APPLICATION NOTE

BRANCH SRX SERIES SERVICES GATEWAYS GOLDEN CONFIGURATIONS

How to Configure Branch SRX Series Services Gateways for Several Common Deployment Scenarios

Table of Contents

Table of Figures

Introduction

The purpose of this application note is to walk the reader through the steps necessary to configure out-of-the-box branch Juniper Networks® SRX Series Services Gateways out to provide secure connectivity to the Internet and remote sites. The example configurations can be leveraged to build more complicated configurations that will meet the security requirements of modern branch and remote offices.

After reading this document, you should be able to configure a branch SRX Series gateway to pass traffic and provide several common security services.

Scope

This paper introduces the Juniper Networks Junos® operating system command-line interface (CLI) and helps the reader configure an SRX Series device for the first time and provide a building block for more advanced configurations. It does not include advanced security configuration examples or network design guidelines. Additional Juniper Networks documentation is available for readers at **www.juniper.net/techpubs/software/Junos/index.html#srx**.

Design Considerations

Hardware Requirements

Juniper Networks Branch SRX Series Services Gateways for the branch (Certain features described in this document are not available across the entire SRX Series platform. Readers should consult Juniper Networks product-specific literature for more details.).

Software Requirements

Junos OS Release 10.0 or later for all SRX Series Services Gateways (A more recent release is required for all SRX Series Services Gateways supported and released after 9.5.).

Description and Deployment Scenario

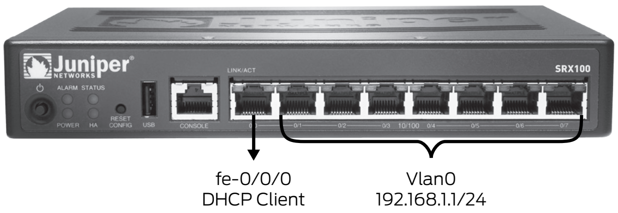
The included examples are not intended to be Juniper recommended configurations, as they only meet the security requirements of the simplest deployments such as a small home office. However, with some modification, they can be used to connect and secure larger remote and branch offices to a larger central site.

The approach of this document is to begin with an SRX Series appliance as it ships from the factory and progressively work through the steps necessary to build a usable base configuration.

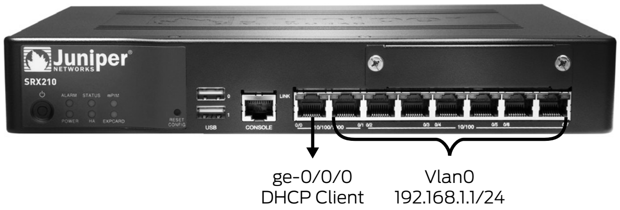
Default Configuration—Junos OS Release 10.0 and Later

The first configuration is often associated with default firewall behavior. Juniper Networks SRX100 Services Gateway, SRX210 Services Gateway, and SRX240 Services Gateway have all of their interfaces configured in a similar fashion. The interface ge-0/0/0 is in Layer 3 mode, and all the other interfaces are switched and assigned to a VLAN. A VLAN interface is created to route traffic from the interfaces in the VLAN. All traffic between the ports within the VLAN is locally switched.

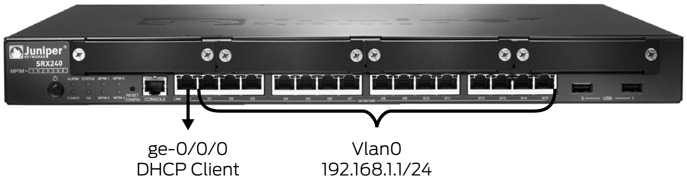
SRX100



SRX210



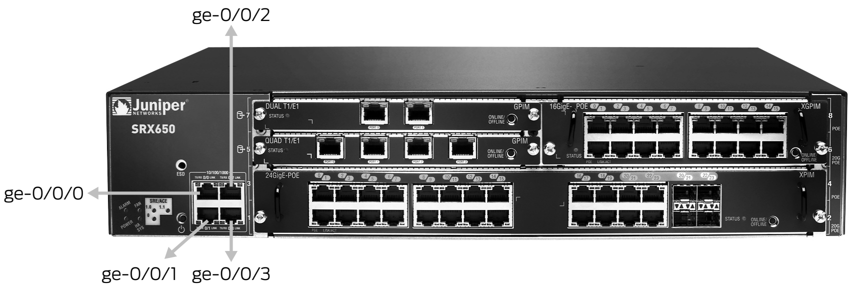
SRX240



The following default configurations apply to the SRX100, SRX210, and SRX240 factory default settings.

INTERFACE	SECURITY ZONE	DHCP STATE	IP ADDRESS
ge-0/0/0 (for SRX210 and SRX240) fe-0/0/0 (for SRX100)	untrust	Client	Dynamically Assigned
vlan0	trust	Server	192.168.1.1/24

SRX650



The default configuration for the interfaces on the SRX650 is different. All the interfaces are configured as Layer 3 interfaces. The following table summarizes the default interface configuration on the SRX650.

INTERFACE	SECURITY ZONE	DHCP STATE	IP ADDRESS
ge-0/0/0	untrust	Client	Dynamically Assigned
ge-0/0/1	trust	Server	192.168.1.1/24
ge-0/0/2	trust	Server	192.168.2.1/24
ge-0/0/3	trust	Server	192.168.3.1/24

By default, the following security policies and NAT rules are created on the SRX Series security policies.

SOURCE ZONE	DESTINATION ZONE	POLICY ACTION
trust	untrust	permit

NAT Rule

SOURCE ZONE	DESTINATION ZONE	NAT ACTION
trust	untrust	Source NAT to untrust zone interface

Using the Default Configuration for Network Access

To illustrate a common default firewall configuration, an SRX210 is used, and the following design assumptions are made:

- The protected network is connected to interface ge-0/0/1 and fe-0/0/2 in the trust zone.
- Connectivity to the Internet is through interface ge-0/0/0 in the untrust zone.
- The IP address of interface ge-0/0/0 is assigned via DHCP.

Note: The interfaces ge-0/0/1 and fe-0/0/2 are a part of the default VLAN. The protected hosts can be connected to any one of the ports that are part of the default VLAN.

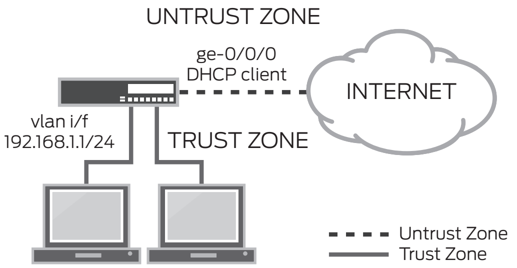


Figure 1: Branch office network infrastructure

Configuration

An SRX Series device can be configured from the CLI or through Juniper Networks J-Web Software GUI. In this example to use J-Web, connect a management PC to interface ge-0/0/1. The IP address of the PC can be statically configured or assigned by the factory default DHCP server enabled on VLAN interface.

For this example, the SRX Series device is configured using the CLI, and the management PC is assigned an IP address from the DHCP server process on the SRX Series gateway.

To access an SRX Series device with the Junos OS CLI:

- Connect one end of the console cable to the serial port adapter, plug the adapter into a serial port on the PC or laptop, and plug the other end of the cable into the console port on the SRX Series device.
- Start the terminal emulation program on the PC or laptop, select the COM port, and configure the following port settings: 9600 (bits per second), 8 (data bits), none (parity), 1 (stop bits), and none (flow control).
- Press the POWER button on the router, and verify that the POWER LED turns green.
- Log in as *root*, and press Enter at the Password prompt. (*When booting the factory default configuration, you do not need to enter a password.*)
- Enter the UNIX shell after you are authenticated through the CLI:

```
Amnesiac (ttyu0)

login: root
Password:

--- JUNOS 10.0R1.8 built 2009-08-01 09:23:09 UTC
```

- At the % prompt, type “cli” to start the CLI and press Enter. The prompt changes to an angle bracket (>) when you enter CLI operational mode.

```
root@% cli
root>
```

- At the (>) prompt, type “configure” and press Enter. The prompt changes from > to # when you enter configuration mode.

```
root> configure
Entering configuration mode
[edit]
root#
```

To configure the SRX Series device to be deployed in the network to securely pass traffic using the default configuration, use the following two commands:

1. Create a password for the root user to manage the SRX Series device.

```
set system root authentication plain-text-password (will prompt for password)
```

2. Use the “commit” command at the CLI prompt to activate the configuration.

```
commit
```

Default Firewall Configuration—Junos OS Release 9.6 and Earlier

The first configuration is often associated with default firewall behavior. All outbound traffic from a private network is allowed and uses source NAT, while inbound traffic from the Internet not matching an established session is blocked.

The first time that a branch SRX Series gateway is powered on, it boots using the factory default configuration as follows:

- A trust zone and untrust zone are created.
- Interface ge-0/0/0 is assigned the IP address 192.168.1.1 and is bound to the trust zone.
- A DHCP server instance is enabled on interface ge-0/0/0.
- Three security policies, one inter-zone and two intra-zone, are created:
  - trust zone to trust zone (intra-zone)—default permit policy
  - trust zone to untrust zone (inter-zone)—default permit policy
  - untrust zone to trust zone (inter-zone)—default deny policy

To illustrate a common default firewall configuration, an SRX210 is used, and the following design assumptions are made:

- The protected network is connected to interface ge-0/0/0 in the trust zone.
- Connectivity to the Internet is through interface fe-0/0/7 in the untrust zone.
- The IP address of interface fe-0/0/7 is either statically configured or assigned via DHCP.

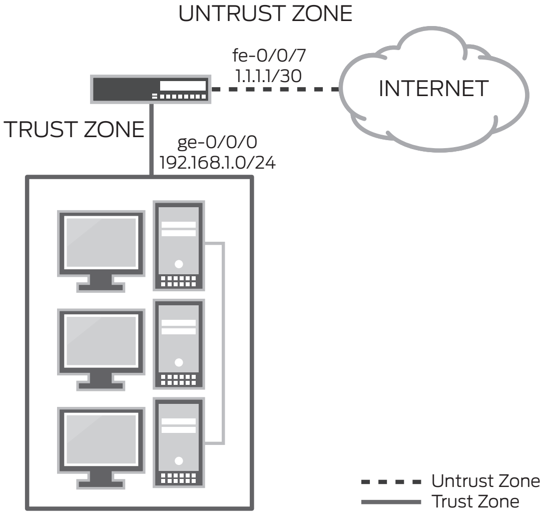


Figure 2: Branch office network infrastructure

Configuration

An SRX Series device can be configured from the CLI or through the J-Web GUI. To use J-Web, connect a management PC to interface ge-0/0/0. The IP address of the PC can be statically configured or assigned by the factory default DHCP server enabled on ge-0/0/0.

For this example, the SRX Series device is configured using the CLI, and the management PC is assigned a static IP address of 192.168.1.10/24 with a default gateway of 192.168.1.1.

To access an SRX Series device with the Junos OS CLI:

- Connect one end of the console cable to the serial port adapter, plug the adapter into a serial port on the PC or laptop, and plug the other end of the cable into the console port on the SRX Series device.
- Start the terminal emulation program on the PC or laptop, select the COM port, and configure the following port settings: 9600 (bits per second), 8 (data bits), none (parity), 1 (stop bits), and none (flow control).
- Press the POWER button on the router, and verify that the POWER LED turns green.
- Log in as root, and press Enter at the Password prompt. (W*hen booting the factory default configuration, you do not need to enter a password.*)
- Enter the UNIX shell after you are authenticated through the CLI:

  Amnesiac (ttyu0)

  ```
  login: root
  Password:

  JUNOS 9.4B3 built 2008-12-19 00:28:15 UTC
  root@%
  ```

- At the % prompt, type “cli” to start the CLI and press Enter. The prompt changes to an angle bracket (>) when you enter CLI operational mode.

  ```
  root@% cli
  root>
  ```

- At the (>) prompt, type “configure” and press Enter. The prompt changes from > to # when you enter configuration mode.

  ```
  root> configure
  Entering configuration mode

  [edit]
  root#
  ```

Configuring Management Access

Next, the SRX Series device is configured to allow secure management access and apply NAT to all outbound traffic.

1. Set the root user password.

```
set system root-authentication plain-text-password(will prompt for password)
```

2. Set the system host name.

```
set system host-name mysrx
```

3. Assign interface fe-0/0/7 to the untrust zone (zone names are case sensitive).

```
set security zone security-zone untrust interface fe-0/0/7
```

4. Set name server parameter.

```
set system name-server <ip address>
```

5. fe-0/0/7 IP address and default route configuration.

   a) To assign the IP address and gateway statically:

```
set interfaces fe-0/0/7 unit 0 family inet address 1.1.1.1/30
set routing-options static route 0.0.0.0/0 next-hop < ip address of the
upstream router>
```

   b) To configure interfaces fe-0/0/7 to obtain an IP address and default gateway from a DHCP server:

```
set interfaces fe-0/0/7 unit 0 family inet dhcp
set security zones security-zone untrust interfaces fe-0/0/7.0 host-inbound-
traffic system-services dhcp
```

6. Create a NAT rule for source translation of all Internet-bound traffic.

```
set security nat source rule-set interface-nat from zone trust
set security nat source rule-set interface-nat to zone untrust
set security nat source rule-set interface-nat rule rule1 match source-address
0.0.0.0/0 destination-address 0.0.0.0/0
set security nat source rule-set interface-nat rule rule1 then source-nat interface
```

7. Use the “commit” command at the CLI prompt to activate the configuration.

```
commit
```

Firewall Configuration for Outbound Access Using Integrated Routing and Bridging (IRB)

To eliminate the need for an external switch (if the SRX Series device has enough available ports), an SRX Series gateway can be configured to provide switching and routing simultaneously. Starting with Junos OS Release 10.0, the factory default configuration has integrated routing and bridging (IRB) enabled.

An SRX Series device uses virtual L3 interfaces to support IRB, equivalent to routing between a set of switched and routed interfaces. Today, this design is widely adopted on enterprise switches. Implementing route bridging in a security device is more challenging than in a switch because security policies are applied to both inter-zone and intra-zone traffic. Junos OS implements IRB with the help of VLANs combined with interfaces. A VLAN is a collection of interfaces that can be grouped together into a broadcast domain. Junos OS-based switches Ethernet frames within a VLAN rather than routing IP packets. A virtual interface, called *VLAN*, is used to route traffic between the switched ports and routed ports. This architectural approach is very similar to connecting a standalone switch to a port on the firewall.

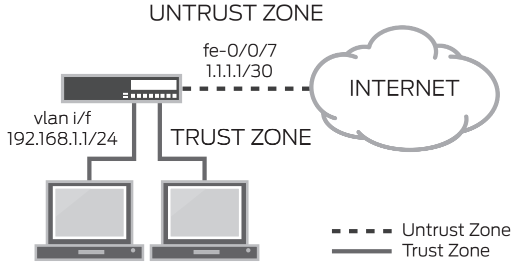


Figure 3: Branch office network infrastructure with IRB

Note: Readers might want to skip this configuration and try it at the end as subsequent examples build upon the first example.

- To illustrate this firewall configuration, make the following design assumptions:
- Interface fe-0/0/7 provides connection to the Internet.
- A VLAN is created by grouping the following interfaces:
  - ge-0/0/0
  - ge-0/0/1
  - fe-0/0/2
  - fe-/0/0/3
- A VLAN interface with an IP address 192.168.1.1/24 is created to route traffic between switch ports and the routed interface fe-0/0/7.

Configuration

1. Remove the factory default IP address from the interface ge-0/0/0.

```
delete interfaces ge-0/0/0 unit 0 family inet
```

2. Configure Ethernet switching on the interfaces that are part of the VLAN.

```
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family ethernet-switching
set interfaces fe-0/0/2 unit 0 family ethernet-switching
set interfaces fe-0/0/3 unit 0 family ethernet-switching
```

3. Configure a VLAN interface to route traffic between the switched ports and routed interface.

```
set interfaces vlan unit 0 family inet address 192.168.1.1/24
```

4. Assign a VLAN interface to the default VLAN.

```
set vlans default l3-interface vlan.0
```

Note: SRX Series gateways are preconfigured with a system-defined VLAN with name "default" and VLAN-ID "1."

5. Assign the VLAN interface to the trust security zone.

```
set security zones security-zone trust interfaces vlan.0
```

Advanced Configuration

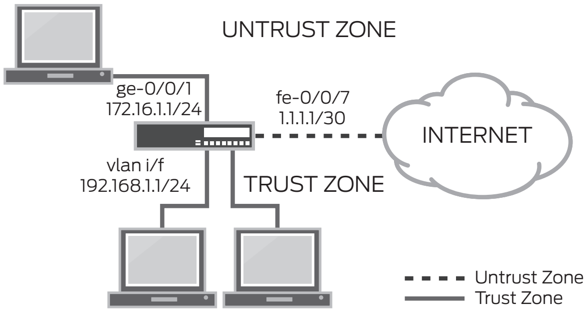


Figure 4: Branch office with three zones

This scenario uses the following design assumptions:

1. Create an administrative user to manage the SRX Series device.

2. Create a read-only administrative user.

3. Set system hostname.

4. Set the DNS server and NTP server parameters.

5. A DMZ zone is created for securing server access with an IP address of 172.16.1.1/24 and enabling "ping" service on the zone.

6. Interface ge-0/0/1 is assigned to the DMZ zone.

7. Interface ge-0/0/0 provides connectivity to the Internet.

8. All networking parameters are statically assigned.

9. The following security policies are required:

   a. Allow HTTPS traffic from the untrust zone to the DMZ zone.

   b. Allow DNS traffic from the DMZ zone to the untrust zone.

   c. Allow SSH and HTTPS traffic from the host 192.168.1.200/24 from the trust zone to the server in the DMZ zone.

Configuring Steps

All the commands are executed from the configuration mode unless otherwise noted.

1. Creating the administrative user to manage the SRX Series device.

```
set system login user <username> class super-user
set system login user <username> authentication plain-text-password (will prompt
for password)
```

2. Creating the read-only administrative user.

```
set system login user <username> class read-only
set system login user <username> authentication plain-text-password (will prompt
for password)
```

3. Setting the system hostname.

```
set system host-name mysrx
```

4. Setting the DNS and NTP servers.

```
set system name-server <ip address of server>
set date ntp <server_ip address>- This is an operational mode command. Operational
mode commands can be executed in the configuration mode by using the key word “run”
```

5. Creating the DMZ zone and allowing ping service.

```
set security zones security-zone dmz host-inbound-traffic system-services ping
```

6. Assigning interface ge-0/0/1 to the DMZ zone.

```
set security zones security-zone dmz interfaces ge-0/0/1
```

Note: If using the factory default with Junos OS 10.0 release, all of the interfaces except ge-0/0/0 will have ethernet switching enabled by default. This configuration is accomplished by applying ethernet switching to a group “interface-trust” and applying the group configuration to the interfaces.

```
delete interfaces interface-range interfaces-trust member ge-0/0/1
```

7. Configuring networking parameters.

a. Assigning IP address

```
set interfaces ge-0/0/0 unit 0 family inet address 1.1.1.1/30
set interfaces ge-0/0/1 unit 0 family inet address 172.16.1.1/24
```

b. Creating a default route

```
set routing-options static route 0.0.0.0/0 next-hop <ip address>
```

8. Configuring security policies.

a. Security policy from untrust to DMZ

```
set security zones security-zone dmz address-book address webserver
172.16.1.250/24 -  Creates an address book entry for the webserver
set security policies from-zone untrust to-zone dmz policy webserver-access match
source-address any
set security policies from-zone untrust to-zone dmz policy webserver-access match
destination-address webserver
set security policies from-zone untrust to-zone dmz policy webserver-access match
application junos-https
set security policies from-zone untrust to-zone dmz policy webserver-access then
permit
```

b. Security policy from DMZ to untrust

```
set security policies from-zone dmz to-zone untrust policy dns-access match
source-address webserver
set security policies from-zone dmz to-zone untrust policy webserver-access match
destination-address any
set security policies from-zone dmz to-zone untrust policy webserver-access match
application junos-dns
set security policies from-zone dmz to-zone untrust policy webserver-access then
permit
```

c. Allow SSH and HTTPS traffic from the host 192.168.1.200/24 from trust zone to DMZ zone server

```
set security zones security-zone trust address-book address mgt-pc
192.168.1.200/24 -  Creates an address book entry for the management PC

set applications application-set mgt-services application junos-https
set applications application-set mgt-services application junos-ssh

set security policies from-zone trust to-zone dmz policy mgt-access match source-
address mgt-pc
set security policies from-zone trust to-zone dmz policy mgt-access match
destination-address webserver
set security policies from-zone trust to-zone dmz policy mgt-access match
application mgt-services
set security policies from-zone trust to-zone dmz policy mgt-access then permit
set security policies from-zone trust to-zone dmz policy mgt-access then log
session-init
```

IPsec VPN Configuration

To illustrate a site-to-site IPsec VPN configuration, simply add VPN specifics to the first configuration using the following design parameters:

- A route-based IPsec VPN with preshared keys is used between sites.
- The protected network is connected to interface ge-0/0/0 in the trust zone.
- Connectivity to the Internet is through fe-0/0/7 in the untrust zone.
- The remote IPsec endpoint IP address is 1.1.1.2, and the protected subnet at the remote site is 10.1.1.0/24.
- All traffic to the subnet 10.1.1.0/24 is encrypted.

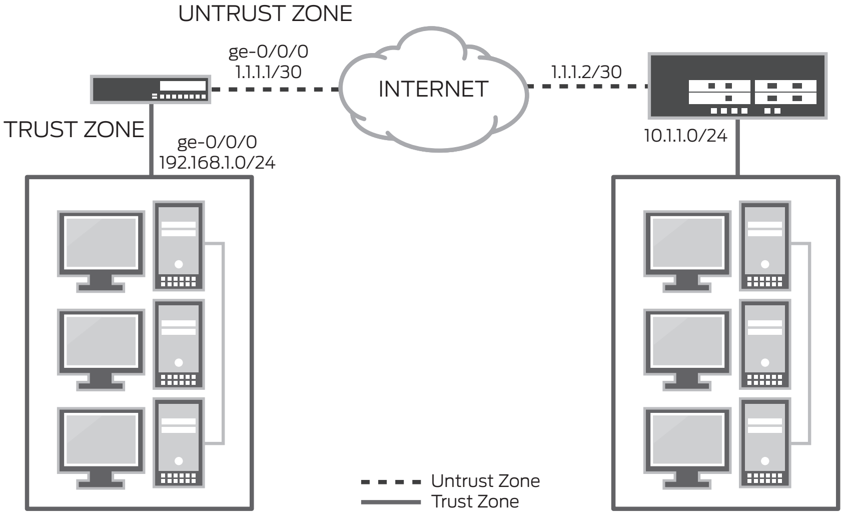


Figure 5: IPsec corporate and branch office network infrastructure

Configuration

To illustrate the simplicity of setting up IPsec tunnels, the command sequence is divided into to four repeatable steps. Readers should refer to standard Juniper Networks documentation to further understand the various IKE/IPsec configuration options.

1. Create a secure tunnel interface.

```
set interfaces st0 unit 0 family inet
set security zones security-zone trust interfaces st0.0
```

2. Configure routing.

```
set routing-options static route 10.1.1.0/24 next-hop st0.0
```

3. Enable IKE services on the external interface.

```
set security zones security-zone untrust interface ge-0/0/0 host-inbound-traffic
system-services ike
```

4. Configure IKE Phase 1 parameters.

```
set security ike proposal P1-AES authentication-method pre-shared-keys
set security ike proposal P1-AES dh-group group2
set security ike proposal P1-AES authentication-algorithm sha1
set security ike proposal P1-AES encryption-algorithm aes-128-cbc

set security ike policy ike-policy-1 mode main
set security ike policy ike-policy-1 proposals P1-AES
set security ike policy ike-policy-1 pre-shared-key ascii-text juniper
set security ike gateway gw1 address 1.1.1.2
set security ike gateway gw1 external-interface ge-0/0/0.0
set security ike gateway gw1 ike-policy ike-policy-1
```

5. Configure IPsec Phase 2 parameters.

```
set security ipsec proposal P2-AES protocol esp
set security ipsec proposal P2-AES authentication-algorithm hmac-sha1-96
set security ipsec proposal P2-AES encryption-algorithm aes-128-cbc

set security ipsec policy ipsec-policy-1 proposals P2-AES
set security ipsec policy ipsec-policy-1 perfect-forward-secrecy keys group2
set security ipsec vpn vpn1 ike gateway gw1
set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy-1
set security ipsec vpn vpn1 establish-tunnels immediately
set security ipsec vpn vpn1 bind-interface st0.0
```

6. Use the “commit” command at the CLI prompt in the configuration mode to activate the configuration.

```
Commit.
```

UTM Configuration

The example continues with the addition of several common UTM features to the configuration. Before configuring any UTM features, the UTM feature license must be installed on the device.

The license keys can be installed using one of the following two methods. These commands are operational mode commands.

1. Download from LMS server directly (recommended—access to the Internet is required for this operation).

```
request system license update
```

2. Install manually (this process is used when the license keys are available as text file).

```
request system license add terminal
```

You can now verify that the license was installed using the operational mode command “show system license.”

Antivirus Configuration

Having the SRX Series use the express antivirus engine to scan HTTP traffic is also very easy.

1. Configure the SRX Series device to use the express antivirus engine.

```
set security utm feature-profile anti-virus type juniper-express-engine
```

2. Configure a UTM policy to use the predefined antivirus profile http-profile "junos-eav-defaults."

```
set security utm utm-policy custom-utm-policy anti-virus http-profile junos-eav-
defaults
```

3. Apply the UTM policy to the existing trust to untrust security policy.

```
set security policies from-zone trust to-zone untrust policy default-permit then
permit application-services utm-policy custom-utm-policy
```

4. Use the "commit" command at the CLI prompt in the configuration mode to activate the configuration

```
Commit.
```

Note: The predefined profile "junos-eav-defaults" is preconfigured with antivirus engine fallback options, scanning options, and notification messages. The defaults can be viewed by using the operational mode command:

```
show configuration groups junos-defaults security utm feature-profile anti-virus
juniper-express-engine profile junos-eav-defaults
```

Web Filtering Configuration

Using the SRX Series to filter Web traffic is also very straightforward.

1. Configure the SRX Series to use the integrated Web filtering engine.

```
set security utm feature-profile web-filtering type surf-control-integrated
```

2. Configure the predefined Web filtering profile "junos-wf-cpa-default" to use the utm-policy configured earlier.

```
set security utm utm-policy custom-utm-policy web-filtering http-profile junos-wf-
cpa-default
```

3. Use the "commit" command at the CLI prompt in the configuration mode to activate the configuration.

```
Commit.
```

Note: The predefined profile "junos-wf-cpa-default" is configured to use the SurfControl CPA URL category database hosted by Websense that contains over 26 million websites, classified into 40 easy-to-use categories.

```
show configuration groups junos-defaults security utm feature-profile web-filtering
surf-control-integrated
```

IDP Series Configuration

The SRX Series offers the same set of IDP signatures that are available on Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to secure networks against attacks. In this example configuration, the SRX Series device is configured to use a predefined IDP Series policy to secure the network.

1. Download and install the latest security package.

```
request security idp security-package download
request security idp security-package install
```

2. Download and install the IDP security policy templates.

```
request security idp security-package download policy-templates
request security idp security-package install policy-templates
```

3. Enable the templates.xsl scripts file. (At commit time, the Junos OS management process—mgd—searches the /var/db/scripts/commit directory for scripts and runs the script against the candidate configuration database to ensure the configuration conforms to the rules dictated by the scripts.)

```
set system scripts commit file templates.xsl
```

4. Commit the configuration.

```
commit
```

5. Configure an active IDP policy.

```
set security idp active-policy Recommended
```

Note: We recommend a predefined IDP policy. Use “set security idp active-policy ?” to view the list of IDP policies.

6. Enable IDP Series detection on the existing firewall security policy from the trust zone to the untrust zone.

```
set security policies from-zone trust to-zone untrust policy default-permit then
permit application-services idp
```

Appendix

Factory Default Configuration Junos OS Release 10.0

```
set system autoinstallation delete-upon-commit
set system autoinstallation traceoptions level verbose
set system autoinstallation traceoptions flag all
set system autoinstallation interfaces ge-0/0/0 bootp
set system name-server 208.67.222.222
set system name-server 208.67.220.220
set system services ssh
set system services telnet
set system services web-management http interface vlan.0
set system services web-management https system-generated-certificate
set system services web-management https interface vlan.0
set system services dhcp router 192.168.1.1
set system services dhcp pool 192.168.1.0/24 address-range low 192.168.1.2
set system services dhcp pool 192.168.1.0/24 address-range high 192.168.1.254
set system services dhcp propagate-settings ge-0/0/0.0
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file messages any critical
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands error
set system max-configurations-on-flash 5
set system max-configuration-rollbacks 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set interfaces interface-range interfaces-trust member ge-0/0/1
set interfaces interface-range interfaces-trust member fe-0/0/2
set interfaces interface-range interfaces-trust member fe-0/0/3
set interfaces interface-range interfaces-trust member fe-0/0/4
set interfaces interface-range interfaces-trust member fe-0/0/5
set interfaces interface-range interfaces-trust member fe-0/0/6
set interfaces interface-range interfaces-trust member fe-0/0/7
set interfaces interface-range interfaces-trust unit 0 family ethernet-switching
vlan members vlan-trust
set interfaces ge-0/0/0 unit 0
set interfaces vlan unit 0 family inet address 192.168.1.1/24
set security nat source rule-set trust-to-untrust from zone trust
set security nat source rule-set trust-to-untrust to zone untrust
set security nat source rule-set trust-to-untrust rule source-nat-rule match
source-address 0.0.0.0/0
set security nat source rule-set trust-to-untrust rule source-nat-rule then source-
nat interface
set security screen ids-option untrust-screen icmp ping-death
set security screen ids-option untrust-screen ip source-route-option
set security screen ids-option untrust-screen ip tear-drop
set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200
set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood destination-threshold
2048
set security screen ids-option untrust-screen tcp syn-flood timeout 20
set security screen ids-option untrust-screen tcp land
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces vlan.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services dhcp
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic
system-services tftp
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then
permit
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface vlan.0
```

Summary

Branch SRX Series Services Gateways provide all the features required to securely connect modern remote and branch offices in a one-box solution. Junos OS offers users unparalleled flexibility designed to meet the most demanding network requirements. After reading this document, you can configure a branch SRX Series device to securely pass traffic. With a little practice, you can create advanced configurations required for more complex deployments.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3500153-005-EN Mar 2010

♻ Printed on recycled paper