    - `general_remote_end_address_ipv6` |
| general_select_local_gateway | WAN1, WAN2, WAN3, or WAN4 | Specifies the local WAN interface that the VPN tunnel uses as the local endpoint. |
| general_remote_end_point_type | IP-Address or FQDN | Specifies whether the remote endpoint is defined by an IP address or a domain name:  
  • **IP-Address**. Depending on the setting of the `general_ip_version` keyword, you need to either issue the `general_remote_end_point_ip_address` keyword and specify an IPv4 address or issue the `general_remote_end_point_ipv6_address` keyword and specify an IPv6 address.  
  • **FQDN**. You need to issue the `general_remote_end_point fqdn` keyword and specify a domain name. |
| general_remote_end_point fqdn | domain name | If the `general_remote_end_point_type` keyword is set to `FQDN`, the domain name (FQDN) of the remote endpoint. |
| general_remote_end_point ip_address | ipaddress | If the `general_remote_end_point_type` keyword is set to `IP-Address`, and if the `general_ip_version` keyword is set to IPv4, the IPv4 address of the remote endpoint. |
### VPN Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>general_remote_end_point_ipv6_address</td>
<td>ipv6-address</td>
<td>If the <code>general_remote_end_point_type</code> keyword is set to <code>IP-Address</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv6</code>, the IPv6 address of the remote endpoint.</td>
</tr>
<tr>
<td>general_enable_netbios</td>
<td>Y or N</td>
<td>Enables or disables NetBIOS broadcasts to travel over the VPN tunnel.</td>
</tr>
</tbody>
</table>
| general_enable_rollover                     | Y or N                                        | Enables or disables VPN rollover mode. If VPN rollover mode is enabled, you need to issue the `general_rollover_gateway` keyword to specify the WAN interface to which the VPN rollover should occur.  

**Note:** Rollover mode functions only when the IP version is IPV4. |
| general_rollover_gateway                   | WAN1, WAN2, WAN3, or WAN4                     | If VPN rollover mode is enabled, specifies the WAN interface to which the rollover should occur. |
| general_enable_auto_initiate_policy        | Y or N                                        | Enables or disables the automatic establishment of the VPN tunnel when there is no traffic.  

**Note:** You cannot enable automatic establishment of the VPN tunnel if the `direction_type` keyword under the `vpn ipsec ikepolicy configure <ike policy name>` command is set to `Responder`. |
| general_enable_keep_alive                  | Y or N                                        | Enables or disables the VPN firewall to send keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. If you enable keep-alives, you also need to issue the following keywords:  

- Either `general_ping_ipaddress` to specify an IPv4 address or `general_ping_ipaddress6` to specify an IPv6 address.  
- `general_keep_alive_detection_period` to specify the detection period.  
- `general_keep_alive_failure_count` to specify the failure count. |
| general_ping_ipaddress                     | ipaddress                                     | The IPv4 address to send keep-alive requests to. |
| general_ping_ipaddress6                   | ipv6-address                                  | The IPv6 address to send keep-alive requests to. |
## VPN Mode Configuration Commands

### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>general_keep_alive_detection_period</code></td>
<td><code>seconds</code></td>
<td>The period in seconds between consecutive keep-alive requests, which are sent only when the IPSec traffic is idle.</td>
</tr>
<tr>
<td><code>general_keep_alive_failure_count</code></td>
<td><code>number</code></td>
<td>The maximum number of keep-alive request failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer.</td>
</tr>
</tbody>
</table>

### Traffic selector settings—Local address information

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| `general_local_network_type` | `ANY`, `SINGLE`, `RANGE`, `SUBNET` | Specifies the address or addresses that are part of the VPN tunnel on the VPN firewall:  
  - **ANY**: All computers and devices on the network.  
  - **SINGLE**: A single IP address on the network. Depending on the setting of the `general_ip_version` keyword, issue one of the following keywords:  
    - `general_local_start_address` to specify an IPv4 address.  
    - `general_local_start_address_ipv6` to specify an IPv6 address.  
  - **RANGE**: A range of IP addresses on the network. Depending on the setting of the `general_ip_version` keyword, issue one of the following sets of keywords:  
    - `general_local_start_address` and `general_local_end_address` to specify IPv4 addresses.  
    - `general_local_start_address_ipv6` and `general_local_end_address_ipv6` to specify IPv6 addresses.  
  - **SUBNET**: A subnet on the network. Depending on the setting of the `general_ip_version` keyword, issue one of the following sets of keywords:  
    - `general_local_start_address` to specify an IPv4 address and `general_local_subnet_mask` to specify a subnet mask.  
    - `general_local_start_address_ipv6` to specify an IPv6 address and `general_local_ipv6_prefix_length` to specify a prefix length. |
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>general_local_start_address</code></td>
<td><code>ipaddress</code></td>
<td>If the <code>general_local_network_type</code> keyword is set to <code>SINGLE</code>, <code>RANGE</code>, or <code>SUBNET</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv4</code>, specifies the local IPv4 (start) address.</td>
</tr>
<tr>
<td><code>general_local_end_address</code></td>
<td><code>ipaddress</code></td>
<td>If the <code>general_local_network_type</code> keyword is set to <code>RANGE</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv4</code>, specifies the local IPv4 end address.</td>
</tr>
<tr>
<td><code>general_local_subnet_mask</code></td>
<td><code>subnet mask</code></td>
<td>If the <code>general_local_network_type</code> keyword is set to <code>SUBNET</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv4</code>, specifies the subnet mask.</td>
</tr>
<tr>
<td><code>general_local_start_address_ipv6</code></td>
<td><code>ipv6-address</code></td>
<td>If the <code>general_local_network_type</code> keyword is set to <code>SINGLE</code>, <code>RANGE</code>, or <code>SUBNET</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv6</code>, specifies the local IPv6 (start) address.</td>
</tr>
<tr>
<td><code>general_local_end_address_ipv6</code></td>
<td><code>ipv6-address</code></td>
<td>If the <code>general_local_network_type</code> keyword is set to <code>RANGE</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv6</code>, specifies the local IPv6 end address.</td>
</tr>
<tr>
<td><code>general_local_ipv6_prefix_length</code></td>
<td><code>prefix length</code></td>
<td>If the <code>general_local_network_type</code> keyword is set to <code>SUBNET</code>, and if the <code>general_ip_version</code> keyword is set to <code>IPv6</code>, specifies the prefix length.</td>
</tr>
</tbody>
</table>
### Traffic selector settings—Remote address information

<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| general_remote_network_type                   | ANY, SINGLE, RANGE, or SUBNET                    | Specifies the address or addresses that are part of the VPN tunnel on the remote end:  
  - **ANY.** All computers and devices on the network.  
  - **SINGLE.** A single IP address on the network. Depending on the setting of the `general_ip_version` keyword, issue one of the following sets of keywords:  
    - `general_remote_start_address` to specify an IPv4 address.  
    - `general_remote_start_address_ipv6` to specify an IPv6 address.  
  - **RANGE.** A range of IP addresses on the network. Depending on the setting of the `general_ip_version` keyword, issue one of the following sets of keywords:  
    - `general_remote_start_address` and `general_remote_end_address` to specify IPv4 addresses.  
    - `general_remote_start_address_ipv6` and `general_remote_end_address_ipv6` to specify IPv6 addresses.  
  - **SUBNET.** A subnet on the network. Depending on the setting of the `general_ip_version` keyword, issue one of the following sets of keywords:  
    - `general_remote_start_address` to specify an IPv4 address and `general_remote_subnet_mask` to specify a subnet mask.  
    - `general_remote_start_address_ipv6` to specify an IPv6 address and `general_remote_ipv6_prefix_length` to specify a prefix length. |
<p>| general_remote_start_address                  | ipaddress                                       | If the <code>general_remote_network_type</code> keyword is set to SINGLE, RANGE, or SUBNET, and if the <code>general_ip_version</code> keyword is set to IPv4, specifies the remote IPv4 (start) address. |
| general_remote_end_address                    | ipaddress                                       | If the <code>general_remote_network_type</code> keyword is set to RANGE, and if the <code>general_ip_version</code> keyword is set to IPv4, specifies the remote IPv4 end address. |</p>
<table>
<thead>
<tr>
<th>Keyword (might consist of two separate words)</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>general_remote_subnet_mask</td>
<td>subnet mask</td>
<td>If the <code>general_remote_network_type</code> keyword is set to SUBNET, and if the <code>general_ip_version</code> keyword is set to IPv4, specifies the subnet mask.</td>
</tr>
<tr>
<td>general_remote_start_address_ipv6</td>
<td>ipv6-address</td>
<td>If the <code>general_remote_network_type</code> keyword is set to SINGLE, RANGE, or SUBNET, and if the <code>general_ip_version</code> keyword is set to IPv6, specifies the remote IPv6 (start) address.</td>
</tr>
<tr>
<td>general_remote_end_address_ipv6</td>
<td>ipv6-address</td>
<td>If the <code>general_remote_network_type</code> keyword is set to RANGE, and if the <code>general_ip_version</code> keyword is set to IPv6, specifies the remote IPv6 end address.</td>
</tr>
<tr>
<td>general_remote_ipv6_prefix_length</td>
<td>prefix length</td>
<td>If the <code>general_remote_network_type</code> keyword is set to SUBNET, and if the <code>general_ip_version</code> keyword is set to IPv6, specifies the prefix length.</td>
</tr>
</tbody>
</table>

**Manual policy settings—Inbound policy**

<table>
<thead>
<tr>
<th>manual_spi_in</th>
<th>number</th>
<th>The Security Parameter Index (SPI) for the inbound policy as a hexadecimal value between 3 and 8 characters.</th>
</tr>
</thead>
</table>
| manual_encryption_algorithm | None, DES, 3DES, AES-128, AES-192, AES-256 | Specifies the encryption algorithm, if any, to negotiate the security association (SA):  
  • None.  
  • DES. Data Encryption Standard (DES).  
  • 3DES. Triple DES.  
  • AES-128. Advanced Encryption Standard (AES) with a 128-bit key size.  
  • AES-192. AES with a 192-bit key size.  
  • AES-256. AES with a 256-bit key size. |
| manual_encryption_key_in                 | key | The encryption key for the inbound policy. The length of the key depends on setting of the `manual_encryption_algorithm` keyword. |
| manual_encryption_key_out                | key | The encryption key for the outbound policy. The length of the key depends on setting of the `manual_encryption_algorithm` keyword. |
### Manual policy settings—Outbound policy

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>manual_spi_out</td>
<td>number</td>
<td>The Security Parameters Index (SPI) for the outbound policy as a hexadecimal value between 3 and 8 characters.</td>
</tr>
</tbody>
</table>
| manual_authentication_algorithm  | MD5 or SHA-1                                       | Specifies the authentication algorithm for the security association (SA):  
  • SHA-1. Hash algorithm that produces a 160-bit digest.  
  • MD5. Hash algorithm that produces a 128-bit digest. |
| manual_authentication_key_in     | key                                               | The encryption key for the inbound policy. The length of the key depends on setting of the manual_authentication_algorithm keyword. |
| manual_authentication_key_out    | key                                               | The encryption key for the outbound policy. The length of the key depends on setting of the manual_authentication_algorithm keyword. |

### Auto policy settings

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_sa_lifetime Kbytes</td>
<td>number</td>
<td>The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. Either issue the auto_sa_lifetime Kbytes keywords and specify the number of bytes, or issue the auto_sa_lifetime seconds keywords and specify the period in seconds.</td>
</tr>
<tr>
<td>auto_sa_lifetime seconds</td>
<td>seconds</td>
<td></td>
</tr>
</tbody>
</table>
| auto_encryption_algorithm        | None, DES, 3DES, AES-128, AES-192, AES-256        | Specifies the encryption algorithm, if any, to negotiate the security association (SA):  
  • None.  
  • DES. Data Encryption Standard (DES).  
  • 3DES. Triple DES.  
  • AES-128. Advanced Encryption Standard (AES) with a 128-bit key size.  
  • AES-192. AES with a 192-bit key size.  
  • AES-256. AES with a 256-bit key size. |
### VPN Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

#### Command example:

```
SRX5308> vpn ipsec vpnpolicy configure SRX-to-Paris
vpn-config[vpn-policy]> general_policy_type Auto-Policy
vpn-config[vpn-policy]> general_ip_version IPv4
vpn-config[vpn-policy]> general_select_local_gateway WAN1
vpn-config[vpn-policy]> general_enable_rollover Y
vpn-config[vpn-policy]> general_rollover_gateway WAN2
vpn-config[vpn-policy]> general_remote_end_point_type IP-Address
vpn-config[vpn-policy]> general_remote_end_point_ip_address 10.112.71.154
vpn-config[vpn-policy]> general_local_network_type SUBNET
vpn-config[vpn-policy]> general_local_start_address 192.168.1.0
vpn-config[vpn-policy]> general_local_subnet_mask 255.255.255.0
vpn-config[vpn-policy]> general_remote_network_type SUBNET
vpn-config[vpn-policy]> general_remote_start_address 192.168.50.0
vpn-config[vpn-policy]> general_remote_subnet_mask 255.255.255.255
vpn-config[vpn-policy]> auto_sa_lifetime seconds 3600
vpn-config[vpn-policy]> auto_encryption_algorithm 3DES
vpn-config[vpn-policy]> auto_authentication_algorithm SHA-1
vpn-config[vpn-policy]> auto_select_ike_policy SRX-to-Paris
vpn-config[vpn-policy]> save
```

**Related show command:** `show vpn ipsec vpnpolicy setup` and `show vpn ipsec vpnpolicy status`
**vpn ipsec vpnpolicy delete <vpn policy name>**
This command deletes a VPN policy by specifying the name of the VPN policy.

**Format**

```
vpn ipsec vpnpolicy delete <vpn policy name>
```

**Mode**

vpn

**Related show command:** *show vpn ipsec vpnpolicy setup*

---

**vpn ipsec vpnpolicy disable <vpn policy name>**
This command disables a VPN connection by specifying the name of the VPN policy.

**Format**

```
vpn ipsec vpnpolicy disable <vpn policy name>
```

**Mode**

vpn

**Related show command:** *show vpn ipsec vpnpolicy setup*

---

**vpn ipsec vpnpolicy enable <vpn policy name>**
This command enables a VPN connection by specifying the name of the VPN policy.

**Format**

```
vpn ipsec vpnpolicy enable <vpn policy name>
```

**Mode**

vpn

**Related show command:** *show vpn ipsec vpnpolicy setup*

---

**vpn ipsec vpnpolicy connect <vpn policy name>**
This command establishes a VPN connection by specifying the name of the VPN policy.

**Format**

```
vpn ipsec vpnpolicy connect <vpn policy name>
```

**Mode**

vpn

**Related show command:** *show vpn ipsec vpnpolicy setup* and *show vpn ipsec vpnpolicy status*
**VPN Mode Configuration Commands**

```plaintext
vpn ipsec vpnpolicy drop <vpn policy name>
```

This command terminates an active VPN connection by specifying the name of the VPN policy.

**Format**

<table>
<thead>
<tr>
<th>Format</th>
<th>vpn ipsec vpnpolicy drop &lt;vpn policy name&gt;</th>
</tr>
</thead>
</table>

**Mode**

<table>
<thead>
<tr>
<th>Mode</th>
<th>vpn</th>
</tr>
</thead>
</table>

**Related show command:** *show vpn ipsec vpnpolicy setup* and *show vpn ipsec vpnpolicy status*

---

**IPSec VPN Mode Config Commands**

```plaintext
vpn ipsec mode_config configure <record name>
```

This command configures a Mode Config record. After you have issued the `vpn ipsec mode_config configure` command to specify a record name, you enter the `vpn-config [modeConfig]` mode, and then you can configure one keyword and associated parameter or associated keyword or associated keyword at a time in the order that you prefer.

**Step 1**

<table>
<thead>
<tr>
<th>Format</th>
<th>vpn ipsec mode_config configure &lt;record name&gt;</th>
</tr>
</thead>
</table>

**Mode**

<table>
<thead>
<tr>
<th>Mode</th>
<th>vpn</th>
</tr>
</thead>
</table>

**Step 2**

<table>
<thead>
<tr>
<th>Format</th>
<th>first_pool_start_ip &lt;ipaddress&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>first_pool_end_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>second_pool_start_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>second_pool_end_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>third_pool_start_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>third_pool_end_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>wins_server_primary_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>wins_server_secondary_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>dns_server_primary_ip &lt;ipaddress&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>dns_server_secondary_ip &lt;ipaddress&gt;</td>
</tr>
</tbody>
</table>
pfs_key_group {N | Y {dh_group {Group1_768_bit | Group2_1024_bit | Group5_1536_bit}}} 

sa_lifetime_type {Seconds {sa_lifetime <seconds>} | KBytes {sa_lifetime <KBytes>}} 

encryption_algorithm {None | DES | 3DES | AES-128 | AES-192 | AES-256} 

integrity_algorithm {MD5 | SHA-1} 

local_ip <ipaddress> 

local_subnet_mask <subnet mask> 

Mode  

vpn-config [modeConfig] 

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client pool</td>
<td></td>
<td></td>
</tr>
<tr>
<td>first_pool_start_ip</td>
<td>ipaddress</td>
<td>The start IP address for the first Mode Config pool.</td>
</tr>
<tr>
<td>first_pool_end_ip</td>
<td>ipaddress</td>
<td>The end IP address for the first Mode Config pool.</td>
</tr>
<tr>
<td>second_pool_start_ip</td>
<td>ipaddress</td>
<td>The start IP address for the second Mode Config pool.</td>
</tr>
<tr>
<td>second_pool_end_ip</td>
<td>ipaddress</td>
<td>The end IP address for the second Mode Config pool.</td>
</tr>
<tr>
<td>third_pool_start_ip</td>
<td>ipaddress</td>
<td>The start IP address for the third Mode Config pool.</td>
</tr>
<tr>
<td>third_pool_end_ip</td>
<td>ipaddress</td>
<td>The end IP address for the third Mode Config pool.</td>
</tr>
<tr>
<td>wins_server_primary_ip</td>
<td>ipaddress</td>
<td>The IP address of the first WINS server.</td>
</tr>
<tr>
<td>wins_server_secondary_ip</td>
<td>ipaddress</td>
<td>The IP address of the second WINS server.</td>
</tr>
<tr>
<td>dns_server_primary_ip</td>
<td>ipaddress</td>
<td>The IP address of the first DNS server that is used by remote VPN clients.</td>
</tr>
<tr>
<td>dns_server_secondary_ip</td>
<td>ipaddress</td>
<td>The IP address of the second DNS server that is used by remote VPN clients.</td>
</tr>
<tr>
<td>Traffic tunnel security level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pfs_key_group</td>
<td>Y or N</td>
<td>Enables or disables Perfect Forward Secrecy (PFS). If you enable PFS, you need to issue the dh_group keyword to specify a group.</td>
</tr>
<tr>
<td>dh_group</td>
<td>Group1_768_bit, Group2_1024_bit, or Group5_1536_bit</td>
<td>Specifies the Diffie-Hellman (DH) group, which sets the strength of the algorithm in bits. The higher the group, the more secure the exchange.</td>
</tr>
</tbody>
</table>
## VPN Mode Configuration Commands

### Command example:

```plaintext
SRX5308> vpn ipsec mode_config configure EMEA Sales
vpn-config[modeConfig]> first_pool_start_ip 172.16.100.1
vpn-config[modeConfig]> first_pool_end_ip 172.16.100.99
vpn-config[modeConfig]> second_pool_start_ip 172.16.200.1
vpn-config[modeConfig]> second_pool_end_ip 172.16.200.99
vpn-config[modeConfig]> dns_server_primary_ip 192.168.1.1
vpn-config[modeConfig]> pfs_key_group Y
vpn-config[modeConfig]> dh_group Group2_1024_bit
vpn-config[modeConfig]> sa_lifetime_type Seconds
vpn-config[modeConfig]> sa_lifetime 3600
vpn-config[modeConfig]> encryption_algorithm 3DES
vpn-config[modeConfig]> integrity_algorithm SHA-1
vpn-config[modeConfig]> local_ip 192.168.1.0
vpn-config[modeConfig]> local_subnet_mask 255.255.255.0
vpn-config[modeConfig]> save
```
Related show command: `show vpn ipsec mode_config setup`

**vpn ipsec mode_config delete <record name>**

This command deletes a Mode Config record by specifying its record name.

**Format**

```
vpn ipsec mode_config delete <record name>
```

**Mode**

vpn

Related show command: `show vpn ipsec mode_config setup`

---

**SSL VPN Portal Layout Commands**

**vpn sslvpn portal_layouts add**

This command configures a new SSL VPN portal layout. After you have issued the `vpn sslvpn portal_layouts add` command, you enter the `vpn-config [portal-settings]` mode, and then you can configure one keyword and associated parameter or associated keyword or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
vpn sslvpn portal_layouts add
```

**Mode**

vpn

**Step 2 Format**

```
portal_name <portal name>
portal_title <portal title>
banner_title <banner title>
banner_message <message text>
display_banner {Y | N}
enable_httpmetatags {Y | N}
enableactivex_web_cache_cleaner {Y | N}
enable_vpntunnel {Y | N}
enable_portforwarding {Y | N}
```

**Mode**

`vpn-config [portal-settings]`

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portal_name</td>
<td>portal name</td>
<td>The portal name (alphanumeric string).</td>
</tr>
<tr>
<td>portal_title</td>
<td>portal title</td>
<td>The portal title (alphanumeric string). Place text that consists of more than one word between quotes.</td>
</tr>
</tbody>
</table>
### Command example:

```plaintext
SRX5308> vpn sslvpn portal_layouts add
vpn-config[portal-settings]> portal_name CSup
vpn-config[portal-settings]> banner_title "Welcome to Customer Support"
vpn-config[portal-settings]> banner_message "In case of login difficulty, call 123-456-7890."
vpn-config[portal-settings]> display_banner Y
vpn-config[portal-settings]> enable_httpmetatags Y
vpn-config[portal-settings]> enable_activex_web_cache_cleaner Y
vpn-config[portal-settings]> enable_vpntunnel Y
vpn-config[portal-settings]> save
```

Related show command: `show vpn sslvpn portal_layouts`

---

### vpn sslvpn portal_layouts edit <row id>

This command configures an existing SSL VPN portal layout. After you have issued the `vpn sslvpn portal_layouts edit` command to specify the row to be edited, you enter the vpn-config [portal-settings] mode, and then you can configure one keyword and associated parameter or associated keyword or associated keyword at a time in the order that you prefer. You cannot change the name of the portal layout.
**Step 1 Format**  
```
vpn sslvpn portal_layouts edit <row id>
```

**Mode**  
```
vpn
```

**Step 2 Format**  
```
portal_title <portal title>
banner_title <banner title>
banner_message <message text>
display_banner {Y | N}
enable_httpmetatags {Y | N}
enable_ACTIVEX_web_cache_cleaner {Y | N}
enable_vpntunnel {Y | N}
enable_portforwarding {Y | N}
```

**Mode**  
```
vpn-config [portal-settings]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portal_title</td>
<td>portal title</td>
<td>The portal title (alphanumeric string). Place text that consists of more than one word between quotes.</td>
</tr>
<tr>
<td>banner_title</td>
<td>banner name</td>
<td>The banner title (alphanumeric string). Place text that consists of more than one word between quotes.</td>
</tr>
<tr>
<td>banner_message</td>
<td>message text</td>
<td>The banner message (alphanumeric string). Place text that consists of more than one word between quotes.</td>
</tr>
<tr>
<td>display_banner</td>
<td>Y or N</td>
<td>Enables or disables display of the banner message.</td>
</tr>
<tr>
<td>enable_httpmetatags</td>
<td>Y or N</td>
<td>Enables or disables HTTP meta tags.</td>
</tr>
<tr>
<td>enable_ACTIVEX_web_cache_cleaner</td>
<td>Y or N</td>
<td>Enables or disables the ActiveX web cache cleaner.</td>
</tr>
<tr>
<td>enable_vpntunnel</td>
<td>Y or N</td>
<td>Enables or disables the VPN tunnel.</td>
</tr>
<tr>
<td>enable_portforwarding</td>
<td>Y or N</td>
<td>Enables or disables port forwarding.</td>
</tr>
</tbody>
</table>

**Related show command:**  
```
show vpn sslvpn portal_layouts
```
**VPN Mode Configuration Commands**

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

**VPN SSLVPN Configuration Commands**

**vpn sslvpn portal_layouts delete <row id>**
This command deletes an SSL VPN portal layout by specifying its row ID.

**Format**
```
vpn sslvpn portal_layouts delete <row id>
```

**Mode**
```
vpn
```

**Related show command:** `show vpn sslvpn portal_layouts`

---

**vpn sslvpn portal_layouts set-default <row id>**
This command configures an SSL VPN portal as the default portal by specifying its row ID.

**Format**
```
vpn sslvpn portal_layouts set-default <row id>
```

**Mode**
```
vpn
```

**Related show command:** `show vpn sslvpn portal_layouts`

---

**SSL VPN Authentication Domain Commands**

**vpn sslvpn users domains add**
This command configures a new authentication domain that is not limited to SSL VPN users.

After you have issued the `vpn sslvpn users domains add` command, you enter the `vpn-config [user-domains]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

**Format**
```
vpn sslvpn users domains add
```

**Mode**
```
vpn
```
**Step 2 Format**

```
domain_name <domain name>
portal <portal name>

authentication_type {LocalUserDatabase | Radius-PAP | Radius-CHAP | Radius-MSCHAP | Radius-MSCHAPv2 | WIKID-PAP | WIKID-CHAP | MIAS-PAP | MIAS-CHAP | NTDomain | ActiveDirectory | LDAP}

authentication_server1 <ipaddress>
authentication_secret <secret>

workgroup <group name>

ldap_base_dn <distinguished name>

active_directory_domain <domain name>
```

**Mode**

`vpn-config [user-domains]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>domain name</td>
<td>The domain name (alphanumeric string).</td>
</tr>
<tr>
<td>portal</td>
<td>portal name</td>
<td>The portal name (alphanumeric string).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> For information about how to configure a portal, see <a href="#">SSL VPN Portal Layout Commands.</a></td>
</tr>
</tbody>
</table>
| authentication_type          | LocalUserDatabase, Radius-PAP, Radius-CHAP, Radius-MSCHAP, Radius-MSCHAPv2, WIKID-PAP, WIKID-CHAP, MIAS-PAP, MIAS-CHAP, NTDomain, ActiveDirectory, or LDAP | Specifies the authentication method that is applied to the domain. Note the following:
|                              |                                                  | • For all selections with the exception of LocalUserDatabase, you need to issue the authentication_server1 keyword and specify an IP address. |
|                              |                                                  | • For all PAP and CHAP selections, you need to issue the authentication_secret keyword and specify a secret. |
|                              |                                                  | • For the NTDomain selection, you need to issue the workgroup keyword and specify the workgroup. |
|                              |                                                  | • For the ActiveDirectory selection, you need to issue the active_directory_domain keyword and specify the Active Directory. |
|                              |                                                  | • For the LDAP selection, you need to issue the ldap_base_dn keyword and specify a DN. |
| authentication_server1       | ipaddress                                        | The IP address of the authentication server.                                |
| authentication_secret        | secret                                           | The authentication secret (alphanumeric string).                            |
| workgroup                    | group name                                       | The NT domain workgroup name (alphanumeric string).                        |
### Command example:

SRX5308\> **vpn sslvpn users domains add**
vpn-config[user-domains]\> **active_directory_domain** Headquarter
vpn-config[user-domains]\> **portal** CSup
vpn-config[user-domains]\> **authentication_type** LDAP
vpn-config[user-domains]\> **authentication_server1** 192.168.24.118
vpn-config[user-domains]\> **ldap_base_dn** dc=netgear,dc=com
vpn-config[user-domains]\> **save**

**Related show command:** `show vpn sslvpn users domains`

---

**vpn sslvpn users domains edit <row id>**

This command configures an existing authentication domain that is not limited to SSL VPN users. After you have issued the `vpn sslvpn users domains edit` command to specify the row to be edited, you enter the vpn-config [user-domains] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the domain and the type of authentication.

**Step 1 Format**

```
vpn sslvpn users domains edit <row id>
```

**Mode**

`vpn`

**Step 2 Format**

```
portal <portal name>
authentication_server1 <ipaddress>
authentication_secret <secret>
workgroup <group name>
ldap_base_dn <distinguished name>
active_directory_domain <domain name>
```

**Mode**

`vpn-config [user-domains]`
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

VPN Mode Configuration Commands

237

VPN Mode Configuration Commands

VPN Mode Configuration Commands

Related show command: show vpn sslvpn users domains

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portal</td>
<td>portal name</td>
<td>The portal name (alphanumeric string).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> For information about how to configure a portal, see SSL VPN Portal Layout Commands.</td>
</tr>
<tr>
<td>authentication_server1</td>
<td>ipaddress</td>
<td>The IP address of the authentication server.</td>
</tr>
<tr>
<td>authentication_secret</td>
<td>secret</td>
<td>The authentication secret (alphanumeric string).</td>
</tr>
<tr>
<td>workgroup</td>
<td>group name</td>
<td>The NT domain workgroup name (alphanumeric string).</td>
</tr>
<tr>
<td>ldap_base_dn</td>
<td>distinguished name</td>
<td>The LDAP base distinguished name (DN; alphanumeric string). Do not include spaces.</td>
</tr>
<tr>
<td>active_directory_domain</td>
<td>domain name</td>
<td>The Active Directory domain name (alphanumeric string).</td>
</tr>
</tbody>
</table>

Related show command: show vpn sslvpn users domains

**vpn sslvpn users domains delete <row id>**

This command deletes an SSL VPN authentication domain by specifying its row ID.

**Format**

vpn sslvpn users domains delete <row id>

**Mode**

vpn

Related show command: show vpn sslvpn users domains

**vpn sslvpn users domains disable_Local_Authentication {Y | N}**

This command enables or disables local authentication of users globally by specifying Y (local authentication is disabled) or N (local authentication is enabled).

**Format**

vpn sslvpn users domains disable_Local_Authentication {Y | N}

**Mode**

vpn

Related show command: show vpn sslvpn users domains
SSL VPN Authentication Group Commands

**vpn sslvpn users groups add**

This command configures a new authentication group that is not limited to SSL VPN users. After you have issued the `vpn sslvpn users groups add` command, you enter the vpn-config [user-groups] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
vpn sslvpn users groups add
```

**Mode**

```
vpn
```

**Step 2 Format**

```
domain_name <domain name>
group_name <group name>
idle_timeout <minutes>
```

**Mode**

```
vpn-config [user-groups]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>domain name</td>
<td>The domain name (alphanumeric string) to which the group belongs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> For information about configuring domains, see SSL VPN Authentication Domain Commands.</td>
</tr>
<tr>
<td>group_name</td>
<td>group name</td>
<td>The group name (alphanumeric string).</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>minutes</td>
<td>The idle time-out in minutes.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn sslvpn users groups add
vpn-config[user-groups]> domain_name Headquarter
vpn-config[user-groups]> group_name Sales
vpn-config[user-groups]> idle_timeout 15
vpn-config[user-groups]> save
```

**Related show command:** `show vpn sslvpn users groups`

---

**vpn sslvpn users groups edit <row id>**

This command configures an existing authentication group that is not limited to SSL VPN users. After you have issued the `vpn sslvpn users groups edit <row id>` command to specify the row to be edited, you enter the vpn-config [user-groups] mode, and then you can change the idle time-out only.
VPN Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**Step 1** Format  
```
vpn sslvpn users groups edit <row_id>
```

Mode  
```
vpn
```

**Step 2** Format  
```
idle_timeout <minutes>
```

Mode  
```
vpn-config [user-groups]
```

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idle_timeout</td>
<td>minutes</td>
<td>The idle time-out in minutes.</td>
</tr>
</tbody>
</table>

Related show command:  
```
show vpn sslvpn users groups
```

---

**vpn sslvpn users groups delete <row_id>**

This command deletes an authentication group by specifying its row ID.

Format  
```
vpn sslvpn users groups delete <row_id>
```

Mode  
```
vpn
```

Related show command:  
```
show vpn sslvpn users groups
```

---

**SSL VPN User Commands**

**vpn sslvpn users users add**

This command configures a new user account. The command is not limited to SSL VPN users. After you have issued the `vpn sslvpn users users add` command, you enter the `vpn-config [users]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format  
```
vpn sslvpn users users add
```

Mode  
```
vpn
```
**Step 2** Format

```
user_name <user name>
user_type {SSLVPNUser | Administrator | Guest | IPSECVPNUser | L2TPUser | PPTPUser}
group <group name>
password <password>
confirm_password <password>
idle_timeout <minutes>
```

**Mode**

```
vpn-config [users]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_name</td>
<td>user name</td>
<td>The user name (alphanumeric string)</td>
</tr>
<tr>
<td>user_type</td>
<td>SSLVPNUser, Administrator, Guest, IPSECVPNUser, L2TPUser, or PPTPUser</td>
<td>Specifies the user type.</td>
</tr>
<tr>
<td>group</td>
<td>group name</td>
<td>The group name (alphanumeric string) to which the user belongs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: For information about how to configure groups, see SSL VPN Authentication Group Commands.</td>
</tr>
<tr>
<td>password</td>
<td>password</td>
<td>The password (alphanumeric string) that is assigned to the user. You need to issue the confirm_password keyword and confirm the password.</td>
</tr>
<tr>
<td>confirm_password</td>
<td>password</td>
<td>The confirmation of the password.</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>minutes</td>
<td>The idle time-out in minutes.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn sslvpn users users add
vpn-config[users]> user_name PeterBrown
vpn-config[users]> user_type SSLVPNUser
vpn-config[users]> group Sales
vpn-config[users]> password 3goTY5!Of6hh
vpn-config[users]> confirm_password 3goTY5!Of6hh
vpn-config[users]> idle_timeout 10
vpn-config[users]> save
```

**Related show command:** `show vpn sslvpn users users`
VPN Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**vpn sslvpn users users edit <row id>**

This command configures an existing user account. The command is not limited to SSL VPN users. After you have issued the `vpn sslvpn users users edit` command to specify the row to be edited, you enter the vpn-config [users] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the user or the group to which the user is assigned. The changes you can make to the user type are restricted.

**Step 1 Format**
```
vpn sslvpn users users edit <row id>
```

**Mode** vpn

**Step 2 Format**
```
user_type {SSLVPNUser | Administrator | Guest | IPSECVPNUser | L2TPUser | PPTPUser}
password <password>
confirm_password <password>
idle_timeout <minutes>
```

**Mode** vpn-config [users]

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_type</td>
<td>SSLVPNUser, Administrator, Guest, IPSECVPNUser, L2TPUser, or PPTPUser</td>
<td>Specifies the user type. <strong>Note:</strong> You cannot change an existing user from the L2TPUser or PPTPUser user type to another type or from another type to the L2TPUser or PPTPUser type.</td>
</tr>
<tr>
<td>password</td>
<td>password</td>
<td>The password (alphanumeric string) that is assigned to the user. You need to issue the confirm_password keyword and confirm the password.</td>
</tr>
<tr>
<td>confirm_password</td>
<td>password</td>
<td>The confirmation of the password.</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>minutes</td>
<td>The idle time-out in minutes.</td>
</tr>
</tbody>
</table>

**Related show command:** `show vpn sslvpn users users`

---

**vpn sslvpn users users delete <row id>**

This command deletes a user account by specifying its row ID.

**Format**
```
vpn sslvpn users users delete <row id>
```

**Mode** vpn
Related show command: `show vpn sslvpn users users`

---

**vpn sslvpn users users login_policies <row id>**

This command configures the login policy for a user. The command is not limited to SSL VPN users. After you have issued the `vpn sslvpn users users login_policies` command to specify the row ID that represents the user, you enter the `vpn-config [user-login-policy]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1** Format

```
vpn sslvpn users users login_policies <row id>
```

**Mode**

`vpn`

**Step 2** Format

```
deny_login_from_wan_interface {Y | N}
disable_login {Y | N}
```

**Mode**

`vpn-config [user-login-policy]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>AssociatedKeyword to Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny_login_from_wan_interface</td>
<td>Y or N</td>
<td>Enables or disables login from the WAN interface.</td>
</tr>
<tr>
<td>disable_login</td>
<td>Y or N</td>
<td>Enables or disables login from any interface.</td>
</tr>
</tbody>
</table>

Command example:

```
SRX5308> vpn sslvpn users users login_policies 4
vpn-config[user-login-policy]> deny_login_from_wan_interface N
vpn-config[user-login-policy]> disable_login N
vpn-config[user-login-policy]> save
```

Related show command: `show vpn sslvpn users users and show vpn sslvpn users login_policies <row id>`

---

**vpn sslvpn users users ip_policies configure <row id>**

This command configures source IP addresses from which a user is either allowed or denied access. The command is not limited to SSL VPN users. After you have issued the `vpn sslvpn users users ip_policies configure` command to specify the row ID that represents the user, you enter the `vpn-config [user-ip-policy]` mode, and then you can
configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
vpn sslvpn users users ip_policies configure <row id>
```

**Mode**

```
vpn
```

**Step 2 Format**

```
allow_login_from_defined_addresses {Y | N}
ip_version {IPv4 | IPv6}
```

```
source_address_type {IPAddress {{source_address <ipaddress>} | {source_address6 <ipv6-address>}} | IPNetwork
{{source_address <ipaddress>} {mask_length <mask length>} | {source_address6 <ipv6-address>} \{prefix_length <prefix_length>\}}
```

**Mode**

```
vpn-config [user-ip-policy]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow_login_from_defined_addresses</td>
<td>Y or N</td>
<td>Allows or denies login from a single-source IP address or network IP addresses.</td>
</tr>
<tr>
<td>ip_version</td>
<td>IPv4 or IPv6</td>
<td>Specifies the IP version of the source IP address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv4. The IP address or network address is defined by an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You need to issue the source_address keyword and specify an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For a network address, you also need to issue the mask_length keyword and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specify a subnet mask length.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6. The IP address or network address is defined by an IPv6 address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You need to issue the source_address6 keyword and specify an IPv6 address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For a network address, you also need to issue the prefix_length keyword and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specify a prefix length.</td>
</tr>
</tbody>
</table>
Keyword | Associated Keyword to Select or Parameter to Type | Description
--- | --- | ---
source_address_type | IPAddress or IPNetwork | Specifies the source address type:
- IPAddress. A single IP address. The setting of the ip_version keyword determines whether you need to issue the source_address keyword and specify an IPv4 address or issue the source_address6 keyword and specify an IPv6 address.
- IPNetwork. A subnet of IP addresses. The setting of the ip_version keyword determines whether you need to issue the mask_length keyword and specify an IPv4 subnet mask or issue the prefix_length keyword and specify an IPv6 prefix length.
source_address | ipaddress | The IPv4 IP address or network address if the ip_version keyword is set to IPv4.
mask_length | mask length | If the source_address_type keyword is set to IPNetwork and the ip_version keyword is set to IPv4, the mask length of the IPv4 network.
source_address6 | ipv6-address | The IPv6 IP address or network address if the ip_version keyword is set to IPv6.
prefix_length | prefix length | If the source_address_type keyword is set to IPNetwork and the ip_version keyword is set to IPv6, the prefix length of the IPv6 network.

Command example:

SRX5308> vpn sslvpn users users ip_policies configure 4
vpn-config[user-ip-policy]> allow_login_from_defined_addresses Y
vpn-config[user-ip-policy]> ip_version IPv4
vpn-config[user-ip-policy]> source_address_type IPAddress
vpn-config[user-ip-policy]> source_address 10.156.127.39
vpn-config[user-ip-policy]> save

Related show command: show vpn sslvpn users users and show vpn sslvpn users ip_policies <row id>
VPN Mode Configuration Commands

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

### vpn sslvpn users users ip_policies delete <row id>

This command deletes a source IP address for a user by specifying the row ID of the table.

**Format**

```
vpn sslvpn users users ip_policies delete <row id>
```

**Mode**

`vpn`

**Related show command:** show vpn sslvpn users users and show vpn sslvpn users ip_policies <row id>

---

### vpn sslvpn users users browser_policies <row id>

This command configures a client browser from which a user is either allowed or denied access. The command is not limited to SSL VPN users. After you have issued the `vpn sslvpn users users browser_policies` command to specify the row ID that represents the user, you enter the `vpn-config [user-browser-policy]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
vpn sslvpn users users browser_policies <row id>
```

**Mode**

`vpn`

**Step 2 Format**

```
add_browser {InternetExplorer | NetscapeNavigator | Opera | Firefox | Mozilla}
delete_browser {InternetExplorer | NetscapeNavigator | Opera | Firefox | Mozilla}
enable_or_disable_login_from_defined_browsers {Y | N}
```

**Mode**

`vpn-config [user-browser-policy]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add_browser</td>
<td>InternetExplorer, NetscapeNavigator, Opera, Firefox, or Mozilla</td>
<td>Adds a browser to the browser list. By default, there are no browsers on the browser list.</td>
</tr>
<tr>
<td>delete_browser</td>
<td>InternetExplorer, NetscapeNavigator, Opera, Firefox, or Mozilla</td>
<td>Removes a browser from the browser list (after you first have added the browser to the browser list).</td>
</tr>
</tbody>
</table>
### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

#### VPN Mode Configuration Commands

**VPN Mode Configuration Commands**

**Command example:**

```plaintext
SRX5308> vpn sslvpn users users browser_policies 4
vpn-config[user-browser-policy]> add_browser NetscapeNavigator
vpn-config[user-browser-policy]> enable_or_disable_login_from_defined_browsers N
vpn-config[user-browser-policy]> save
vpn-config[user-browser-policy]> add_browser InternetExplorer
vpn-config[user-browser-policy]> enable_or_disable_login_from_defined_browsers N
vpn-config[user-browser-policy]> save
```

**Related show command:** 

- `show vpn sslvpn users users` and `show vpn sslvpn users browser_policies`  
  `<row id>`

---

### SSL VPN Port Forwarding Commands

**vpn sslvpn portforwarding appconfig add**

This command configures a new SSL port forwarding application. After you have issued the `vpn sslvpn portforwarding appconfig add` command, you enter the `vpn-config [portforwarding-settings]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

**Format**

```plaintext
vpn sslvpn portforwarding appconfig add
```

**Mode**

```plaintext
vpn
```

**Step 2**

**Format**

```plaintext
server_ip <ipaddress>
port <number>
```

**Mode**

```plaintext
vpn-config [portforwarding-settings]
```
VPN Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_ip</td>
<td>ipaddress</td>
<td>The IP address of the local server that hosts the application.</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>The TCP port number of the local server that hosts the application.</td>
</tr>
</tbody>
</table>

Command example:

SRX5308> vpn sslvpn portforwarding appconfig add
vpn-config[portforwarding-settings]> server_ip 192.168.51.227
vpn-config[portforwarding-settings]> port 3389
vpn-config[portforwarding-settings]> save

Related show command: show vpn sslvpn portforwarding appconfig

---

vpn sslvpn portforwarding appconfig delete <row id>

This command deletes an SSL port forwarding application by specifying its row ID.

Format        vpn sslvpn portforwarding appconfig delete <row id>
Mode          vpn

Related show command: show vpn sslvpn portforwarding appconfig

---

vpn sslvpn portforwarding hostconfig add

This command configures a new host name for an SSL port forwarding application. After you have issued the vpn sslvpn portforwarding hostconfig add command, you enter the vpn-config [portforwarding-host-settings] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 Format    vpn sslvpn portforwarding hostconfig add
Mode            vpn

Step 2 Format    server_ip <ipaddress>
                 domain_name <domain name>
Mode            vpn-config [portforwarding-host-settings]
**VPN Mode Configuration Commands**

---

**ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308**

---

**Command example:**

SRX5308> **vpn sslvpn portforwarding hostconfig add**
vpn-config[portforwarding-host-settings]> **server_ip 192.168.51.227**
vpn-config[portforwarding-host-settings]> **domain_name RemoteDesktop**
vpn-config[portforwarding-host-settings]> **save**

**Related show command:** `show vpn sslvpn portforwarding hostconfig`

---

**SSL VPN Client and Client Route Commands**

**vpn sslvpn client ipv4**

This command configures the SSL client IP address range. After you have issued the `vpn sslvpn client ipv4` command, you enter the vpn-config [sslvpn-client-ipv4-settings] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

Format: `vpn sslvpn client ipv4`

Mode: `vpn`

---

**VPN Mode Configuration Commands**

248
### Step 2 Format

**enable_full_tunnel** `{Y | N}`

dns_suffix `<suffix>`

**primary_dns** `<ipaddress>`

**secondary_dns** `<ipaddress>`

**begin_client_address** `<ipaddress>`

**end_client_address** `<ipaddress>`

Mode `vpn-config [sslvpn-client-ipv4-settings]`

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| enable_full_tunnel    | Y or N                                           | Enables or disables full-tunnel support:  
• **Yes**. Enables full-tunnel support.  
• **No**. Disables full-tunnel support and enables split-tunnel support. If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you need to add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel (see the `vpn sslvpn route add` command). |
| dns_suffix            | suffix                                           | The DNS suffix to be appended to incomplete DNS search strings. This setting is optional.                                                                                                                   |
| primary_dns           | ipaddress                                        | The IP address of the primary DNS server. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel has been established. |
| secondary_dns         | ipaddress                                        | The IP address of the secondary DNS server. This setting is optional.                                                                                                                                       |
| begin_client_address  | ipaddress                                        | The start IP address of the IPv4 client range. The default address is 192.168.251.1.                                                                                                                      |
| end_client_address    | ipaddress                                        | The end IP address of the IPv4 client range. The default address is 192.168.251.254.                                                                                                                       |

**Command example:**

```
SRX5308> vpn sslvpn client ipv4
vpn-config[sslvpn-client-ipv4-settings]> enable_full_tunnel Y
vpn-config[sslvpn-client-ipv4-settings]> primary_dns 192.168.10.5
vpn-config[sslvpn-client-ipv4-settings]> secondary_dns 192.168.10.6
vpn-config[sslvpn-client-ipv4-settings]> begin_client_address 192.168.251.1
vpn-config[sslvpn-client-ipv4-settings]> end_client_address 192.168.251.254
vpn-config[sslvpn-client-ipv4-settings]> save
```

**Related show command:** `show vpn sslvpn client`
vpn sslvpn client ipv6

This command configures the SSL client IP address range. After you have issued the `vpn sslvpn client ipv6` command, you enter the vpn-config [sslvpn-client-ipv6-settings] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**
Format: `vpn sslvpn client ipv6`
Mode: `vpn`

**Step 2**
Format: `enable_full_tunnel {Y | N}`

- `begin_client_address <ipv6-address>`
- `end_client_address <ipv6-address>`

Mode: `vpn-config [sslvpn-client-ipv6-settings]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable_full_tunnel</code></td>
<td>Y or N</td>
<td>Enables or disables full-tunnel support:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Yes. Enables full-tunnel support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No. Disables full-tunnel support and enables split-tunnel support. If you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enable split-tunnel support and you assign an entirely different subnet to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the VPN tunnel clients from the subnet that is used by the local network,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>you need to add a client route to ensure that a VPN tunnel client connects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to the local network over the VPN tunnel (see the <code>vpn sslvpn route add</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>command).</td>
</tr>
<tr>
<td><code>begin_client_address</code></td>
<td><code>ipv6-address</code></td>
<td>The start IP address of the IPv6 client range. The default address is 4000::1.</td>
</tr>
<tr>
<td><code>end_client_address</code></td>
<td><code>ipv6-address</code></td>
<td>The end IP address of the IPv6 client range. The default address is 4000::200.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn sslvpn client ipv6
vpn-config[sslvpn-client-ipv6-settings]> enable_full_tunnel N
vpn-config[sslvpn-client-ipv6-settings]> begin_client_address 4000::1000:2
vpn-config[sslvpn-client-ipv6-settings]> end_client_address 4000::1000:50
vpn-config[sslvpn-client-ipv6-settings]> save
```

Related show command: `show vpn sslvpn client`
**vpn sslvpn route add**

This command configures a static client route to a destination network. After you have issued the `vpn sslvpn route add` command, you enter the vpn-config [sslvpn-route-settings] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

---

**Note:** When full-tunnel support is enabled, client routes are not operable. For clients routes to be operable, split-tunnel support should be enabled.

---

**Step 1**

**Format**

```
vpn sslvpn route add
```

**Mode**

```
vpn
```

**Step 2**

**Format**

```
ip_version {IPv4 {destination_network <ipaddress>} {subnet_mask <subnet mask>} | IPv6 {destination_network6 <ipv6-address>}{prefix_length <prefix length>}}
```

**Mode**

```
vpn-config [sslvpn-route-settings]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_version</td>
<td>IPv4 or IPv6</td>
<td>Specifies the IP version of the destination network for the route:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv4. The network address is an IPv4 address. You need to issue the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination_network and subnet_mask keywords and specify an IPv4 address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and subnet mask.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6. The network address is an IPv6 address. You need to issue the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination_network6 and prefix_length keywords and specify an IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>address and prefix length.</td>
</tr>
<tr>
<td>destination_network</td>
<td>ipaddress</td>
<td>If the ip_version keyword is set to IPv4, the IPv4 address of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination network for the route.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>subnet mask</td>
<td>If the ip_version keyword is set to IPv4, the subnet mask of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination network for the route.</td>
</tr>
<tr>
<td>destination_network6</td>
<td>ipv6-address</td>
<td>If the ip_version keyword is set to IPv6, the IPv6 address of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination network for the route.</td>
</tr>
<tr>
<td>prefix_length</td>
<td>prefix length</td>
<td>If the ip_version keyword is set to IPv6, the prefix length of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination network for the route.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn sslvpn route add
vpn-config[sslvpn-route-settings]> ip_version IPv4
vpn-config[sslvpn-route-settings]> destination_network 192.168.4.20
vpn-config[sslvpn-route-settings]> subnet_mask 255.255.255.254
vpn-config[sslvpn-route-settings]> save
```
Related show command: `show vpn sslvpn route`

---

**vpn sslvpn route delete <row id>**

This command deletes a client route by specifying its row ID.

**Format**

`vpn sslvpn route delete <row id>`

**Mode**

`vpn`

Related show command: `show vpn sslvpn route`

---

**SSL VPN Resource Commands**

**vpn sslvpn resource add**

This command adds a new resource. After you have issued the `vpn sslvpn resource add` command, you enter the `vpn-config [sslvpn-resource-settings]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

**Format**

`vpn sslvpn resource add`

**Mode**

`vpn`

**Step 2**

**Format**

`resource_name <resource name>`

`service_type {VPNTunnel | PortForwarding | All}`

**Mode**

`vpn-config [sslvpn-resource-settings]`

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resource_name</td>
<td><code>resource name</code></td>
<td>The resource name (alphanumeric string).</td>
</tr>
<tr>
<td>service_type</td>
<td>VPNTunnel, PortForwarding, or All</td>
<td>Specifies the type of service to which the resource applies:</td>
</tr>
<tr>
<td></td>
<td>• VPNTunnel. The resource applies only to a VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tunnel.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PortForwarding. The resource applies only to port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>forwarding.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• All. The resource applies both to a VPN tunnel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and to port forwarding.</td>
<td></td>
</tr>
</tbody>
</table>
Command example:

SRX5308> vpn sslvpn resource add
vpn-config[sslvpn-resource-settings]> resource_name TopSecure
vpn-config[sslvpn-resource-settings]> service_type PortForwarding
vpn-config[sslvpn-resource-settings]> save

Related show command: show vpn sslvpn resource

---

**vpn sslvpn resource delete <row id>**

This command deletes a resource by specifying its row ID.

<table>
<thead>
<tr>
<th>Format</th>
<th>vpn sslvpn resource delete &lt;row id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>vpn</td>
</tr>
</tbody>
</table>

Related show command: show vpn sslvpn resource

---

**vpn sslvpn resource configure add <resource name>**

This command configures a resource object. (You first need to add a resource with the **vpn sslvpn resource add** command.) After you have issued the **vpn sslvpn resource configure add** command to specify the resource name, you enter the **vpn-config [sslvpn-resource-settings]** mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**  | Format | vpn sslvpn resource configure add <resource name> |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>vpn</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**  | Format | object_type {IPAddress | IPNetwork} |
|-------------|--------|-----------------|

For a single IP address:

<table>
<thead>
<tr>
<th>ip_version</th>
<th>object_address &lt;ipaddress&gt;</th>
<th>IPv6 (object_address6 &lt;ipv6-address&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_port</td>
<td>&lt;port number&gt;</td>
<td>end_port &lt;port number&gt;</td>
</tr>
</tbody>
</table>
For an IP network:

```
ip_version {IPv4 {object_address <ipaddress>} {mask_length <subnet mask length>} | IPv6 {object_address6 <ipv6-address>} {mask_length <prefix length>}}
start_port <port number>
end_port <port number>
```

## Mode

VPN Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| object_type   | IPAddress or IPNetwork                           | Specifies the source address type for the object:  
  • IPAddress. A single IP address. The setting of the ip_version keyword determines whether you need to issue the object_address keyword and specify an IPv4 address or the object_address6 keyword and specify an IPv6 address.  
  • IPNetwork. A subnet of IP addresses. The setting of the ip_version keyword determines whether you need to issue the object_address and mask_length keywords and specify an IPv4 network address and mask length or issue the object_address6 and mask_length keywords and specify an IPv6 network address and prefix length. |
| ip_version    | IPv4 or IPv6                                      | Specifies the IP version of the IP address or IP network:  
  • IPv4. The IP address or IP network is defined by an IPv4 address. You need to issue the object_address keyword and specify an IPv4 address. For a network address, you also need to issue the mask_length keyword and specify a subnet mask length.  
  • IPv6. The IP address or network address is defined by an IPv6 address. You need to issue the object_address6 keyword and specify an IPv6 address. For a network address, you also need to issue the mask_length keyword and specify a prefix length. |
| object_address| ipaddress                                         | The IPv4 address, if the policy is for an IPv4 address or IPv4 network. |
| object_address6| ipv6-address                                     | The IPv6 address, if the policy is for an IPv6 address or IPv6 network. |
VPN Mode Configuration Commands

**Command example:**

```bash
SRX5308#add TopSecure
vpn-config[sslvpn-resource-settings]> object_type IPNetwork
vpn-config[sslvpn-resource-settings]> ip_version IPv4
vpn-config[sslvpn-resource-settings]> object_address 192.168.30.56
vpn-config[sslvpn-resource-settings]> mask_length 24
vpn-config[sslvpn-resource-settings]> start_port 3391
vpn-config[sslvpn-resource-settings]> end_port 3393
vpn-config[sslvpn-resource-settings]> save
```

**Related show command:** `show vpn sslvpn resource_object <resource name>`

---

### `vpn sslvpn resource configure delete <row id>`

This command deletes a resource object by specifying its row ID. To delete the resource itself, use the `vpn sslvpn resource delete <row id>` command.

**Format**

```
vpn sslvpn resource configure delete <row id>
```

**Mode**

`vpn`

**Related show command:** `show vpn sslvpn resource_object <resource name>`

---

### Table: Keyword, Associated Keyword and Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| `mask_length` | `subnet mask length` or `prefix length`          | The nature of this keyword and parameter depend on the setting of the `ip_version` and `object_type` keywords:
|               |                                                   | • If the `ip_version` keyword is set to IPv4 and the `object_type` keyword is set to `IPNetwork`, the subnet mask length of the IPv4 network.        |
|               |                                                   | • If the `ip_version` keyword is set to IPv6 and the `object_type` keyword is set to `IPNetwork`, the prefix length of the IPv6 network.        |
| `start_port`  | `number`                                         | The start port number for the port range that applies to the object.                                                                                                                                     |
| `end_port`    | `number`                                         | The end port number for the port range that applies to the object.                                                                                                                                         |
SSL VPN Policy Commands

**vpn sslvpn policy add**

This command configures a new SSL VPN policy. After you have issued the `vpn sslvpn policy add` command, you enter the `vpn-config [sslvpn-policy-settings]` mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

```
vpn sslvpn policy add
```

**Mode**

```
vpn
```

**Step 2 Format**

```
policy_name <policy name>
policy_type {Global | Group {policy_owner <group name>} | User {policy_owner <user name>}}
destination_object_type {NetworkResource | IPAddress | IPNetwork | All}
```

In addition to a policy name, policy type, and destination object type, configure the following for a network resource:

```
ip_version {IPv4 | IPv6}
resource_name <resource name>
policy_permission {Permit | Deny}
```

In addition to a policy name, policy type, and destination object type, configure the following for an IP address:

```
ip_version {IPv4 {policy_address <ipaddress>} | IPv6 {policy_address6 <ipv6-address>}}
start_port <port number>
end_port <port number>
service_type {VPNTunnel | PortForwarding | All}
policy_permission {Permit | Deny}
```

In addition to a policy name, policy type, and destination object type, configure the following for an IP network:

```
ip_version {IPv4 {policy_address <ipaddress>} | IPv6 {policy_address6 <ipv6-address>} {policy_mask_length <subnet mask>} | IPv6 {policy_address6 <ipv6-address> {policy_ipv6_prefix_length <prefix length>}}
start_port <port number>
end_port <port number>
service_type {VPNTunnel | PortForwarding | All}
policy_permission {Permit | Deny}
```
In addition to a policy name, policy type, and destination object type, configure the following for all addresses (that is, the destination_object_type keyword is set to All):

- **ip_version**: IPv4 | IPv6
- **start_port**: <port number>
- **end_port**: <port number>
- **service_type**: VPNTunnel | PortForwarding | All
- **policy_permission**: Permit | Deny

**Mode**

```
vpn-config [sslvpn-policy-settings]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy_name</td>
<td>policy name</td>
<td>The policy name (alphanumeric string).</td>
</tr>
<tr>
<td>policy_type</td>
<td>Global, Group, or User</td>
<td>Specifies the SSL VPN policy type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Global</strong>: The policy is global and includes all groups and users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Group</strong>: The policy is limited to a single group. For information about</td>
</tr>
<tr>
<td></td>
<td></td>
<td>how to create groups, see SSL VPN Authentication Group Commands. You need</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to issue the policy_owner keyword and specify the group name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>User</strong>: The policy is limited to a single user. For information about</td>
</tr>
<tr>
<td></td>
<td></td>
<td>how to create user accounts, see SSL VPN User Commands. You need to issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the policy_owner keyword and specify the user name.</td>
</tr>
<tr>
<td>policy_owner</td>
<td>group name or user name</td>
<td>Specifies the owner of the policy. The owner depends on the setting of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policy_type keyword:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Group</strong>: Specify the group name to which the policy applies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>User</strong>: Specify the user name to which the policy applies.</td>
</tr>
</tbody>
</table>
## VPN Mode Configuration Commands

### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| destination_object_type | NetworkResource, IPAddress, IPNetwork, or All    | Specifies the policy destination type, which determines how the policy is applied, and, in turn, which keywords you need to issue to specify the policy:  
  • **NetworkResource.** The policy is applied to an existing IPv4 or IPv6 resource. For information about how to create and configure network resources, see SSL VPN Resource Commands. You need to issue the following keywords and their associated parameters and keywords:
    - policy_name
    - ip_version
    - resource_name
    - policy_permission
    - policy_owner if the policy_type keyword is set to Group or User.  
  • **IPAddress.** The policy is applied to a single IPv4 or IPv6 address. You need to issue the following keywords and their associated parameters and keywords:
    - policy_name
    - ip_version
    - policy_address or policy_address6 (depending on the setting of the ip_version keyword)
    - start_port and end_port
    - service_type
    - policy_permission
    - policy_owner if the policy_type keyword is set to Group or User. |
### VPN Mode Configuration Commands

#### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

**destination_object_type**

*NetworkResource, IPAddress, IPNetwork, or All*

(continued)

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| IPNetwork | - *policy_name*  
- *ip_version*  
- *policy_address* and *policy_mask_length* or *policy_address6* and *policy_ipv6_prefix_length* (depending on the setting of the *ip_version* keyword)  
- *start_port* and *end_port*  
- *service_type*  
- *policy_permission*  
- *policy_owner* if the *policy_type* keyword is set to *Group* or *User*.  | • *IPNetwork*. The policy is applied to an IPv4 or IPv6 network address. You need to issue the following keywords and their associated parameters and keywords: |
| All | - *policy_name*  
- *ip_version*  
- *start_port* and *end_port*  
- *service_type*  
- *policy_permission*  
- *policy_owner* if the *policy_type* keyword is set to *Group* or *User*.  | • *All*. The policy is applied to all addresses. You need to issue the following keywords and their associated parameters and keywords: |

**resource_name**

*resource name*

The name of a resource that you configured with the `vpn sslvpn resource add` command. This keyword and parameter apply only if the policy is for a network resource.

**policy_permission**

*Permit or Deny*

Specifies whether the policy permits or denies access.
### VPN Mode Configuration Commands

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_version</td>
<td>IPv4 or IPv6</td>
<td>Specifies the IP version that applies to the policy:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>IPv4</strong>. The policy is for an IPv4 network resource, IPv4 address, IPv4 network, or for all IPv4 addresses. For an IP address or IP network, you need to issue the <code>policy_address</code> keyword and specify an IPv4 address. For a network address, you also need to issue the <code>policy_mask_length</code> keyword and specify a subnet mask.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>IPv6</strong>. The policy is for an IPv6 network resource, IPv6 address, IPv6 network, or for all IPv6 addresses. For an IP address or IP network, you need to issue the <code>policy_address6</code> keyword and specify an IPv6 address. For a network address, you also need to issue the <code>policy_ipv6_prefix_length</code> keyword and specify a prefix length.</td>
</tr>
<tr>
<td>policy_address</td>
<td>ipaddress</td>
<td>The IPv4 address, if the policy is for an IPv4 address or IPv4 network.</td>
</tr>
<tr>
<td>policy_mask_length</td>
<td>subnet mask</td>
<td>The subnet mask, if the policy is for an IPv4 network.</td>
</tr>
<tr>
<td>policy_address6</td>
<td>ipv6-address</td>
<td>The IPv6 address, if the policy is for an IPv6 address or IPv6 network.</td>
</tr>
<tr>
<td>policy_ipv6_prefix_length</td>
<td>prefix length</td>
<td>The prefix length, if the policy is for an IPv6 network.</td>
</tr>
<tr>
<td>start_port</td>
<td>port number</td>
<td>The start port number for a policy port range. (This does not apply if the policy is for a network resource.)</td>
</tr>
<tr>
<td>end_port</td>
<td>port number</td>
<td>The end port number for a policy port range. (This does not apply if the policy is for a network resource.)</td>
</tr>
<tr>
<td>service_type</td>
<td>VPNTunnel, PortForwarding, or All</td>
<td>Specifies the service type for the policy:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>VPNTunnel</strong>. The policy is applied only to a VPN tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>PortForwarding</strong>. The policy is applied only to port forwarding.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>All</strong>. The policy is applied both to a VPN tunnel and to port forwarding.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn sslvpn policy add
vpn-config[sslvpn-policy-settings]> policy_name RoadWarriorPolicy
```
Related show command: show vpn sslvpn policy

vpn sslvpn policy edit <row id>

This command configures an existing SSL VPN policy. After you have issued the vpn sslvpn policy edit command to specify the row to be edited (for row information, see the output of the show vpn sslvpn policy command), you enter the vpn-config [sslvpn-policy-settings] mode. You can then configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the policy type, policy owner, destination object, IP version, or service type.

Step 1 Format

Mode

Step 2 Format

policy_name <policy name>

In addition to the policy name, you can change the following for a network resource:

resource_name <resource name>
policy_permission {Permit | Deny}

In addition to the policy name, you can change the following for an IP address:

{[policy_address <ipaddress>] | [policy_address6 <ipv6-address>])

start_port <port number>
end_port <port number>
policy_permission {Permit | Deny}
In addition to the policy name, you can change the following for an IP network:

```
{policy_address <ipaddress>} | {policy_mask_length <subnet mask>}
{policy_address6 <ipv6-address>} | {policy_ipv6_prefix_length <prefix_length>}
```

```
start_port <port number>
end_port <port number>
policy_permission [Permit | Deny]
```

In addition to the policy name, you can change the following for all addresses (that is, the destination_object_type keyword is set to All):

```
start_port <port number>
end_port <port number>
policy_permission [Permit | Deny]
```

### Mode

```
vpn-config [sslvpn-policy-settings]
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy_name</td>
<td>policy name</td>
<td>The policy name (alphanumeric string).</td>
</tr>
<tr>
<td>policy_address</td>
<td>ipaddress</td>
<td>The IPv4 address, if the policy is for an IPv4 address or IPv4 network.</td>
</tr>
<tr>
<td>policy_mask_length</td>
<td>subnet mask</td>
<td>The subnet mask, if the policy is for an IPv4 network.</td>
</tr>
<tr>
<td>policy_address6</td>
<td>ipv6-address</td>
<td>The IPv6 address, if the policy is for an IPv6 address or IPv6 network.</td>
</tr>
<tr>
<td>policy_ipv6_prefix_length</td>
<td>prefix length</td>
<td>The prefix length, if the policy is for an IPv6 network.</td>
</tr>
<tr>
<td>start_port</td>
<td>port number</td>
<td>The start port number for a policy port range. (This does not apply if the policy is for a network resource.)</td>
</tr>
<tr>
<td>end_port</td>
<td>port number</td>
<td>The end port number for a policy port range. (This does not apply if the policy is for a network resource.)</td>
</tr>
<tr>
<td>resource_name</td>
<td>resource name</td>
<td>The name of a resource that you configured with the vpn sslvpn resource add command. This keyword and parameter apply only if the policy is for a network resource.</td>
</tr>
<tr>
<td>policy_permission</td>
<td>Permit or Deny</td>
<td>Specifies whether the policy permits or denies access.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn sslvpn policy edit 2
vpn-config[sslvpn-policy-settings]> policy_name RoadWarriorPolicyIII
vpn-config[sslvpn-policy-settings]> start_port 35406
```
VPN Mode Configuration Commands

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Related show command: `show vpn sslvpn policy`

**vasion Server Command**

**vpn sslvpn policy delete <row id>**

This command deletes an SSL VPN policy by specifying its row ID.

**Format**

```
vpn sslvpn policy delete <row id>
```

**Mode**

```
vpn
```

Related show command: `show vpn sslvpn policy`

**VPN Mode Configuration Commands**

263
### Primary RADIUS server

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables the primary RADIUS server.</td>
</tr>
<tr>
<td>radius-server</td>
<td>ipaddress</td>
<td>The IPv4 address of the primary RADIUS server.</td>
</tr>
<tr>
<td>secret</td>
<td>secret</td>
<td>The secret phrase (alphanumeric string) for the primary RADIUS server.</td>
</tr>
<tr>
<td>nas_identifier</td>
<td>identifier</td>
<td>The NAS ID for the primary RADIUS server.</td>
</tr>
</tbody>
</table>

### Backup RADIUS server

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup_server_enable</td>
<td>Y or N</td>
<td>Enables or disables the backup RADIUS server.</td>
</tr>
<tr>
<td>backup_radius_server</td>
<td>ipaddress</td>
<td>The IPv4 address of the backup RADIUS server.</td>
</tr>
<tr>
<td>backup_server_secret</td>
<td>secret</td>
<td>The secret phrase (alphanumeric string) for the backup RADIUS server.</td>
</tr>
<tr>
<td>backup_server_nas_identifier</td>
<td>identifier</td>
<td>The NAS ID for the backup RADIUS server.</td>
</tr>
</tbody>
</table>

### Connection configuration

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>seconds</td>
<td>The connection time-out in seconds for the RADIUS server.</td>
</tr>
<tr>
<td>retries</td>
<td>number</td>
<td>The number of connection retry attempts for the RADIUS server.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn ipsec radius configure
vpn-config[radius-config]> enable Y
vpn-config[radius-config]> radius-server 192.168.4.2
vpn-config[radius-config]> secret Hlo0ole1H12aaq43
vpn-config[radius-config]> nas_identifier SRX5308-Bld3
vpn-config[radius-config]> backup_server_enable Y
vpn-config[radius-config]> backup_radius_server 192.168.4.3
vpn-config[radius-config]> backup_server_secret Hduo0oplH54bqX91
vpn-config[radius-config]> backup_server_nas_identifier SRX5308-Bld3
vpn-config[radius-config]> timeout 30
vpn-config[radius-config]> retries 4
vpn-config[radius-config]> save
```
PPTP Server Commands

`vpn pptp server configure`

This command configures the PPTP server. After you have issued the `vpn pptp server configure` command, you enter the pptp-server-config [policy] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1 Format**

`vpn pptp server configure`

**Mode**

`vpn`

**Step 2 Format**

`enable {Y | N}`

`start_address <ipaddress>`

`end_address <ipaddress>`

`idle_timeout <minutes>`

**Mode**

`pptp-server-config [policy]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables the PPTP server.</td>
</tr>
<tr>
<td>start_address</td>
<td>ipaddress</td>
<td>The start IPv4 address of the PPTP server range.</td>
</tr>
<tr>
<td>end_address</td>
<td>ipaddress</td>
<td>The end IPv4 address of the PPTP server range.</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>minutes</td>
<td>The idle time-out after which the connection is terminated.</td>
</tr>
</tbody>
</table>

**Command example:**

```
SRX5308> vpn pptp server configure
pptp-server-config[policy]> enable Y
pptp-server-config[policy]> start_address 192.168.112.1
pptp-server-config[policy]> end_address 192.168.112.25
pptp-server-config[policy]> idle_timeout 10
pptp-server-config[policy]> save
```

**Related show command:** `show vpn pptp server setup` and `show vpn pptp server connections`
L2TP Server Commands

**vpn l2tp server configure**

This command configures the L2TP server. After you have issued the `vpn l2tp server configure` command, you enter the vpn-config [l2tp-config] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

**Step 1**

Format: `vpn l2tp server configure`
Mode: `vpn`

**Step 2**

Format: `enable {Y | N}`
`start_address <ipaddress>`
`end_address <ipaddress>`
`idle_timeout <minutes>`

Mode: `vpn-config [l2tp-config]`

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Associated Keyword to Select or Parameter to Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Y or N</td>
<td>Enables or disables the L2TP server.</td>
</tr>
<tr>
<td>start_address</td>
<td>ipaddress</td>
<td>The start IPv4 address of the L2TP server range.</td>
</tr>
<tr>
<td>end_address</td>
<td>ipaddress</td>
<td>The end IPv4 address of the L2TP server range.</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>minutes</td>
<td>The idle time-out after which the connection is terminated.</td>
</tr>
</tbody>
</table>

**Command example:**

SRX5308> `vpn l2tp server configure`
`vpn-config[12tp-config]> enable Y`
`vpn-config[12tp-config]> start_address 192.168.112.1`
`vpn-config[12tp-config]> end_address 192.168.112.25`
`vpn-config[12tp-config]> idle_timeout 10`
`vpn-config[12tp-config]> save`

**Related show command:** `show vpn l2tp server setup` and `show vpn l2tp server connections`
Overview of the Show Commands

This chapter provides an overview of all show commands for the four configuration command modes. The chapter includes the following sections:

• Network Settings (Net Mode) Show Commands
• Security Settings (Security Mode) Show Commands
• Administrative and Monitoring Settings (System Mode) Show Commands
• VPN Settings (VPN Mode) Show Commands

Network Settings (Net Mode) Show Commands

Enter the `show net ?` command at the CLI prompt to display the submodes in the show net mode. The following table lists the submodes and their commands in alphabetical order:

Table 12. Show commands: show net mode

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddns</td>
<td><code>show net ddns setup</code></td>
<td>Display the Dynamic DNS configuration.</td>
</tr>
<tr>
<td>dmz</td>
<td><code>show net dmz ipv4 setup</code></td>
<td>Display the IPv4 DMZ configuration.</td>
</tr>
<tr>
<td></td>
<td><code>show net dmz ipv6 setup</code></td>
<td>Display the IPv6 DMZ configuration.</td>
</tr>
<tr>
<td>ethernet</td>
<td>`show net ethernet {interface name</td>
<td>all}`</td>
</tr>
<tr>
<td>ipv6</td>
<td><code>show net ipv6 ipmode setup</code></td>
<td>Display the IPv6 routing mode configuration.</td>
</tr>
<tr>
<td>ipv6_tunnel</td>
<td><code>show net ipv6_tunnel setup</code></td>
<td>Display the IPv6 tunnel configuration.</td>
</tr>
<tr>
<td></td>
<td><code>show net ipv6_tunnel status</code></td>
<td>Display the status of the IPv6 tunnels.</td>
</tr>
<tr>
<td>lan</td>
<td><code>show net lan available_lan_hosts list</code></td>
<td>Display the IPv4 hosts.</td>
</tr>
<tr>
<td></td>
<td><code>show net lan dhcp leased_clients list</code></td>
<td>Display the LAN clients that received a leased DHCP IP address.</td>
</tr>
<tr>
<td></td>
<td><code>show net lan dhcp logs</code></td>
<td>Display the LAN DHCP log.</td>
</tr>
</tbody>
</table>
Table 12. Show commands: show net mode (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>lan (continued)</td>
<td>show net lan dhcp reserved_ip setup</td>
<td>Display information about the DHCP clients, including the assigned (reserved) IP addresses.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv4 advanced setup</td>
<td>Display the advanced IPv4 LAN configuration.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv4 detailed setup &lt;vlan id&gt;</td>
<td>Display the detailed configuration for a VLAN.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv4 multiHoming</td>
<td>Display the LAN secondary IPv4 addresses.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv4 setup</td>
<td>Display the IPv4 LAN configuration.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv4 traffic_meter setup</td>
<td>Display the LAN traffic meter configuration.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv4 traffic_meter detailed_setup &lt;row id&gt;</td>
<td>Display the detailed traffic meter information for a specified IP address.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv6 multiHoming</td>
<td>Display the LAN secondary IPv6 addresses.</td>
</tr>
<tr>
<td></td>
<td>show net lan ipv6 setup</td>
<td>Display the IPv6 LAN configuration.</td>
</tr>
<tr>
<td></td>
<td>show net lan lan_groups</td>
<td>Display the LAN groups.</td>
</tr>
<tr>
<td>protocol binding</td>
<td>show net protocol_binding setup</td>
<td>Display the protocol bindings.</td>
</tr>
<tr>
<td>qos</td>
<td>show net qos setup</td>
<td>Display the WAN QoS configuration.</td>
</tr>
<tr>
<td>radvd</td>
<td>show net radvd dmz setup</td>
<td>Display the DMZ RADVD configuration.</td>
</tr>
<tr>
<td></td>
<td>show net radvd lan setup</td>
<td>Display the LAN RADVD configuration.</td>
</tr>
<tr>
<td>routing</td>
<td>show net routing dynamic setup</td>
<td>Display the dynamic routing configuration.</td>
</tr>
<tr>
<td></td>
<td>show net routing static ipv4 setup</td>
<td>Display the IPv4 static routes configuration.</td>
</tr>
<tr>
<td></td>
<td>show net routing static ipv6 setup</td>
<td>Display the IPv6 static routes configuration.</td>
</tr>
<tr>
<td>siit</td>
<td>show net siit setup</td>
<td>Displays the status of the Stateless IP/ICMP Translation.</td>
</tr>
<tr>
<td>statistics</td>
<td>show net statistics {interface name</td>
<td>all}</td>
</tr>
<tr>
<td>wan</td>
<td>show net wan port_setup &lt;wan interface&gt;</td>
<td>Display the configuration for a WAN interface.</td>
</tr>
<tr>
<td></td>
<td>show net wan ipv4 secondary_addresses &lt;wan interface&gt;</td>
<td>Display the secondary IPv4 addresses for a WAN interface.</td>
</tr>
<tr>
<td></td>
<td>show net wan ipv4 setup &lt;wan interface&gt;</td>
<td>Display the IPv4 configuration for a WAN interface.</td>
</tr>
<tr>
<td></td>
<td>show net wan wan ipv4 status &lt;wan interface&gt;</td>
<td>Display the IPv4 connection status for a WAN interface.</td>
</tr>
</tbody>
</table>
Table 13. Show commands: show security mode

Table 12. Show commands: show net mode (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan (continued)</td>
<td>show net wan wan ipv6 setup &lt;wan interface&gt;</td>
<td>Display the IPv6 configuration for a WAN interface.</td>
</tr>
<tr>
<td></td>
<td>show net wan wan ipv6 status &lt;wan interface&gt;</td>
<td>Display the IPv6 connection status for a WAN interface.</td>
</tr>
<tr>
<td>wan_settings</td>
<td>show net wan_settings wanmode</td>
<td>Display the IPv4 WAN routing mode.</td>
</tr>
</tbody>
</table>

Security Settings (Security Mode) Show Commands

Enter the `show security ?` command at the CLI prompt to display the submodes in the show security mode. The following table lists the submodes and their commands in alphabetical order:

Table 13. Show commands: show security mode

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>address_filter</td>
<td>show security address_filter enable_email_log</td>
<td>Display the configuration of the IP/MAC binding log.</td>
</tr>
<tr>
<td></td>
<td>show security address_filter ip_or_mac_binding setup</td>
<td>Display the IPv4 and IPv6 MAC bindings.</td>
</tr>
<tr>
<td></td>
<td>show security address_filter mac_filter setup</td>
<td>Display the MAC addresses for source MAC filtering.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>show security bandwidth profile setup</td>
<td>Display the configured bandwidth profiles.</td>
</tr>
<tr>
<td>content_filter</td>
<td>show security content_filter block_group</td>
<td>Display the groups for which content filtering is enabled.</td>
</tr>
<tr>
<td></td>
<td>show security content_filter blocked_keywords</td>
<td>Display the keywords that are blocked.</td>
</tr>
<tr>
<td></td>
<td>show security content_filter content_filtering</td>
<td>Display the status of content filtering and the web components.</td>
</tr>
<tr>
<td></td>
<td>show security content_filter trusted_domains</td>
<td>Display the trusted domains.</td>
</tr>
<tr>
<td>firewall</td>
<td>show security firewall advanced algs</td>
<td>Display whether or not SIP ALG is enabled.</td>
</tr>
<tr>
<td></td>
<td>show security firewall attack_checks igmp</td>
<td>Display whether or not the IGMP proxy is enabled.</td>
</tr>
<tr>
<td></td>
<td>show security firewall attack_checks setup ipv4</td>
<td>Display which WAN and LAN security checks are enabled for IPv4.</td>
</tr>
<tr>
<td></td>
<td>show security firewall attack_checks setup ipv6</td>
<td>Display which WAN and LAN security checks are enabled for IPv6.</td>
</tr>
<tr>
<td></td>
<td>show security firewall attack_checks vpn_passsthrough setup</td>
<td>Display which VPN pass-through features are enabled.</td>
</tr>
</tbody>
</table>
Table 13. Show commands: show security mode (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>firewall (continued)</td>
<td>show security firewall ipv4 setup dmz_wan</td>
<td>Display the IPv4 DMZ WAN firewall rules.</td>
</tr>
<tr>
<td></td>
<td>show security firewall ipv4 setup lan_dmz</td>
<td>Display the IPv4 LAN DMZ firewall rules.</td>
</tr>
<tr>
<td></td>
<td>show security firewall ipv4 setup lan_wan</td>
<td>Display the IPv4 LAN WAN firewall rules.</td>
</tr>
<tr>
<td></td>
<td>show security firewall ipv6 setup</td>
<td>Display all IPv6 firewall rules.</td>
</tr>
<tr>
<td></td>
<td>show security firewall session_limit</td>
<td>Display the session limit settings.</td>
</tr>
<tr>
<td></td>
<td>show security firewall session_settings</td>
<td>Display the session time-out settings.</td>
</tr>
<tr>
<td>porttriggering_rules</td>
<td>show security porttriggering_rules setup</td>
<td>Display the port triggering rules.</td>
</tr>
<tr>
<td></td>
<td>show security porttriggering_rules status</td>
<td>Display the port triggering status.</td>
</tr>
<tr>
<td>schedules</td>
<td>show security schedules setup</td>
<td>Display the configured schedules.</td>
</tr>
<tr>
<td>services</td>
<td>show security services setup</td>
<td>Display the configured custom services.</td>
</tr>
<tr>
<td></td>
<td>show security services qos_profile setup</td>
<td>Display the configured QoS profiles.</td>
</tr>
<tr>
<td></td>
<td>show security services ip_group ip_setup</td>
<td>Display the configured IP groups.</td>
</tr>
<tr>
<td>upnp</td>
<td>show security upnp portmap</td>
<td>Display the UPnP portmap table.</td>
</tr>
<tr>
<td></td>
<td>show security upnp setup</td>
<td>Display the UPnP configuration.</td>
</tr>
</tbody>
</table>

Administrative and Monitoring Settings (System Mode) Show Commands

Enter the `show system ?` command at the CLI prompt to display the submodes in the show system mode. The following table lists the submodes and their commands in alphabetical order:

Table 14. Show commands: show system mode

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>not applicable</td>
<td>show sysinfo</td>
<td>Display system information, including MAC addresses, serial number, and firmware version.</td>
</tr>
<tr>
<td></td>
<td>show system firmware_version</td>
<td>Display the firmware version.</td>
</tr>
<tr>
<td>logging</td>
<td>show system logging remote setup</td>
<td>Display the configuration and the schedule of the email logs.</td>
</tr>
<tr>
<td></td>
<td>show system logging setup</td>
<td>Display the configuration of the IPv4 and IPv6 logs.</td>
</tr>
<tr>
<td>logs</td>
<td>show system logs</td>
<td>Display the system logs.</td>
</tr>
</tbody>
</table>

Overview of the Show Commands
Table 14. Show commands: show system mode (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_management</td>
<td>show system remote_management setup</td>
<td>Display the configuration of remote management for Telnet and HTTPS access.</td>
</tr>
<tr>
<td>snmp</td>
<td>show system snmp sys</td>
<td>Display the SNMP system configuration of the SNMP agent and the SNMP system information of the wireless VPN firewall.</td>
</tr>
<tr>
<td></td>
<td>show system snmp trap [agent ipaddress]</td>
<td>Display the SNMP trap configuration of the SNMP agent.</td>
</tr>
<tr>
<td>status</td>
<td>show system status</td>
<td>Display the system status information.</td>
</tr>
<tr>
<td>time</td>
<td>show system time setup</td>
<td>Display the time configuration and the configuration of the NTP server.</td>
</tr>
<tr>
<td>traffic_meter</td>
<td>show system traffic_meter setup &lt;wan interface&gt;</td>
<td>Display the configuration of the traffic meter and the Internet traffic statistics.</td>
</tr>
</tbody>
</table>

VPN Settings (VPN Mode) Show Commands

Enter the show vpn ? command at the CLI prompt to display the submodes in the show vpn mode. The following table lists the submodes and their commands in alphabetical order:

Table 15. Show commands: show vpn mode

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec</td>
<td>show vpn ipsec ikepolicy setup</td>
<td>Display the IKE policies.</td>
</tr>
<tr>
<td></td>
<td>show vpn ipsec logs</td>
<td>Display the IPSec VPN logs.</td>
</tr>
<tr>
<td></td>
<td>show vpn ipsec mode_config setup</td>
<td>Display the Mode Config records.</td>
</tr>
<tr>
<td></td>
<td>show vpn ipsec radius [ipaddress]</td>
<td>Display the configuration of all or a specific RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>show vpn ipsec vpnpolicy setup</td>
<td>Display the IPSec VPN policies.</td>
</tr>
<tr>
<td></td>
<td>show vpn ipsec vpnpolicy status</td>
<td>Display status information about the active and nonactive IPSec VPN policies.</td>
</tr>
<tr>
<td>l2tp</td>
<td>show vpn l2tp server connections</td>
<td>Display the users that are connected through the L2TP server.</td>
</tr>
<tr>
<td></td>
<td>show vpn l2tp server setup</td>
<td>Display the configuration of the PPTP server.</td>
</tr>
<tr>
<td>pptp</td>
<td>show vpn pptp server connections</td>
<td>Display the users that are connected through the PPTP server.</td>
</tr>
<tr>
<td></td>
<td>show vpn pptp server setup</td>
<td>Display the configuration of the L2TP server.</td>
</tr>
</tbody>
</table>
### Table 15. Show commands: show vpn mode (continued)

<table>
<thead>
<tr>
<th>Submode</th>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslvpn</td>
<td>show vpn sslvpn client</td>
<td>Display the SSL VPN client range and configuration.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn logs</td>
<td>Display the SSL VPN logs.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn policy</td>
<td>Display the SSL VPN policies.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn portal_layouts</td>
<td>Display the SSL VPN portal layout.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn portforwarding appconfig</td>
<td>Display the SSL VPN port forwarding application configuration.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn portforwarding hostconfig</td>
<td>Display the SSL VPN port forwarding host configuration.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn resource</td>
<td>Display the SSL VPN resource configuration.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn resource_object &lt;resource name&gt;</td>
<td>Display the detailed configuration for a specific resource object.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn route</td>
<td>Display the SSL VPN client routes.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users active_users</td>
<td>Display the active SSL VPN users.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users browser_policies &lt;row id&gt;</td>
<td>Display the login restrictions based on web browsers for a specific user.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users domains</td>
<td>Display the domain configurations.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users groups</td>
<td>Display the group configurations.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users ip_policies &lt;row id&gt;</td>
<td>Display the login restrictions based on IP addresses for a specific user.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users login_policies &lt;row id&gt;</td>
<td>Display the login restrictions based on login policies for a specific user.</td>
</tr>
<tr>
<td></td>
<td>show vpn sslvpn users users</td>
<td>Display the user account configurations.</td>
</tr>
</tbody>
</table>
This chapter explains the show commands and associated parameters for the four configuration command modes. The chapter includes the following sections:

- Network Settings (Net Mode) Show Commands
- Security Settings (Security Mode) Show Commands
- Administrative and Monitoring Settings (System Mode) Show Commands
- VPN Settings (VPN Mode) Show Commands

### Network Settings (Net Mode) Show Commands

This section contains the following subsections:

- WAN IPv4 and WAN IPv6 Show Commands
- IPv6 Mode, IPv6 Tunnel, and SIIT Show Commands
- LAN DHCP Show Commands
- Dynamic DNS Show Commands
- IPv4 LAN Show Commands
- IPv6 LAN Show Commands
- DMZ Show Commands
- Routing Show Commands
- Network Statistics Show Commands

#### WAN IPv4 and WAN IPv6 Show Commands

**show net wan_settings wanmode**

This command displays the IPv4 WAN routing mode:

Routing Mode between WAN and LAN

NAT is Enabled
show net wan port_setup <wan interface>

This command displays the configuration of a WAN port. For the WAN interface, type **WAN1**, **WAN2**, **WAN3**, or **WAN4**.

WAN1 Port Setup

_____________________
MTU Type: Default
Port Speed: Auto Sense

WAN MODE Setup

_____________________
WAN Mode: Primary Wan Mode Using WAN1
Auto Rollover: Auto Rollover is Disabled
WAN Failure Detection Method: WAN DNS Servers
Retry Interval: 30
Failover After: 4

Router's MAC Address for WAN1

_____________________
MAC Address Type: This MAC Address
MAC Address: 00:00:00:00:11:22

Upload/Download Settings for WAN1

_____________________
WAN Connection Type: DSL
WAN Connection Speed Upload Type: Custom
WAN Connection Speed Upload: 1500
WAN Connection Speed Download Type: 1 Gbps
WAN Connection Speed Download: 1000000

show net wan wan ipv4 setup <wan interface>

This command displays the IPv4 configuration for a WAN interface. For the WAN interface, type **WAN1**, **WAN2**, **WAN3**, or **WAN4**.

Broadband Setup

_____________________
STATIC Configuration:
Internet (IP) Address Source: Use Static IP Address
IP Address: 10.139.54.228
IP Subnet Mask: 255.255.255.248
Gateway IP Address: 10.139.54.225
Domain Name Servers (DNS) Source: Use these DNS Servers
Primary DNS Server: 10.80.130.23
Secondary DNS Server: 10.80.130.24

**show net wan wan ipv4 status <wan interface>**

This command displays the IPv4 WAN connection status. For the WAN interface, type **WAN1**, **WAN2**, **WAN3**, or **WAN4**.

**WAN1 Status**

WAN1 Status (Ipv4):
MAC Address: AA:AB:BB:00:00:02
IPv4 Address: 10.139.54.228 / 255.255.255.248
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: STATIC
IPv4 Connection State: Connected
Link State: LINK UP
WAN Mode: Use only single WAN portWAN1
Gateway: 10.139.54.225
Primary DNS: 10.80.130.23
Secondary DNS: 8.8.8.8

**show net wan wan ipv4 secondary_addresses <wan interface>**

This command displays the secondary IPv4 addresses for a WAN interface. For the WAN interface, type **WAN1**, **WAN2**, **WAN3**, or **WAN4**.

**WAN2 Secondary Addresses**

List of Secondary WAN addresses

Row Id: 1
IP Address: 10.168.50.1
Subnet Mask: 255.255.255.0
show net wan wan ipv6 setup <wan interface>

This command displays the IPv6 WAN configuration. For the WAN interface, type WAN1, WAN2, WAN3, or WAN4.

IPv6 WAN1 Setup

________________
Dynamic IPv6 (DHCP) Configuration:
Stateless Address Auto Configuration: Enabled
Prefix Delegation: Disabled

show net wan wan ipv6 status <wan interface>

This command displays the IPv6 WAN1 connection status. For the WAN interface, type WAN1, WAN2, WAN3, or WAN4.

IPv6 WAN1 Status

________________
IPv6 Connection Type: Dynamic IPv6 (DHCP)
IPv6 Connection State: Connected
IPv6 Address: fe80::a8ab:bbff:fe00:2
IPv6 Prefix Length: 64
Default IPv6 Gateway:
Primary DNS Server:
Secondary DNS Server:

show net protocol_binding setup

This command displays the protocol bindings:

List of Protocol Bindings.

__________________________
ROW ID State   Service Local Gateway Source Network Destination Network
______ _______ _______ ______________ ___________________
1      Enabled FTP     WAN1          Any            10.122.178.214
2      Enabled PPTP    WAN3          Any            Any
3      Enabled ANY     WAN1          Any            Any
show net qos setup

This command displays the WAN QoS configuration:

Quality of Service

Enabled: Yes
QoS Type: Rate Control

List of Network QoS Profiles

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>QoS Type</th>
<th>Interface Name</th>
<th>ServiceName</th>
<th>Direction</th>
<th>Rate</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rate Control</td>
<td>WAN2</td>
<td>HTTP</td>
<td>Inbound</td>
<td>7500 - 15000</td>
<td>192.168.110.2 - 192.168.110.199</td>
</tr>
<tr>
<td>2</td>
<td>Priority</td>
<td>WAN1</td>
<td>RTSP:TCP</td>
<td>Inbound Traffic High</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

IPv6 Mode, IPv6 Tunnel, and SIIT Show Commands

show net ipv6 ipmode setup

This command displays the IPv6 routing mode configuration:

IP MODE

IPv4 only mode : Disabled
IPv4/IPv6 mode : Enabled

show net ipv6_tunnel setup

This command displays the IPv6 tunnel configuration:

IPv6 Tunnels

6 to 4 Tunneling

Automatic Tunneling is Enabled

List of Available ISATAP Tunnels

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>LocalEndpoint</th>
<th>ISATAP Subnet Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.1</td>
<td>FE80:2006::</td>
</tr>
<tr>
<td>2</td>
<td>10.29.33.4</td>
<td>2004::</td>
</tr>
</tbody>
</table>
show net ipv6_tunnel status

This command displays the status of the IPv6 tunnels:

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>IPv6 Address(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>sit0-WAN1</td>
<td>2002:408b:36e2::408b:36e2/64, ::127.0.0.1/96, ::176.16.2.1/96, ::192.168.1.1/96,</td>
</tr>
<tr>
<td></td>
<td>::192.168.20.1/96, ::192.168.70.1/96, ::64.139.54.226/96</td>
</tr>
<tr>
<td>isatap1-LAN</td>
<td>fe80::5efe:c0a8:101/64</td>
</tr>
<tr>
<td>isatap2-LAN</td>
<td>::10.29.33.4/128, fe80::5efe:a1d:2104/64</td>
</tr>
</tbody>
</table>

show net siit setup

This command displays the status of the Stateless IP/ICMP Translation (SIIT):

<table>
<thead>
<tr>
<th>SIIT Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

LAN DHCP Show Commands

show net lan dhcp leased_clients list

This command displays the LAN clients that received a leased DHCP IP address:

List of Available DHCP Leased Clients

show net lan dhcp logs

This command displays the LAN DHCP log:

Jul 10 10:23:50 SRX5308 local7.info dhcpd: Wrote 0 deleted host decls to leases file.
Jul 10 10:23:51 SRX5308 local7.info dhcpd: Listening on LPF/eth0.4094/00:00:00:00:00:00/176.16.2.0/24
Jul 10 10:23:51 SRX5308 local7.info dhcpd: Sending on   LPF/eth0.4094/00:00:00:00:00:00/176.16.2.0/24
Jul 10 10:23:51 SRX5308 local7.err dhcpd: No subnet declaration for eth0.20 (192.168.70.1).
show net lan dhcp reserved_ip setup

This command displays information about the DHCP clients, including the assigned (reserved) IP addresses:

List of DHCP Reserved Addresses

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Group</th>
<th>Profile Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPhoneRoom12</td>
<td>192.168.1.100</td>
<td>d1:d2:44:45:9e:9f</td>
<td>GROUP1</td>
<td>Default</td>
</tr>
<tr>
<td>SalesServer</td>
<td>192.168.70.15</td>
<td>a1:c1:33:44:2a:2b</td>
<td>GROUP5</td>
<td>Sales</td>
</tr>
<tr>
<td>Mobile3008</td>
<td>192.168.90.22</td>
<td>a1:b1:11:12:1a:12</td>
<td>Management</td>
<td>Marketing</td>
</tr>
<tr>
<td>FN_Server</td>
<td>192.168.70.2</td>
<td>a1:a2:a3:11:bc:de</td>
<td>Management</td>
<td>Sales</td>
</tr>
</tbody>
</table>

Dynamic DNS Show Commands

show net ddns setup

This command displays the Dynamic DNS configuration:

WAN Mode

Single Port WAN1

WAN1 Dynamic DNS service currently disabled

___________________________________________

WAN2 Dynamic DNS service currently disabled

___________________________________________

WAN3 Dynamic DNS service currently disabled

___________________________________________

WAN4 Dynamic DNS service currently disabled

___________________________________________
IPv4 LAN Show Commands

show net lan ipv4 setup

This command displays the IPv4 LAN configuration:

VLAN Profiles

<table>
<thead>
<tr>
<th>Status</th>
<th>Profile Name</th>
<th>VLAN Id</th>
<th>IPv4 Address</th>
<th>Subnet Mask</th>
<th>DHCP Status</th>
<th>Server Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Default</td>
<td>1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>DHCP Server</td>
<td>192.168.1.100 - 192.168.1.254</td>
</tr>
<tr>
<td>Enabled</td>
<td>Sales</td>
<td>20</td>
<td>192.168.70.1</td>
<td>255.255.255.0</td>
<td>Disabled</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Disabled</td>
<td>Marketing</td>
<td>40</td>
<td>192.168.90.5</td>
<td>255.255.255.128</td>
<td>Disabled</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Default VLAN

Port1: Sales
Port2: Default
Port3: Default
Port4: DMZ

show net lan ipv4 detailed setup <vlan id>

This command displays the detailed configuration for a VLAN. For the VLAN ID, type a VLAN number.

Detailed Setup (IPv4) of VLAN :- Default

Status: Enabled
Profile Name: Default
VLAN Id: 1
IPv4 Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: DHCP Server
Server Address: 192.168.1.100 - 192.168.1.254
Primary DNS Server: 
Secondary DNS Server: 
WINS Server: 
Lease Time: 24
LDAP Status: Disabled
DNS Proxy: Enabled
Inter VLAN Routing: Disabled
**show net ethernet {interface name | all}**

This command displays the MAC address and VLAN status for a single or all Ethernet interfaces.

SRX5308> **show net ethernet eth0**

VLAN ID: 1
Interface Name: eth0
VLAN Enabled: N
Native VLAN: N

SRX5308> **show net ethernet all**

Ethernet Interfaces

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Interface Name</th>
<th>VLAN Enabled</th>
<th>Native VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth0</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>1</td>
<td>eth1</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

**show net lan ipv4 advanced setup**

This command displays the advanced IPv4 LAN configuration:

LAN Advanced Setup

<table>
<thead>
<tr>
<th>VLAN MAC Settings:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address for VLANs: Unique</td>
</tr>
<tr>
<td>Advanced Settings:</td>
</tr>
<tr>
<td>ARP Broadcast: Enabled</td>
</tr>
</tbody>
</table>

**show net lan available_lan_hosts list**

This command displays the IPv4 hosts (that is, the known computers and devices in the LAN):

List of Available Lan Hosts

___________________________
**show net lan lan_groups**

This command displays the LAN groups:

```
Row ID : Group Name
1       GROUP1
2       GROUP2
3       Finance
4       GROUP4
5       GROUP5
6       SalesEMEA
7       SalesAmericas
8       Management
```

**show net lan ipv4 multiHoming**

This command displays the LAN secondary IP addresses:

```
IPv4 LAN Multi-homing
Available Secondary LAN IPs :-
Row Id IP Address     Subnet Mask
______ ______________ _______________
1      192.168.20.1   255.255.255.0
2      192.168.70.240 255.255.255.128
```

**show net lan ipv4 traffic_meter setup**

This command displays the LAN traffic meter configuration:

```
LAN Traffic Meter Table
Row Id LAN IP Address Direction       Limit (MB) Traffic (MB) State
______ ______________ _______________ __________ ____________ _______
1      192.168.11.68  Download Only   30000      0            Allowed
2      192.168.11.204 Both Directions 45000      0            Allowed
```
show net lan ipv4 traffic_meter detailed_setup <row id>

**Note:** The row ID refers to the LAN Traffic Meter Table in the output of the show net lan ipv4 traffic_meter setup command.

This command displays the detailed traffic meter information for the specified IP address:

LAN Traffic Meter Account

LAN IP Address: 192.168.11.204

Direction: Both Directions

Limit in (MB): 45000

Traffic Counter

Traffic Counter: Restart Counter

Restart Time (HH/MM-Day of Month): 12/0-1
Send e-mail before restarting Counter: Disabled

When Limit is reached

Send e-mail alert: Disabled

LAN IP Traffic Statistics

Start Date / Time: Sun Jul 1 00:00:16 2012

Outgoing Traffic Volume: 0
Incoming Traffic Volume: 0
Average per day:
% of Standard Limit:
State: Allowed
IPv6 LAN Show Commands

**show net lan ipv6 setup**

This command displays the IPv6 LAN configuration:

IPv6 LAN Configuration

______________________

LAN TCP/IP Setup:
IPv6 Address: fec0::1
IPv6 Prefix Length: 64

DHCPv6:
DHCP Status: Disable DHCPv6 Server
DHCP Mode: Stateless
Prefix Delegation: Disable
Domain Name: netgear.com
Server Preference: 255
DNS Servers: Use Below
Primary DNS Server:
Secondary DNS Server:
Lease/Rebind Time: 86400

List of IPv6 Address Pools

__________________________

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Start Address</th>
<th>End Address</th>
<th>Prefix Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>fec0::db8:2</td>
<td>fec0::db8:199</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>fec0::db8:10a1:1</td>
<td>fec0::db8:10a1:300</td>
<td>10</td>
</tr>
</tbody>
</table>

List of Prefixes for Prefix Delegation

______________________________________

<table>
<thead>
<tr>
<th>Row Id</th>
<th>IPv6 Prefix</th>
<th>IPv6 Prefix Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8::</td>
<td>64</td>
</tr>
<tr>
<td>2</td>
<td>2001:db8:ac2::</td>
<td>64</td>
</tr>
</tbody>
</table>
**show net radvd lan setup**

This command displays the LAN RADVD configuration:

Router Advertisement Daemon (RADVD)

RADVD Status: Enabled
Advertise Mode: Unsolicited Multicast
Advertise Interval: 30
RA Flags

Managed: Disabled
Other: Enabled
Router Preference: High
MTU: 1500
Router Lifetime: 3600 Seconds

List of Available Prefixes to Advertise

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>IPv6 Prefix</th>
<th>IPv6 Prefix Length</th>
<th>Life Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2002:408b:36e4:a::</td>
<td>64</td>
<td>43200</td>
</tr>
<tr>
<td>2</td>
<td>FE80:0:0:CC40::</td>
<td>64</td>
<td>21600</td>
</tr>
</tbody>
</table>

**show net lan ipv6 multiHoming**

This command displays the LAN secondary IPv6 addresses:

IPv6 LAN Multi-homing

Available Secondary LAN IPs:

Row Id: 1
IPv6 Address: 2001:db8:3000::2192
Prefix Length: 10
DMZ Show Commands

show net dmz ipv4 setup

This command displays the IPv4 DMZ configuration:

DMZ Setup
________

IPv4 Address: 176.16.2.1
Subnet Mask: 255.255.255.0
DHCP Setup Configuration:
DHCP Mode: DHCP Server
Domain Name: netgear.com
Starting IP Address: 176.16.2.100
Ending IP Address: 176.16.2.254
Primary DNS Server:
Secondary DNS Server:
WINS Server:
Lease Time in hrs : 24
LDAP Status: Disabled
DNS Proxy: Enabled

show net dmz ipv6 setup

This command displays the IPv6 DMZ configuration:

DHCP Setup Configuration
________________________

IPv6 Address: 176::1
Prefix Length: 64
DHCP Status: DHCP Server Enabled
Mode: Stateless
Domain Name: netgear.com
DNS Server: Use DNS Proxy
Lease Time in Sec : 86400
Starting IP Address : 176::1100 176::2031:1500
Ending IP Address   : 176::1220 176::2031:1650
Pool Prefix Length  : 56 56
show net radvd dmz setup

This command displays the DMZ RADVD configuration:

Router Advertisement Daemon ( RADVD )

RADVD Status: Enabled
Advertise Mode: Unsolicited Multicast
Advertise Interval: 30
RA Flags

Managed: Disabled
Other: Enabled
Router Preference: High
MTU: 1500
Router Lifetime: 3600 Seconds

List of Available Prefixes to Advertise

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>IPv6 Prefix</th>
<th>IPv6 Prefix Length</th>
<th>Life Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8:abdd::</td>
<td>64</td>
<td>3600</td>
</tr>
<tr>
<td>2</td>
<td>2002:408b:36e2:2727::</td>
<td>64</td>
<td>7200</td>
</tr>
</tbody>
</table>
Routing Show Commands

**show net routing dynamic setup**

This command displays the dynamic routing configuration:

Dynamic Routing
_______________
RIP
___
RIP Direction Both
RIP Version RIP-2M
Authentication for RIP-2B/2M: Enabled
First Key Parameters
MD5 Key Id: 1
MD5 Auth Key: *****
Not Valid Before: 2011/12/01@07:00:00
Not Valid After: 2012/12/31@23:59:59
Second Key Parameters
MD5 Key Id: 2
MD5 Auth Key: *****
Not Valid Before: 2012/12/31@24:00:00
Not Valid After: 2013/03/31@23:59:59

**show net routing static ipv4 setup**

This command displays the IPv4 static routes configuration:

<table>
<thead>
<tr>
<th>Name</th>
<th>Destination</th>
<th>Gateway</th>
<th>Interface</th>
<th>Metric</th>
<th>Active</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orly</td>
<td>10.118.215.178</td>
<td>10.192.44.13</td>
<td>WAN1</td>
<td>7</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**show net routing static ipv6 setup**

This command displays the IPv6 static routes configuration:

<table>
<thead>
<tr>
<th>Name</th>
<th>Destination</th>
<th>Gateway</th>
<th>Interface</th>
<th>Metric</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFO2</td>
<td>2002:201b:24e2::1001</td>
<td>FE80::2001:5efe:ab23</td>
<td>WAN1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Network Statistics Show Commands

`show net statistics {interface name | all}`

This command displays the network statistics for a single or all Ethernet interfaces:

SRX5308> `show net statistics eth0`

Interface Statistics

____________________

IFACE: eth0
PktRx: 5688
ktTx: 5651
ByteRx: 654963
ByteTx: 4834187
ErrRx: 0
ErrTx: 0
DropRx: 0
DropTx: 0
Mcast: 0
Coll: 0

SRX5308> `show net statistics all`

Interface Statistics

____________________

<table>
<thead>
<tr>
<th>IFACE</th>
<th>PktRx</th>
<th>Pkt</th>
<th>ByteRx</th>
<th>ByteTx</th>
<th>ErrRx</th>
<th>ErrTx</th>
<th>DropRx</th>
<th>DropTx</th>
<th>Mcast</th>
<th>Coll</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>20802</td>
<td>31569</td>
<td>2148358</td>
<td>38409384</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>eth1</td>
<td>359059</td>
<td>186965</td>
<td>61156441</td>
<td>28586367</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Security Settings (Security Mode) Show Commands

This section contains the following subsections:

- **Services Show Command**
- **Schedules Show Command**
- **Firewall Rules Show Command**
- **Attack Checks Show Commands**
- **Session Limits Show Commands**
- **Advanced Firewall Show Commands**
- **Address Filter Show Commands**
- **Port Triggering Show Commands**
- **UPnP Show Commands**
- **Bandwidth Profiles Show Command**
- **Content Filtering Show Commands**

**Services Show Command**

`show security services setup`

This command displays the configured custom services:

**List of Available Custom Services**

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Name</th>
<th>Type</th>
<th>ICMP Type / Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>76</td>
<td>Ixia</td>
<td>TCP</td>
<td>10115-10117</td>
</tr>
<tr>
<td>77</td>
<td>RemoteManagement</td>
<td>TCP</td>
<td>8888-8888</td>
</tr>
<tr>
<td>78</td>
<td>Traceroute</td>
<td>ICMP</td>
<td>20</td>
</tr>
</tbody>
</table>
**show security services qos_profile setup**

This command displays the configured Qos profiles:

List of QoS Profiles

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Profile Name</th>
<th>QoS Type</th>
<th>QoS Value</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Voice</td>
<td>DSCP</td>
<td>24</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Video</td>
<td>IP-Precedence</td>
<td>5</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Standard</td>
<td>IP-Precedence</td>
<td>0</td>
<td>Default</td>
</tr>
</tbody>
</table>

**show security services ip_group ip_setup**

This command displays the configured IP groups:

List of IP Group's IP Table

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>IP Group</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TechSuppport</td>
<td>10.55.3.201</td>
</tr>
<tr>
<td>2</td>
<td>TechSuppport</td>
<td>10.167.88.241</td>
</tr>
<tr>
<td>3</td>
<td>VIPcustomers</td>
<td>10.222.24.190</td>
</tr>
<tr>
<td>4</td>
<td>VIPcustomers</td>
<td>10.147.219.43</td>
</tr>
</tbody>
</table>
Schedules Show Command

show security schedules setup

This command displays the configured schedules:

Schedules

List of Available Schedules

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Name</th>
<th>Days</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>schedule1</td>
<td>Monday, Wednesday, Friday</td>
<td>07:15 AM</td>
<td>06:30 PM</td>
</tr>
<tr>
<td>2</td>
<td>schedule2</td>
<td>All Days</td>
<td>12:00 AM</td>
<td>11:59 PM</td>
</tr>
<tr>
<td>3</td>
<td>schedule3</td>
<td>All Days</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
</tbody>
</table>

Firewall Rules Show Command

show security firewall ipv4 setup lan_wan

This command displays the configured IPv4 LAN WAN firewall rules:

Default Outbound Policy for IPv4 : Allow Always

LAN WAN Outbound Rules.

<table>
<thead>
<tr>
<th>ROWID</th>
<th>Status</th>
<th>Service Name</th>
<th>Filter</th>
<th>LAN User</th>
<th>WAN User QoS Profile</th>
<th>Bandwidth Profile</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Enabled</td>
<td>HTTP</td>
<td>ALLOW Always</td>
<td>SalesAmerica</td>
<td>Any</td>
<td>PriorityQueue</td>
<td>Never</td>
</tr>
<tr>
<td>30</td>
<td>Enabled</td>
<td>AIM</td>
<td>BLOCK by schedule,otherwise allow</td>
<td>Any</td>
<td>Voice</td>
<td>NONE</td>
<td>Always</td>
</tr>
</tbody>
</table>

LAN WAN Inbound Rules.

<table>
<thead>
<tr>
<th>ROWID</th>
<th>Status</th>
<th>Service Name</th>
<th>Filter</th>
<th>LAN Server IP Address</th>
<th>LAN User</th>
<th>WN User</th>
<th>Destination QoS Profile</th>
<th>Bandwidth Profile</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Enabled</td>
<td>FTP</td>
<td>ALLOW Always</td>
<td>192.168.5.71</td>
<td>Any</td>
<td>None</td>
<td>NONE</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Enabled</td>
<td>RTSP:TCP</td>
<td>BLOCK by schedule,otherwise allow 192.168.20.1Y</td>
<td>VIPcustomers WANI</td>
<td>Voice</td>
<td>NONE</td>
<td>Always</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**show security firewall ipv4 setup dmz_wan**

This command displays the configured IPv4 DMZ WAN firewall rules:

Default Outbound Policy for IPv4: Allow Always

DMZ WAN Outbound Rules.

<table>
<thead>
<tr>
<th>ROWID</th>
<th>Status</th>
<th>Service Name</th>
<th>Filter</th>
<th>DMZ User</th>
<th>WAN User</th>
<th>QoS Profile</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Enabled</td>
<td>CU-SEEME:TCP</td>
<td>BLOCK by schedule, otherwise allow</td>
<td>Any</td>
<td>Any</td>
<td>Video</td>
<td>Never</td>
</tr>
<tr>
<td>23</td>
<td>Enabled</td>
<td>ANY</td>
<td>BLOCK Always</td>
<td>Any</td>
<td>Any</td>
<td>None</td>
<td>Never</td>
</tr>
</tbody>
</table>

DMZ WAN Inbound Rules.

<table>
<thead>
<tr>
<th>ROWID</th>
<th>Status</th>
<th>Service Name</th>
<th>Filter</th>
<th>DMZ Server IP Address</th>
<th>DMZ User</th>
<th>WAN User</th>
<th>Destination</th>
<th>QoS Profile</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Enabled</td>
<td>BOOTP_CLIENT</td>
<td>ALLOW Always</td>
<td>192.168.24.112</td>
<td>10.132.215.4</td>
<td>10.168.50.1</td>
<td>None</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Enabled</td>
<td>ANY</td>
<td>BLOCK Always</td>
<td></td>
<td>Any</td>
<td>WAN1</td>
<td>Any</td>
<td>None</td>
<td>Never</td>
</tr>
</tbody>
</table>

**show security firewall ipv4 setup lan_dmz**

This command displays the configured IPv4 LAN DMZ firewall rules:

Default Outbound Policy for IPv4: Allow Always

LAN DMZ Outbound Rules.

<table>
<thead>
<tr>
<th>ROWID</th>
<th>Status</th>
<th>Service Name</th>
<th>Filter</th>
<th>LAN User</th>
<th>DMZ User</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Enabled</td>
<td>FTP</td>
<td>ALLOW Always</td>
<td>GROUP4</td>
<td>176.14.2.30 - 176.14.2.79</td>
<td>Never</td>
</tr>
<tr>
<td>25</td>
<td>Enabled</td>
<td>ANY</td>
<td>BLOCK Always</td>
<td>Any</td>
<td>Any</td>
<td>Never</td>
</tr>
</tbody>
</table>

LAN DMZ Inbound Rules.

<table>
<thead>
<tr>
<th>ROWID</th>
<th>Status</th>
<th>Service Name</th>
<th>Filter</th>
<th>DMZ User</th>
<th>LAN User</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Enabled</td>
<td>SSH:UDP</td>
<td>BLOCK by schedule, otherwise allow</td>
<td>176.16.2.101</td>
<td>192.168.5.108</td>
<td>Always</td>
</tr>
<tr>
<td>26</td>
<td>Enabled</td>
<td>ANY</td>
<td>BLOCK Always</td>
<td>Any</td>
<td>Any</td>
<td>Never</td>
</tr>
</tbody>
</table>
show security firewall ipv6 setup

This command displays all configured IPv6 firewall rules:

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Status</th>
<th>Action</th>
<th>Source Users</th>
<th>Destination Users</th>
<th>Log</th>
<th>QoS Priority</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>130</td>
<td>Enabled</td>
<td>ALLOW Always</td>
<td>2002::B3241B1:fD41</td>
<td>FEC0::db8:145</td>
<td>Always</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>131</td>
<td>Enabled</td>
<td>ALLOW Always</td>
<td>Any</td>
<td>Any</td>
<td>Never</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>Enabled</td>
<td>ALLOW Always</td>
<td>Any</td>
<td>Any</td>
<td>Never</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>133</td>
<td>Enabled</td>
<td>ALLOW Always</td>
<td>Any</td>
<td>Any</td>
<td>Never</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>134</td>
<td>Enabled</td>
<td>ALLOW by schedule,otherwise block</td>
<td>FEC0::db8:10a1:121 - FEC0::db8:10a1:299</td>
<td>2001:db6::30f4:fbbf:ccbc</td>
<td>Never</td>
<td>Normal-Service</td>
<td>schedule1</td>
</tr>
<tr>
<td>135</td>
<td>Enabled</td>
<td>BLOCK Always</td>
<td>Any</td>
<td>Any</td>
<td>Always</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>136</td>
<td>Enabled</td>
<td>BLOCK Always</td>
<td>Any</td>
<td>Any</td>
<td>Always</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>Enabled</td>
<td>BLOCK ICMPv6-TYPE-134</td>
<td>Any</td>
<td>176::1121 - 176::1142</td>
<td>Always</td>
<td>Normal-Service</td>
<td></td>
</tr>
<tr>
<td>138</td>
<td>Enabled</td>
<td>BLOCK Always</td>
<td>Any</td>
<td>Any</td>
<td>Always</td>
<td>Normal-Service</td>
<td></td>
</tr>
</tbody>
</table>

Attack Checks Show Commands

show security firewall attack_checks igmp

This command displays whether the IGMP proxy is enabled:

IGMP Configuration

---

Igmp Proxy: Disabled

show security firewall attack_checks setup ipv4

This command displays which WAN and LAN security checks are enabled for IPv4:

Attack Checks

---

WAN Security Checks:

- Respond to ping on Wan : No
- Enable Stealth mode  : Yes
- Block TCP Flood      : Yes

LAN Security Checks:

- Block UDP Flood      : No
- Disable Ping Reply on LAN Ports : Yes

Show Commands
**show security firewall attack_checks setup ipv6**

This command displays which security checks are enabled for IPv6:

```
Attack Checks IPv6
```

- **WAN Security Checks:**
  - Respond to ping on Wan: No
  - VPN IPSec Passthrough: Yes

**show security firewall attack_checks vpn_passthrough setup**

This command displays which VPN pass-through features are enabled:

```
Passthrough
```

- **IPSec VPN Passthrough:**
  - IPSec Passthrough: Enabled
  - PPTP Passthrough: Disabled
  - L2TP Passthrough: Enabled

**Session Limits Show Commands**

**show security firewall session_limit**

This command displays the session limit settings:

```
Session Settings
```

- Session Limit Enable: Enabled
- Connection Limit Type: 0
- User Connection Limit: 80
- TCP Session Timeout Duration: 3600 (Secs)
- UDP Session Timeout Duration: 180 (Secs)
- ICMP Session Timeout Duration: 120 (Secs)
show security firewall session_settings

This command displays the session time-out settings:

Session Settings

TCP Session Timeout Duration: 3600 (Secs)
UDP Session Timeout Duration: 180 (Secs)
ICMP Session Timeout Duration: 120 (Secs)

Advanced Firewall Show Commands

show security firewall advanced algs

This command displays whether or not SIP ALG is enabled:

ALGs

Sip: Disabled

Address Filter Show Commands

show security address_filter enable_email_log

This command displays the configuration of the IP/MAC binding log:

Email logs for IP/MAC binding violation IPv4

Email logs for IP/MAC binding violation: Enabled

Email logs for IP/MAC binding violation IPv6

Email logs for IP/MAC binding violation: Disabled

show security address_filter ip_or_mac_binding setup

This command displays the IP/MAC bindings:

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Name</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Log Dropped Packets</th>
<th>IP Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PhoneConfRoom52</td>
<td>d1:e1:55:54:8e:7f</td>
<td>192.151.1.107</td>
<td>Disabled</td>
<td>IPv4</td>
</tr>
<tr>
<td>2</td>
<td>FinanceServer3</td>
<td>c3:e3:ee:f2:a2:db</td>
<td>fec0::db8:10b1:166</td>
<td>Enabled</td>
<td>IPv6</td>
</tr>
</tbody>
</table>
show security address_filter mac_filter setup

This command displays the configuration of the MAC filter and the MAC addresses for source MAC filtering:

Source MAC Filter

MAC Filtering: Enabled
Policy for MAC Addresses: Block and Permit the rest

List of Available MAC Addresses

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>aa:11:bb:22:cc:33</td>
</tr>
<tr>
<td>2</td>
<td>a1:b2:c3:de:11:22</td>
</tr>
<tr>
<td>3</td>
<td>a1:b2:c3:de:11:25</td>
</tr>
</tbody>
</table>

Port Triggering Show Commands

show security porttriggering_rules setup

This command displays the port triggering rules:

Port Triggering

List of Available Port Triggering Rules

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Name</th>
<th>Enable</th>
<th>Type</th>
<th>Interface</th>
<th>Outgoing Start Port</th>
<th>Outgoing End Port</th>
<th>Incoming Start Port</th>
<th>Incoming End Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Skype</td>
<td>Yes</td>
<td>TCP</td>
<td>LAN</td>
<td>61196</td>
<td>61196</td>
<td>61197</td>
<td>61197</td>
</tr>
</tbody>
</table>
**show security porttriggering_rules status**

This command displays the port triggering status:

PortTriggering Rules Status

---

### UPnP Show Commands

**show security upnp portmap**

This command displays the UPnP portmap table:

UPnP Portmap Table

---

**show security upnp setup**

This command displays the UPnP configuration:

UPnP configuration

---

Advertisement Period: 60
Advertisement Time To Live: 6

### Bandwidth Profiles Show Command

**show security bandwidth profile setup**

This command displays the configured bandwidth profiles:

List of Available Bandwidth Profiles

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Name</th>
<th>Direction</th>
<th>Inbound Bandwidth Range</th>
<th>Outbound Bandwidth Range</th>
<th>Is Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PriorityQueue</td>
<td>Inbound</td>
<td>10000-100000</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>BusinessLevel1</td>
<td>Both Directions</td>
<td>7500-25000</td>
<td>5000-10000</td>
<td>1</td>
</tr>
</tbody>
</table>
Content Filtering Show Commands

```
show security content_filter content_filtering
```

This command displays the status of content filtering and the web components:

```
Content Filtering
_________________
WAN Security Checks

Content Filtering : Enabled

LAN Security Checks
-------------------
Proxy : Disabled
Java : Enabled
ActiveX : Enabled
Cookies : Disabled
```

```
show security content_filter block_group
```

This command displays the groups for which content filtering is enabled:

```
Blocked Groups
______________
List of Blocked Groups

Blocked Groups: GROUP1, GROUP2, Finance, Management
Unblocked Groups : GROUP4, GROUP5, SalesEMEA, SalesAmericas
```
**show security content_filter blocked_keywords**

This command displays the keywords that are blocked:

Blocked Keywords

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Blocked Keyword</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>casino</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>nude</td>
<td>Enabled</td>
</tr>
<tr>
<td>4</td>
<td>gambl*</td>
<td>Enabled</td>
</tr>
<tr>
<td>5</td>
<td>guns</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**show security content_filter trusted_domains**

This command displays the trusted domains:

List of available Approved URLs

<table>
<thead>
<tr>
<th>ROW ID</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>netgear</td>
</tr>
<tr>
<td>2</td>
<td>google.com</td>
</tr>
<tr>
<td>3</td>
<td><a href="http://www.irs.gov">www.irs.gov</a></td>
</tr>
</tbody>
</table>

**Administrative and Monitoring Settings (System Mode)**

**Show Commands**

This section contains the following subsections:

- *Remote Management Show Command*
- *SNMP Show Commands*
- *Time Show Command*
- *Firmware Version Show Command*
- *Status Show Command*
- *WAN Traffic Meter Show Command*
- *Logging Configuration Show Commands*
- *Logs Show Commands*
Remote Management Show Command

**show system remote_management setup**

This command displays the configuration of remote management for Telnet and HTTPS access:

Remote Mgmt Configuration for telnet

```
IPv4 access granted to everyone
IPv6 access granted to a range of IPs from : FEC0::3001 to FEC0::3100
port being used : 23
```

Remote Mgmt Configuration for https

```
IPv4 access granted to everyone
IPv6 access granted to everyone
port being used : 445
```

SNMP Show Commands

**show system snmp trap [agent ipaddress]**

This command displays the SNMP trap configuration of an SNMP agent:

Trap Agent IP Address

```
IP Address: 10.118.33.245
Subnet Mask: 255.255.255.0
Port: 162
Community: public
```
show system snmp sys
This command displays the SNMP system configuration of the VPN firewall:
SNMP System Configuration
_________________________
SysContact: AdminSRX@netgear.com
SysLocation: San Jose
SysName: SRX5308-Bld3

Time Show Command
show system time setup
This command displays the time configuration and the configuration of the NTP server:
Time Zone & NTP Servers Configuration
_____________________________________
Current Time: Tuesday, July 10, 2012, 18:50:09 (GMT -0800)
Timezone: (GMT-08:00) Pacific Time(Canada)
Automatically Adjust for Daylight Savings Time: Yes
Default NTP servers used : Yes

Firmware Version Show Command
show system firmware_version
This command displays the firmware version:
Firmware Version : 4.2.0-18
Secondary Firmware Version : 4.2.0-14
**Status Show Command**

*show system status*

This command displays the system status (also referred to as router status) information:

**System Info**

System Name: SRX5308  
Firmware Version: 4.2.0-18  
Secondary Firmware Version: 4.2.0-14

**Lan Port 1 Information**

VLAN Profile: Sales  
VLAN ID: 20  
MAC Address: 00:00:00:00:00:08  
IP Address: 192.168.70.1  
Subnet Mask: 255.255.255.0  
DHCP Status: Disabled

**Lan Port 2 Information**

VLAN Profile: Default  
VLAN ID: 1  
MAC Address: 00:00:00:00:00:01  
IP Address: 192.168.1.1  
Subnet Mask: 255.255.255.0  
DHCP Status: Enabled

**Lan Port 3 Information**

VLAN Profile: Marketing  
VLAN ID: 40  
MAC Address: 00:00:00:00:00:04  
IP Address: 192.168.90.5  
Subnet Mask: 255.255.255.128  
DHCP Status: Enabled

**Lan Port 4/DMZ Information**

VLAN Profile: DMZ
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

VLAN ID: 4094
MAC Address: 00:00:00:00:00:06
IP Address: 176.16.2.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

Broadband Information for WAN1

MAC Address: 00:00:00:00:11:22
IPv4 Address: 10.139.54.228 / 255.255.255.248
IPv6 Address: ::ffff:0:a86:5d9 / 96, fe80::200:ff:fe00:1122 / 64
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: STATIC
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connected
Link State: LINK UP
Upload Connection Speed: 1500
Download Connection Speed: 1000000
Gateway: 10.139.54.225
Primary DNS: 10.80.130.23
Secondary DNS: 8.8.8.8
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):

Broadband Information for WAN2

MAC Address: 00:00:00:00:00:01
IPv4 Address: 0.0.0.0 / 0.0.0.0
IPv6 Address:
Wan State: DOWN
NAT (IPv4 only): Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Not Yet Connected
IPv6 Connection State: Not Yet Connected
Link State: LINK DOWN
Upload Connection Speed: 1000000
Download Connection Speed: 1000000
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):

Broadband Information for WAN3

MAC Address: 00:00:00:00:00:01
IPv4 Address: 0.0.0.0 / 0.0.0.0
IPv6 Address:
Wan State: DOWN
NAT (IPv4 only): Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Not Yet Connected
IPv6 Connection State: Not Yet Connected
Link State: LINK DOWN
Upload Connection Speed: 1000000
Download Connection Speed: 1000000
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):

Broadband Information for WAN4

MAC Address: 00:00:00:00:00:01
IPv4 Address: 0.0.0.0 / 0.0.0.0
IPv6 Address: fe80::21e:2aff:fe3d:284a / 64
Wan State: DOWN
NAT (IPv4 only): Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Not Yet Connected
IPv6 Connection State: Not Yet Connected
Link State: LINK DOWN
Upload Connection Speed: 1000000
Download Connection Speed: 1000000
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):

**WAN Traffic Meter Show Command**

*show system traffic_meter setup <wan interface>*

This command displays the configuration of the traffic meter and the Internet traffic statistics. For the WAN interface, type **WAN1, WAN2, WAN3, or WAN4**.

Enable Traffic Meter

<table>
<thead>
<tr>
<th>Traffic Meter is Enabled</th>
</tr>
</thead>
</table>

Limit Type Both Directions

<table>
<thead>
<tr>
<th>Monthly Limit in (MB): 255000</th>
</tr>
</thead>
</table>

Increase this month limit: Enabled

<table>
<thead>
<tr>
<th>Increase limit by in (MB): 125000</th>
</tr>
</thead>
</table>

This month limit:

<table>
<thead>
<tr>
<th>Traffic Counter</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Traffic Counter: Specific Time</th>
</tr>
</thead>
</table>

Restart Time (HH:MM-Day of Month): 12:0 AM - 1
Send e-mail before restarting: Enabled
When Limit is reached

<table>
<thead>
<tr>
<th>Show Commands</th>
</tr>
</thead>
</table>

306
Traffic Block Status: Block All Traffic Except Email

Send e-mail alert: Enabled

Internet Traffic Statistics


Outgoing Traffic Volume: 0
Incoming Traffic Volume: 0
Average per day: 0
% of Standard Limit: 0
% of this Month's Limit: 0

Logging Configuration Show Commands

**show system logging setup**

This command displays the configuration of the IPv4 and IPv6 logs:

Logging Config

Routing Logs

LAN to WAN

Accepted Packets: Disabled
Dropped Packets: Disabled

WAN to LAN

Accepted Packets: Disabled
Dropped Packets: Disabled

DMZ to WAN

Accepted Packets: Disabled
Dropped Packets: Disabled
### ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

#### WAN to DMZ
- **Accepted Packets:** Disabled
- **Dropped Packets:** Disabled

#### LAN to DMZ
- **Accepted Packets:** Disabled
- **Dropped Packets:** Disabled

#### DMZ to LAN
- **Accepted Packets:** Disabled
- **Dropped Packets:** Disabled

#### System Logs
- **Change of time by NTP:** Disabled
- **Login attempts:** Disabled
- **Secure Login attempts:** Disabled
- **Reboots:** Disabled
- **All Unicast Traffic:** Disabled
- **All Broadcast/Multicast Traffic:** Disabled
- **WAN Status:** Disabled
- **Resolved DNS Names:** Disabled
- **VPN Logs:** Disabled
- **DHCP Server:** Disabled

#### Other Event Logs
- **Source MAC Filter:** Disabled
- **Session Limit:** Disabled
- **Bandwidth Limit:** Disabled
**show system logging remote setup**

This command displays the configuration and the schedule of the email logs:

Log Identifier: SRX5308-BLD3

Enable E-Mail Logs

__________________

E-Mail Server Address: SMTP.Netgear.com
Return E-Mail Address: SRX5308@netgear.com
Send to E-Mail Address: admin2@netgear.com
Authentication: No Authentication
Respond to Identd from SMTP Server: N

Send E-mail logs by Schedule

____________________________

Unit: Weekly
Day: Sunday
Time: 03 AM

Syslog Configuration

____________________

Syslog Server: Disabled

**Logs Show Commands**

**show system logs**

This command displays the system logs (the following example shows only part of the command output):

Tue Jul 10 10:23:55 2012 (GMT -0800) [SRX5308][Kernel][KERNEL] p->perfect 0000000000000000 p->h a80000417bab200
Tue Jul 10 10:23:55 2012 (GMT -0800) [SRX5308][Kernel][KERNEL] HTB: quantum of class 10001 is big. Consider r2q change.
Tue Jul 10 10:24:00 2012 (GMT -0800) [SRX5308][Kernel][KERNEL] eth0.1: del 01:00:5e:7f:ff:fa mcast address from master interface
Tue Jul 10 10:24:00 2012 (GMT -0800) [SRX5308][Kernel][KERNEL] eth0.1: add
01:00:5e:7f:ff:fa mcast address to master interface
Tue Jul 10 10:24:00 2012 (GMT -0800) [SRX5308][Kernel][KERNEL]
tcindex_destroy(tp a800000416f94600),p a80000041696d680
Tue Jul 10 10:24:00 2012 (GMT -0800) [SRX5308][Kernel][KERNEL] tcindex_walk(tp
a800000416f94600,walker a800000415f4f900),p a80000041696d680
Tue Jul 10 10:24:00 2012 (GMT -0800) [SRX5308][Kernel][KERNEL] tcindex_delete(tp
a800000416f94600,arg 0xa800000416981e08),p a80000041696d680,f 0000000000000000

**show sysinfo**

This command displays system information, including MAC addresses, serial number, and
firmware version:

System - Manufacturer Information
******************************
hwver: 00:00:A0:03reginfo: 0x0005
numofimages : 1

currimage: 1
mac address : E0469A1D1A9C

vlan[0] MAC : e0469ald1a9f
vlan[1] MAC : e0469ald1aa0
vlan[2] MAC : e0469ald1aa1
vlan[3] MAC : e0469ald1aa2
vlan[4] MAC : e0469ald1aa3
vlan[5] MAC : e0469ald1aa4
vlan[7] MAC : e0469ald1aa6
vlan[8] MAC : e0469ald1aa7
vlan[9] MAC : e0469ald1aa8
vlan[10] MAC : e0469ald1aa9
vlan[12] MAC : e0469ald1aab
vlan[13] MAC : e0469ald1aac
vlan[14] MAC : e0469ald1aad
WAN MAC : e0469ald1a9d

pcbasn number : S.YXZ18U00E0
serial number : 2JF119BY001B0

image 0 : 4.1.1-8
image 1 : 0
productId : SRX5308

mac0cnt0: 0x22
mac0cnt1: 0x0
mac0cnt2: 0x0
mac0cnt3: 0x0
**************************

### VPN Settings (VPN Mode) Show Commands

This section contains the following subsections:

- **IPSec VPN Show Commands**
- **SSL VPN Show Commands**
- **SSL VPN User Show Commands**
- **RADIUS Server Show Command**
- **PPTP Server Show Commands**
- **L2TP Server Show Commands**

#### IPSec VPN Show Commands

**show vpn ipsec ikepolicy setup**

This command displays the IKE policies:

*List of IKE Policies*

<table>
<thead>
<tr>
<th>Name</th>
<th>Mode</th>
<th>Local ID</th>
<th>Remote ID</th>
<th>Encryption</th>
<th>Authentication</th>
<th>DH Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>iphone</td>
<td>aggressive</td>
<td>10.139.54.228</td>
<td>0.0.0.0</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>Group 2 (1024 bit)</td>
</tr>
<tr>
<td>SRX5308-to-Peer44</td>
<td>main</td>
<td>fe80::a8ab:bbff:fe00:2</td>
<td>peer44.com</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Group 2 (1024 bit)</td>
</tr>
<tr>
<td>SRX-to-Paris</td>
<td>main</td>
<td>10.139.54.228</td>
<td>10.112.71.154</td>
<td>3DES</td>
<td>SHA-1</td>
<td>Group 2 (1024 bit)</td>
</tr>
</tbody>
</table>

**show vpn ipsec vpnpolicy setup**

This command displays the IPSec VPN policies:

*Status Name* | *Type* | *IPSec Mode* | *Local* | *Remote* | *Auth* | *Encr* |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled SRX5308-to-Peer44</td>
<td>Auto Policy Tunnel Mode</td>
<td>2002:408b:36e4:a8ab:bbff:fe00:1 / 64</td>
<td>64</td>
<td>SHA-1</td>
<td>3DES</td>
<td></td>
</tr>
<tr>
<td>Enabled SRX-to-Paris</td>
<td>Auto Policy Tunnel Mode</td>
<td>192.168.1.0 / 255.255.255.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show vpn ipsec vpnpolicy status

This command displays status information about the active and nonactive IPSec VPN policies.

Note: This example does not relate to the previous two examples, nor to the examples in Chapter 8, VPN Settings (VPN Mode) Show Commands.

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Policy Name</th>
<th>Endpoint</th>
<th>tx ( KB )</th>
<th>tx ( Packets )</th>
<th>State</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GW1-to-GW2</td>
<td>10.144.28.226</td>
<td>0.00</td>
<td>0</td>
<td>IPsec SA Not Established</td>
<td>Connect</td>
</tr>
<tr>
<td>2</td>
<td>SRX-to-IPv6Peer</td>
<td>2001::da21:1316:dfee:e33c</td>
<td>0.00</td>
<td>0</td>
<td>IPsec SA Not Established</td>
<td>Connect</td>
</tr>
<tr>
<td>3</td>
<td>10.100.10.1</td>
<td>10.153.46.120</td>
<td>7.01</td>
<td>31</td>
<td>IPsec SA Established</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>10.100.10.2</td>
<td>10.153.46.120</td>
<td>6.68</td>
<td>29</td>
<td>IPsec SA Established</td>
<td>Drop</td>
</tr>
</tbody>
</table>

show vpn ipsec mode_config setup

This command displays the Mode Config records:

List of Mode Config Records

<table>
<thead>
<tr>
<th>Record Name</th>
<th>Pool Start IP</th>
<th>Pool End IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMEA Sales</td>
<td>172.16.100.1</td>
<td>172.16.100.99</td>
</tr>
<tr>
<td>iphone</td>
<td>192.168.22.1</td>
<td>192.168.22.2</td>
</tr>
</tbody>
</table>

show vpn ipsec logs

This command displays the IPSec VPN logs (the following example shows only part of the command output):

Wed Jul 11 12:24:36 2012 (GMT -0800): [SRX5308] [IKE] INFO: Re-using previously generated policy: 100.10.10.2/32[0] 0.0.0.0/0[0] proto=any dir=in
Wed Jul 11 12:24:36 2012 (GMT -0800): [SRX5308] [IKE] INFO: IPsec-SA established: ESP/Tunnel 173.11.109.158->64.139.54.228 with spi=73255174(0x45dc906)
Wed Jul 11 12:24:36 2012 (GMT -0800): [SRX5308] [IKE] INFO: IPsec-SA established: ESP/Tunnel 10.139.54.228->172.11.109.158 with spi=7343706(0x700e5a)
SSL VPN Show Commands

**show vpn sslvpn client**

This command displays the SSL VPN client ranges and configurations:

SSL VPN Client(IPv4)
_____________

Enable Full Tunnel Support: Yes
DNS Suffix:
Primary DNS Server: 192.168.10.5
Secondary DNS Server: 192.168.10.6
Client Address Range Begin: 192.168.251.1
Client Address Range End: 192.168.251.254

SSL VPN Client(IPv6)
_____________

Enable Full Tunnel Support: No
DNS Suffix:
Primary DNS Server:
Secondary DNS Server:
Client Address Range Begin: 4000::1
Client Address Range End: 4000::200

**show vpn sslvpn logs**

This command displays the SSL VPN logs (the following example shows only part of the command output):

Mon Jul  9 11:00:18 2012(GMT -0800) [SRX5308][SSLVPN][SSLVPN] SSL_INFO : Login Successful for geardomain user admin(Admin) from host 10.110.205.58
Mon Jul  9 12:04:09 2012(GMT -0800) [SRX5308][SSLVPN][SSLVPN] SSL_INFO : user admin is Logged-Out successfully from host 10.110.205.58
Mon Jul  9 12:04:20 2012(GMT -0800) [SRX5308][SSLVPN][SSLVPN] SSL_INFO : Login Successful for geardomain user techwriter(Admin) from host 10.110.205.58
Mon Jul  9 16:00:34 2012(GMT -0800) [SRX5308][SSLVPN][SSLVPN] SSL_INFO : Login Successful for geardomain user techwriter(Admin) from host 10.110.205.58
Mon Jul  9 16:10:54 2012(GMT -0800) [SRX5308][SSLVPN][SSLVPN] SSL_INFO : Login Successful for geardomain user admin(Admin) from host 10.110.205.58
**show vpn sslvpn policy**

This command displays the SSL VPN policies:

**SSL VPN Policies**

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Policy Name</th>
<th>Policy Type</th>
<th>Service Type</th>
<th>Destination Object</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RoadWarriorPolicy</td>
<td>global</td>
<td>VPN Tunnel</td>
<td>RoadWarrior</td>
<td>Permit</td>
</tr>
<tr>
<td>2</td>
<td>RoadWarriorPolicyII</td>
<td>global</td>
<td>VPN Tunnel</td>
<td>10.201.33.200:35401-35405</td>
<td>Deny</td>
</tr>
<tr>
<td>3</td>
<td>GuestFTPPolicy</td>
<td>user</td>
<td>Port Forwarding</td>
<td>0.0.0.0:25077-25078</td>
<td>Deny</td>
</tr>
</tbody>
</table>

**show vpn sslvpn portal_layouts**

This command displays the SSL VPN portal layouts:

**List of Layouts**

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Layout Name</th>
<th>Description</th>
<th>Use Count</th>
<th>Portal URL (IPv4)</th>
<th>Portal URL (IPv6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSL-VPN*</td>
<td>Welcome to Netgear Configur...</td>
<td>4</td>
<td><a href="https://10.139.54.228/portal/SSL-VPN">https://10.139.54.228/portal/SSL-VPN</a></td>
<td>https://[fe80::e246:9aff:fe1d:1a9d]/portal/SSL-VPN</td>
</tr>
<tr>
<td>2</td>
<td>CSup</td>
<td>In case of login difficulty...</td>
<td>1</td>
<td><a href="https://10.139.54.228/portal/CSup">https://10.139.54.228/portal/CSup</a></td>
<td>https://[fe80::e246:9aff:fe1d:1a9d]/portal/CSup</td>
</tr>
</tbody>
</table>

**show vpn sslvpn portforwarding appconfig**

This command displays the SSL VPN port forwarding application configuration:

**Port Forwarding Application Configuration**

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Server IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.51.227</td>
<td>3389</td>
</tr>
<tr>
<td>2</td>
<td>192.168.51.230</td>
<td>4009</td>
</tr>
</tbody>
</table>
show vpn sslvpn portforwarding hostconfig

This command displays the SSL VPN port forwarding host configuration:

Port Forwarding Host Configuration

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Server IP</th>
<th>FQDN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.51.227</td>
<td>RemoteDesktop</td>
</tr>
<tr>
<td>2</td>
<td>192.168.51.230</td>
<td>Support.app.com</td>
</tr>
</tbody>
</table>

show vpn sslvpn resource

This command displays the SSL VPN resource configuration:

RESOURCES

<table>
<thead>
<tr>
<th>Row Id</th>
<th>Resource Name</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TopSecure</td>
<td>Port Forwarding</td>
</tr>
<tr>
<td>2</td>
<td>FTPServer</td>
<td>Port Forwarding</td>
</tr>
<tr>
<td>3</td>
<td>RoadWarrior</td>
<td>VPN Tunnel</td>
</tr>
</tbody>
</table>

show vpn sslvpn resource_object <resource name>

This command displays the detailed configuration for the specified resource object. Type the name of a resource object that is displayed in the output of the show vpn sslvpn resource command.

RESOURCE OBJECTS

<table>
<thead>
<tr>
<th>Row Id: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Type: IP Address</td>
</tr>
<tr>
<td>Object Address: 192.168.144.23</td>
</tr>
<tr>
<td>Mask Length: 32</td>
</tr>
<tr>
<td>Start Port: 40133</td>
</tr>
<tr>
<td>End Port: 40140</td>
</tr>
</tbody>
</table>
show vpn sslvpn route

This command displays the SSL VPN client routes:

Configured Client Routes

<table>
<thead>
<tr>
<th>Row</th>
<th>Destination Network</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.4.20</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>2</td>
<td>2001:abcf:1241:dffe::22</td>
<td>10</td>
</tr>
</tbody>
</table>

SSL VPN User Show Commands

show vpn sslvpn users domains

This command displays the domain configurations:

List of Domains

<table>
<thead>
<tr>
<th>Row_Id</th>
<th>Domain Name</th>
<th>Authentication Type</th>
<th>Portal Layout Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>geardomain*</td>
<td>Local User Database</td>
<td>SSL-VPN</td>
</tr>
<tr>
<td>2</td>
<td>Headquarter</td>
<td>LDAP</td>
<td>CSup</td>
</tr>
<tr>
<td>3</td>
<td>LevelI_Support</td>
<td>Local User Database</td>
<td>SSL-VPN</td>
</tr>
<tr>
<td>4</td>
<td>TEST</td>
<td>wikid_pap</td>
<td>SSL-VPN</td>
</tr>
</tbody>
</table>

show vpn sslvpn users groups

This command displays the group configurations:

List of Groups

<table>
<thead>
<tr>
<th>Row_Id</th>
<th>Name</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>geardomain*</td>
<td>geardomain</td>
</tr>
<tr>
<td>2</td>
<td>Headquarter</td>
<td>Headquarter</td>
</tr>
<tr>
<td>3</td>
<td>Sales</td>
<td>Headquarter</td>
</tr>
<tr>
<td>4</td>
<td>LevelI_Support</td>
<td>LevelI_Support</td>
</tr>
<tr>
<td>5</td>
<td>TEST</td>
<td>TEST</td>
</tr>
</tbody>
</table>
**show vpn sslvpn users users**

This command displays the user account configurations:

List of Users

<table>
<thead>
<tr>
<th>Row_Id</th>
<th>User Name</th>
<th>Group</th>
<th>Type</th>
<th>Authentication Domain</th>
<th>Login Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>admin*</td>
<td>geardomain</td>
<td>Administrator</td>
<td>geardomain</td>
<td>Enabled (LAN and WAN)</td>
</tr>
<tr>
<td>2</td>
<td>guest*</td>
<td>geardomain</td>
<td>Guest</td>
<td>geardomain</td>
<td>Enabled (LAN only)</td>
</tr>
<tr>
<td>3</td>
<td>admin2</td>
<td>geardomain</td>
<td>Administrator</td>
<td>geardomain</td>
<td>Enabled (LAN and WAN)</td>
</tr>
<tr>
<td>4</td>
<td>PeterBrown</td>
<td>Sales</td>
<td>SSL VPN User</td>
<td>Headquarter</td>
<td>Enabled (LAN and WAN)</td>
</tr>
<tr>
<td>5</td>
<td>JohnD_Company</td>
<td>LevelI_Support</td>
<td>SSL VPN User</td>
<td>LevelI_Support</td>
<td>Enabled (LAN and WAN)</td>
</tr>
<tr>
<td>6</td>
<td>chin</td>
<td>geardomain</td>
<td>Administrator</td>
<td>geardomain</td>
<td>Enabled (LAN and WAN)</td>
</tr>
<tr>
<td>7</td>
<td>iphone</td>
<td></td>
<td>IPSEC VPN User</td>
<td></td>
<td>Enabled (LAN and WAN)</td>
</tr>
</tbody>
</table>

**show vpn sslvpn users login_policies <row id>**

*Note:* The row ID refers to the List of Users table in the output of the `show vpn sslvpn users users` command.

This command displays the login restrictions based on login policies for the specified user:

User Login Policies

User Name: PeterBrown
Disable Login: No
Deny Login from Wan Interface: No
show vpn sslvpn users ip_policies <row id>

**Note:** The row ID refers to the List of Users table in the output of the `show vpn sslvpn users users` command.

This command displays the login restrictions based on IP addresses for the specified user:

**User Ip Policies**

User Name: PeterBrown
Allow Login from Defined Address: Yes

**Ip Addresses**

Row_Id: 1
Source Address Type: IP Address
Network/IP Address: 10.156.127.39
Mask Length: 32

show vpn sslvpn users browser_policies <row id>

**Note:** The row ID refers to the List of Users table in the output of the `show vpn sslvpn users users` command.

This command displays the login restrictions based on web browsers for the specified user:

**User Browser Policies**

User Name: PeterBrown
Allow Login from Defined Browser: No

**Defined Browsers**

Internet Explorer
Netscape Navigator
show vpn sslvpn users active_users

This command displays the active SSL VPN users:

UserName: : admin
GroupName: : geardomain
LoginAddress: : 10.116.205.166
LoginTime: : Thu Jul 12 10:31:38 2012 (GMT -0800)

RADIUS Server Show Command

show vpn ipsec radius [ipaddress]

This command displays the configuration of all RADIUS servers or of a specified RADIUS server:

• All RADIUS Servers:
  
  SRX5308> show vpn ipsec radius

  Configured RADIUS Client

  ____________________________
  Server IP   Server Port Timeout Retries NAS Identifier
  _______________ ___________ _______ _______ ______________
  192.168.4.2 1812        30      4       SRX5308
  192.168.4.3 1812        30      4       SRX5308

• A specified RADIUS server:
  
  SRX5308> show vpn ipsec radius 192.168.4.2

  RADIUS Configuration

  ____________________________
  Auth Server IP Address: 192.168.4.2
  Auth Port: 1812
  Timeout (in seconds): 30
  Retries: 4
  Secret: sharedsecret
  NAS Identifier: SRX5308
PPTP Server Show Commands

`show vpn pptp server setup`
This command displays the configuration of the PPTP server:

PPTP Server Configuration

PPTP Server Status: Enabled
PPTP Starting IP Address: 10.119.215.1
PPTP server Ending IP Address: 10.119.215.26
PPTP server Idle Timeout: 999

`show vpn pptp server connections`
This command displays the users that are connected through the PPTP server:

List of PPTP Active Users

L2TP Server Show Commands

`show vpn l2tp server setup`
This command displays the configuration of the L2TP server:

L2TP Server Configuration

L2TP Server Status: Enabled
L2TP Starting IP Address: 192.168.112.1
L2TP server Ending IP Address: 192.168.112.25
L2TP server Idle Timeout: 10

`show vpn l2tp server connections`
This command displays the users that are connected through the L2TP server:

List of L2TP Active Users
This chapter explains the configuration commands, keywords, and associated parameters in the Util mode. The chapter includes the following sections:

- Overview Util Commands
- Firmware Backup, Restore, and Upgrade Commands
- Diagnostic Commands

**Overview Util Commands**

Enter the `util ?` command at the CLI prompt to display the utility commands in the util mode. The following table lists the commands in alphabetical order:

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>util backup_configuration</code></td>
<td>Back up the configuration file of the VPN firewall to a TFTP server.</td>
</tr>
<tr>
<td><code>util dns_lookup</code></td>
<td>Look up the IP address of a domain name.</td>
</tr>
<tr>
<td><code>util firmware_upgrade</code></td>
<td>Upgrade the firmware of the VPN firewall from a TFTP server.</td>
</tr>
<tr>
<td><code>util ping</code></td>
<td>Ping an IP address.</td>
</tr>
<tr>
<td><code>util ping_through_vpn_tunnel</code></td>
<td>Ping a VPN endpoint IP address.</td>
</tr>
<tr>
<td><code>util reboot</code></td>
<td>Reboot the VPN firewall.</td>
</tr>
<tr>
<td><code>util restore_factory_defaults</code></td>
<td>Restore the VPN firewall to factory default settings.</td>
</tr>
<tr>
<td><code>util routing_table_ipv4</code></td>
<td>Display the IPv4 routing table.</td>
</tr>
<tr>
<td><code>util routing_table_ipv6</code></td>
<td>Display the IPv6 routing table.</td>
</tr>
<tr>
<td><code>util traceroute</code></td>
<td>Trace a route to an IP address.</td>
</tr>
<tr>
<td><code>util upload_configuration</code></td>
<td>Upload a previously backed-up configuration file of the VPN firewall from a TFTP server</td>
</tr>
</tbody>
</table>
Firmware Backup, Restore, and Upgrade Commands

util backup_configuration

This command backs up the configuration file of the VPN firewall to a TFTP server.

Format               util backup_configuration <destination file name> <tftp server address>
Mode                  util

util upload_configuration

This command uploads a previously backed-up configuration file of the VPN firewall from a TFTP server.

Format               util upload_configuration <source file name> <tftp server address>
Mode                  util

util firmware_upgrade

This command upgrades the firmware of the VPN firewall from a TFTP server.

Format               util firmware_upgrade <source file name> <tftp server address>
Mode                  util

util reboot

This command reboots the VPN firewall. It takes about 3 minutes for the VPN firewall to come back up.

Format               util reboot
Mode                  util
**util restore_factory_defaults**

This command restores the VPN firewall to factory default settings. It takes about 3 minutes for the VPN firewall to come back up.

**Format**

```
util restore_factory_defaults
```

**Mode**

```
util
```

---

**Diagnostic Commands**

**util dns_lookup**

This command looks up the IP address of a domain name.

**Format**

```
util dns_lookup <domain name>
```

**Mode**

```
util
```

SRX5308> util dns_lookup netgear.com
Server: 66.80.130.23
Address 1: 66.80.130.23 ns1.megapath.net
Name: netgear.com
Address 1: 206.16.44.90

---

**util ping**

This command pings an IP address with 56 data bytes and displays the ping information.

**Format**

```
util ping <ipaddress>
```

**Mode**

```
util
```

SRX5308> util ping 10.136.216.82
PING 10.136.216.82 (10.136.216.82): 56 data bytes
64 bytes from 10.136.216.82: seq=0 ttl=48 time=69.168 ms
64 bytes from 10.136.216.82: seq=1 ttl=48 time=112.606 ms
64 bytes from 10.136.216.82: seq=2 ttl=48 time=46.531 ms
64 bytes from 10.136.216.82: seq=3 ttl=48 time=49.804 ms
64 bytes from 10.136.216.82: seq=4 ttl=48 time=51.247 ms
--- 10.136.216.82 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 46.531/65.871/112.606 ms

---
**util ping_through_vpn_tunnel**

This command pings a VPN endpoint IP address with 56 data bytes through a VPN tunnel and displays the ping information.

**Format**

util ping_through_vpn_tunnel <ipaddress>

**Mode**

util

SRX5308> util ping_through_vpn_tunnel 10.136.24.128
Pinging 192.168.1.1 from 5
Ping passed
64 bytes from 10.136.24.128: icmp_seq=0 ttl=64
64 bytes from 10.136.24.128: icmp_seq=1 ttl=64
64 bytes from 10.136.24.128: icmp_seq=2 ttl=64
64 bytes from 10.136.24.128: icmp_seq=3 ttl=64
64 bytes from 10.136.24.128: icmp_seq=4 ttl=64

---

**util traceroute**

This command traces a route to an IP address.

**Format**

util traceroute <ipaddress>

**Mode**

util

SRX5308> util traceroute 10.136.24.128
traceroute to 10.136.24.128 (10.136.24.128), 30 hops max, 40 byte packets
1   (10.136.24.128)  0.516 ms  0.227 ms  0.218 ms

---

**util routing_table_ipv4**

This command displays the IPv4 routing table.

**Format**

util routing_table_ipv4

**Mode**

util

---

**util routing_table_ipv6**

This command displays the IPv6 routing table.

**Format**

util routing_table_ipv6

**Mode**

util
CLI Command Index

N
net ddns configure 53
net dmz ipv4 configure 74
net dmz ipv6 configure 76
net dmz ipv6 pool configure 77
net ethernet configure 58
net ipv6 ipmode configure 46
net ipv6_tunnel isatap add 50
net ipv6_tunnel isatap delete 52
net ipv6_tunnel isatap edit 51
net ipv6_tunnel six_to_four configure 52
net lan dhcp reserved_ip configure 60
net lan dhcp reserved_ip delete 62
net lan ipv4 advanced configure 59
net lan ipv4 configure 54
net lan ipv4 default_vlan 59
net lan ipv4 delete 57
net lan ipv4 disable 57
net lan ipv4 enable 57
net lan ipv4 multi_homing add 62
net lan ipv4 multi_homing delete 63
net lan ipv4 multi_homing edit 63
net lan ipv4 traffic_meter configure 64
net lan ipv4 traffic_meter delete 66
net lan ipv6 configure 66
net lan ipv6 multi_homing add 69
net lan ipv6 multi_homing delete 71
net lan ipv6 multi_homing edit 70
net lan ipv6 pool add 68
net lan ipv6 pool delete 69
net lan ipv6 pool edit 68
net lan ipv6 prefix_delegation add 72
net lan ipv6 prefix_delegation delete 74
net lan ipv6 prefix_delegation edit 73
net lan lan_groups edit 62
net protocol_binding add 39
net protocol_binding delete 45
net protocol_binding disable 45
net protocol_binding edit 42
net protocol_binding enable 46
net qos configure 80
net qos profile add 81
net qos profile delete 92
net qos profile disable 92
net qos profile edit 86
net qos profile enable 93
net radvd configure dmz 78
net radvd configure lan 71
net radvd pool dmz delete 78
net routing dynamic configure 95
net routing static ipv4 configure 93
net routing static ipv4 delete 94
net routing static ipv4 delete_all 95
net routing static ipv6 configure 98
net routing static ipv6 delete 99
net routing static ipv6 delete_all 100
net siit configure 50
net wan port_setup configure 27
net wan wan ipv4 secondary_address add 37
net wan wan ipv4 secondary_address delete 37
net wan wan1 ipv4 configure 32
net wan wan1 ipv6 configure 47
net wan_settings load_balancing configure 38
net wan_settings wanmode configure 31

S
security address_filter ip_or_mac_binding add 170
security address_filter ip_or_mac_binding delete 172
security address_filter ip_or_mac_binding edit 171
security address_filter ip_or_mac_binding enable_email_log 172
security address_filter mac_filter configure 168
security address_filter mac_filter source add 169
security address_filter mac_filter source delete 170
security bandwidth enable_bandwidth_profiles 177
security bandwidth profile add 177
security bandwidth profile delete 179
security bandwidth profile edit 178
security content_filter blocked_keywords add 183
security content_filter blocked_keywords delete 184
ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

vpn sslvpn client ipv4 248
vpn sslvpn client ipv6 250
vpn sslvpn policy add 256
vpn sslvpn policy delete 263
vpn sslvpn policy edit 261
vpn sslvpn portal_layouts add 231
vpn sslvpn portal_layouts delete 234
vpn sslvpn portal_layouts edit 232
vpn sslvpn portal_layouts set-default 234
vpn sslvpn portforwarding appconfig add 246
vpn sslvpn portforwarding appconfig delete 247
vpn sslvpn portforwarding hostconfig add 247
vpn sslvpn portforwarding hostconfig delete 248
vpn sslvpn resource add 252
vpn sslvpn resource configure add 253
vpn sslvpn resource configure delete 255
vpn sslvpn resource delete 253
vpn sslvpn route add 251
vpn sslvpn route delete 252
vpn sslvpn users domains add 234
vpn sslvpn users domains delete 237
vpn sslvpn users domains disable_Local_Authentication 237
vpn sslvpn users domains edit 236
vpn sslvpn users groups add 238
vpn sslvpn users groups delete 239
vpn sslvpn users groups edit 238
vpn sslvpn users users add 239
vpn sslvpn users users browser_policies 245
vpn sslvpn users users delete 241
vpn sslvpn users users edit 241
vpn sslvpn users users ip_policies configure 242
vpn sslvpn users users ip_policies delete 245
vpn sslvpn users users login_policies 242