JUNIPER NETWORKS | Engineering Simplicity

Guided Setup: How to Configure and Operate Juniper SRX 300 Series Firewalls

Guided Setup: How to Configure and Operate Juniper SRX 300 Series Firewalls

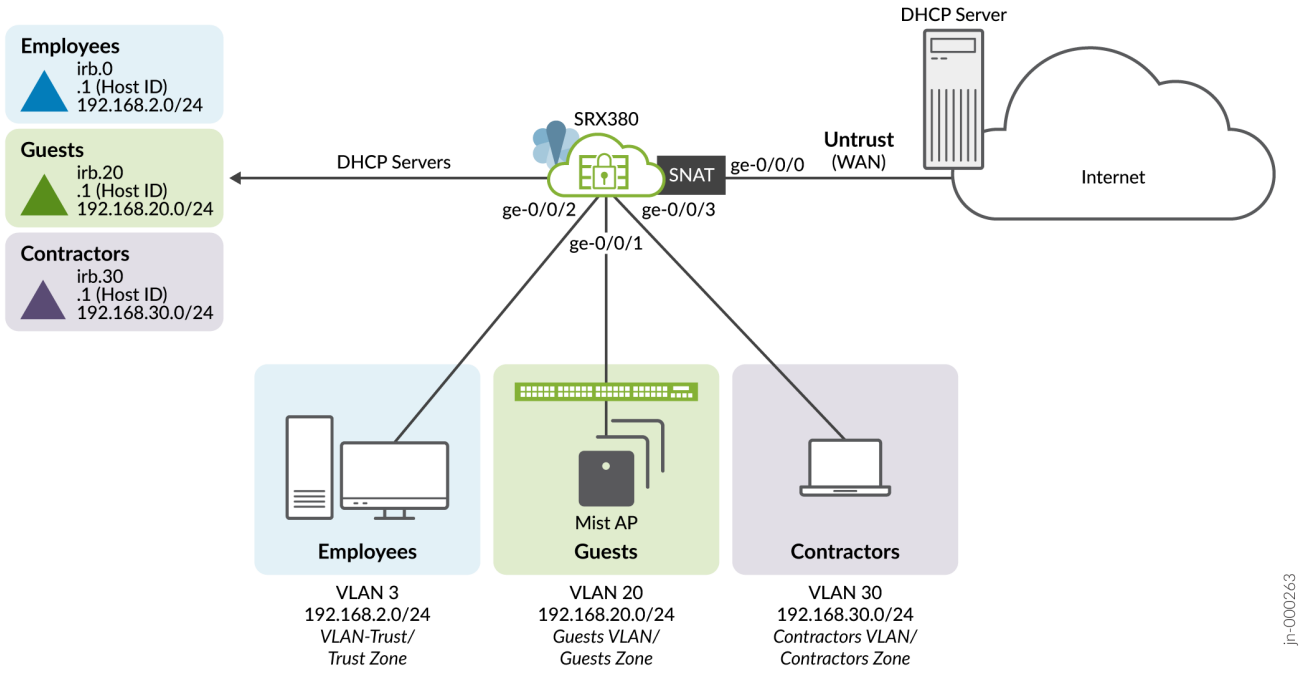
IN THIS GUIDE

About This Guide

Welcome back! You're the new owner of a branch SRX services gateway. In the companion Day One+ guide, you learned how to install and power on the SRX. We also showed you how to perform basic initial configuration using the CLI.

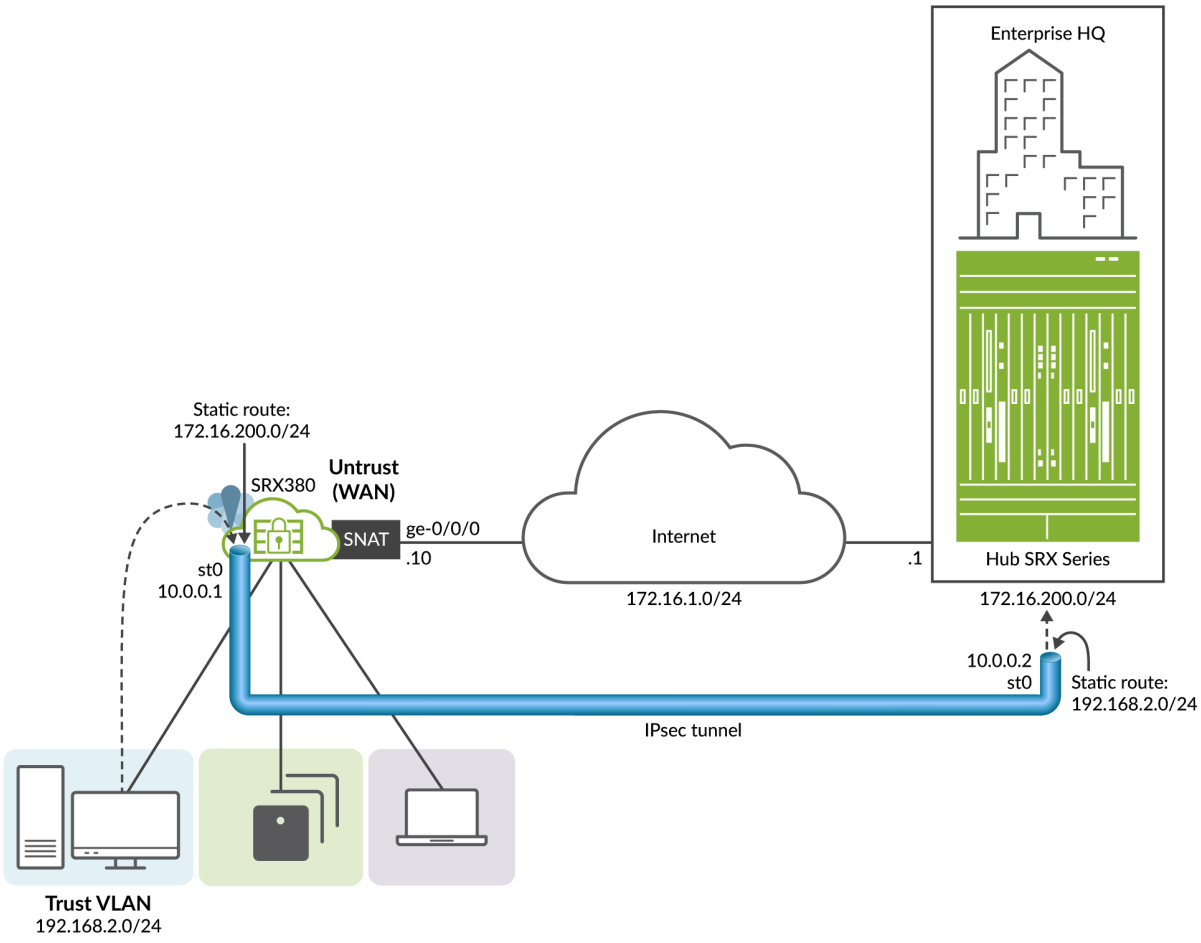
If you're eager to start using your SRX to provide secure branch connectivity, then you've come to the right place. In this guide, we'll walk you through a typical "Day in the Life" of an SRX administrator who's tasked with securely bringing a new branch office online.

In just a few quick steps, we'll have your branch office up, running, and secured! Here's what your SRX based branch office will soon look like:



When finished, you'll have VLANs, security zones, and policies that enforce your connectivity and security requirements.

Here's the highlights of your IPsec VPN. The IPsec VPN securely connects your new branch office to a remote location over the Internet.



This guide covers how to:

- Verify Default Branch Connectivity
- Configure Secure Local Branch Connectivity
- Verify Secured LAN Connectivity
- Configure an IPsec VPN
- Verify Your IPsec VPN

This guide is applicable to the SRX300, SRX320, SRX340, SRX345, and SRX380 branch SRX models. We developed and tested the procedures in this guide using an SRX380 running Junos OS release 21.4R1. The SRX380 has a dedicated management interface and supports 16x1GE and 4x10GE network interfaces. Other SRX branch models have a different port configuration and management interface, but all branch SRX models have a similar factory-default configuration.

NOTE: We'll provide a lot of links to the main documentation along the way to keep reminding you of where to find additional details. See Table 4 for additional information about the many features you can configure for the Juniper Networks SRX Services Gateway .

Step 1: Verify and Secure Local Branch Connectivity

IN THIS SECTION

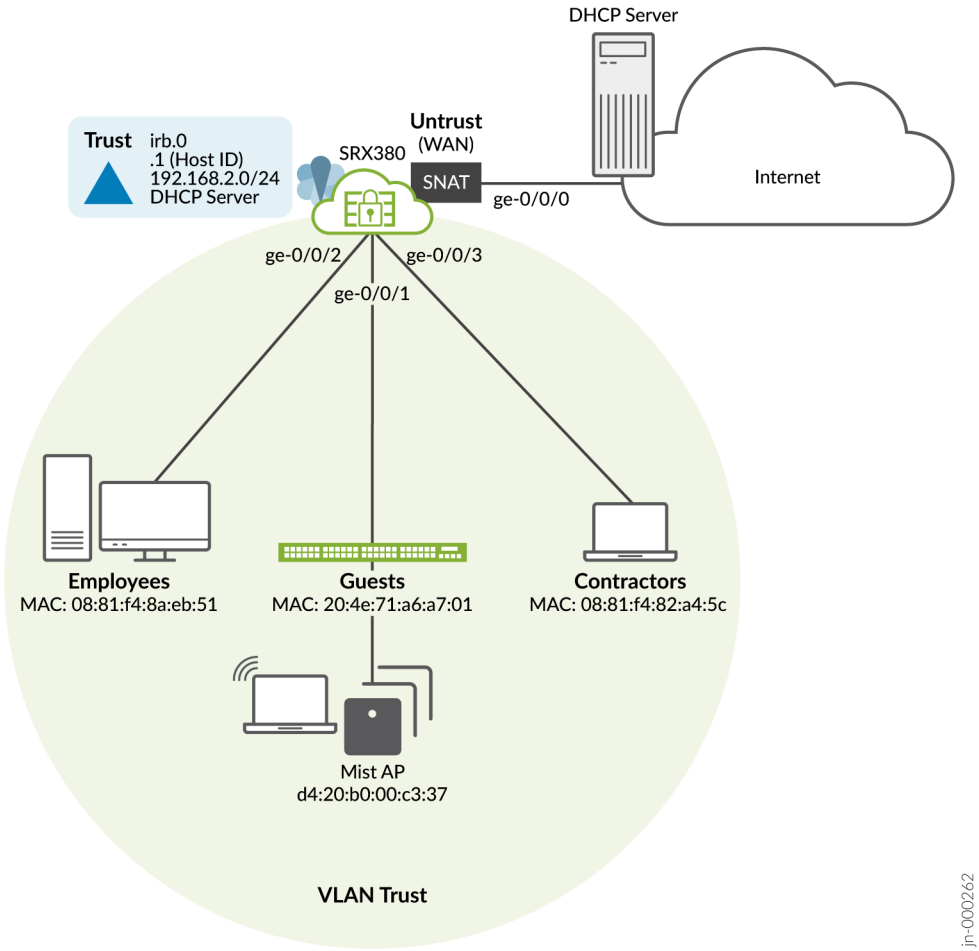
There's no better way to get to know your SRX than to just jump in and start using it. First, let's use the CLI to verify the operational state of your SRX. This step assumes you've done the initial configuration using the factory defaults, as described in the Day One+ guide. At this point, you should have both local and Internet connectivity for your branch.

Understand Branch SRX Default Connectivity

IN THIS SECTION

Secure Local Branch Connectivity on page 5 shows the ending state of your branch office after you've done the initial configuration. We'll show you how to leverage the SRX factory-default configuration to get the branch online quickly.

Figure 1: Branch SRX Default Connectivity



First, a few reminders about the Day One+ ending state for your branch SRX:

How to Access the CLI

There are several ways to access the SRX CLI. In all cases, you log in as the root user using the password that you configured in the Day One+ procedure:

- Direct console access with a serial port
- SSH access:
  - Access via a trust zone device

You can SSH to 192.168.2.1 from a device attached to a local LAN port in the Trust VLAN.

- Access via a management interface

  If the SRX has a dedicated management interface (fxp0), SSH to 192.168.1.1 from a device attached to the out of band management network.

- Remote access

  To access the SRX remotely, use the IP address assigned by the WAN provider to the ge-0/0/0 interface. Simply issue the `show interfaces ge-0/0/0 terse` command on the SRX to confirm the address assigned by the provider to the WAN interface.

Default LAN Port Configuration

- Devices attached to the LAN ports are configured to use DHCP. They receive their network configuration from the SRX. These devices obtain an IP address from the 192.168.2.0/24 address pool using the SRX as a default gateway.
- The *trust* zone LAN ports are in the same subnet with Layer 2 connectivity. All traffic is permitted between *trust* interfaces.
- All traffic originating in the *trust* zone is permitted in the *untrust* zone. Matching response traffic is allowed back from the *untrust* zone to the *trust* zone. Traffic that originates from the *untrust* zone is blocked from the *trust* zone.
- The SRX performs source Network Translation (source NAT) using the WAN interface's IP address for traffic originating from the *trust* zone and sent to the WAN *untrust* zone.
- Traffic associated with specific system services (HTTPS, DHCP, TFTP, and SSH) is permitted from the*untrust* zone to the local host. All local host services and protocols are allowed for traffic that originates in the *trust* zone.

Verify Default Branch Connectivity

IN THIS SECTION

First, let's verify the default WAN and LAN connectivity on the SRX.

Verify WAN Connectivity

IN THIS SECTION

Confirm the DHCP Client on the WAN Interface

Verify that the WAN interface received an IP address from the DHCP service provided by the Internet Service Provider (ISP). In the default configuration, the ge-0/0/0 interface is part of the *untrust* zone and is set as a DHCP client.

```
root@branch_SRX> show dhcp client binding
IP address        Hardware address   Expires     State      Interface
172.16.1.10       78:4f:9b:26:21:f5  77215       BOUND      ge-0/0/0.0
```

Confirm Internet Connectivity

Confirm Internet access with a successful ping to *www.juniper.net*.

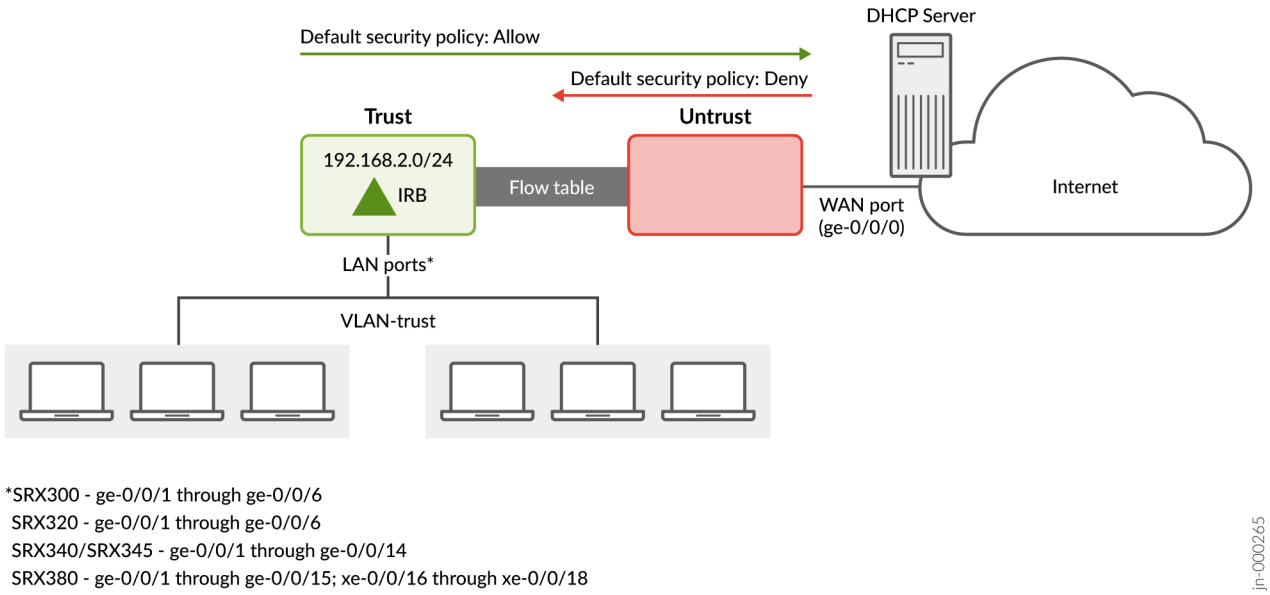
```
root@branch_SRX> ping www.juniper.net inet count 2
PING e1824.dscb.akamaiedge.net (104.100.54.237): 56 data bytes
64 bytes from 104.100.54.237: icmp_seq=0 ttl=47 time=7.268 ms
64 bytes from 104.100.54.237: icmp_seq=1 ttl=47 time=9.803 ms

--- e1824.dscb.akamaiedge.net ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.268/8.536/9.803/1.267 ms
```

Verify LAN Connectivity

IN THIS SECTION

Verify LAN connectivity. Branch SRX Default Security Policies on page 8 summarizes the factory default security zones and their behavior. Refer to Branch SRX Factory Defaults on page 5 for details on the physical connectivity and MAC addresses used by the various LAN devices.

Figure 2: Branch SRX Default Security Policies



While the port type and count varies between branch SRX models (SRX 300 Series), the factory default configuration results in the same type of connectivity:

- All LAN ports have full Layer 2 connectivity within the *trust* zone
- Traffic sent from any LAN port is allowed in the *untrust* zone
- Return traffic from the *untrust* zone is permitted back to the *trust* zone
- Traffic that originates in the *untrust* zone is blocked from the *trust* zone

Keep these defaults in mind as you continue to verify default connectivity.

Confirm LAN DHCP Server

Verify that the SRX assigns IP addresses to the LAN clients. Recall that in the factory default configuration, a Layer 3 capable Integrated Routing and Bridging (IRB) interface functions as a DCHP server for all LAN ports. Refer to Figure 1 on page 5 to map the MAC addresses shown in the output to the devices and SRX ports used in our branch office.

```
root@branch_SRX> show dhcp server binding
IP address        Session Id  Hardware address   Expires     State      Interface
192.168.2.5       3530        08:81:f4:82:a4:5c  70025       BOUND      irb.0
192.168.2.8       3529        08:81:f4:8a:eb:51  68662       BOUND      irb.0
```

```
192.168.2.13      3534        20:4e:71:a6:a7:01  86366       BOUND      irb.0
192.168.2.7       3535        d4:20:b0:00:c3:37  86126       BOUND      irb.0
```

The output confirms that the SRX device correctly assigns IP addresses from the default 192.168.2.0/24 address pool to the LAN clients.

Display VLANs

In the factory-default configuration, all LAN ports are in the same VLAN (*vlan-trust*) with full (unfiltered) Layer 2 connectivity for the shared 192.168.2.0/24 IP subnet. Use the `show vlans` command to display all VLANs on the device.

```
root@branch_SRX> show vlans

Routing instance        VLAN name             Tag          Interfaces
default-switch          default               1
                                                           ge-0/0/1.0*
                                                           ge-0/0/10.0
                                                           ge-0/0/11.0
                                                           ge-0/0/12.0
                                                           ge-0/0/13.0
                                                           ge-0/0/14.0
                                                           ge-0/0/15.0
                                                           ge-0/0/2.0*
                                                           ge-0/0/3.0*
                                                           ge-0/0/4.0
                                                           ge-0/0/5.0
                                                           ge-0/0/6.0
                                                           ge-0/0/7.0
                                                           ge-0/0/8.0
                                                           ge-0/0/9.0
                                                           xe-0/0/16.0
                                                           xe-0/0/17.0
                                                           xe-0/0/18.0
```

The output shows there are two VLANs: the `default` VLAN, assigned VLAN ID 1, and the *vlan-trust* VLAN, assigned VLAN ID 3. In the factory-default configuration, no interfaces are associated with the default VLAN. All the LAN ports are associated with the *vlan-trust* VLAN. Again, all interfaces assigned to the same VLAN have full connectivity at Layer 2.

Verify MAC Address Learning

Issue the `show ethernet-switching table` command to verify MAC learning in the *vlan-trust* VLAN.

```
root@branch_SRX> show ethernet-switching table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C - Control MAC
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)


Ethernet switching table : 6 entries, 6 learned
Routing instance : default-switch
    Vlan                MAC                 MAC         Age    Logical                NH        RTR
    name                address             flags              interface              Index     ID
    vlan-trust          08:81:f4:82:a4:5c   D             -    ge-0/0/3.0             0         0
    vlan-trust          08:81:f4:8a:eb:51   D             -    ge-0/0/2.0             0         0
    vlan-trust          20:4e:71:a6:a7:01   D             -    ge-0/0/1.0             0         0
```

The output confirms the expected MAC address learning for our LAN clients in the *vlan-trust* VLAN.

NOTE: In a VLAN, MAC address learning occurs anytime a device sends any type of traffic. The SRX learns based on the source MAC address. This learning builds the Ethernet switching table that is used to forward traffic, based on the destination MAC address. Broadcast, unknown unicast, and multicast (BUM) traffic is flooded to all ports in the VLAN. In our case, the use of DHCP to obtain an IP address is enough to trigger the MAC address learning shown.

Confirm LAN Connectivity in the Trust Zone

To confirm LAN connectivity in the *trust* zone, simply send a ping between LAN clients. Alternatively, you can send pings from the SRX to each LAN client. For verification, log in to an employee device attached to the SRX ge-0/0/2 interface, and test connectivity to both the IRB interface in the SRX, and to the LAN device attached to the SRX's ge-0/0/1 interface. Use the MAC and IP addresses shown in the preceding command output.

First, confirm the employee device interface parameters. Specifically, the MAC and IP addresses:

```
root@employee> show interfaces ge-1/0/1
Physical interface: ge-1/0/1, Enabled, Physical link is Up
  Interface index: 153, SNMP ifIndex: 522
  Link-level type: Ethernet, MTU: 1514, MRU: 1522, LAN-PHY mode, Speed: 1000mbps, BPDU Error: None, Loop Detect
PDU Error: None,
  . . .
  Current address: 08:81:f4:8a:eb:51, Hardware address: 08:81:f4:8a:eb:51
  . . .
```

```
  Logical interface ge-1/0/1.0 (Index 338) (SNMP ifIndex 598)
    Flags: Up SNMP-Traps 0x0 Encapsulation: ENET2
    Input packets : 1338313
    Output packets: 40277
    Protocol inet, MTU: 1500
    Max nh cache: 75000, New hold nh limit: 75000, Curr nh cnt: 1, Curr new hold cnt: 0, NH drop cnt: 0
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 192.168.2/24, Local: 192.168.2.8, Broadcast: 192.168.2.255
    Protocol multiservice, MTU: Unlimited
      Flags: Is-Primary
```

Next, test the expected LAN connectivity with a ping to the SRX's IRB interface and to the LAN device attached to the ge-0/0/1 interface. As shown above, the LAN device on ge-0/0/1 is assigned IP address 192.168.2.13:

```
root@employee> ping 192.168.2.1 count 2
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: icmp_seq=0 ttl=64 time=0.938 ms
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.893 ms

--- 192.168.2.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.893/0.915/0.938/0.023 ms

root@employee> ping 192.168.2.13 count 2
PING 192.168.2.13 (192.168.2.13): 56 data bytes
64 bytes from 192.168.2.13: icmp_seq=0 ttl=64 time=2.798 ms
64 bytes from 192.168.2.13: icmp_seq=1 ttl=64 time=1.818 ms

--- 192.168.2.13 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.818/2.308/2.798/0.490 ms

root@employee> traceroute 192.168.2.13
traceroute to 192.168.2.13 (192.168.2.13), 30 hops max, 40 byte packets
 1  192.168.2.13 (192.168.2.13)  1.759 ms  1.991 ms  1.786 ms
```

The pings are successful which verifies the expected connectivity for the trust VLAN ports. The added traceroute output confirms the shared IP subnet, and resulting direct connectivity, for the LAN stations. This connectivity will change when you later deploy multiple VLANs and IP subnets to secure local branch connectivity.

Verify LAN to WAN Connectivity with Source NAT

Send a ping to an Internet destination from a LAN client. If desired, you can source a ping from the SRX's IRB interface to exercise the same packet flow. The goal is to verify that traffic originating in the *trust* zone flows to the *untrust* zone with source NAT . This provides the LAN station with Internet connectivity.

Let's test Internet connectivity from the LAN client attached to the SRX ge-0/0/2 interface by sending a ping to the *juniper.net* website.

```
root@employee> ping www.juniper.net count 2 inet

PING e1824.dscb.akamaiedge.net (104.100.54.237): 56 data bytes
64 bytes from 104.100.54.237: icmp_seq=0 ttl=44 time=4.264 ms
64 bytes from 104.100.54.237: icmp_seq=1 ttl=44 time=4.693 ms

--- e1824.dscb.akamaiedge.net ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 4.264/4.479/4.693/0.214 ms

root@employee> show route 104.100.54.237

inet.0: 23 destinations, 23 routes (22 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Access-internal/12] 3w6d 01:45:40, metric 0
                    >  to 192.168.2.1 via ge-1/0/1.0
```

The ping is successful which confirms LAN to WAN connectivity. The output of the `show route` command confirms that the LAN station sends the test traffic to the SRX as its default gateway.

It's important to note that sending a ping from a LAN station to an Internet destination involves packet flow from the *trust* zone to *untrust* zone. The SRX is a flow-based device. A security policy is needed to permit flows between zones. As we noted in Branch SRX Default Security Policies on page 8, the factory-default policies allow *trust* to *untrust* packet flows.

View the flow session table to confirm that there are active sessions between the LAN clients and the WAN.

```
root@branch_SRX> show security flow session

Session ID: 8590056439, Policy name: trust-to-untrust/5, State: Stand-alone, Timeout: 2, Valid
  In: 192.168.2.8/28282 --> 104.100.54.237/56711;icmp, Conn Tag: 0x0, If: irb.0, Pkts: 1, Bytes: 84,
  Out: 104.100.54.237/56711 --> 172.16.1.10/7273;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1, Bytes: 84,
. . .
```

The output shows that your test traffic successfully created a flow table entry. A second entry for the same flow confirms that the SRX performed source NAT on the traffic (using 172.16.1.10 from its WAN interface), before sending the ping to the destination at 104.100.54.237 (www.juniper.net). This confirms that the traffic is permitted to flow from

the *trust* zone to the *untrust* zone with source NAT. Your successful ping from a LAN station to *www.juniper.net* confirms the expected factory-default LAN-WAN connectivity.

Next, we'll show you how to alter the default LAN connectivity to secure the local branch according to your requirements.

Configure Secure Local Branch Connectivity

IN THIS SECTION

Now that you've verified the LAN/WAN connectivity, you're ready to use the Junos CLI to deploy VLANs and related policies to secure LAN and WAN connectivity.

SRX platforms are all about security. It's what they do. Securing local and Internet connectivity in this modern age is critically important. We'll show you how to configure the SRX to meet your security needs.

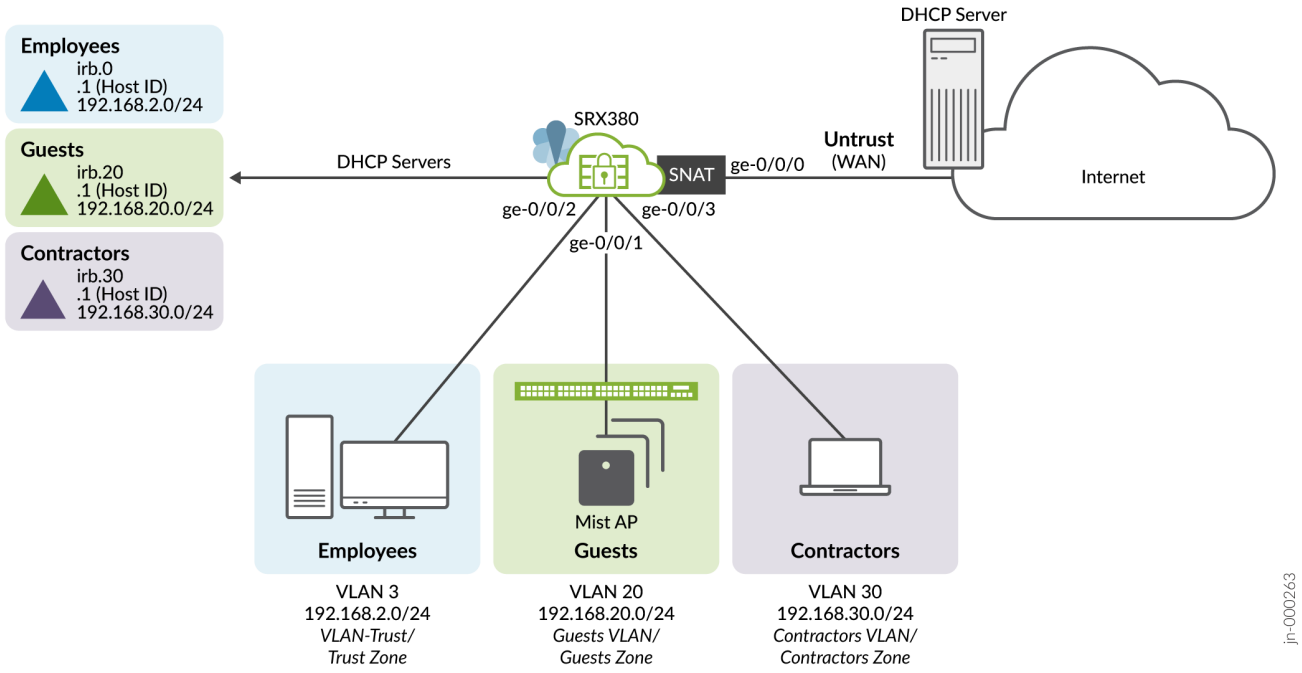
Configure VLANs and Security Policies

IN THIS SECTION

Local Branch Connectivity Goals

Figure 3 on page 14 details the local branch office connectivity goals used in these procedures.

Figure 3: Secure Local Branch Connectivity



Here's how we'll achieve these goals:

- Place employees in the Trust VLAN (*vlan-trust*)/*trust* zone. Allow them full Internet access and the ability to initiate specific connectivity to devices in the *contractors* zone.
- The branch handles retail sales and provides free Wi-Fi to patrons. Place the *guests* VLAN in the *guests* zone and allow limited Internet access.
- Contractors are working on a new web-based business application in the local branch. Place the contractors in the *contractors* VLAN/zone and don't allow them Internet access. Contractors can't initiate communications to either the *trust* or *guests* zones.

The following table summarizes the VLAN connectivity requirements:

Table 1: VLAN Connectivity Requirements

VLAN ID	Name/Zone	Subnet	Internet Access?	Security Policy
3 *	vlan-trust/trust *	192.168.2.0/24 *	Full *	• trust to untrust * • source NAT * • trust to local host, all services and protocols * • trust to contractors, HTTP/HTTPS and ping
20	guests	192.168.20.0/24	HTTP and HTTPS only	• guests to untrust, HTTP/ HTTPS, and ping • source NAT • guests to local host, DHCP and ping only
30	contractors	192.168.30.0/24	No	• contractors can't initiate to trust, guest, or untrust zones • contractors to local host, DHCP and ping only

NOTE: The entries in the table marked with an "*" for *vlan-trust* are already in place through the factory-default configuration. We told you this would be easy! All that is needed for the factory-default *trust* zone is to add a security policy that permits the specified protocols from the *trust* zone to the *contractors* zone.

Permit Trust to Contractors Zone Traffic

To meet the stated connectivity goals, create a security policy to allow specific traffic (HTTP/HTTPS and ping) from the *trust* zone to the *contractors* zone. As a security appliance, the SRX has a default *deny-all* policy for inter-zone traffic. In the factory-default configuration, traffic is permitted from the *trust* to *untrust* zones only.

```
set security policies from-zone trust to-zone contractors policy trust-to-contractors match source-address any
set security policies from-zone trust to-zone contractors policy trust-to-contractors match destination-address
any
set security policies from-zone trust to-zone contractors policy trust-to-contractors match application junos-
http
set security policies from-zone trust to-zone contractors policy trust-to-contractors match application junos-
https
```

```
set security policies from-zone trust to-zone contractors policy trust-to-contractors match application junos-
ping
set security policies from-zone trust to-zone contractors policy trust-to-contractors then permit
```

NOTE: In this example, we keep it simple and match on any source or destination IP address. Here, we simply match on the source and destination zone for policy control. For better security, consider defining address book entries for the *trust* and *contractors* subnet, which are 192.168.2.0/24 and 192.168.30.0/24 prefixes in this branch office. With an address book entry, you can match on `source-address` *trust* and `destination-address` *contractors*.

Further, you can add host-specific address book entries to control the specific IP addresses that are allowed to communicate between zones. If you use a host-specific IP address in your policy, be sure you assign a static IP address to related hosts. If you recall, we use DHCP in this example. So, if a lease times out or a client machine reboots, the client machines will automatically be assigned a new IP address unless you've assigned static IP addresses to the related hosts.

Configure a Guests VLAN, Security Zone, and Security Policies

Let's get those guests up and running. After all, they have web shopping to do! At a high level, this task involves these key parts:

- Define the *guest* VLAN and associate it with one or more LAN interfaces
- Define the VLAN's integrated routing and bridging (IRB) interface
- Configure a DHCP server to assign IP addresses to members of the VLAN
- Define a security zone and policy in accordance with the connectivity needs for the VLAN

1. Log in as root to the branch SRX device. You can use console or SSH access. Start the CLI, and enter configuration mode.

```
login:
branch_SRX (ttyu0)

root@branch_SRX% cli
root@branch_SRX> configure
Entering configuration mode

[edit]
root@branch_SRX#
```

2. Define the *guests* VLAN and associate it with an IRB interface. This IRB interface serves as the default gateway for the devices on the VLAN.

```
[edit]
root@branch_SRX# set vlans guests vlan-id 20
root@branch_SRX# set vlans guests l3-interface irb.20
```

3. Place the ge-0/0/1 interface into the *guests* VLAN. In the default configuration, this interface, like most, belongs to the *trust* VLAN. You begin by deleting the interface's current VLAN association so you can replace it with the updated *guests* VLAN.

```
[edit]
root@branch_SRX# delete interfaces ge-0/0/1 unit 0
root@branch_SRX# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members guests
```

4. Configure the IRB interface for the *guests* VLAN. This step assigns an IP subnet to the VLAN. In this example, you match the VLAN ID to the IRB unit number to make things easier to remember. This association is for convenience only. You can use any unused unit number for this step.

```
[edit]
root@branch_SRX# set interfaces irb unit 20 family inet address 192.168.20.1/24
```

5. Configure the DHCP server for the *guests* VLAN. Note that the VLAN's IRB interface is configured as the DHCP server interface. This configuration assigns IP addresses from the specified range, and also assigns the client a default route and a public DNS server address. The default route points to the VLAN's IRB as the next hop for all non-local (inter-VLAN and LAN to WAN) traffic.

```
[edit]
root@branch_SRX# set system services dhcp-local-server group GUEST-POOL interface irb.20
root@branch_SRX# set access address-assignment pool GUEST-POOL family inet network 192.168.20.0/24
root@branch_SRX# set access address-assignment pool GUEST-POOL family inet range GUEST-POOL-IP-RANGE low
192.168.20.10
root@branch_SRX# set access address-assignment pool GUEST-POOL family inet range GUEST-POOL-IP-RANGE high
192.168.20.100
root@branch_SRX# set access address-assignment pool GUEST-POOL family inet dhcp-attributes domain-name srx-
branch.com
root@branch_SRX# set access address-assignment pool GUEST-POOL family inet dhcp-attributes name-server
8.8.8.8
root@branch_SRX# set access address-assignment pool GUEST-POOL family inet dhcp-attributes router
192.168.20.1
```

6. Members of the *guests* VLAN are provided with Internet access. Because the local branch is using local-use only RFC-1918 IP addresses, Internet access requires that the SRX perform source NAT to the WAN interface IP address.

Only globally-routable IP addresses can be used over the Internet. Here's how to define a source NAT policy for the *guests* VLAN:

```
[edit]
root@branch_SRX# set security nat source rule-set guests-to-untrust from zone guests
root@branch_SRX# set security nat source rule-set guests-to-untrust to zone untrust
root@branch_SRX# set security nat source rule-set guests-to-untrust rule guest-nat-rule match source-address
0.0.0.0/0
root@branch_SRX# set security nat source rule-set guests-to-untrust rule guest-nat-rule then source-nat
interface
```

7. Almost done. Next, you create the *guests* security zone. As part of this process, you place the related VLAN's IRB into the new zone. Part of a zone's definition is to specify the protocols and services that are allowed to flow from that zone to the SRX device's control plane.

   For this example, you allow users in the *guests* VLAN to initiate DHCP and ping traffic to the local control plane. This allows the guest to request an IP address using DHCP, and to ping their VLAN's IRB for debugging purposes, while blocking all other services and protocols to the local host. As a result, users in the *guest* zone are blocked from initiating Telnet or SSH to the branch SRX. In contrast, users in the *trust* zone are allowed to initiate SSH connections to the SRX.

```
[edit]
root@branch_SRX# set security zones security-zone guests interfaces irb.20
root@branch_SRX# set security zones security-zone guests host-inbound-traffic system-services dhcp
root@branch_SRX# set security zones security-zone guests host-inbound-traffic system-services ping
```

8. The last step is to define the security policies for the *guests* VLAN. To keep the configuration statements shorter, we "park" ourselves at the `[edit security policies]` hierarchy. To limit Internet access, your policy provides support only for HTTP, HTTPS, DNS, and ping.

```
[edit security policies ]
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust match source-address any
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust match destination-address any
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust match application junos-http
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust match application junos-https
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust match application junos-ping
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust match application junos-dns-
udp
root@branch_SRX# set from-zone guests to-zone untrust policy guests-to-untrust then permit
```

Quick Configurations

IN THIS SECTION

Guests VLAN Quick Configuration

Here's the complete configuration for defining the *guests* VLAN and its security policies in set format. To get up and running quickly, simply edit the configuration statements as needed for your environment and paste them into your SRX.

```
set vlans guests vlan-id 20
set vlans guests l3-interface irb.20

delete interfaces ge-0/0/1 unit 0
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members guests

set interfaces irb unit 20 family inet address 192.168.20.1/24

set system services dhcp-local-server group GUEST-POOL interface irb.20

set access address-assignment pool GUEST-POOL family inet network 192.168.20.0/24
set access address-assignment pool GUEST-POOL family inet range GUEST-POOL---IP-RANGE low 192.168.20.10
set access address-assignment pool GUEST-POOL family inet range GUEST-POOL---IP-RANGE high 192.168.20.100
set access address-assignment pool GUEST-POOL family inet dhcp-attributes domain-name srx-branch.com
set access address-assignment pool GUEST-POOL family inet dhcp-attributes name-server 8.8.8.8
set access address-assignment pool GUEST-POOL family inet dhcp-attributes router 192.168.20.1

set security nat source rule-set guests-to-untrust from zone guests
set security nat source rule-set guests-to-untrust to zone untrust
set security nat source rule-set guests-to-untrust rule guest-nat-rule match source-address 0.0.0.0/0
set security nat source rule-set guests-to-untrust rule guest-nat-rule then source-nat interface

set security zones security-zone guests interfaces irb.20
set security zones security-zone guests host-inbound-traffic system-services dhcp
set security zones security-zone guests host-inbound-traffic system-services ping

set security policies from-zone guests to-zone untrust policy guests-to-untrust match source-address any
set security policies from-zone guests to-zone untrust policy guests-to-untrust match destination-address any
set security policies from-zone guests to-zone untrust policy guests-to-untrust match application junos-http
set security policies from-zone guests to-zone untrust policy guests-to-untrust match application junos-https
```

```
set security policies from-zone guests to-zone untrust policy guests-to-untrust match application junos-ping
set security policies from-zone guests to-zone untrust policy guests-to-untrust match application junos-dns-udp
set security policies from-zone guests to-zone untrust policy guests-to-untrust then permit
```

Contractors VLAN Quick Configuration

The *contractors* VLAN and related security zone is similar to that detailed above for the *guests* VLAN. We save some paper by jumping straight to the Quick Configuration for the *contractors* VLAN.

NOTE: The lack of security policy definition for the *contractors* zone is significant. With out an explicit policy, the default *deny all* policy is in full effect for any inter-zone traffic initiated from this zone! The result is that all traffic that initiates in the *contractors* zone is blocked from entering all other zones.

```
set vlans contractors vlan-id 30
set vlans contractors l3-interface irb.30

delete interfaces ge-0/0/3 unit 0
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members contractors

set interfaces irb unit 30 family inet address 192.168.30.1/24

set system services dhcp-local-server group CONTRACTORS-POOL interface irb.30

set access address-assignment pool CONTRACTORS-POOL family inet network 192.168.30.0/24
set access address-assignment pool CONTRACTORS-POOL family inet range CONTRACTORS-POOL-IP-RANGE low
192.168.30.10
set access address-assignment pool CONTRACTORS-POOL family inet range CONTRACTORS-POOL-IP-RANGE high
192.168.30.100
set access address-assignment pool CONTRACTORS-POOL family inet dhcp-attributes domain-name srx-branch.com
set access address-assignment pool CONTRACTORS-POOL family inet dhcp-attributes name-server 8.8.8.8
set access address-assignment pool CONTRACTORS-POOL family inet dhcp-attributes router 192.168.30.1

set security zones security-zone contractors interfaces irb.30
set security zones security-zone contractors host-inbound-traffic system-services dhcp
set security zones security-zone contractors host-inbound-traffic system-services ping
```

Be sure to commit your configuration to activate the changes on the branch SRX.

Results

The results of your secure VLAN configuration are displayed in Junos curly brace format. We've omitted the factory-default configuration from the below for brevity.

```
root@branch_SRX# [edit]
root@branch-srx# show interfaces irb
 . . .
unit 20 {
    family inet {
        address 192.168.20.1/24;
    }
}
unit 30 {
    family inet {
        address 192.168.30.1/24;
    }
}

[edit]
root@branch-srx# show vlans
contractors {
    vlan-id 30;
    l3-interface irb.30;
}
guests {
    vlan-id 20;
    l3-interface irb.20;
}
. . .
group CONTRACTORS-POOL {
    interface irb.30;
}
group GUEST-POOL {
    interface irb.20;
}
[edit]
root@branch-srx# show access address-assignment
. . .
pool CONTRACTORS-POOL {
    family inet {
        network 192.168.30.0/24;
        range CONTRACTORS-POOL-IP-RANGE {
            low 192.168.30.10;
            high 192.168.30.100;
        }
```

```
        dhcp-attributes {
            domain-name srx-branch.com;
            name-server {
                8.8.8.8;
            }
            router {
                192.168.30.1;
            }
        }
    }
}
pool GUEST-POOL {
    family inet {
        network 192.168.20.0/24;
        range GUEST-POOL---IP-RANGE {
            low 192.168.20.10;
            high 192.168.20.100;
        }
        dhcp-attributes {
            domain-name srx-branch.com;
            name-server {
                8.8.8.8;
            }
            router {
                192.168.20.1;
            }
        }
    }
}
. . .
nat {
    source {
        rule-set guests-to-untrust {
            from zone guests;
            to zone untrust;
            rule guest-nat-rule {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
```

```
}

policies {
. . .
    from-zone guests to-zone untrust {
        policy guests-to-untrust {
            match {
                source-address any;
                 destination-address any;
                application [ junos-http junos-https junos-ping junos-dns-udp ];
            }
            then {
                permit;
            }
        }
    }
}

zones {
. . .
    security-zone contractors {
        host-inbound-traffic {
            system-services {
                dhcp;
                ping;
            }
        }
        interfaces {
            irb.30;
        }
    }
    security-zone guests {
        host-inbound-traffic {
            system-services {
                dhcp;
                ping;
            }
        }
        interfaces {
            irb.20;
        }
    }

}
```

Next, we'll show you how to verify that your configuration is working as expected to secure local branch communications.

Verify Secured LAN Connectivity

IN THIS SECTION

Now that you've configured VLANs and security polices to secure local branch communications, let's quickly confirm that the branch VLAN connectivity works as expected. The validation process is similar to the one you used to validate default connectivity. The main difference is that now, these verification steps occur in the context of a specific VLAN/security zone. And, of course, given the VLAN changes you made, you no longer expect full connectivity between the LAN ports.

Verify LAN DHCP Servers

Verify that the SRX has assigned IP addresses to the LAN clients.

```
root@branch-srx> show dhcp server binding
IP address        Session Id  Hardware address   Expires     State      Interface
192.168.30.10     3543        08:81:f4:82:a4:5c  46482       BOUND      irb.30
192.168.2.8       3538        08:81:f4:8a:eb:51  61414       BOUND      irb.0
192.168.20.10     3542        20:4e:71:a6:a7:01  46622       BOUND      irb.20
192.168.20.11     3544        d4:20:b0:00:c3:37  46621       BOUND      irb.20
```

Notice that the devices have the same MAC addresses as before (see Branch SRX Default Connectivity on page 5), but now, they're associated with different IP subnets and IRB units, based on their respective VLAN assignment. The display confirms at least one device is in the *vlan-trust*, the *guests*, and the *contractors* VLANs. This output confirms that your DHCP servers function properly within each VLAN.

Verify your VLAN configuration.

```
root@branch-srx> show vlans
Routing instance        VLAN name            Tag          Interfaces
default-switch          contractors          30
                                                          ge-0/0/3.0*
default-switch          default              1

default-switch          guests               20
```

```
                                                    ge-0/0/1.0*
default-switch          vlan-trust          3
                                                    ge-0/0/2.0*
...
```

The output confirms that you have correctly configured the *guests* and *contractors* VLANs.

Verify the Guests VLAN

Verify that devices in the *guests* VLAN and zone can access the Internet. You confirm Internet access with a successful ping to www.juniper.net. Recall that your branch office design states guests are only allowed to send HTTP/HTTPS and ping traffic to the Internet.

```
user@guest-device> ping www.juniper.net inet count 2
PING e1824.dscb.akamaiedge.net (104.100.54.237): 56 data bytes
64 bytes from 104.100.54.237: icmp_seq=0 ttl=46 time=5.323 ms
64 bytes from 104.100.54.237: icmp_seq=1 ttl=46 time=6.204 ms

--- e1824.dscb.akamaiedge.net ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 5.323/5.764/6.204/0.441 ms
```

If your *guests* zone device supports a command line HTTP client, like CURL, use it to verify HTTP access to the Internet. You can always use a web browser if the device has a GUI interface to test web connectivity.

```
user@guest-device curl --head www.juniper.net
HTTP/1.1 301 Moved Permanently
Content-Type: text/html
Location: https://www.juniper.net/
Content-Length: 0
Date: Mon, 18 Apr 2022 22:32:15 GMT
Connection: keep-alive
```

We won't bother trying to find an Internet connected machine to confirm that all other services, that is, SSH, Telnet, FTP, and so on won't work. One option here is to temporarily remove the policy rule that allows ICMP from the *guests* to the *untrust* zone. Once the change takes effect the ping to *www.juniper.net* should time-out.

We'll finish validating the *guests* VLAN by confirming that guest devices are unable to ping the IRB interface in either the *trust* or *contractors* zones.

```
user@guest-device> ping 192.168.2.1 count 1
PING 192.168.2.1 (192.168.2.1): 56 data bytes

--- 192.168.2.1 ping statistics ---
```

```
1 packets transmitted, 0 packets received, 100% packet loss

user@guest-device ping 192.168.30.1 count 1
PING 192.168.30.1 (192.168.30.1): 56 data bytes

--- 192.168.30.1 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
```

The pings to the IRB interfaces in the *trust* and *contractors* zones fail, as expected. Although not shown, pings initiated from guests to end stations in the *trust* or *contractors* zones also fail. Again, you need an explicit policy to permit traffic to flow between zones. For guest users, the only security policy in effect is to allow HTTP and ping traffic to the *untrust* zone.

Validate Employee VLAN

Verify that the employees in the *trust* zone can access the Internet.

```
user@employee-device> ping www.juniper.net inet count 2
PING e1824.dscb.akamaiedge.net (104.100.54.237): 56 data bytes
64 bytes from 104.100.54.237: icmp_seq=0 ttl=44 time=4.762 ms
64 bytes from 104.100.54.237: icmp_seq=1 ttl=44 time=5.075 ms

--- e1824.dscb.akamaiedge.net ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 4.762/4.918/5.075/0.157 ms
```

Verify that the employees can ping the contractors.

```
user@employee-device> ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10): 56 data bytes
--- 192.168.30.10 ping statistics ---
38 packets transmitted, 0 packets received, 100% packet loss
```

The output shows that the ping is not successful. See "Debug Connectivity Issues" on page 26 for information about how to debug this issue.

Debug Connectivity Issues

Let's try to debug the issue of the employees being unable to ping the contractors. We'll use traceoptions to debug the packet flow as the packets traverse from the *trust* zone to the *contractors* zone. At a minimum, the `traceoptions` configuration must include a target file and a flag. The argument to the `file` command specifies the file name that stores the trace output. The argument(s) to the `flag` command defines the type of events to be traced.

```
[edit]
root@branch-srx# set security flow traceoptions file flow-debug
```

```
root@branch-srx# set security flow traceoptions flag basic-datapath
root@branch-srx# commit
```

With the tracing activated, generate pings from the *trust* zone to the *contractors* zone. While the pings are failing, use the `show log <log_name>` CLI command along with the `find` switch to quickly locate areas of interest in the trace log file.

```
root@branch-srx> show log flow-debug | find 192.168.30
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:flow_ipv4_rt_lkup success 192.168.30.1, iifl 0x48, oifl 0x0
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:flow_first_routing: setting out_vrf_id in lpak to 0, grp 0
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:Changing out-ifp from .local..0 to irb.30 for dst: 192.168.30.1 in
vr_id:0
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:  routed (x_dst_ip 192.168.30.1) from trust (irb.0 in 0) to irb.30,
Next-hop: 192.168.30.1
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:Policy lkup: vsys 0 zone(7:trust) -> zone(9:contractors) scope:0
 src vrf (0) dsv vrf (0) scope:0
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:             192.168.2.2/2048 -> 192.168.30.1/34912 proto 1
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
 src vrf (0) dsv vrf (0) scope:34912
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:             192.168.2.2/2048 -> 192.168.30.1/34912 proto 1
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:flow_first_policy_search: policy search from zone trust-> zone
contractors (0x0,0x3d56010a,0x10a), result: 0xfa3c538, pending: 0?
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:flow_first_policy_search: dynapp_none_policy: TRUE, uc_none_policy:
TRUE, is_final: 0x0, is_explicit: 0x0, policy_meta_data: 0x0
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:  app 0, timeout 60s, curr ageout 60s
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:  packet dropped, denied by policy
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:  denied by policy default-policy-logical-system-00(2), dropping pkt
Apr 20 03:22:36 03:22:36.712246:CID-0:RT:  packet dropped,  policy deny.
. . .
```

The highlighted entries confirm that the test traffic sent from the *trust* zone to the *contractors* zone is being dropped. The message says `denied by policy default-policy-logical-system` which indicates there isn't a policy to allow this traffic.

You must have a policy to allow traffic to flow between zones. Add the below configuration to configure a security policy that allows the desired traffic types between the *trust* zone and the *contractors* zone. The configuration is in Quick Configuration set format, so you can simply paste it into the branch SRX at the `[edit]` hierarchy:

```
set security policies from-zone trust to-zone contractors policy trust-to-contractors match source-address any
set security policies from-zone trust to-zone contractors policy trust-to-contractors match destination-address
any
set security policies from-zone trust to-zone contractors policy trust-to-contractors match application junos-
http
set security policies from-zone trust to-zone contractors policy trust-to-contractors match application junos-
ping
set security policies from-zone trust to-zone contractors policy trust-to-contractors then permit
```

Be sure to commit your changes. Now, the ping from the *trust* zone to the *contractors* zone should succeed. Now that your debugging is complete, remove the security flow traceoptions configuration .

```
[edit]
root@branch-srx# delete security flow traceoptions
root@branch-srx# commit
```

Contractors VLAN

Verify that the contractors cannot communicate with the clients in the *trust* or *guests* zones.

Only the ping to the IRB interface (irb.30) should succeed. Because the client IP addresses can change with updated DHCP assignments, we opt to test inter-zone connectivity by pinging the IRB interface for a given zone. In this example, the IP addresses assigned to the IRB interfaces are static and therefore won't change over time.

```
user@contractor-device> ping 192.168.30.1 count 2
PING 192.168.30.1 (192.168.30.1): 56 data bytes
64 bytes from 192.168.30.1: icmp_seq=0 ttl=64 time=0.929 ms
64 bytes from 192.168.30.1: icmp_seq=1 ttl=64 time=0.864 ms

--- 192.168.30.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.829/0.866/0.929/0.036 ms
```

As expected, the ping from a contractor zone device to the IRB interface for the *contractors* zone succeeds. Now, you verify the *lack* of connectivity to the *trust* and *guests* zones. Refer to Secure Local Branch Connectivity on page 14 for details on the addresses assigned to the IRB interfaces in this example.

```
user@contractor-device> ping 192.168.2.1 count 2
PING 192.168.2.1 (192.168.2.1): 56 data bytes

--- 192.168.2.1 ping statistics ---
2 packets transmitted, 0 packets received, 100% packet loss
```

```
user@contractor-device> ping 192.168.20.1 count 2
PING 192.168.20.1 (192.168.20.1): 56 data bytes

--- 192.168.20.1 ping statistics ---
2 packets transmitted, 0 packets received, 100% packet loss
```

The output shows that only the ping to 192.168.30.1 (assigned to irb.30) is successful. This confirms that contractors are unable to access the *trust* and *guests* zones.

Confirm that the contractors cannot access the Internet.

```
user@contractor-device>  ping www.juniper.net inet count 1
ping: cannot resolve www.juniper.net: Host name lookup failure

user@contractor-device> ping 8.8.8.8 count 1
PING 8.8.8.8 (8.8.8.8): 56 data bytes

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
```

Notice that the attempt to ping *www.juniper.net* returns a *hostname lookup* failure message. This branch office doesn't have a local DNS server and relies on a public DNS service that is reachable only over the Internet. The failure to resolve the host name is a good indication that contractors are correctly blocked from Internet access. As a final confirmation, ping the public DNS server by its IP address. Again, the ping fails as expected.

These results complete validation of the branch office's secure local connectivity. Good job! In the next step, we'll show you how to establish secure connectivity over the Internet.

Step 2: Configure and Verify an IPsec VPN

IN THIS SECTION

It has been a big day, we know. Before you go home, there's one more ask for the new branch office. You'll need to establish a secure IPsec VPN tunnel to the remote corporate office. This tunnel allows members of the *trust* zone to securely reach specific corporate resources on the 172.16.200.0/24 subnet over the Internet.

Secure tunnels are a key feature of SRX platforms. Being able to send sensitive traffic over the public Internet without concern for eavesdropping, or data theft, is no small task. An IPsec VPN lets you securely tunnel traffic through the public Internet. Because the traffic is tunneled, there's no need to perform source NAT.

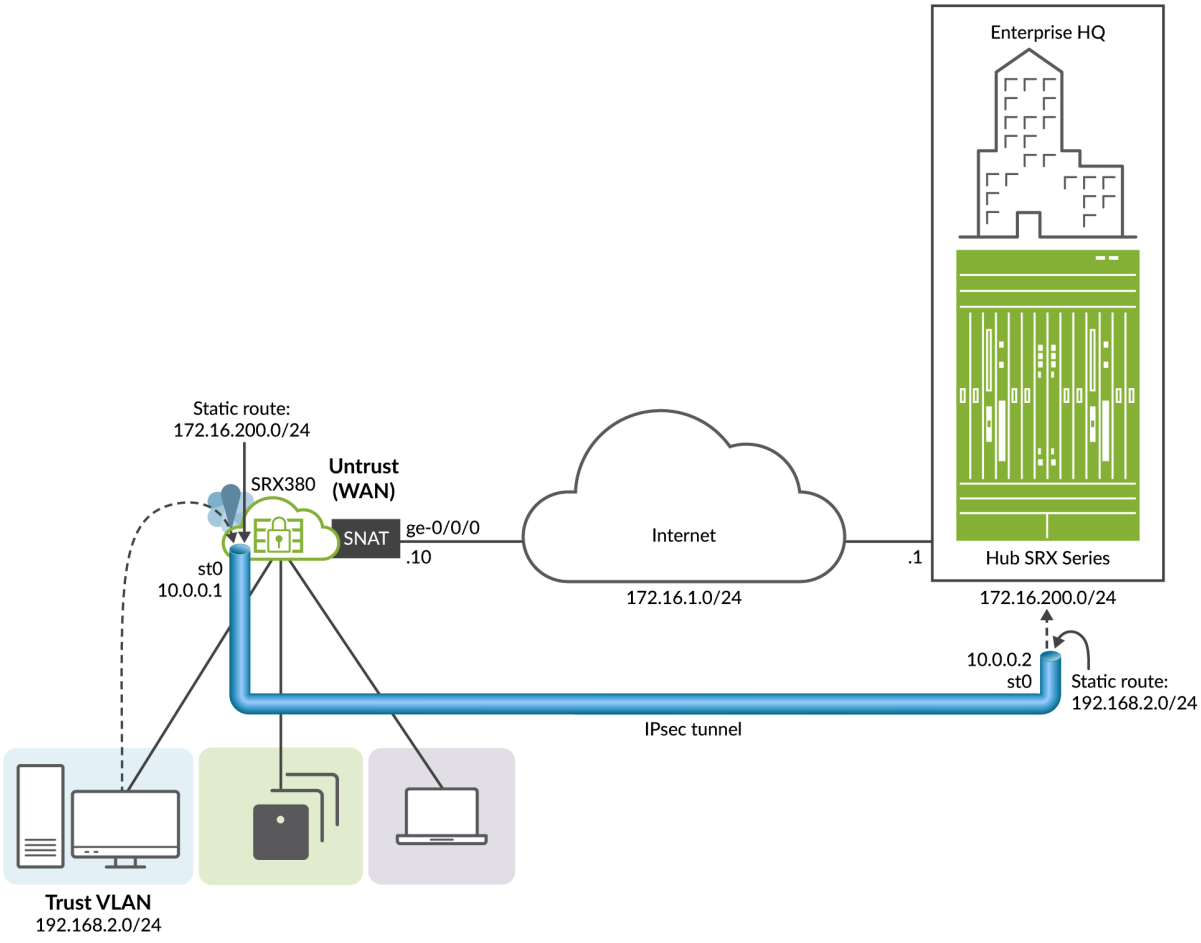
Don't worry, we'll make this easy for you!

This step covers how to:

- Configure st0 tunnel interfaces
- Configure static routing to steer traffic into the IPsec tunnel

- Configure IKE and IPsec parameters for a dynamic route-based VPN
- Adjust security policies to ensure that only traffic from the *trust* zone sent to 172.16.200.0/24 is presented to the IPsec tunnel
- Use the Junos CLI to verify IPsec VPN operation

Figure 4: An IPsec VPN for Secure Branch to Remote Office Connectivity



IPsec VPN Overview

In this example, traffic sent from the *trust* zone to 172.16.200.0/24 uses the IPsec tunnel. This traffic bypasses source NAT and exits the remote end with the original source IP from the 192.168.2.0/24 *trust-vlan* subnet.

The tunnel operates point-to-point between the branch and the remote office. This makes IP address assignment optional. In this example, we assign addresses to the tunnel endpoints to permit ping testing as a diagnostic aid. A static route is used at each end to direct traffic into the tunnel. Note that the static route at the remote location matches the

192.168.2.0/24 subnet of the *trust* zone. You must match on this address because source NAT does not occur for traffic using the tunnel.

> **NOTE**: The topology shows a cloud between the branch and remote location. Typically this cloud is the Internet. To reduce the number of devices in our topology, we have a direct connection between the branch and remote locations. As a result, we have a single 172.16.1.0/24 subnet that spans the Internet cloud.
>
> This means that later, when you define the Internet Key Exchange (IKE) local and remote gateways, the two endpoints share the 172.16.1.0/24 subnet. There's no difference in configuration or operation if the IKE gateways are on remote subnets. Specifying a remote IKE gateway is the typical use case when the two sites have intervening hops through the Internet.

Configure an IPsec VPN

IN THIS SECTION

IPSec VPN Design Goals

Your IPsec VPN must meet these criteria:

- Configure a dynamic IPsec VPN to support DHCP address assignment to the WAN interface by the Internet service provider.
- Ensure that only traffic originating in the trust zone is able to use the IPsec tunnel.
- Ensure that only traffic destined to the 172.168.200.0/24 subnet uses the IPsec tunnel.

We'll use the parameters in Table 1 to configure an IPsec VPN.

Table 2: IPsec VPN Parameters

Parameter	Value
Tunnel interface	st0
Branch Tunnel IP	10.0.0.1/24

Table 2: IPsec VPN Parameters *(Continued)*

Parameter	Value
Corporate Tunnel IP	10.0.0.2/24
IKE Proposal	standard
IKE mode	aggressive
Pre-shared key	"srx_branch"
Tunnel establishment	immediately
Branch identity	branch
Corporate identity	hq
Tunnel security zone	vpn

Configure a Route-Based IPsec VPN

Let's get going and configure an IPsec VPN!

1. Log in as root on the device console. Start the CLI, and enter configuration mode.

```
login:
branch_srx (ttyu0)

root@branch_srx% cli
root@branch_srx> configure
Entering configuration mode

[edit]
root@branch_srx#
```

2. Configure the st0 tunnel interface. An unnumbered tunnel is supported in this scenario. Here, we opt to number the tunnel end points. One benefit of numbering the tunnel is to permit ping testing of the tunnel end points to help debug any connectivity issues.

```
[edit]
root@branch_srx# set interfaces st0 unit 0 family inet address 10.0.0.1/24
```

3. Define a static route to direct traffic destined to 172.16.200.0/24 into the IPsec tunnel.

```
[edit]
root@branch_srx# set routing-options static route 172.16.200.0/24 next-hop st0.0
```

4. Configure the IKE parameters. The local-identity and remote-identity parameters are important for supporting a dynamic IPsec VPN. When static IP addresses are used, you define a local and remote IKE gateway specifying those static IP addresses.

   By the way, we'll be configuring security stuff for a bit so you park yourself at the `[edit security]` hierarchy:

```
[edit security]
root@branch_srx# set ike proposal standard authentication-method pre-shared-keys
root@branch_srx# set ike policy ike-pol mode aggressive
root@branch_srx# set ike policy ike-pol proposals standard
root@branch_srx# set ike policy ike-pol pre-shared-key ascii-text branch_srx
root@branch_srx# set ike gateway ike-gw ike-policy ike-pol
root@branch_srx# set ike gateway ike-gw address 172.16.1.1
root@branch_srx# set ike gateway ike-gw local-identity hostname branch
root@branch_srx# set ike gateway ike-gw remote-identity hostname hq
root@branch_srx# set ike gateway ike-gw external-interface ge-0/0/0
```

   NOTE: To support a dynamic IPsec VPN, the remote end must have the `set security ike gateway ike-gw dynamic hostname <name>` statement configured in the IKE proposal. When the remote end initiates a connection, the name is used to match the IKE proposal rather than an IP. This method is used when IP addresses can change due to dynamic assignment.

5. Configure the IPsec tunnel parameters.

```
[edit security]
root@branch_srx# set ipsec proposal standard
root@branch_srx# set ipsec policy ipsec-pol proposals standard
root@branch_srx# set ipsec vpn to_hq bind-interface st0.0
root@branch_srx# set ipsec vpn to_hq ike gateway ike-gw
root@branch_srx# set ipsec vpn to_hq ike ipsec-policy ipsec-pol
root@branch_srx# set ipsec vpn to_hq establish-tunnels immediately
```

6. Adjust the security policies to create a *vpn* zone, and to permit traffic to flow from the *trust* zone to the *vpn* zone. We configure the *vpn* zone to allow host-bound ping for use in debugging, given we opted to number our IPsec tunnel. In this step, you also place the IPsec tunnel interface in the *vpn* zone.

```
[edit security]
root@branch_srx# set policies from-zone trust to-zone vpn policy trust-to-vpn match source-address any
root@branch_srx# set policies from-zone trust to-zone vpn policy trust-to-vpn match destination-address any
root@branch_srx# set policies from-zone trust to-zone vpn policy trust-to-vpn match application any
root@branch_srx# set policies from-zone trust to-zone vpn policy trust-to-vpn then permit

root@branch_srx# set security zones security-zone vpn host-inbound-traffic system-services ping
root@branch_srx# set zones security-zone vpn interfaces st0.0
```

> **NOTE**: In this example, we keep it simple and match on any source or destination IP address. We rely on the static route to only direct traffic destined to the remote site into the tunnel. For better security, consider defining address book entries for the local branch 192.168.2.0/24 and the remote 172.16.200.0/24 subnets. With address book entries defined for the two subnets, you match on `source-address` *<source_name>* and `destination-address` *<dest_name>* in your security policy. Including the source and destination subnets in your policy makes it that much more explicit as to the traffic that is able to use the tunnel.

7. Hang in there, you're almost done. Recall that IKE is used to negotiate the shared keys for securing the IPsec tunnel. IKE messages must be sent and received over the WAN interface to establish the tunnel on the st0 interface. You'll need to modify the local host services that are accessible over the *untrust* WAN interface to include IKE.

```
[edit security]
root@branch_srx# set zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services
ike
```

That's it. You've configured the IPsec route-based VPN at the branch location. Be sure to commit your changes.

Results

Let's display the result of your IPsec route-based VPN configuration. We omit parts of the default configuration for brevity.

```
[edit]
root@branch-srx# show interfaces st0
unit 0 {
    family inet {
        address 10.0.0.1/24;
    }
}
```

```
[edit]
root@branch-srx# show routing-options
static {
    route 172.16.200.0/24 next-hop st0.0;
}
 ike {
    proposal standard {
        authentication-method pre-shared-keys;
    }
    policy ike-pol {
        mode aggressive;
        proposals standard;
        pre-shared-key ascii-text "$9$Yj4oGjHmf5FJGi.m56/dVwgZjk.5T39"; ## SECRET-DATA
    }
    gateway ike-gw {
        ike-policy ike-pol;
        address 172.16.1.1;
        local-identity hostname branch;
        remote-identity hostname hq;
        external-interface ge-0/0/0;
    }
}
ipsec {
    proposal standard;
    policy ipsec-pol {
        proposals standard;
    }
    vpn to_hq {
        bind-interface st0.0;
        ike {
            gateway ike-gw;
            ipsec-policy ipsec-pol;
        }
        establish-tunnels immediately;
    }
}

. . .
policies {
. . .
    from-zone trust to-zone vpn {
        policy trust-to-vpn {
            match {
                source-address any;
                destination-address any;
                application any;
            }
```

```
            then {
                permit;
            }
        }
    }

}
zones {
..
    security-zone untrust {
        screen untrust-screen;
        interfaces {
            ge-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
             . . .
                        ike;
                   . . .
                    }
                }
            }
        }
    }
    . . .
    security-zone vpn {
        host-inbound-traffic {
            system-services {
                ping;
            }
        }
        interfaces {
            st0.0;
        }
    }
}
```

Be sure to commit your configuration to activate the changes on the branch SRX.

Quick Configurations

IN THIS SECTION

Quick Configuration: Branch Office

To quickly configure an IPsec VPN, use the following `set` statements. Simply edit the configuration statements as needed for your environment, and paste them into your SRX.

Here's the IPsec VPN configuration for the branch SRX:

```
set security ike proposal standard authentication-method pre-shared-keys
set security ike policy ike-pol mode aggressive
set security ike policy ike-pol proposals standard
set security ike policy ike-pol pre-shared-key ascii-text "$9$Yj4oGjHmf5FJGi.m56/dVwgZjk.5T39"
set security ike gateway ike-gw ike-policy ike-pol
set security ike gateway ike-gw address 172.16.1.1
set security ike gateway ike-gw local-identity hostname branch
set security ike gateway ike-gw remote-identity hostname hq
set security ike gateway ike-gw external-interface ge-0/0/0

set security ipsec proposal standard
set security ipsec policy ipsec-pol proposals standard
set security ipsec vpn to_hq bind-interface st0.0
set security ipsec vpn to_hq ike gateway ike-gw
set security ipsec vpn to_hq ike ipsec-policy ipsec-pol
set security ipsec vpn to_hq establish-tunnels immediately

set security policies from-zone trust to-zone vpn policy trust-to-vpn match source-address any
set security policies from-zone trust to-zone vpn policy trust-to-vpn match destination-address any
set security policies from-zone trust to-zone vpn policy trust-to-vpn match application any
set security policies from-zone trust to-zone vpn policy trust-to-vpn then permit

set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services ike
set security zones security-zone vpn interfaces st0.0
set security zones security-zone vpn host-inbound-traffic system-services ping

set interfaces st0 unit 0 family inet address 10.0.0.1/24

set routing-options static route 172.16.200.0/24 next-hop st0.0
```

Quick Configuration: Remote Location

For completeness, here's the matching IPsec VPN Quick Configuration for the remote site. It's similar to the one we detailed for the branch. The key differences are that we use the `dynamic hostname` statement, and a different destination for the static route used to steer traffic into the tunnel. We allow ping in the *vpn* zone at the remote site. As a result,

you ping both the tunnel endpoints (we numbered our tunnel), as well as the loopback interface. The loopback interface at the remote site represents the 172.16.200.0/24 subnet. The remote site's lo0 interface is placed in the *vpn* zone.

```
set security ike proposal standard authentication-method pre-shared-keys
set security ike policy ike-pol mode aggressive
set security ike policy ike-pol proposals standard
set security ike policy ike-pol pre-shared-key ascii-text "$9$1POEhrKMX7NbSrvLXNY2puORyKWLN-wg"
set security ike gateway ike-gw ike-policy ike-pol
set security ike gateway ike-gw dynamic hostname branch
set security ike gateway ike-gw local-identity hostname hq
set security ike gateway ike-gw external-interface ge-0/0/6

set security ipsec proposal standard
set security ipsec policy ipsec-pol proposals standard
set security ipsec vpn to_hq bind-interface st0.0
set security ipsec vpn to_hq ike gateway ike-gw
set security ipsec vpn to_hq ike ipsec-policy ipsec-pol
set security ipsec vpn to_hq establish-tunnels immediately

set security policies from-zone trust to-zone vpn policy trust-to-vpn match source-address any
set security policies from-zone trust to-zone vpn policy trust-to-vpn match destination-address any
set security policies from-zone trust to-zone vpn policy trust-to-vpn match application any
set security policies from-zone trust to-zone vpn policy trust-to-vpn then permit

set security zones security-zone untrust interfaces ge-0/0/6.0 host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/6.0 host-inbound-traffic system-services ping

set security zones security-zone vpn interfaces st0.0
set security zones security-zone vpn interfaces lo0.0
set security zones security-zone vpn host-inbound-traffic system-services ping

set interfaces lo0 unit 0 family inet address 172.16.200.1/32
set interfaces st0 unit 0 family inet address 10.0.0.2/24

set routing-options static route 192.168.2.0/24 next-hop st0.0
```

Be sure to commit the changes. In the next section, we'll show you how to verify that your IPsec tunnel works correctly.

Verify Your IPsec VPN

IN THIS SECTION

Now we'll show you how to quickly confirm that your route-based IPsec VPN is doing its job of protecting your sensitive data.

Confirm Licensing Status

SRX Security Gateways have many advanced features. For example, deep packet inspection (DPI), real-time antivirus (AV) scanning, cloud-based URL blocking, and so on. Some of these features require a license. Many use a hard licensing model, which means the feature is disabled until you add the necessary license. However, you might be able to configure the feature without receiving any type of license warning. For information about feature-based licenses, see Licenses for SRX Series. For information about subscription-based licenses, see Flex Software License for SRX Series Devices.

It's always a good idea to display the licensing status of your SRX, especially when adding new features, like the IPsec VPN you just turned up.

```
root@branch-srx> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  remote-access-ipsec-vpn-client        0            2           0    permanent
  remote-access-juniper-std             0            2           0    permanent

Licenses installed: none
```

The output is good news. It shows that no specific licenses exist on the device. It also confirms that none of the features configured require any special add-on licensing. The base model license for the branch SRX includes support for VLANs, DHCP services, and basic IPsec VPNs.

Verify IKE Session

Verify that the SRX has successfully established an IKE association with the remote site:

```
root@branch-srx> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
3318115 UP     2ed75d71d9aeb5c5  680391201477e65b  Aggressive     172.16.1.1
```

The output shows an established IKE session to the remote site at 172.16.1.1.

Verify the IPsec Tunnel

Verify IPsec tunnel establishment:

```
root@branch-srx> show security ipsec security-associations
Total active tunnels: 1     Total Ipsec sas: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:3des/sha1   4f03e41c 947/ unlim   -   root 500   172.16.1.1
  >131073 ESP:3des/sha1   70565ffd 947/ unlim   -   root 500   172.16.1.1
```

The output confirms IKE session establishment to the remote site at 172.16.1.1.

Verify Tunnel Interface Status

Verify that the tunnel interface is operational (and it must be operational, given the successful establishment of the IPsec tunnel). Also, check that you can ping the remote tunnel endpoint:

```
root@branch-srx> show interfaces terse st0
Interface               Admin Link Proto    Local                 Remote
st0                     up    up
st0.0                   up    up   inet     10.0.0.1/24

root@branch-srx> show route 10.0.0.2

inet.0: 19 destinations, 19 routes (19 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/24        *[Direct/0] 00:11:19
                    >  via st0.0

root@branch-srx> ping 10.0.0.2 count 2
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=64 time=17.862 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=2.318 ms
```

```
--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.318/10.090/17.862/7.772 ms
```

Verify Static Routing for the IPsec Tunnel

Verify that the (static) route to the remote subnet correctly points to the IPsec tunnel interface as a next hop:

```
root@branch-srx> show route 172.16.200.0

inet.0: 16 destinations, 16 routes (16 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.200.0/24    *[Static/5] 00:45:52
                    >  via st0.0
```

Verify Trust Zone Traffic Uses the Tunnel

Generate traffic from a trust zone device to a destination in the 172.16.200.0/24 subnet. We assigned address 172.16.200.1/32 to the remote location's loopback interface, and placed it into the *vpn* zone. This address provides a target to ping. If all is working, these pings should succeed.

To confirm this traffic is using the IPsec VPN, follow these steps.

1. Clear the statistics for the IPsec tunnel.

```
root@branch-srx> clear security ipsec statistics
```

2. Generate a known number of pings to the 172.16.200.1 destination from a trust zone client.

```
user@trust-device> ping 172.16.200.1 count 100 rapid
PING 172.16.200.1 (172.16.200.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.200.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.895/1.062/2.322/0.326 ms
```

3. Display tunnel usage statistics.

```
root@branch-srx> show security ipsec statistics
ESP Statistics:
  Encrypted bytes:            13600
  Decrypted bytes:             8400
  Encrypted packets:            100
  Decrypted packets:            100
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

This completes the verification of the IPsec VPN. Congratulations on the new branch location!

Step 3: What's Next

Congratulations! You've got your branch office configured for secure local communications, Internet access, and IPsec VPN for secure communications to a remote site. And, you've confirmed that it's all working to your expectations.

With minor adaptation, the procedures in this guide apply to the whole family of branch SRX devices. This guide focuses on the needs of a typical small branch office, and how to leverage the factory defaults of your new SRX device to quickly get a remote branch online.

We showed you how to configure the SRX using the Junos CLI. SRX devices also support cloud-based provisioning for those who prefer a GUI interface and/or require the advanced features cloud-based management offers. A companion guide in this series provides coverage of a day in the life for a cloud-based user.

Table 3: Task Summary

If you want to	Then

Verify factory-default operation	Use the Junos CLI to confirm the Day One+ ending state operation. • Confirm the WAN interface DHCP assignment and default route • Verify SRX default DHCP server for LAN ports • Confirm Layer 2 connectivity for ports in the default trust VLAN • Inspect flows for traffic allowed from the *trust* to *untrust* zones
Configure VLANs to isolate local traffic	See VLANs for more details on configuring VLANs. • Define VLANs • Configure an IRB interface for each VLAN • Configure DHCP servers for each VLAN to support auto-configuration of attached devices • Define security zones for the new VLANs • Define a security policy to control inter-VLAN traffic • Use a security policy to block source NAT and access to the *untrust* (Internet access) zone
Verify VLAN Operation	Confirm expected connectivity between the VLANs. • Verify DHCP server operation • Use security flow trace options to troubleshoot a connectivity issue • Add a security policy to provide the expected connectivity • Define a security policy to control inter-VLAN traffic
Configure an IPsec route-based VPN to a remote location	Add an IPsec VPN to provide secure communications over the Internet. This IPsec VPN supports dynamic address assignment at the branch office. • Define IKE and IPsec parameters • Configure the st.0 tunnel interfaces • Add a static route to direct desired traffic into the VPN • Create a *vpn* zone and a related security policy to allow traffic from the *trust* to *vpn* zone • Define a security policy to control inter-VLAN traffic

Verify IPsec VPN operation	Confirm successful IKE session and IPsec tunnel establishment. Verify that traffic is using the IPsec tunnel to reach the remote network. • Verify the license status • Confirm the IKE session • Confirm the IPsec tunnel • Verify the static route for the *trust* to the *vpn* zone traffic • Confirm only the desired traffic is using the tunnel
Verify licensing status	Confirm the features you configured don't require additional licensing.

With your branch site online, here are some places and things you might want to check out next.

Table 4: What's Next

If you want to	Then
See the Junos OS documentation	Visit the Junos OS documentation page
Learn more about IPsec VPN architectures and topologies	See Day One: IPsec VPN Cookbook
Learn how to provide wired and Wi-Fi Internet and Intranet access at a branch office	See Branch in a Box
Learn about Application Security	See Understanding Application Security
Learn about the application tracking tool for analyzing bandwidth usage of your network	See Application Tracking
Learn about Unified Threat Management (UTM) feature for SRX devices, which includes functions such as antivirus, antispam, content filtering, and web filtering	See UTM Overview
Set up your SRX device with advanced security measures to protect and defend your network	See SRX Series Up and Running with Advanced Security Services
Get hands-on experience with configuring an IPsec VPN	Visit Juniper Networks Virtual Labs and reserve your free sandbox. You'll find the IPsec VPN sandboxes in the Security category.

Our video library continues to grow! We've created many, many videos that demonstrate how to do everything from install your hardware to configure advanced Junos OS network features. Here are some great video and training resources that will help you expand your knowledge of Junos OS and branch SRX devices.

Table 5: Learn With Videos

If you want to	Then
View a Web-based training video which provides an overview of the SRX320 and describes how to install and configure it	Visit the SRX300 and SRX320 Services Gateways Overview and Deployment (WBT) page
Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies	See Learning With Juniper on the Juniper Networks main YouTube page
View a list of the many free technical trainings we offer at Juniper	Visit the Getting Started page on the Juniper Learning Portal