



vGW Series Interoperability



Published: 2015-02-19

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

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.

vGW Series Interoperability

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	ix
	Documentation and Release Notes	ix
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Part 1	STRM Series	
Chapter 1	vGW Series and STRM	3
	Configuring vGW Series to Send Syslog and Netflow Data to Juniper Networks STRM Series Devices	3
Part 2	IDP Series	
Chapter 2	vGW Series and IDP	9
	Configuring the vGW Series and IDP Series Inter-Operation	9
Part 3	SRX Series Devices	
Chapter 3	vGW Series and SRX Series Devices	13
	vGW Series and SRX Series Security Zones	13
	About SRX Series Services Gateway Security Zones	13
	SRX Series Services Gateway Zones and the vGW Series	14
	Enabling the Junoscript Interface for vGW Series	14
	Configuring Zone Objects for vGW Series Interoperability with SRX Series Devices	15
	About Populating vGW Series Records to SRX Series Zone Address Books	17
	Validating vGW Series Interoperability with SRX Series Zones	17
Part 4	Index	
	Index	21

List of Figures

Part 1	STRM Series	
Chapter 1	vGW Series and STRM	3
	Figure 1: vGW Series Configuration for Syslog and NetFlow to a STRM Series	
	Device	4
	Figure 2: STRM Source Log Definition for vGW Series	5

List of Tables

About the Documentation	ix
Table 1: Notice Icons	x
Table 2: Text and Syntax Conventions	x

About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

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>.

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
<code>Fixed-width text like this</code>	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<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@# set system domain-name <i>domain-name</i>

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

Convention	Description	Examples
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">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(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">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can 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 <https://www.juniper.net/cgi-bin/docbugreport/>.

- E-mail—Send your comments to 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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

STRM Series

- [vGW Series and STRM on page 3](#)

CHAPTER 1

vGW Series and STRM

- [Configuring vGW Series to Send Syslog and Netflow Data to Juniper Networks STRM Series Devices on page 3](#)

Configuring vGW Series to Send Syslog and Netflow Data to Juniper Networks STRM Series Devices

Integration of vGW Series with Security Threat Response Manager (STRM) Series devices provides for defense-in-depth control in the virtualized server environment. This topic covers vGW Series Syslog and Netflow integration configuration with the Juniper Networks STRM Series device.

vGW Series and STRM Series integration brings STRM Series benefits such as centralized log and event management, network-wide threat detection, and compliance reporting to the virtualized data center. This integration gives you a single-pane, comprehensive, and consistent view of your physical and virtual infrastructure.

vGW Series and STRM Series have two points of integration. vGW Series exports the following information to the STRM Series device:

- Syslog firewall logs and event messages.
- NetFlow statistics on traffic between virtual machines (VMs).

You use the Settings > Global page to configure the vGW Security Design VM to send Syslog logs and events and NetFlow VM traffic information to the STRM Series device. See [Figure 1 on page 4](#).

Figure 1: vGW Series Configuration for Syslog and NetFlow to a STRM Series Device

The figure displays four screenshots of the vGW Series configuration interface:

- External Inspection Devices:** A table with columns for #, Name, and IP Address. Row 1 is filled with '1', 'STRM', and '10.10.10.8'. Rows 2, 3, and 4 are empty. A 'Save' button is at the bottom right.
- Global Settings Rules:** A table with columns for #, Rule, and Allow. Row 1 is '1', 'IPv6 traffic', and an unchecked checkbox. Row 2 is '2', 'Non-IP and non-ARP traffic', and an unchecked checkbox. A 'Save' button is at the bottom right.
- External Logging:** Radio buttons for 'No Syslog', 'Send Syslog from vGW management server', and 'Send Syslog from Firewalls'. The 'Send Syslog from Firewalls' option is selected, with a checked checkbox for 'Send firewall logs to vGW management server'. Below, 'Syslog Server' is '10.10.10.8', 'Syslog Server Port' is '514', and 'Transport Protocol' is 'udp'. A 'Save' button is at the bottom right.
- NetFlow Configuration:** A checked checkbox for 'Enable'. Below, 'NetFlow collector address' is '10.10.10.8' and 'NetFlow collector port' is '2055'. A 'Save' button is at the bottom right.

Syslog. For Syslog, you configure information on both vGW Series and the STRM Series device:

- You configure information about the STRM Series device on the vGW Series Settings > Global pane.
- The Syslog format is particular to a specific device. Therefore, for STRM to be able to recognize and parse vGW Series incoming messages, you must specify the vGW Series log source on STRM.

Syslog Configuration on vGW Series.

Configure vGW Series for Syslog external logging to the STRM Series device.

1. In the External Inspection Devices pane, enter STRM for the name of the external device and specify the STRM Series device's IP address.
2. In the External Logging pane, select **Send Syslog from Firewalls**. If you want to send the firewall logs to the vGW Security Design VM also, select the check box.
3. To identify the STRM Series device as the Syslog server, specify its IP address in the External Logging pane.
4. Select UDP as the transport protocol.

vGW Series Configuration on STRM.

1. Define vGW Series as the log source in the STRM Series device to identify the Syslogs that you are sending. See [Figure 2 on page 5](#).

Figure 2: STRM Source Log Definition for vGW Series

Add a log source	
Log Source Name	vGW
Log Source Description	My Virtual Gatekeeper
Log Source Type	Juniper vGW
Protocol Configuration	Syslog
Log Source Identifier	10.10.10.10
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: strm-console
Coalescing Events	<input checked="" type="checkbox"/>
Store Event Payload	<input checked="" type="checkbox"/>
Please select any groups you would like this log source to be a member of:	

NetFlow.

The STRM Series device can listen for NetFlow messages on port 2055 from any device because NetFlow has a standard format. If you specify 2055 for the port on the vGW Series configuration, you do not need to configure NetFlow on the STRM Series device.

In the Settings > Global > NetFlow Configuration pane, configure vGW Series NetFlow to send VM traffic statistics to the STRM Series device. See [Figure 1 on page 4](#).

1. Select the **Enable** check box.
2. Specify the IP address of the NetFlow collector and the destination port to use.



NOTE: The standard specification is UDP port 2055, but other values like 9555 or 9995 are sometimes used. If you use another value, you must configure vGW Series NetFlow information on the STRM Series device.

**Related
Documentation**

- *Understanding the vGW Series Main Module*
- *Understanding the vGW Series Security Alert Settings*
- *Understanding the vGW Security Design VM*
- *Understanding vGW Series*
- *Adding and Editing vGW Series Machines Definitions (VMware)*

PART 2

IDP Series

- [vGW Series and IDP on page 9](#)

CHAPTER 2

vGW Series and IDP

- [Configuring the vGW Series and IDP Series Inter-Operation on page 9](#)

Configuring the vGW Series and IDP Series Inter-Operation

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances provides features that protect the network from a wide range of attacks. Using stateful intrusion detection and prevention techniques, the IDP Series provides protection against worms, trojans, spyware, keyloggers, and other malware. Its feature set includes stateful signature detection, protocol and anomaly detection, QoS/DiffServ marking, VLAN-aware rules, role-based administration, separation of domains and management activities, IDP Reporter, and traffic pattern profiling.

Before you configure interoperability between the vGW Series and the IDP Series, you must configure the Intrusion Detection System as an external inspection device and configure an appropriate redirection rule for it using the Global section of the Security Settings module.

The External Inspection Devices page allows you to enter the name and IP address of the device to which traffic is sent for further analysis.

To configure the vGW Series and IDP Series inter-operation:

1. Log into the NSM for your environment.
2. Create a Security Policy for the Inter-VM communication:
 - a. In the notification section of the policy, select **Logging**.
 - b. Enable the policy for traffic between any source and destination.
 - c. Set the action to **None**.

You can inspect traffic anomalies between VMs using this security policy.

3. Enable GRE decapsulation support on the IDS device for which you created the security policy.
4. Select **Device Manager** > Security Devices.
5. Select **Sensor Settings** > **Run-Time Parameters**.
6. Select **Enable GRE decapsulation** support.

To verify that you set the parameter correctly, enter the following command on the command line of the IDP Series device:

```
ser@host# scio const -s s0 get sc_gre_decapsulation
```

After you have completed these steps, you can test the configuration. Once the above steps are complete (including the creation of the External Inspection Device and relevant security policy in vGW Security Design VM) you can test the configuration by triggering any attack in the Juniper Networks database.

Related Documentation

- *Understanding vGW Series*

PART 3

SRX Series Devices

- [vGW Series and SRX Series Devices on page 13](#)

CHAPTER 3

vGW Series and SRX Series Devices

- [vGW Series and SRX Series Security Zones on page 13](#)
- [Enabling the Junoscript Interface for vGW Series on page 14](#)
- [Configuring Zone Objects for vGW Series Interoperability with SRX Series Devices on page 15](#)
- [About Populating vGW Series Records to SRX Series Zone Address Books on page 17](#)
- [Validating vGW Series Interoperability with SRX Series Zones on page 17](#)

vGW Series and SRX Series Security Zones

This topic includes the following sections:

- [About SRX Series Services Gateway Security Zones on page 13](#)
- [SRX Series Services Gateway Zones and the vGW Series on page 14](#)

About SRX Series Services Gateway Security Zones

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

Security zones are logical entities to which one or more interfaces on the SRX Series device are bound.

On a single SRX Series 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. You can define many security zones, bringing finer granularity to your physical 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.

SRX Series devices support many types of security zones.

SRX Series Services Gateway Zones and the vGW Series

vGW Series zone synchronization feature provides an automated way to link the vGW Series virtualized security layer with the SRX Series Services Gateway physical device and network security.

vGW Series zone feature simplifies VM-to-zone mapping by importing into the virtualized environment zones configured on SRX Series devices.

You can use these zone assignments to:

- Apply zone policies to use between VMs.
- Integrate zones with compliance checking to ensure that VMs are attached only to authorized zones.

The process that the vGW Series undertakes to synchronize SRX Series zones with VMs consists of a number of steps, including defining:

- An SRX object. This process entails obtaining zone configuration information from the SRX Series device, mapping zones to the vGW Series interface, and associating VLANs or network ranges with each zone.
- Zones as Smart Groups within the vGW Series based on the VLANs and the networks associated with each zone.

vGW Series also validates that Smart Groups dynamically associated with each VM are associated with the appropriate zone. This process allows for policy enforcement between vGW Series VMs and SRX Series zone compliance validations.

Related Documentation

- *Understanding vGW Series*
- For additional information on vGW Series integration with other Juniper Networks products, including in-depth coverage of STRM, SRX for zone synchronization, and SRX-IDP, see the Security Virtualization Application note at <http://www.juniper.net/us/en/solutions/enterprise/data-center/secure>.

Enabling the Junoscript Interface for vGW Series

To allow the vGW Series to gain access to the SRX Series device for zone synchronization, you must enable the secure Junoscript XML scripting API. To do so:

1. Generate a digital Secure Sockets Layer (SSL) certificate, and install it on the SRX Series device.
 - a. Enter the following openssl command in your SSH command-line interface on a BSD or Linux system on which openssl is installed. The openssl command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout mycert.pem -out mycert.pem
```

- b. Type the appropriate information in the identification form, when prompted. For example, type US for the county name.
- c. Copy the certificate that you generated from the operating system to the SRX Series device. In this example, the certificate is copied to the `/var/tmp/` directory.

```
scp mycert.pem user@host:/var/tmp/
```

- d. Install the mycert.pem SSL certificate on the SRX Series device. Using the CLI, enter the following statement in configuration mode:

```
[edit]
user@host# set security certificates local mycert load-key-file
/var/tmp/mycert.pem
```

2. Enable HTTPS for Web management access at the system level. Specify the SSL certificate and the web management port.

You can enable HTTPS access on specified interfaces. If you do not specify an interface, HTTPS is enabled on all interfaces. In this example, `ge-0/0/0.0` is used.

```
[edit]
user@host# set system services web-management https local-certificate mycert
user@host# set system services web-management https interface ge-0/0/0.0
user@host# set system services web-management https port 443
```

3. Configure the *zone* to allow HTTPS as the protocol for host inbound traffic for Web management on all of its interfaces.

```
[edit]
user@host# set security zones security-zone trust host-inbound-traffic system services
https
```

4. Configure the IP address for the interface, if it is not already configured.
5. Enable Junoscript communications using the newly created certificate:

```
[edit] user@srx# set system services xnm-ssl local-certificate mycert
```

Related Documentation

- [vGW Series and SRX Series Security Zones on page 13](#)
- [Understanding the vGW Series SRX Zones Settings](#)
- [About Populating vGW Series Records to SRX Series Zone Address Books on page 17](#)
- [Understanding vGW Series](#)

Configuring Zone Objects for vGW Series Interoperability with SRX Series Devices

To create a new SRX Series zone object, using the vGW Security Design VM interface:

1. Select the Settings module.
 - a. In the Security Settings box on the left pane, select **SRX Zones**.
 - b. Click the **Add** button on the lower right side of the page.

The Add SRX Zone dialog box appears.

- c. Specify the following information for the SRX Series zone in the Add SRX Zone pane:

- **Name**—A short descriptive name for the SRX Series zone object. This name is used in VM zone labels.
- **Host**—Device management IP address on the SRX Series device used to connect to the vGW Security Design VM.
- **Port**—TCP port used to connect to the SRX Series device through the Junoscript interface.
- **Login and Password**—Credentials used to authenticate to the SRX Series device.

The account for the SRX Series zone object requires read access to the SRX Series device's zones, interface, network, and routing configuration. Optionally, it requires write access to the Address Book for each zone to populate it with VM entries.

If you do not want the system to enter VM objects in the SRX Series device's address book, you do not need to provide write access.

- **VMs associated with this SRX**—This optional parameter specifies the VMs scope. It can be a smart group that defines VMs that are relevant to the SRX Series device.

2. Define synchronization intervals and relevant interfaces, by clicking **Load Zones** after you save the SRX Series zone object definition.

After the zone synchronization process has completed, a list of zones that the vGW Series retrieved appears. You can select the zones to import into the vGW Series as VM zone groupings.

You can configure zone synchronization to automatically poll the SRX Series device for zone updates.

To configure the vGW Series automatic zone synchronization process to control synchronization update, specify the following information:

- **Update Frequency**—How often to query the SRX Series device for updates (interval).
- **Relevant Interfaces**—Select the SRX Series device interfaces to be monitored by vGW Series. vGW Series discovers any new zones assigned to the relevant interfaces and adds them for monitoring.

SRX Series zones that participate in the synchronization process are automatically created in the vGW Series as VM Smart Groups. A Smart Group is created based on the following parameters:

- VLANs associated with the SRX Series device interface.
- The subnet defined on the SRX Series device interface and routes defined within a zone.

If the zone synchronization configuration includes a VM associated selection, the group you select is included in the Smart Group Definition.

- Related Documentation**
- [vGW Series and SRX Series Security Zones on page 13](#)
 - [About Populating vGW Series Records to SRX Series Zone Address Books on page 17](#)
 - [Understanding vGW Series](#)

About Populating vGW Series Records to SRX Series Zone Address Books

vGW Series to SRX Series zones synchronization feature allows VM records to be populated in the SRX Series address book for the zone that the VM belongs to. This allows the VM-to-zone mapping validation to occur within the context of the SRX Series device management.

When a VM record is added to an SRX Series device's zone address book, it is created with the name of the VM as defined in vCenter. A string is prepended to the name of the VM in its address book entry to indicate that it is an auto-generated VM record. By default, the string "VM-" is used, but you can change the name in the synchronization dialog box. If you change this string, vGW will attempt to update all of your existing entries to use the new string. Your existing entries are not lost or removed.

- Related Documentation**
- [vGW Series and SRX Series Security Zones on page 13](#)
 - [Configuring Zone Objects for vGW Series Interoperability with SRX Series Devices on page 15](#)
 - [Validating vGW Series Interoperability with SRX Series Zones on page 17](#)
 - [Understanding vGW Series](#)

Validating vGW Series Interoperability with SRX Series Zones

When the VM zone attachment information is accessible within the vGW Security Design VM, you can incorporate it into the policy automation and compliance checking procedures.

For VMs that do not meet compliance requirements, immediate action can be taken. You can create a noncompliant group and group policy to lock out noncompliant VMs from the network. Any noncompliant VMs are added to this group.

- Related Documentation**
- [Configuring Zone Objects for vGW Series Interoperability with SRX Series Devices on page 15](#)
 - [About Populating vGW Series Records to SRX Series Zone Address Books on page 17](#)
 - [vGW Series and SRX Series Security Zones on page 13](#)
 - [Understanding vGW Series](#)

PART 4

Index

- [Index on page 21](#)

Index

Symbols

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

A

address books.....	17
--------------------	----

B

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

C

comments, in configuration statements.....	xi
compliance check procedures	
VM-to-zone mapping attachment.....	17
conventions	
text and syntax.....	x
curly braces, in configuration statements.....	xi
customer support.....	xii
contacting JTAC.....	xii

D

documentation	
comments on.....	xi

F

font conventions.....	x
-----------------------	---

G

group policy	
for checking VM-to-zone mapping	17

I

IDP Series interoperation.....	9
--------------------------------	---

J

Junoscript XML interface.....	14
-------------------------------	----

M

manuals	
comments on.....	xi

N

Netflow	
to Juniper STRM devices.....	3

P

parentheses, in syntax descriptions.....	xi
--	----

S

SRX Series devices.....	15, 17
SRX Series zones	
SRX Series interoperability.....	15
VM-to-zone mapping.....	17
STRM Series devices.....	3
support, technical See technical support	
syntax conventions.....	x
Syslog	
to Juniper STRM devices.....	3

T

technical support	
contacting JTAC.....	xii

V

vGW Series and Juniper Networks interoperation	
IDP Series inter-operation.....	9
vGW Series interoperability	
creating SRX Series zone objects.....	15
Junoscript XML interface.....	14
populating zone address books with VM	
records.....	17
SRX Series devices.....	15
SRX Series zone objects.....	15, 17
STRM Series devices.....	3
VM-to-zone mapping.....	17

Z

zone address books.....	17
zones.....	15, 17

