



---

Junos<sup>®</sup> OS

# Security Zones and Interfaces Feature Guide for Security Devices

Release

12.1X47-D10



---

Modified: 2015-12-23

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

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

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

*Junos<sup>®</sup> OS Security Zones and Interfaces Feature Guide for Security Devices*  
12.1X47-D10  
Copyright © 2015, Juniper Networks, Inc.  
All rights reserved.

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

#### YEAR 2000 NOTICE

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

#### END USER LICENSE AGREEMENT

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

# Table of Contents

	About the Documentation . . . . .	xi
	Documentation and Release Notes . . . . .	xi
	Supported Platforms . . . . .	xi
	Using the Examples in This Manual . . . . .	xi
	Merging a Full Example . . . . .	xii
	Merging a Snippet . . . . .	xii
	Documentation Conventions . . . . .	xiii
	Documentation Feedback . . . . .	xv
	Requesting Technical Support . . . . .	xv
	Self-Help Online Tools and Resources . . . . .	xv
	Opening a Case with JTAC . . . . .	xvi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Security Zones . . . . .</b>	<b>3</b>
	Security Zones and Interfaces Overview . . . . .	3
	Understanding Security Zone Interfaces . . . . .	4
	Understanding Functional Zones . . . . .	4
	Understanding Security Zones . . . . .	4
<b>Chapter 2</b>	<b>Inbound Traffic . . . . .</b>	<b>7</b>
	Understanding How to Control Inbound Traffic Based on Traffic Types . . . . .	7
	Understanding How to Control Inbound Traffic Based on Protocols . . . . .	8
<b>Chapter 3</b>	<b>TCP-Reset Parameters . . . . .</b>	<b>11</b>
	Understanding How to Identify Duplicate Sessions Using the TCP-Reset Parameter . . . . .	11
<b>Chapter 4</b>	<b>DNS . . . . .</b>	<b>13</b>
	DNS Overview . . . . .	13
	DNS Components . . . . .	13
	DNS Server Caching . . . . .	13
	DNSSEC Overview . . . . .	14
	DNS Proxy Overview . . . . .	14
	DNS Proxy Cache . . . . .	15
	DNS Proxy with Split DNS . . . . .	15
	Dynamic Domain Name System Client . . . . .	17
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 5</b>	<b>Security Zones . . . . .</b>	<b>23</b>
	Example: Creating Security Zones . . . . .	23

<b>Chapter 6</b>	<b>Inbound Traffic</b> . . . . .	<b>27</b>
	Supported System Services for Host Inbound Traffic . . . . .	27
	Example: Controlling Inbound Traffic Based on Traffic Types . . . . .	29
	Example: Controlling Inbound Traffic Based on Protocols . . . . .	32
<b>Chapter 7</b>	<b>TCP-Reset Parameter</b> . . . . .	<b>35</b>
	Example: Configuring the TCP-Reset Parameter . . . . .	35
<b>Chapter 8</b>	<b>DNS</b> . . . . .	<b>37</b>
	Example: Configuring the TTL Value for DNS Server Caching . . . . .	37
	Example: Configuring DNSSEC . . . . .	38
	Example: Configuring Keys for DNSSEC . . . . .	38
	Example: Configuring Secure Domains and Trusted Keys for DNSSEC . . . . .	39
	Configuring the Device as a DNS Proxy . . . . .	41
<b>Chapter 9</b>	<b>Configuration Statements</b> . . . . .	<b>43</b>
	Security Configuration Statement Hierarchy . . . . .	43
	[edit security zones] Hierarchy Level . . . . .	45
	address (Security Address Book) . . . . .	47
	address-set . . . . .	48
	application-tracking (Security Zones) . . . . .	49
	description (Security Zone) . . . . .	50
	dns-proxy . . . . .	51
	dynamic-dns . . . . .	52
	forward-only (DNS) . . . . .	53
	functional-zone . . . . .	54
	host-inbound-traffic . . . . .	55
	interfaces (Security Zones) . . . . .	56
	management (Security Zones) . . . . .	57
	protocols (Security Zones Host Inbound Traffic) . . . . .	58
	protocols (Security Zones Interfaces) . . . . .	60
	screen (Security Zones) . . . . .	61
	secure-domains . . . . .	61
	secure-neighbor-discovery . . . . .	62
	security-zone . . . . .	63
	system-services (Security Zones Host Inbound Traffic) . . . . .	65
	system-services (Security Zones Interfaces) . . . . .	67
	tcp-rst . . . . .	68
	traceoptions (System Services DNS) . . . . .	69
	vrrp . . . . .	71
	zones . . . . .	72
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 10</b>	<b>Operational Commands</b> . . . . .	<b>77</b>
	clear system services dns dns-proxy . . . . .	78
	show security zones . . . . .	79
	show security zones type . . . . .	82
	show system services dns dns-proxy . . . . .	85
	show system services dynamic-dns . . . . .	88

## Part 4

## Index

Index .....	93
-------------	----



# List of Figures

Part 1	Overview	
Chapter 4	DNS .....	13
	Figure 1: DNS Proxy with Split DNS .....	16
	Figure 2: Dynamic DNS .....	18



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>xi</b>
	Table 1: Notice Icons . . . . .	xiii
	Table 2: Text and Syntax Conventions . . . . .	xiii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Inbound Traffic . . . . .</b>	<b>7</b>
	Table 3: Supported Inbound System Protocols . . . . .	8
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 6</b>	<b>Inbound Traffic . . . . .</b>	<b>27</b>
	Table 4: System Services for Host Inbound Traffic . . . . .	27
	Table 5: Protocols for Host Inbound Traffic . . . . .	28
<b>Chapter 9</b>	<b>Configuration Statements . . . . .</b>	<b>43</b>
	Table 6: Category Names . . . . .	70
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 10</b>	<b>Operational Commands . . . . .</b>	<b>77</b>
	Table 7: show security zones Output Fields . . . . .	79
	Table 8: show security zones type Output Fields . . . . .	82
	Table 9: show system services dns-proxy . . . . .	85
	Table 10: show system services dynamic-dns . . . . .	88



# About the Documentation

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

## Documentation and Release Notes

---

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

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

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

## Supported Platforms

---

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

- [SRX Series](#)
- [LN Series](#)

## Using the Examples in This Manual

---

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

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

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

## Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

## Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the **load** command, see the *CLI User Guide*.

## Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"><li>Introduces or emphasizes important new terms.</li><li>Identifies guide names.</li><li>Identifies RFC and Internet draft titles.</li></ul>	<ul style="list-style-type: none"><li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li><li><i>Junos OS CLI User Guide</i></li><li>RFC 1997, <i>BGP Communities Attribute</i></li></ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name domain-name</b>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"><li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric metric&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(string1   string2   string3)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ community-ids ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

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

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

## Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:  
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:  
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

## Opening a Case with JTAC

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

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

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

## PART 1

# Overview

- [Security Zones on page 3](#)
- [Inbound Traffic on page 7](#)
- [TCP-Reset Parameters on page 11](#)
- [DNS on page 13](#)



## CHAPTER 1

# Security Zones

- [Security Zones and Interfaces Overview on page 3](#)
- [Understanding Functional Zones on page 4](#)
- [Understanding Security Zones on page 4](#)

## Security Zones and Interfaces Overview

---

**Supported Platforms**   [LN Series, SRX Series](#)

Interfaces act as a doorway through which traffic enters and exits a Juniper Networks device. Many interfaces can share exactly the same security requirements; however, different interfaces can also have different security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together into a single *security zone*.

A *security zone* is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies.

Security zones are logical entities to which one or more interfaces are bound. With many types of Juniper Networks devices, you can define multiple security zones, the exact number of which you determine based on your network needs.

On a single device, you can configure multiple security zones, dividing the network into segments to which you can apply various security options to satisfy the needs of each segment. At a minimum, you must define two security zones, basically to protect one area of the network from the other. On some security platforms, you can define many security zones, bringing finer granularity to your network security design—and without deploying multiple security appliances to do so.

From the perspective of security policies, traffic enters into one security zone and goes out on another security zone. This combination of a **from-zone** and a **to-zone** is defined as a *context*. Each context contains an ordered list of policies. For more information on policies, see *Security Policies Overview*.

This topic includes the following sections:

- [Understanding Security Zone Interfaces on page 4](#)

## Understanding Security Zone Interfaces

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone.

Through the policies you define, you can permit traffic between zones to flow in one direction or in both. With the routes that you define, you specify the interfaces that traffic from one zone to another must use. Because you can bind multiple interfaces to a zone, the routes you chart are important for directing traffic to the interfaces of your choice.

An interface can be configured with an IPv4 address, IPv6 address, or both.

### Related Documentation

- [Understanding Functional Zones on page 4](#)
- [Example: Creating Security Zones on page 23](#)
- [Understanding How to Control Inbound Traffic Based on Traffic Types on page 7](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## Understanding Functional Zones

**Supported Platforms**   [LN Series, SRX Series](#)

A functional zone is used for special purposes, like management interfaces. Currently, only the management (MGT) zone is supported. Management zones have the following properties:

- Management zones host management interfaces.
- Traffic entering management zones does not match policies; therefore, traffic cannot transit out of any other interface if it was received in the management interface.
- Management zones can only be used for dedicated management interfaces.

### Related Documentation

- [Security Zones and Interfaces Overview on page 3](#)
- [Example: Creating Security Zones on page 23](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## Understanding Security Zones

**Supported Platforms**   [LN Series, SRX Series](#)

Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them.

Security zones have the following properties:

- **Policies**—Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall. For more information, see *Security Policies Overview*.
- **Screens**—A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful. For more information, see *Reconnaissance Deterrence Overview*.
- **Address books**—IP addresses and address sets that make up an address book to identify its members so that you can apply policies to them. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and Domain Name System (DNS) names. For more information, see *Example: Configuring Address Books and Address Sets*.
- **TCP-RST**—When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set.
- **Interfaces**—List of interfaces in the zone.

Security zones have the following preconfigured zone:

- **Trust zone**—Available only in the factory configuration and is used for initial connection to the device. After you commit a configuration, the trust zone can be overridden.

**Related  
Documentation**

- [Security Zones and Interfaces Overview on page 3](#)
- [Understanding Functional Zones on page 4](#)
- [Example: Creating Security Zones on page 23](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*



## CHAPTER 2

# Inbound Traffic

- [Understanding How to Control Inbound Traffic Based on Traffic Types on page 7](#)
- [Understanding How to Control Inbound Traffic Based on Protocols on page 8](#)

## Understanding How to Control Inbound Traffic Based on Traffic Types

---

**Supported Platforms** [LN Series, SRX Series](#)

This topic describes how to configure zones to specify the kinds of traffic that can reach the device from systems that are directly connected to its interfaces.

Note the following:

- You can configure these parameters at the zone level, in which case they affect all interfaces of the zone, or at the interface level. (Interface configuration overrides that of the zone.)
- You must enable all expected host-inbound traffic. Inbound traffic destined to this device is dropped by default.
- You can also configure a zone's interfaces to allow for use by dynamic routing protocols.

This feature allows you to protect the device against attacks launched from systems that are directly or indirectly connected to any of its interfaces. It also enables you to selectively configure the device so that administrators can manage it using certain applications on certain interfaces. You can prohibit use of other applications on the same or different interfaces of a zone. For example, most likely you would want to ensure that outsiders not use the Telnet application from the Internet to log into the device because you would not want them connecting to your system.

**Related Documentation**

- [Security Zones and Interfaces Overview on page 3](#)
- [Supported System Services for Host Inbound Traffic on page 27](#)
- [Understanding How to Identify Duplicate Sessions Using the TCP-Reset Parameter on page 11](#)
- [Example: Controlling Inbound Traffic Based on Traffic Types on page 29](#)
- [\*Security Zones and Interfaces Feature Guide for Security Devices\*](#)

## Understanding How to Control Inbound Traffic Based on Protocols

### Supported Platforms [LN Series, SRX Series](#)

This topic describes the inbound system protocols on the specified zone or interface.

Any host-inbound traffic that corresponds to a protocol listed under the host-inbound traffic option is allowed. For example, if anywhere in the configuration, you map a protocol to a port number other than the default, you can specify the protocol in the host-inbound traffic option, and the new port number will be used. [Table 3 on page 8](#) lists the supported protocols. A value of **all** indicates that traffic from all of the following protocols is allowed inbound on the specified interfaces (of the zone, or a single specified interface).

**Table 3: Supported Inbound System Protocols**

Supported System Services			
all	igmp	pim	sap
bfd	ldp	rip	vrrp
bgp	msdp	ripng	nhrp
router-discovery	dvmrp	ospf	rsvp
pgm	ospf3		



**NOTE:** If DVMRP or PIM is enabled for an interface, IGMP and MLD host-inbound traffic is enabled automatically. Because IS-IS uses OSI addressing and should not generate any IP traffic, there is no host-inbound traffic option for the IS-IS protocol.



**NOTE:** You do not need to configure Neighbor Discovery Protocol (NDP) on host-inbound traffic, because the NDP is enabled by default.

Configuration option for IPv6 Neighbor Discovery Protocol (NDP) is available. The configuration option is **set protocol neighbor-discovery onlink-subnet-only** command. This option will prevent the device from responding to a Neighbor Solicitation (NS) from a prefix which was not included as one of the device interface prefixes.



**NOTE:** The Routing Engine needs to be rebooted after setting this option to remove any possibility of a previous IPv6 entry from remaining in the forwarding-table.

- Related Documentation**
- [Security Zones and Interfaces Overview on page 3](#)
  - [Understanding How to Control Inbound Traffic Based on Traffic Types on page 7](#)
  - [Understanding How to Identify Duplicate Sessions Using the TCP-Reset Parameter on page 11](#)
  - [Example: Controlling Inbound Traffic Based on Protocols on page 32](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*



## CHAPTER 3

# TCP-Reset Parameters

- [Understanding How to Identify Duplicate Sessions Using the TCP-Reset Parameter on page 11](#)

### Understanding How to Identify Duplicate Sessions Using the TCP-Reset Parameter

**Supported Platforms**    [LN Series, SRX Series](#)

When the TCP-RST feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set.

- Related Documentation**
- [Security Zones and Interfaces Overview on page 3](#)
  - [Understanding How to Control Inbound Traffic Based on Traffic Types on page 7](#)
  - [Understanding How to Control Inbound Traffic Based on Protocols on page 8](#)
  - [Example: Configuring the TCP-Reset Parameter on page 35](#)
  - [\*Security Zones and Interfaces Feature Guide for Security Devices\*](#)



## CHAPTER 4

# DNS

- [DNS Overview on page 13](#)
- [DNSSEC Overview on page 14](#)
- [DNS Proxy Overview on page 14](#)

### DNS Overview

---

**Supported Platforms**   [LN Series, SRX Series](#)

A Domain Name System (DNS) is a distributed hierarchical system that converts hostnames to IP addresses. The DNS is divided into sections called zones. Each zone has name servers that respond to the queries belonging to their zones.

This topic includes the following sections:

- [DNS Components on page 13](#)
- [DNS Server Caching on page 13](#)

### DNS Components

DNS includes three main components:

- **DNS resolver** — Resides on the client side of the DNS. When a user sends a hostname request, the resolver sends a DNS query request to the name servers to request the hostname's IP address.
- **Name servers** — Processes the DNS query requests received from the DNS resolver and returns the IP address to the resolver.
- **Resource records** — Data elements that define the basic structure and content of the DNS.

### DNS Server Caching

DNS name servers are responsible for providing the hostname IP address to users. The TTL field in the resource record defines the period for which DNS query results are cached. When the TTL value expires, the name server sends a fresh DNS query and updates the cache.

- Related Documentation**
- [Example: Configuring the TTL Value for DNS Server Caching on page 37](#)
  - [DNSSEC Overview on page 14](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*

---

## DNSSEC Overview

**Supported Platforms** [LN Series](#), [SRX Series](#)

Junos OS devices support the domain name service security extensions (DNSSEC) standard. DNSSEC is an extension of DNS that provides authentication and integrity verification of data by using public-key based signatures.

In DNSSEC, all the resource records in a DNS are signed with the private key of the zone owner. The DNS resolver uses the public key of the owner to validate the signature. The zone owner generates a private key to encrypt the hash of a set of resource records. The private key is stored in RRSIG record. The corresponding public key is stored in the DNSKEY record. The resolver uses the public key to decrypt the RRSIG and compares the result with the hash of the resource record to verify that it has not been altered.

Similarly, the hash of the public DNSKEY is stored in a DS record in a parent zone. The zone owner generates a private key to encrypt the hash of the public key. The private key is stored in the RRSIG record. The resolver retrieves the DS record and its corresponding RRSIG record and public key. Using the public key, the resolver decrypts the RRSIG record and compares the result with the hash of the public DNSKEY to verify that it has not been altered. This establishes a chain of trust between the resolver and the name servers.

- Related Documentation**
- [DNS Overview on page 13](#)
  - [Example: Configuring Keys for DNSSEC on page 38](#)
  - [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 39](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*

---

## DNS Proxy Overview

**Supported Platforms** [LN Series](#), [SRX100](#), [SRX110](#), [SRX210](#), [SRX220](#), [SRX240](#), [SRX550](#), [SRX650](#)

A dynamic name service (DNS) proxy allows clients to use a device as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

- [DNS Proxy Cache on page 15](#)
- [DNS Proxy with Split DNS on page 15](#)
- [Dynamic Domain Name System Client on page 17](#)

## DNS Proxy Cache

When a DNS query is resolved by a DNS proxy, the result is stored in the device's DNS cache. This stored cache helps the device to resolve subsequent queries from the same domain and avoid network latency delay.



**NOTE:** If the proxy cache is not available, the device sends the query to the configured DNS server, which results in network latency delays.

DNS proxy maintains a cache entry for each resolved DNS query. These entries have a time-to-live (TTL) timer so the device purges each entry from the cache as it reaches its TTL and expires. You can clear a cache by using the **clear cache** command, or the cache will automatically expire along with TTL when it goes to zero.

## DNS Proxy with Split DNS

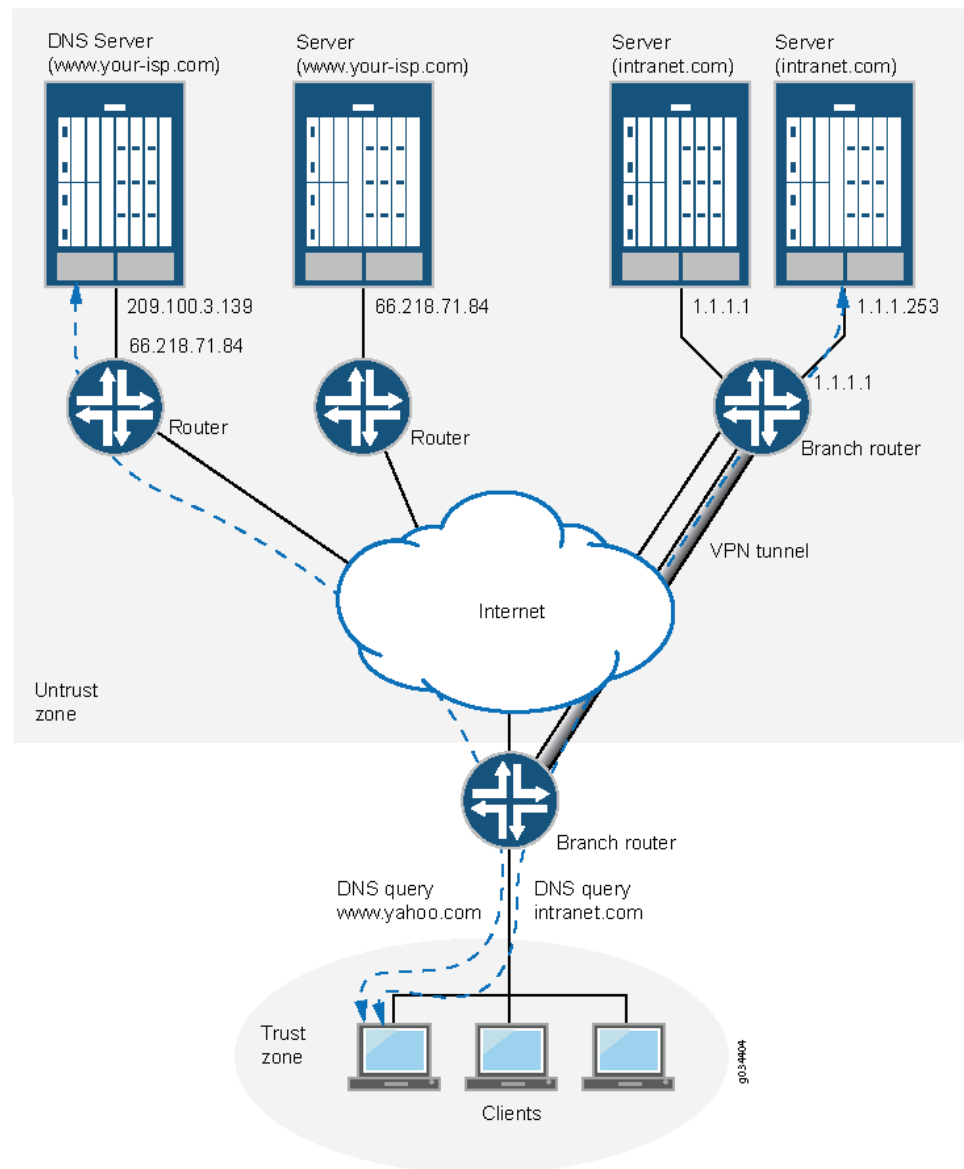
The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate them with a given domain name. When you query that domain name, the device sends the DNS queries to only those name servers that are configured for that domain name to ensure localization of DNS queries.

You can configure the transport method used to resolve a given domain name—for example, when the device connects to the corporate network through an IPsec VPN or any other secure tunnel. When you configure a secure VPN tunnel to transport the domain names belonging to the corporate network, the DNS resolution queries are not leaked to the ISP DNS server and are contained within the corporate network.

You can also configure a set of default domain (\*) and name servers under the default domain to resolve the DNS queries for a domain for which a name server is not configured.

Each DNS proxy must be associated with an interface. If an interface has no DNS proxy configuration, all the DNS queries received on that interface are dropped.

### Figure 1: DNS Proxy with Split DNS



In the corporate network shown in [Figure 1 on page 16](#), a PC client that points to the SRX Series device as its DNS server makes two queries—to `www.your-isp.com` and to `www.intranet.com`. The DNS proxy redirects the `www.intranet.com` query to the `www.intranet.com` DNS server (1.1.1.253), while the `www.your-isp.com` query is redirected to the ISP DNS server (209.100.3.130). Although the query for `www.your-isp.com` is sent to the ISP DNS server as a regular DNS query using clear text protocols (TCP/UDP), the query for the `www.intranet.com` domain goes to the intranet's DNS servers over a secure VPN tunnel.

A split DNS proxy has the following advantages:

- Domain lookups are usually more efficient. For example, DNS queries meant for a corporate domain (such as acme.com) can go to the corporate DNS server exclusively, while all others go to the ISP DNS server. Splitting DNS lookups reduces the load on the corporate server and can also prevent corporate domain information from leaking onto the Internet.
- A DNS proxy allows you to transmit selected DNS queries through a tunnel interface, which prevents malicious users from learning about the internal configuration of a network. For example, DNS queries bound for the corporate server can pass through a tunnel interface to use security features such as authentication and encryption.

## Dynamic Domain Name System Client

Dynamic DNS (DDNS) allows clients to dynamically update IP addresses for registered domain names. This feature is useful when an ISP uses Point-to-Point Protocol (PPP), Dynamic Host Configuration Protocol (DHCP), or external authentication (XAuth) to dynamically change the IP address for a customer premises equipment (CPE) router (such as a security device) that protects a Web server. Internet clients can reach the Web server by using a domain name even if the IP address of the security device has previously changed dynamically.

A DDNS server maintains a list of the dynamically changed addresses and their associated domain names. The device updates these DDNS servers with this information periodically or in response to IP address changes. The Junos OS DDNS client supports popular DDNS servers such as dyndns.org and ddo.jp

Figure 2: Dynamic DNS

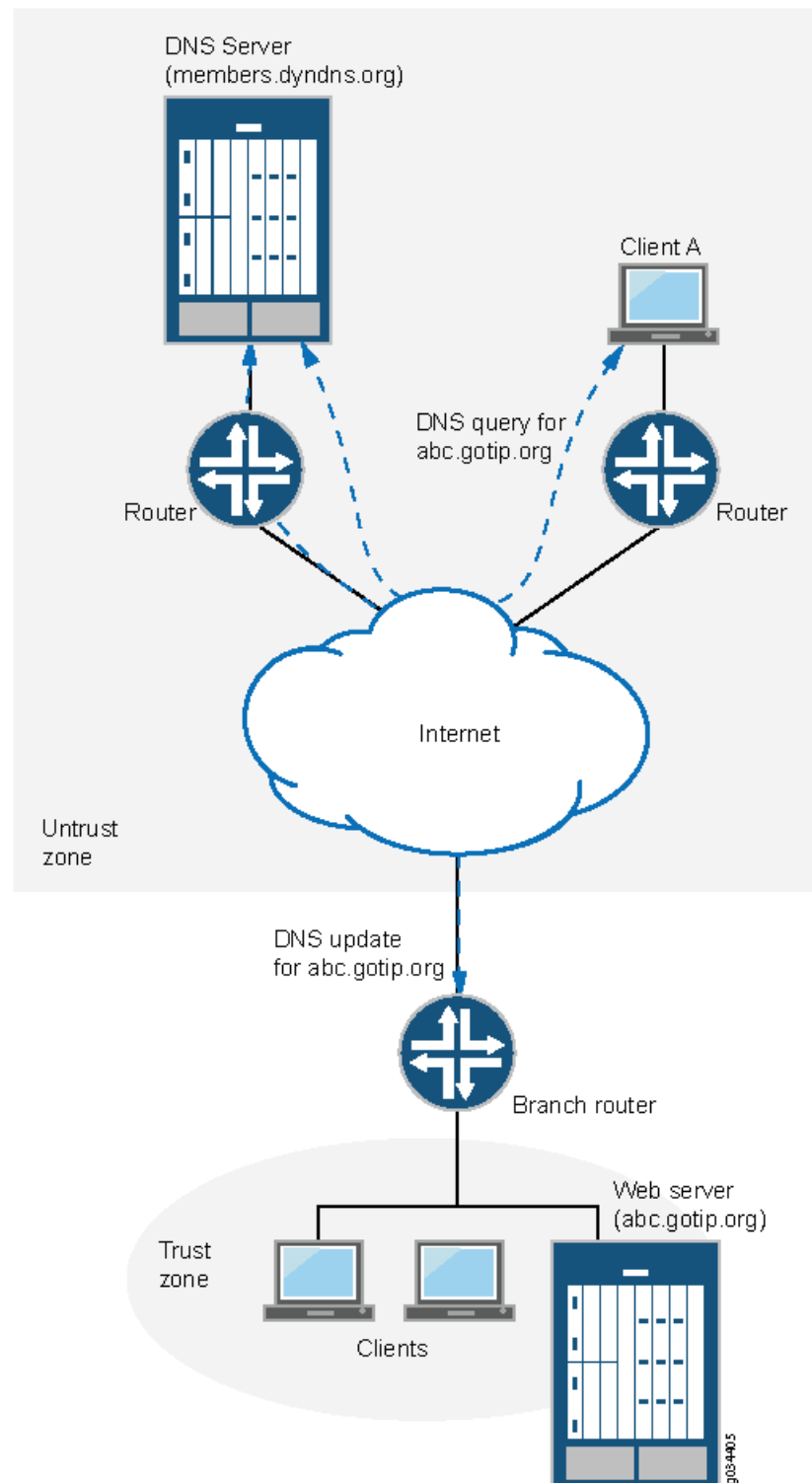


Figure 2 on page 18 illustrates how the DDNS client works. The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the

untrust zone interface on the device. The hostname abc-host.com is registered with the DDNS server and is associated with the IP address of the device's untrust zone interface, which is monitored by the DDNS client on the device. When the IP address of abc-host.com is changed, the DDNS server is informed of the new address.

If a client in the network shown in [Figure 2 on page 18](#) needs to access abc-host.com, the client queries the DNS servers on the Internet. When the query reaches the DDNS server, it resolves the request and provides the client with the latest IP address of abc-host.com.

**Related  
Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*



## PART 2

# Configuration

- [Security Zones on page 23](#)
- [Inbound Traffic on page 27](#)
- [TCP-Reset Parameter on page 35](#)
- [DNS on page 37](#)
- [Configuration Statements on page 43](#)



## CHAPTER 5

# Security Zones

- [Example: Creating Security Zones on page 23](#)

### Example: Creating Security Zones

---

**Supported Platforms**   [LN Series, SRX Series](#)

This example shows how to configure zones and assign interfaces to them. When you configure a security zone, you can specify many of its parameters at the same time.

- [Requirements on page 23](#)
- [Overview on page 23](#)
- [Configuration on page 23](#)
- [Verification on page 25](#)

### Requirements

Before you begin, configure network interfaces. See *Junos OS Interfaces Library for Security Devices*.

### Overview

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone.



**NOTE:** By default, interfaces are in the null zone. The interfaces will not pass traffic until they have been assigned to a zone.



**NOTE:** You can configure 2000 interfaces within a security zone on SRX3400, SRX3600, SRX5600, and SRX5800 devices.

### Configuration

**CLI Quick Configuration**   To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network

configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-0/0/1 unit 0 family inet address 10.12.12.1/24
set interfaces ge-0/0/1 unit 0 family inet6 address fa:43::21/96
set security security-zone ABC interfaces ge-0/0/1.0
```

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To create zones and assign interfaces to them:

1. Configure an Ethernet interface and assign an IPv4 address to it.  

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.12.12.1/24
```
2. Configure an Ethernet interface and assign an IPv6 address to it.  

```
user@host# set interfaces ge-0/0/1 unit 0 family inet6 address fa:43::21/96
```
3. Configure a security zone and assign it to an Ethernet interface.  

```
user@host# set security security-zone ABC interfaces ge-0/0/1.0
```

**Results** From configuration mode, confirm your configuration by entering the **show security zones security-zone ABC** and **show interfaces ge-0/0/1** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show security zones security-zone ABC
...
    interfaces {
        ge-0/0/1.0 {
            ...
        }
    }

[edit]
user@host# show interfaces ge-0/0/1
...
    unit 0 {
        family inet {
            address 10.12.12.1/24;
        }
        family inet6 {
            address fe:43::21/96;
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform this task:

- [Troubleshooting with Logs on page 25](#)

### Troubleshooting with Logs

---

**Purpose** Use these logs to identify any issues.

**Action** From operational mode, enter the **show log messages** command and the **show log dcd** command.

- Related Documentation**
- [Security Zones and Interfaces Overview on page 3](#)
  - [Understanding Functional Zones on page 4](#)
  - [Understanding Security Zones on page 4](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*



## CHAPTER 6

# Inbound Traffic

- [Supported System Services for Host Inbound Traffic on page 27](#)
- [Example: Controlling Inbound Traffic Based on Traffic Types on page 29](#)
- [Example: Controlling Inbound Traffic Based on Protocols on page 32](#)

### Supported System Services for Host Inbound Traffic

---

**Supported Platforms** [LN Series, SRX Series](#)

This topic describes the supported system services for host inbound traffic on the specified zone or interface.

For example, suppose a user whose system was connected to interface **1.3.1.4** in zone **ABC** wanted to telnet into interface **2.1.2.4** in zone **ABC**. For this action to be allowed, the Telnet application must be configured as an allowed inbound service on both interfaces and a policy must permit the traffic transmission.

[Table 4 on page 27](#) shows the system services that can be used for host inbound traffic.

**Table 4: System Services for Host Inbound Traffic**

Host Inbound System Services	
all	any-service
dns	finger
ftp	http
https	indent-reset
ike	netconf
ntp	ping
reverse-ssh	reverse-telnet
rlogin	rpm

Table 4: System Services for Host Inbound Traffic (*continued*)

Host Inbound System Services	
rsh	sip
snmp	snmp-trap
ssh	telnet
tftp	traceroute
xnm-clear-text	xnm-ssl



**NOTE:** On the SRX Series Services Gateways, the `xnm-clear-text` field is enabled in the factory default configuration. This setting enables incoming Junos XML protocol traffic in the trust zone for the device when the device is operating with factory default settings. We recommend you to replace the factory default settings with user-defined configuration which provides additional security once the box is configured. You must delete the `xnm-clear-text` field manually by using the CLI command `delete system services xnm-clear-text`.

Table 5 on page 28 shows the supported protocols that can be used for host inbound traffic.

Table 5: Protocols for Host Inbound Traffic

Protocols	
all	bfd
bgp	dvmrp
igmp	msdp
ospf	nhrp
pgm	ospf3
rip	pim
sap	ripng
	vrrp



**NOTE:** All services (except DHCP and BOOTP) can be configured either per zone or per interface. A DHCP server is configured only per interface because the incoming interface must be known by the server to be able to send out DHCP replies.



**NOTE:** You do not need to configure Neighbor Discovery Protocol (NDP) on host-inbound traffic, because the NDP is enabled by default.

Configuration option for IPv6 Neighbor Discovery Protocol (NDP) is available. The configuration option is **set protocol neighbor-discovery onlink-subnet-only** command. This option will prevent the device from responding to a Neighbor Solicitation (NS) from a prefix which was not included as one of the device interface prefixes.



**NOTE:** The Routing Engine needs to be rebooted after setting this option to remove any possibility of a previous IPv6 entry from remaining in the forwarding-table.

#### Related Documentation

- [Understanding How to Control Inbound Traffic Based on Traffic Types on page 7](#)
- [Example: Controlling Inbound Traffic Based on Traffic Types on page 29](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

## Example: Controlling Inbound Traffic Based on Traffic Types

**Supported Platforms**    [LN Series, SRX Series](#)

This example shows how to configure inbound traffic based on traffic types.

- [Requirements on page 29](#)
- [Overview on page 30](#)
- [Configuration on page 30](#)
- [Verification on page 31](#)

### Requirements

Before you begin:

- Configure network interfaces. See *Junos OS Interfaces Library for Security Devices*.
- Understand Inbound traffic types. See [“Understanding How to Control Inbound Traffic Based on Traffic Types” on page 7](#).

## Overview

By allowing system services to run, you can configure zones to specify different types of traffic that can reach the device from systems that are directly connected to its interfaces. You can configure the different system services at the zone level, in which case they affect all interfaces of the zone, or at the interface level. (Interface configuration overrides that of the zone.)

You must enable all expected host-inbound traffic. Inbound traffic from devices directly connected to the device's interfaces is dropped by default.

## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security zones security-zone ABC host-inbound-traffic system-services all
set security zones security-zone ABC interfaces ge-0/0/1.3 host-inbound-traffic
  system-services telnet
set security zones security-zone ABC interfaces ge-0/0/1.3 host-inbound-traffic
  system-services ftp
set security zones security-zone ABC interfaces ge-0/0/1.3 host-inbound-traffic
  system-services snmp
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic
  system-services all
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic
  system-services ftp except
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic
  system-services http except
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure inbound traffic based on traffic types:

1. Configure a security zone.  

```
[edit]
user@host# edit security zones security-zone ABC
```
2. Configure the security zone to support inbound traffic for all system services.  

```
[edit security zones security-zone ABC]
user@host# set host-inbound-traffic system-services all
```
3. Configure the Telnet, FTP, and SNMP system services at the interface level (not the zone level) for the first interface.  

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.3 host-inbound-traffic system-services telnet
user@host# set interfaces ge-0/0/1.3 host-inbound-traffic system-services ftp
user@host# set interfaces ge-0/0/1.3 host-inbound-traffic system-services snmp
```

4. Configure the security zone to support inbound traffic for all system services for a second interface.

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic system-services all
```

5. Exclude the FTP and HTTP system services from the second interface.

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic system-services ftp
except
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic system-services http
except
```

**Results** From configuration mode, confirm your configuration by entering the **show security zones security-zone ABC**. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security zones security-zone ABC
host-inbound-traffic {
  system-services {
    all;
  }
}
interfaces {
  ge-0/0/1.3 {
    host-inbound-traffic {
      system-services {
        ftp;
        telnet;
        snmp;
      }
    }
  }
  ge-0/0/1.0 {
    host-inbound-traffic {
      system-services {
        all;
        ftp {
          except;
        }
        http {
          except;
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform this task:

- [Troubleshooting with Logs on page 32](#)

### Troubleshooting with Logs

---

<b>Purpose</b>	Use these logs to identify any issues.
<b>Action</b>	From operational mode, enter the <b>show log messages</b> command and the <b>show log dcd</b> command.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding How to Control Inbound Traffic Based on Traffic Types on page 7</a></li><li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li></ul>

## Example: Controlling Inbound Traffic Based on Protocols

---

**Supported Platforms**    [LN Series](#), [SRX Series](#)

This example shows how to enable inbound traffic for an interface.

- [Requirements on page 32](#)
- [Overview on page 32](#)
- [Configuration on page 32](#)
- [Verification on page 33](#)

### Requirements

Before you begin:

- Configure security zones. See [“Example: Creating Security Zones” on page 23](#).
- Configure network interfaces. See *Junos OS Interfaces Library for Security Devices*.

### Overview

Any host-inbound traffic that corresponds to a protocol listed under the host-inbound traffic option is allowed. For example, if anywhere in the configuration you map a protocol to a port number other than the default, you can specify the protocol in the host-inbound traffic option, and the new port number will be used.

A value of **all** indicates that traffic from all of the protocols is allowed inbound on the specified interfaces (of the zone, or a single specified interface).

### Configuration

**CLI Quick Configuration**    To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic protocols
  ospf
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic protocols
  ospf3
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure inbound traffic based on protocols:

1. Configure a security zone.

```
[edit]
user@host# edit security zones security-zone ABC
```

2. Configure the security zone to support inbound traffic based on the ospf protocol for an interface.

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf
```

3. Configure the security zone to support inbound traffic based on the ospf3 protocol for an interface.

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf3
```

**Results** From configuration mode, confirm your configuration by entering the **show security zones security-zone ABC**. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security zones security-zone ABC
interfaces {
  ge-0/0/1.0 {
    host-inbound-traffic {
      protocols {
        ospf;
        ospf3;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform this task:

- [Troubleshooting with Logs on page 33](#)

### [Troubleshooting with Logs](#)

**Purpose** Use these logs to identify any issues.

**Action** From operational mode, enter the **show log messages** command and the **show log dcd** command.

- Related Documentation**
- [Understanding How to Control Inbound Traffic Based on Protocols on page 8](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*

## CHAPTER 7

# TCP-Reset Parameter

- [Example: Configuring the TCP-Reset Parameter on page 35](#)

## Example: Configuring the TCP-Reset Parameter

---

**Supported Platforms**   [LN Series, SRX Series](#)

This example shows how to configure the TCP-Reset parameter for a zone.

- [Requirements on page 35](#)
- [Overview on page 35](#)
- [Configuration on page 35](#)
- [Verification on page 36](#)

### Requirements

Before you begin, configure security zones. See [“Example: Creating Security Zones” on page 23](#).

### Overview

When the TCP-Reset parameter feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set.

### Configuration

#### Step-by-Step Procedure

To configure the TCP-Reset parameter for a zone:

1. Configure a security zone.  
  
[edit]  
user@host# **edit security zones security-zone ABC**
2. Configure the TCP-Reset parameter for the zone.  
  
[edit security zones security-zone ABC]  
user@host# **set tcp-rst**
3. If you are done configuring the device, commit the configuration.  
  
[edit]  
user@host# **commit**

## Verification

To verify the configuration is working properly, enter the **show security zones** command.

### Related Documentation

- [Understanding How to Identify Duplicate Sessions Using the TCP-Reset Parameter on page 11](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

## CHAPTER 8

# DNS

- [Example: Configuring the TTL Value for DNS Server Caching on page 37](#)
- [Example: Configuring DNSSEC on page 38](#)
- [Example: Configuring Keys for DNSSEC on page 38](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 39](#)
- [Configuring the Device as a DNS Proxy on page 41](#)

### Example: Configuring the TTL Value for DNS Server Caching

---

**Supported Platforms**   [LN Series, SRX Series](#)

This example shows how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

- [Requirements on page 37](#)
- [Overview on page 37](#)
- [Configuration on page 38](#)
- [Verification on page 38](#)

#### Requirements

No special configuration beyond device initialization is required before performing this task.

#### Overview

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

## Configuration

### Step-by-Step Procedure

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds.  

```
[edit]  
user@host# set system services dns max-cache-ttl 86400
```
2. Specify the maximum TTL value for negative cached responses, in seconds.  

```
[edit]  
user@host# set system services dns max-ncache-ttl 86400
```
3. If you are done configuring the device, commit the configuration.  

```
[edit]  
user@host# commit
```

## Verification

To verify the configuration is working properly, enter the **show system services** command.

### Related Documentation

- [DNS Overview on page 13](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## Example: Configuring DNSSEC

**Supported Platforms**   [LN Series](#), [SRX Series](#)

DNS-enabled devices run a DNS resolver (proxy) that listens on loopback address 127.0.0.1 or ::1. The DNS resolver performs a hostname resolution for DNSSEC. Users need to set name server IP address to 127.0.0.1 or ::1 so the DNS resolver forwards all DNS queries to DNSSEC instead of to DNS. If the name server IP address is not set, DNS will handle all queries instead of to DNSSEC.

The following example shows how to set the server IP address to 127.0.0.1:

```
[edit]  
user@host# set system name-server 127.0.0.1
```

The DNSSEC feature is enabled by default. You can disable DNSSEC in the server by using the following CLI command:

```
[edit]  
set system services dns dnssec disable
```

### Related Documentation

- [DNSSEC Overview on page 14](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## Example: Configuring Keys for DNSSEC

**Supported Platforms**   [LN Series](#), [SRX Series](#)

You can load a public key from a file or you can copy and paste the key file from a terminal. In both cases, you must save the keys to the configuration instead of to a file. The following example shows how to load a key from a file:

```
[edit system services dns dnssec trusted-keys]
#load-key filename
```

The following example explains how to load the key from a terminal:

```
[edit system services dns dnssec trusted-keys]
# set key "...pasted-text..."
```

If you are done loading the keys from the file or terminal, click **commit** in the CLI editor.

#### Related Documentation

- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 39](#)
- *Security Zones and Interfaces Feature Guide for Security Devices*

## Example: Configuring Secure Domains and Trusted Keys for DNSSEC

**Supported Platforms**    [LN Series, SRX Series](#)

This example shows how to configure secure domains and trusted keys for DNSSEC.

- [Requirements on page 39](#)
- [Overview on page 39](#)
- [Configuration on page 40](#)

### Requirements

Set the name server IP address so the DNS resolver forwards all DNS queries to DNSSEC instead of DNS. See [“Example: Configuring DNSSEC” on page 38](#) for more information.

### Overview

You can configure secure domains and assign trusted keys to the domains. Both signed and unsigned responses can be validated when DNSSEC is enabled.

When you configure a domain as a secure domain and if DNSSEC is enabled, all unsigned responses to that domain are ignored and the server returns a SERVFAIL error code to the client for the unsigned responses. If the domain is not configured as a secure domain, unsigned responses will be accepted.

When the server receives a signed response, it checks if the DNSKEY in the response matches any of the trusted keys that are configured. If it finds a match, the server accepts the signed response.

You can also attach a DNS root zone as a trusted anchor to a secure domain to validate the signed responses. When the server receives a signed response, it queries the DNS root zone for a DS record. When it receives the DS record, it checks if the DNSKEY in the DS record matches the DNSKEY in the signed response. If it finds a match, the server accepts the signed response.

## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set system services dns dnssec secure-domains domain1.net
set system services dns dnssec secure-domains domain2.net
set system services dns dnssec trusted-keys key domain1.net.25633CJ5K3h
set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

**Step-by-Step Procedure** To configure secure domains and trusted keys for DNSSEC:

1. Configure domain1.net and domain2.net as secure domains.

```
[edit]
user@host# set system services dns dnssec secure-domains domain1.net
user@host# set system services dns dnssec secure-domains domain2.net
```

2. Configure trusted keys to domain1.net.

```
[edit]
user@host# set system services dns dnssec trusted-keys key
"domain1.net.25633CJ5K3h"
```

3. Attach a root zone div.isc.org as a trusted anchor to a secure domain.

```
[edit]
user@host# set system services dns dnssec dlv domain domain2.net trusted-anchor
dlv.isc.org
```

**Results** From configuration mode, confirm your configuration by entering the **show system services** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
dns {
  dnssec {
    trusted-keys {
      key domain1.net.25633CJ5K3h; ## SECRET-DATA
    }
    dlv {
      domain domain2.net trusted-anchor dlv.isc.org;
    }
    secure-domains {
      domain1.net;
      domain2.net;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

**Related Documentation**

- [DNSSEC Overview on page 14](#)
- [Example: Configuring Keys for DNSSEC on page 38](#)

- *Security Zones and Interfaces Feature Guide for Security Devices*

## Configuring the Device as a DNS Proxy

**Supported Platforms** [LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650](#)

The Junos operating system (Junos OS) incorporates domain name system (DNS) support, which allows you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS enables a device to reference locations by domain name (such as `www.juniper.net`) in addition to using the routable IP address (207.17.137.68 for `www.juniper.net`).

DNS features include:

- **DNS proxy**—The device proxies hostname resolution requests on behalf of the clients behind the SRX Series device. DNS proxy improves domain lookup performance by using caching.
- **Split DNS**—The device redirects DNS queries over a secure connection to a specified DNS server in the private network. Split DNS prevents malicious users from learning the network configuration, and thus also prevents domain information leaks. Once configured, split DNS operates transparently.
- **Dynamic DNS (DDNS) client**—Servers protected by the device remain accessible despite dynamic IP address changes. For example, a protected Web server continues to be accessible with the same hostname, even after the dynamic IP address is changed because of address reassignment by the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) by Internet service provider (ISP).

To configure the device as a DNS proxy, you enable DNS on a logical interface and configure DNS proxy servers. Configuring a static cache enables branch office and corporate devices to use hostnames to communicate. Configuring dynamic DNS (DDNS) clients allows IP address changes.

Perform the following procedure to configure the device as a DNS proxy server by enabling DNS proxy on a logical interface—for example, `ge-0/0/1.0`—and configuring a set of name servers that are to be used for resolving the specified domain names. You can specify a default domain name by using an asterisk (\*) and then configure a set of name servers for resolution. Use this approach when you need global name servers to resolve domain name entries that do not have a specific name server configured.

### 1. DNS proxy configuration

- Enable DNS proxy on a logical interface.

```
[edit system services]
user@host# set dns dns-proxy interface ge-0/0/1.0
```

- Set a default domain name, and specify global name servers according to their IP addresses.

```
[edit system services]
```

```
user@host# set dns dns-proxy default-domain * forwarders 172.17.28.100
```

- If you are done configuring the device, commit the configuration.

```
[edit]  
user@host# commit
```

To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns dns-proxy
```

## 2. Dynamic DNS proxy configuration

- Enable client.

```
[edit system services]  
user@host# set dynamic-dns client abc.com agent juniper interface ge-0/0/1.0  
username test password test123
```

- If you are done configuring the device, commit the configuration.

```
[edit]  
user@host# commit
```

To verify if the configuration is working properly

```
user@host# show system services dynamic-dns
```

### Related Documentation

- *Security Zones and Interfaces Feature Guide for Security Devices*

## CHAPTER 9

# Configuration Statements

- [Security Configuration Statement Hierarchy on page 43](#)
- [\[edit security zones\] Hierarchy Level on page 45](#)
- [address \(Security Address Book\) on page 47](#)
- [address-set on page 48](#)
- [application-tracking \(Security Zones\) on page 49](#)
- [description \(Security Zone\) on page 50](#)
- [dns-proxy on page 51](#)
- [dynamic-dns on page 52](#)
- [forward-only \(DNS\) on page 53](#)
- [functional-zone on page 54](#)
- [host-inbound-traffic on page 55](#)
- [interfaces \(Security Zones\) on page 56](#)
- [management \(Security Zones\) on page 57](#)
- [protocols \(Security Zones Host Inbound Traffic\) on page 58](#)
- [protocols \(Security Zones Interfaces\) on page 60](#)
- [screen \(Security Zones\) on page 61](#)
- [secure-domains on page 61](#)
- [secure-neighbor-discovery on page 62](#)
- [security-zone on page 63](#)
- [system-services \(Security Zones Host Inbound Traffic\) on page 65](#)
- [system-services \(Security Zones Interfaces\) on page 67](#)
- [tcp-rst on page 68](#)
- [traceoptions \(System Services DNS\) on page 69](#)
- [vrrp on page 71](#)
- [zones on page 72](#)

## Security Configuration Statement Hierarchy

---

**Supported Platforms**    LN Series, SRX Series

Use the statements in the **security** configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, user identification, Unified Threat Management (UTM), and zones. Statements that are exclusive to the SRX Series devices running Junos OS are described in this section.

Each of the following topics lists the statements at a sub-hierarchy of the **[edit security]** hierarchy.

- *[edit security address-book] Hierarchy Level*
- *[edit security alarms] Hierarchy Level*
- *[edit security alg] Hierarchy Level*
- *[edit security analysis] Hierarchy Level*
- *[edit security application-firewall] Hierarchy Level*
- *[edit security application-tracking] Hierarchy Level*
- *[edit security certificates] Hierarchy Level*
- *[edit security datapath-debug] Hierarchy Level*
- *[edit security dynamic-vpn] Hierarchy Level*
- *[edit security firewall-authentication] Hierarchy Level*
- *[edit security flow] Hierarchy Level*
- *[edit security forwarding-options] Hierarchy Level*
- *[edit security forwarding-process] Hierarchy Level*
- *[edit security gprs] Hierarchy Level*
- *[edit security group-vpn] Hierarchy Level*
- *[edit security idp] Hierarchy Level*
- *[edit security ike] Hierarchy Level*
- *[edit security ipsec] Hierarchy Level*
- *[edit security log] Hierarchy Level*
- *[edit security nat] Hierarchy Level*
- *[edit security pki] Hierarchy Level*
- *[edit security policies] Hierarchy Level*
- *[edit security resource-manager] Hierarchy Level*
- *[edit security screen] Hierarchy Level*
- *[edit security softwires] Hierarchy Level*

- [\[edit security ssh-known-hosts\] Hierarchy Level](#)
- [\[edit security traceoptions\] Hierarchy Level](#)
- [\[edit security user-identification\] Hierarchy Level](#)
- [\[edit security utm\] Hierarchy Level](#)
- [\[edit security zones\] Hierarchy Level on page 45](#)

**Related  
Documentation**

- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *CLI User Guide*

## [\[edit security zones\] Hierarchy Level](#)

**Supported Platforms**    [LN Series, SRX Series](#)

```
security {
  zones {
    functional-zone {
      management {
        description text;
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
      }
      interfaces interface-name {
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
      }
    }
    screen screen-name;
  }
}

security-zone zone-name {
  address-book {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
    }
  }
}
```

```
        range-address lower-limit to upper-limit;  
        wildcard-address ipv4-address/wildcard-mask;  
    }  
    address-set address-set-name {  
        address address-name;  
        address-set address-set-name;  
        description text;  
    }  
}  
application-tracking;  
description text;  
host-inbound-traffic {  
    protocols protocol-name {  
        except;  
    }  
    system-services service-name {  
        except;  
    }  
}  
interfaces interface-name {  
    host-inbound-traffic {  
        protocols protocol-name {  
            except;  
        }  
        system-services service-name {  
            except;  
        }  
    }  
}  
screen screen-name;  
tcp-rst;  
}  
}
```

**Related  
Documentation**

- [Security Configuration Statement Hierarchy on page 43](#)
- *Application Tracking Feature Guide for Security Devices*
- *Security Zones and Interfaces Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Unified Access Control Design and Implementation Guide for Security Devices*

## address (Security Address Book)

**Supported Platforms** LN Series, SRX Series

**Syntax**

```
address address-name {
    ip-prefix {
        description text;
    }
    description text;
    dns-name domain-name {
        ipv4-only;
        ipv6-only;
    }
    range-address lower-limit to upper-limit;
    wildcard-address ipv4-address/wildcard-mask;
}
```

**Hierarchy Level** [edit security address-book *book-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS. Support for address range added in Release 12.1 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Add an entry containing an IP address or DNS hostname, or wildcard address to the address book. An address book contains entries for addressable entities in security zones, policies, and NAT rules. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and DNS names.

- Options**
- **address *address-name***—Name of an address entry.
  - **description *text***—Descriptive text about an address entry.
  - **dns-address *domain-name***—DNS address name.
  - ***ip-prefix***—IP address with prefix.
  - **range-address *lower-limit* to *upper-limit***—Address range for an address book.
  - **wildcard-address *ipv4-address/wildcard-mask***—IPv4 wildcard address in the form of A.B.C.D/wildcard-mask.



**NOTE:** IPv6 wildcard address configuration is not supported in this release.

**Required Privilege Level**

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

- Related Documentation**
- *Address Books and Address Sets Feature Guide for Security Devices*
  - *Security Zones and Interfaces Feature Guide for Security Devices*

## address-set

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
address-set address-set-name {  
    address address-name;  
    address-set address-set-name;  
    description text;  
}
```

**Hierarchy Level** [edit security address-book *book-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for nested address sets introduced in Release 11.2 of Junos OS. The **description** option added in Junos OS Release 12.1.

**Description** Specify a collection of addresses, as defined in the **address (Address Book)** statement. Using address sets, you can organize addresses in logical groups and use them to easily configure other features, such as policies and NAT rules. Using this statement, you can also include a description for an address set.

You can also define address sets within address sets.

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

The remaining statements are explained separately. See [CLI Explorer](#).

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

- Related Documentation**
- *Address Books and Address Sets Feature Guide for Security Devices*
  - *Security Zones and Interfaces Feature Guide for Security Devices*

## application-tracking (Security Zones)

---

<b>Supported Platforms</b>	<a href="#">LN Series</a> , <a href="#">SRX Series</a>
<b>Syntax</b>	application-tracking;
<b>Hierarchy Level</b>	[edit security zones security-zone <i>zone-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Enable application tracking support for the zone.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Application Tracking Feature Guide for Security Devices</i></li><li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li></ul>

## description (Security Zone)

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax** `description text;`

**Hierarchy Level** [edit security zones functional-zone management]  
[edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for a security zone.



**NOTE:** The descriptive text should not include characters, such as "<", ">", "&", or "\n".

---

**Options** `text`—Descriptive text about a security zone.

**Range:** 1 through 300 characters



**NOTE:** The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

---

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

## dns-proxy

<b>Supported Platforms</b>	LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650
<b>Syntax</b>	<pre> dns-proxy {   cache <i>hostname</i> inet <i>ip-address</i>;   default-domain <i>domain-name</i> {     forwarders <i>ip-address</i>;   }   interface <i>interface-name</i>;   propogate-setting (enable   disable);   view <i>view-name</i> {     domain <i>domain-name</i> {       forward-only;       forwarders <i>ip-address</i>;     }     match-clients <i>subnet-address</i>;   } } </pre>
<b>Hierarchy Level</b>	[edit system services dns dns-proxy]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D10.
<b>Description</b>	Configure the device as a DNS proxy server by enabling DNS proxy on a logical interface.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> </ul>

## dynamic-dns

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
dynamic-dns {  
  client hostname {  
    agent agent-name;  
    interface interface-name;  
    password server-password;  
    server server-name;  
    username user-name;  
  }  
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Configure the device as a dynamic DNS server that maintains the list of the changed addresses and their associated domain names registered with it. The device updates these DDNS servers with this information periodically or whenever there is a change in IP addresses.

- Options**
- **client**—Specifies the hostname of the registered client.
  - **agent**—Specifies the name of the dynamic DNS agent.
  - **interface**—Specifies the interface whose IP address is mapped to the registered domain name.
  - **password**—Specifies the password.
  - **server**—Specifies the name of the dynamic DNS server that allows dynamic DNS clients to update the IP address changes associated with the registered hostname.
  - **username**—Specifies the dynamic DNS username.

**Required Privilege Level**

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## forward-only (DNS)

---

<b>Supported Platforms</b>	<a href="#">SRX Series</a>
<b>Syntax</b>	forward-only;
<b>Hierarchy Level</b>	[edit system services dns dns-proxy view <i>view-name</i> domain <i>domain-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X46-D10.
<b>Description</b>	Specify that the server to forward only DNS queries. This configuration prevents the device from acquiring public IP addresses, in case the IP address specified in <b>forwarders</b> option is not reachable, by terminating the DNS query.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">DNS Overview on page 13</a></li><li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li></ul>

## functional-zone

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
functional-zone {  
  management {  
    description text;  
    host-inbound-traffic {  
      protocols protocol-name {  
        except;  
      }  
      system-services service-name {  
        except;  
      }  
    }  
  }  
  interfaces interface-name {  
    host-inbound-traffic {  
      protocols protocol-name {  
        except;  
      }  
      system-services service-name {  
        except;  
      }  
    }  
  }  
  screen screen-name;  
}
```

**Hierarchy Level** [edit security zones]

**Release Information** Statement introduced in Junos OS Release 8.5. The **description** option added in Junos OS Release 12.1.

**Description** Configure a functional zone.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

## host-inbound-traffic

<b>Supported Platforms</b>	LN Series, SRX Series
<b>Syntax</b>	<pre> host-inbound-traffic {   protocols protocol-name {     except;   }   system-services service-name {     except;   } } </pre>
<b>Hierarchy Level</b>	[edit security zones functional-zone management], [edit security zones functional-zone management interfaces <i>interface-name</i> ], [edit security zones security-zone <i>zone-name</i> ], [edit security zones security-zone <i>zone-name</i> interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Control the type of traffic that can reach the device from interfaces bound to the zone.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Ethernet Port Switching Feature Guide for Security Devices</i></li> <li>• <i>Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices</i></li> <li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> </ul>

## interfaces (Security Zones)

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
interfaces interface-name {  
  host-inbound-traffic {  
    protocols protocol-name {  
      except;  
    }  
  }  
  system-services service-name {  
    except;  
  }  
}
```

**Hierarchy Level** [edit security zones functional-zone management],  
[edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the set of interfaces that are part of the zone.

**Options** *interface-name* —Name of the interface.

The remaining statements are explained separately. See [CLI Explorer](#).

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

**Related Documentation**

- *Ethernet Port Switching Feature Guide for Security Devices*
- *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
- *Security Zones and Interfaces Feature Guide for Security Devices*
- *Administration Guide for Security Devices*

## management (Security Zones)

**Supported Platforms** [LN Series, SRX Series](#)

**Syntax**

```
management {
  description text;
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
  interfaces interface-name {
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
      system-services service-name {
        except;
      }
    }
  }
  screen screen-name;
}
```

**Hierarchy Level** [edit security zones functional-zone]

**Release Information** Statement introduced in Junos OS Release 8.5. The **description** option added in Junos OS Release 12.1.

**Description** Specify the host for out-of-band management interfaces. You can set firewall options in this zone to protect the management interface from different types of attacks. Because this zone cannot be specified in policies, traffic entering from this zone can only be traffic originating from the device itself and cannot originate from any other zone.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

## protocols (Security Zones Host Inbound Traffic)

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
protocols {  
    (protocol-name | all <protocol-name except>);  
}
```

**Hierarchy Level** [edit security zones security-zone *zone-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of protocol traffic that can reach the device for all interfaces in a zone. You can do this in one of several ways:

- You can enable traffic from each protocol individually.
- You can enable traffic from all protocols.
- You can enable traffic from all but some protocols.

**Options** *protocol-name*—Protocol for which traffic is allowed. The following protocols are supported:

- **all**—Enable traffic from all possible protocols available. Use the *except* option to disallow specific protocols.
- **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) protocol traffic.
- **bgp**—Enable incoming BGP traffic.
- **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.
- **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.
- **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).
- **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.
- **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.
- **ospf**—Enable incoming OSPF traffic.
- **ospf3**—Enable incoming OSPF version 3 traffic.
- **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).
- **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.
- **rip**—Enable incoming RIP traffic.
- **ripng**—Enable incoming RIP next generation traffic.
- **router-discovery**—Enable incoming router discovery traffic.

- **rsvp**—Enable incoming Resource Reservation Protocol (RSVP) traffic (IP protocol number 46).
- **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**. New addresses and ports can be added dynamically. This information must be propagated to the Packet Forwarding Engine (PFE).
- **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

**except**—(Optional) Disable specific incoming protocol traffic, but only when the *all* option has been defined . For example, to enable all but BGP and VRRP protocol traffic:

```
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust host-inbound-traffic protocols bgp except
set security zones security-zone trust host-inbound-traffic protocols vrrp except
```

<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li></ul>

## protocols (Security Zones Interfaces)

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax** `protocols protocol-name {  
except;  
}`

**Hierarchy Level** [edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of routing protocol traffic that can reach the device on a per-interface basis.

- Options**
- **protocol-name** —Protocol for which traffic is allowed. The following protocols are supported:
    - **all**—Enable traffic from all possible protocols available.
    - **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) Protocol traffic.
    - **bgp**—Enable incoming BGP traffic.
    - **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.
    - **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.
    - **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).
    - **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.
    - **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.
    - **ospf**—Enable incoming OSPF traffic.
    - **ospf3**—Enable incoming OSPF version 3 traffic.
    - **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).
    - **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.
    - **rip**—Enable incoming RIP traffic.
    - **ripng**—Enable incoming RIP next generation traffic.
    - **router-discovery**—Enable incoming router discovery traffic.
    - **rsvp**—Enable incoming Resource Resolution Protocol (RSVP) traffic (IP protocol number 46).
    - **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on 224.2.127.254:9875.
    - **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

**except**—(Optional) except can only be used if all has been defined.

<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> </ul>

## screen (Security Zones)

---

<b>Supported Platforms</b>	LN Series, SRX Series
<b>Syntax</b>	screen <i>screen-name</i> ;
<b>Hierarchy Level</b>	[edit security zones functional-zone management], [edit security zones security-zone <i>zone-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Specify a security screen for a security zone.
<b>Options</b>	<i>screen-name</i> —Name of the screen.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> </ul>

## secure-domains

---

<b>Supported Platforms</b>	LN Series, SRX Series
<b>Syntax</b>	secure-domains [ <i>domain-name</i> ];
<b>Hierarchy Level</b>	[edit system services dns dnssec]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure secure domains in the DNS server. The server accepts only signed responses for this domain. For unsigned responses, the server returns SERVFAIL error to the client.
<b>Options</b>	<i>domain-name</i> —Name of the domain.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> </ul>

## secure-neighbor-discovery

---

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
secure-neighbor-discovery {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}
```

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Provide support for protecting Secure Neighbor Discovery Protocol (SEND) messages.

- Options**
- **command *binary-file-path***—Path to the binary process.
  - **disable**—Disable the Secure Neighbor Discovery (SEND) protocol process.
  - **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
    - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
    - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

## security-zone

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
security-zone zone-name {
  address-book {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
      range-address lower-limit to upper-limit;
      wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
      address address-name;
      address-set address-set-name;
      description text;
    }
  }
  application-tracking;
  description text;
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
  }
  system-services service-name {
    except;
  }
}
interfaces interface-name {
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
  }
  system-services service-name {
    except;
  }
}
}
screen screen-name;
tcp-rst;
}
```

**Hierarchy Level** [edit security zones]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

<b>Description</b>	Define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.
<b>Options</b>	<b><i>zone-name</i></b> —Name of the security zone.  The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Ethernet Port Switching Feature Guide for Security Devices</i></li><li>• <i>Junos OS Layer 2 Bridging and Switching Library for Security Devices</i></li><li>• <i>Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices</i></li><li>• <i>Application Tracking Feature Guide for Security Devices</i></li></ul>

## system-services (Security Zones Host Inbound Traffic)

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax** `system-services service-name {  
except;  
}`

**Hierarchy Level** `[edit security zones security-zone zone-name host-inbound-traffic]`

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of traffic that can reach the device for all interfaces in a zone.

- Options**
- ***service-name***—System-service for which traffic is allowed. The following system services are supported:
    - **all**—Enable traffic from the defined system services available on the Routing Engine (RE). Use the *except* option to disallow specific system services.
    - **any-service**—Enable all system services on entire port range including the system services that are not defined.
    - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
    - **dhcp**—Enable incoming DHCP requests.
    - **dhcpv6**—Enable incoming DHCP requests for IPv6.
    - **dns**—Enable incoming DNS services.
    - **finger**—Enable incoming finger traffic.
    - **ftp**—Enable incoming FTP traffic.
    - **http**—Enable incoming J-Web or clear-text Web authentication traffic.
    - **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).
    - **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
    - **ike**—Enable Internet Key Exchange traffic.
    - **lsping**—Enable label switched path ping service.
    - **netconf**—Enable incoming NETCONF service.
    - **ntp**—Enable incoming Network Time Protocol (NTP) traffic.
    - **ping**—Allow the device to respond to ICMP echo requests.
    - **r2cp**—Enable incoming Radio Router Control Protocol traffic.
    - **reverse-ssh**—Reverse SSH traffic.
    - **reverse-telnet**—Reverse Telnet traffic.

- **rlogin**—Enable incoming **rlogin** (remote login) traffic.
- **rpm**—Enable incoming Real-time performance monitoring (RPM) traffic.
- **rsh**—Enable incoming Remote Shell (**rsh**) traffic.
- **sip**—Enable incoming Session Initiation Protocol traffic.
- **snmp**—Enable incoming SNMP traffic (UDP port 161).
- **snmp-trap**—Enable incoming SNMP traps (UDP port 162).
- **ssh**—Enable incoming SSH traffic.
- **telnet**—Enable incoming Telnet traffic.
- **tftp**—Enable TFTP services.
- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).
- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.
- **except**—(Optional) Enable specific incoming system service traffic but only when the *all* option has been defined . For example, to enable all but FTP and HTTP system service traffic:  
  
    set security zones security-zone trust host-inbound-traffic system-services all  
    set security zones security-zone trust host-inbound-traffic system-services ftp except  
    set security zones security-zone trust host-inbound-traffic system-services http except

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

**Related Documentation**      • *Security Zones and Interfaces Feature Guide for Security Devices*

## system-services (Security Zones Interfaces)

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax** `system-services service-name {  
except;  
}`

**Hierarchy Level** [edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of traffic that can reach the device on a particular interface.

- Options**
- ***service-name***—Service for which traffic is allowed. The following services are supported:
    - **all**—Enable all possible system services available on the Routing Engine (RE).
    - **any-service**—Enable services on entire port range.
    - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
    - **dhcp**—Enable incoming DHCP requests.
    - **dhcpv6**—Enable incoming DHCP requests for IPv6.
    - **dns**—Enable incoming DNS services.
    - **finger**—Enable incoming finger traffic.
    - **ftp**—Enable incoming FTP traffic.
    - **http**—Enable incoming J-Web or clear-text Web authentication traffic.
    - **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).
    - **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
    - **ike**—Enable Internet Key Exchange traffic.
    - **netconf SSH**—Enable incoming NetScreen Security Manager (NSM) traffic over SSH.
    - **ntp**—Enable incoming Network Time Protocol (NTP) traffic.
    - **ping**—Allow the device to respond to ICMP echo requests.
    - **r2cp**—Enable incoming Radio Router Control Protocol traffic.
    - **reverse-ssh**—Reverse SSH traffic.
    - **reverse-telnet**—Reverse Telnet traffic.
    - **rlogin**—Enable incoming **rlogin** (remote login) traffic.
    - **rpm**—Enable incoming real-time performance monitoring (RPM) traffic.
    - **rsh**—Enable incoming Remote Shell (**rsh**) traffic.

- **sip**—Enable Incoming Session Initiation protocol (SIP) traffic.
- **snmp**—Enable incoming SNMP traffic (UDP port 161).
- **snmp-trap**—Enable incoming SNMP traps (UDP port 162).
- **ssh**—Enable incoming SSH traffic.
- **telnet**—Enable incoming Telnet traffic.
- **tftp**—Enable TFTP services.
- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).
- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.
- **except**—(Optional) except can only be used if all has been defined.

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

**Related Documentation**

- *Ethernet Port Switching Feature Guide for Security Devices*
- *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## tcp-rst

---

**Supported Platforms** [LN Series, SRX Series](#)

**Syntax** tcp-rst;

**Hierarchy Level** [edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable the device to send a TCP segment with the RST (reset) flag set to 1 (one) in response to a TCP segment with any flag other than SYN set and that does not belong to an existing session.

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

---

## traceoptions (System Services DNS)

---

**Supported Platforms** [LN Series, SRX Series](#)

**Syntax**

```
traceoptions {  
  category {  
    category-type;  
  }  
  file;  
}
```

**Hierarchy Level** [edit system services dns]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Defines tracing options for DNS services.

**Options** **category**—Specifies the logging category. See [Table 6 on page 70](#) for the different logging categories and their descriptions.

**file**—Trace file information.

Table 6: Category Names

Category Name	Description
client	Processing of client requests
config	Configuration file parsing and processing
database	Messages relating to the databases
default	Categories for which there is no specific configuration
delegation-only	Delegation only
dispatch	Dispatching of incoming packets to the server
dnssec	DNSSEC and TSIG protocol processing
edns-disabled	Log query using plain DNS
general	General information
lame-servers	Lame servers
network	Network options
notify	NOTIFY protocol
queries	DNS query resolver
resolver	DNS resolution security
security	Approval and denial of requests
unmatched	Unable to determine the class for messages named
update	Dynamic updates
update-security	Approval and denial of update requests
xfer-in	Zone transfers that the server is receiving xfer-out
xfer-out	Zone transfers that the server is sending

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

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

## vrrp

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax**

```
vrrp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the Virtual Router Redundancy Protocol (VRRP) process.

- Options**
- **command *binary-file-path***—Path to the binary process.
  - **disable**—Disable the VRRP process.
  - **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
    - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
    - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.



**NOTE:** On SRX100, SRX110, SRX210, and SRX220 devices, you cannot configure the same VRRP group ID on different interfaces of a single device

**Required Privilege Level**

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

**Related Documentation**

- *Security Zones and Interfaces Feature Guide for Security Devices*

## zones

Supported Platforms [LN Series](#), [SRX Series](#)

```
Syntax zones {
    functional-zone {
        management {
            description text;
            host-inbound-traffic {
                protocols protocol-name {
                    except;
                }
            }
            system-services service-name {
                except;
            }
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
}

security-zone zone-name {
    address-book {
        address address-name {
            ip-prefix {
                description text;
            }
            description text;
            dns-name domain-name {
                ipv4-only;
                ipv6-only;
            }
            range-address lower-limit to upper-limit;
            wildcard-address ipv4-address/wildcard-mask;
        }
        address-set address-set-name {
            address address-name;
            address-set address-set-name;
            description text;
        }
    }
    application-tracking;
    description text;
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
    }
}
```

```

        system-services service-name {
            except;
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
    tcp-rst;
}

```

<b>Hierarchy Level</b>	[edit security]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The <b>description</b> option added in Junos OS Release 12.1.
<b>Description</b>	<p>A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:</p> <ul style="list-style-type: none"> <li>• Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.</li> <li>• Security zone—Most common type of zone that is used as a building block in policies.</li> </ul>
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Application Tracking Feature Guide for Security Devices</i></li> <li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> <li>• <i>Junos OS Logical Systems Library for Security Devices</i></li> </ul>



## PART 3

# Administration

- [Operational Commands on page 77](#)



## CHAPTER 10

# Operational Commands

- `clear system services dns dns-proxy`
- `show security zones`
- `show security zones type`
- `show system services dns dns-proxy`
- `show system services dynamic-dns`

## clear system services dns dns-proxy

---

<b>Supported Platforms</b>	<a href="#">LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650</a>
<b>Syntax</b>	clear system services dns dns-proxy
<b>Release Information</b>	Command introduced in Junos OS Release 12.1X44-D10.
<b>Description</b>	Clear DNS proxy cache information.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>cache</b>—Clear DNS proxy cache information.</li><li>• <b>statistics</b>—Clear DNS proxy statistics.</li><li>• <b>none</b>—Clear all DNS proxy cache information.</li><li>• <b>hostname</b>—(Optional) Clear DNS proxy cache information from the specified host.</li></ul>
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show system services dns dns-proxy</a></li></ul>
<b>List of Sample Output</b>	<a href="#">clear system services dns dns-proxy on page 78</a>
<b>Output Fields</b>	When you enter this command no output is produced.

## Sample Output

### clear system services dns dns-proxy

```
user@host> clear system services dns dns-proxy cache
user@host> clear system services dns dns-proxy statistics
```

## show security zones

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax** `show security zones`  
`<detail | terse>`  
`< zone-name >`

**Release Information** Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.

**Description** Display information about security zones.

- Options**
- `none`—Display information about all zones.
  - `detail | terse`—(Optional) Display the specified level of output.
  - `zone-name` —(Optional) Display information about the specified zone.

**Required Privilege Level** view

- Related Documentation**
- *Ethernet Port Switching Feature Guide for Security Devices*
  - *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
  - [security-zone on page 63](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*
  - *Junos OS Logical Systems Library for Security Devices*

**List of Sample Output** [show security zones on page 80](#)  
[show security zones abc on page 80](#)  
[show security zones abc detail on page 80](#)  
[show security zones terse on page 81](#)

**Output Fields** [Table 7 on page 79](#) lists the output fields for the **show security zones** command. Output fields are listed in the approximate order in which they appear.

**Table 7: show security zones Output Fields**

Field Name	Field Description
Security zone	Name of the security zone.
Description	Description of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.

Table 7: show security zones Output Fields (*continued*)

Field Name	Field Description
Zone	Name of the zone.
Type	Type of the zone.

## Sample Output

### show security zones

```

user@host> show security zones
Functional zone: management
  Description: This is the management zone.
  Policy configurable: No
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0
Security zone: Host
  Description: This is the host zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    fxp0.0
Security zone: abc
  Description: This is the abc zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0
Security zone: def
  Description: This is the def zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/2.0

```

## Sample Output

### show security zones abc

```

user@host> show security zones abc
Security zone: abc
  Description: This is the abc zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0

```

## Sample Output

### show security zones abc detail

```

user@host> show security zones abc detail

```

```
Security zone: abc
Description: This is the abc zone.
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
  ge-0/0/1.0
```

## Sample Output

### show security zones terse

```
user@host> show security zones terse
Zone           Type
my-internal    Security
my-external    Security
dmz            Security
```

## show security zones type

**Supported Platforms** [LN Series](#), [SRX Series](#)

**Syntax** `show security zones type`  
`(functional | security)`  
`<detail | terse>`

**Release Information** Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.

**Description** Display information about security zones of the specified type.

- Options**
- **functional**—Display functional zones.
  - **security**—Display security zones.
  - **detail | terse**—(Optional) Display the specified level of output.

**Required Privilege Level** view

- Related Documentation**
- [security-zone on page 63](#)
  - *Security Zones and Interfaces Feature Guide for Security Devices*

**List of Sample Output** [show security zones type functional on page 83](#)  
[show security zones type security on page 83](#)  
[show security zones type security terse on page 83](#)  
[show security zones type security detail on page 83](#)

**Output Fields** [Table 8 on page 82](#) lists the output fields for the **show security zones type** command. Output fields are listed in the approximate order in which they appear.

**Table 8: show security zones type Output Fields**

Field Name	Field Description
Security zone	Zone name.
Description	Description of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.
Zone	Name of the zone.
Type	Type of the zone.

## Sample Output

### show security zones type functional

```
user@host> show security zones type functional
Functional zone: management
  Description: management zone
  Policy configurable: No
  Interfaces bound: 0
  Interfaces:
```

## Sample Output

### show security zones type security

```
user@host> show security zones type security
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

## Sample Output

### show security zones type security terse

```
user@host> show security zones type security terse
Zone           Type
trust          Security
untrust        Security
junos-host     Security
```

## Sample Output

### show security zones type security detail

```
user@host> show security zones type security detail
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0
```

Security zone: untrust  
Description: untrust zone  
Send reset for non-SYN session TCP packets: Off  
Policy configurable: Yes  
Interfaces bound: 1  
Interfaces:  
ge-0/0/1.0  
Security zone: junos-host  
Description: junos-host zone  
Send reset for non-SYN session TCP packets: Off  
Policy configurable: Yes  
Interfaces bound: 0  
Interfaces:

## show system services dns dns-proxy

**Supported Platforms** [LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650](#)

**Syntax** `show system services dns dns-proxy`

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display domain name system (DNS) proxy information.

- Options**
- **none**—Display DNS proxy statistics information.
  - **cache**—(Optional) Display the DNS proxy cache.
  - **statistics**—(Optional) Display the DNS proxy statistics.

**Required Privilege Level** view

- Related Documentation**
- [clear system services dns dns-proxy on page 78](#)
  - [dns-proxy on page 51](#)

**List of Sample Output** [show system services dns-proxy statistics on page 86](#)  
[show system services dns-proxy cache on page 86](#)  
[show system services dns-proxy cache <viewname V1> on page 86](#)

**Output Fields** lists the output fields for the `show system services dns-proxy` command. Output fields are listed in the table below:

**Table 9: show system services dns-proxy**

Field Name	Field Description
DNS proxy statistics	<p>Display information about the DNS proxy.</p> <ul style="list-style-type: none"> <li>• <b>Status</b>—State of the proxy server as Enabled or disabled.</li> <li>• <b>Queries received</b>—Number of DNS queries received by the DNS proxy.</li> <li>• <b>Responses sent</b>—Number of DNS responses sent by the DNS proxy.</li> <li>• <b>Queries forwarded</b>—Number of DNS queries forwarded by the DNS proxy.</li> <li>• <b>Negative responses</b>—Number of negative responses the DNS proxy sent to the DNS client.</li> <li>• <b>Retry requests</b>—Number of retries the DNS proxy received from the DNS client.</li> <li>• <b>Pending requests</b>—Number of pending queries the DNS proxy has yet to send the DNS client a response for.</li> <li>• <b>Server failures</b>—Number of DNS proxy server failures.</li> </ul>
Hostname	Hostname of the host that has been cached.

Table 9: show system services dns-proxy (continued)

Field Name	Field Description
IP address	IP address of the host.
Time-to-live	Length of time before an entry is purged from the DNS cache.
Type	Type of DNS Resource Record. For example, A records refer to IPv4 host addresses.
Class	Class of DNS. A parameter used to define a DNS Resource Record. For example, IN class is used for Internet domain names.

## Sample Output

### show system services dns-proxy statistics

```

user@host> show system services dns-proxy statistics
DNS proxy statistics      :
  DNS proxy statistics    :
    Status                 : enabled
    IPv4 Queries received  : 30
    IPv6 Queries received  : 0
    Responses sent         : 30
    Queries forwarded      : 13
    Negative responses     : 23
    Positive responses     : 23
    Retry requests         : 0
    Pending requests       : 0
    Server failures        : 0
    Interfaces             : fe-0/0/0.0, fe-1/0/1.0

```

### show system services dns-proxy cache

```

user@host> show system services dns-proxy cache
Hostname                Time-to-live  Type  Class  IP address/Hostname
juniper.net             408          A     IN     207.17.137.229
whitestar.juniper.net   408          A     IN     172.17.27.50
scarlet.juniper.net     408          A     IN     172.17.28.11
bng-admin1.juniper.net  408          A     IN     10.209.194.131
wf-nis1.juniper.net     408          A     IN     10.10.4.202
asg-ns1.juniper.net     408          A     IN     10.16.0.11
ruby.juniper.net        408          A     IN     172.17.28.100
a.l.google.com          408          A     IN     216.239.53.9
b.l.google.com          408          A     IN     64.233.179.9
maps.l.google.com       408          A     IN     64.233.189.104
c.l.google.com          408          A     IN     64.233.161.9
d.l.google.com          408          A     IN     64.233.183.9
e.l.google.com          408          A     IN     66.102.11.9
g.l.google.com          408          A     IN     64.233.167.9
magenta.juniper.net     408          A     IN     172.17.27.123
mail.juniper.net        408          CNAME IN
magenta.juniper.net

```

### show system services dns-proxy cache <viewname V1>

```

user@host> show system services dns-proxy cache <viewname V1>

```

Hostname	Time-to-live	Type	Class	IP address/Hostname
yahoo.com.	408	A	IN	72.30.38.140
yahoo.com.	408	A	IN	98.139.183.24
yahoo.com.	408	A	IN	209.191.122.70
magenta.juniper.net.	495	A	IN	172.17.27.123
mail.juniper.net.	495	CNAME	IN	magenta.juniper.net.
d.root-servers.net.	424	A	IN	128.8.10.90
e.root-servers.net.	424	A	IN	192.203.230.10
f.root-servers.net.	424	A	IN	192.5.5.241
g.root-servers.net.	424	A	IN	192.112.36.4
h.root-servers.net.	424	A	IN	128.63.2.53
i.root-servers.net.	424	A	IN	192.36.148.17
j.root-servers.net.	424	A	IN	192.58.128.30
m.root-servers.net.	424	A	IN	202.12.27.33

## show system services dynamic-dns

**Supported Platforms** [LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650](#)

**Syntax** `show system services dynamic-dns`

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display information about dynamic DNS clients.

**Required Privilege Level** view

**Related Documentation**

- [dynamic-dns](#)

**List of Sample Output** [show system services dynamic-dns client on page 88](#)  
[show system services dynamic-dns client detail on page 89](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. The following table lists the output fields for the **show system services dynamic-dns** command.

**Table 10: show system services dynamic-dns**

Field Name	Field Description
Hostname	Hostname of the registered client
Server	DDNS server name
Agent	Name of the DDNS agent
Last response	Status of the last response
Last update	Date and time of the last update
Interface	name of the interface

## Sample Output

`show system services dynamic-dns client`

```

user@host> show system services dynamic-dns client
Internal hostname  Server      Last response
jnpr.ddo.jp       ddo.jp      success
jnr.ddo.jp        ddo.jp      failure
newsam.getmyip.com members.dyndns.org nochg
rkhetan.gotdns.com members.dyndns.org nochg

```

**show system services dynamic-dns client detail**

```
user@host>show system services dynamic-dns client detail
Hostname      : jnpr.ddo.jp
Server        : ddo.jp
Agent         : branch-0.1
Last response: success
Last update   : 2006-08-29 04:02:52 PDT
Interface     : fe-0/0/0.0

Hostname      : jnr.ddo.jp
Server        : ddo.jp
Agent         : Branch-0.1
Last response: failure
Last update   : 2006-08-29 04:03:03 PDT
Interface     : fe-0/0/0.0

Hostname      : newsam.getmyip.com
Server        : members.dyndns.org
Agent         : Branch-0.1
Last response: nochg
Last update   : 2006-08-29 04:02:50 PDT
Username      : rkhetan
Interface     : fe-0/0/1.0
```



## PART 4

# Index

- [Index on page 93](#)



# Index

## Symbols

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

## A

address statement	
address book.....	47
address-set statement.....	48
application-tracking statement	
zones.....	49

## B

braces, in configuration statements.....	xiv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv

## C

comments, in configuration statements.....	xiv
configuring	
host inbound traffic.....	7
protocols.....	8
TCP-reset parameter.....	11
conventions	
text and syntax.....	xiii
curly braces, in configuration statements.....	xiv
customer support.....	xv
contacting JTAC.....	xv

## D

description statement.....	50
dlv .....	61
DNS server caching	
configuring TTL value.....	37
dns-proxy.....	51

## DNSSEC

secure domains configuring.....	39
trusted keys configuring.....	39
documentation	
comments on.....	xv
dynamic-dns.....	52

## F

firewall filters	
statistics	
displaying.....	79
font conventions.....	xiii
forward-only (DNS).....	53
functional-zone statement.....	54

## H

host-inbound-traffic statement.....	55
-------------------------------------	----

## I

interfaces.....	4
interfaces statement.....	56

## M

management statement.....	57
manuals	
comments on.....	xv

## P

parentheses, in syntax descriptions.....	xiv
protocols statement	
(Interface Host-Inbound Traffic).....	60
(Zone Host-Inbound Traffic).....	58

## S

screen statement	
(Zones).....	61
Security Configuration Statement Hierarchy.....	43
security zones.....	3
creating.....	4
functional.....	4
host inbound traffic.....	7
protocols.....	8
interfaces.....	4
TCP-reset parameter.....	11
security-zone statement.....	63
show security idp application-identification	
application-system-cache command.....	85, 88
show security zones command.....	79
show security zones type command.....	82

support, technical	See technical support
syntax conventions.....	xiii
system-services statement	
(Interface Host-Inbound Traffic).....	67
(Zone Host-Inbound Traffic).....	65

## T

tcp-rst statement.....	68
technical support	
contacting JTAC.....	xv
traceoptions statement	
(System Services DNS).....	69

## Z

zones	
functional.....	4
security.....	3
zones statement .....	72