Network Configuration Example

Configuring a Small Office for High-Definition Videoconferencing

Published: 2014-01-10

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring a Small Office for High-Definition Videoconferencing
NCE0097

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

Introduction

This document describes the reference architecture for a small office, and provides step-by-step instructions to configure high-definition videoconferencing in a small office. It also provides troubleshooting tips to assist in detecting network configuration issues. Although the end-to-end solution includes the Polycom® video communication infrastructure, this document primarily focuses on the configuration of Juniper Networks® SRX Series Services Gateways.

Advantages of Using High-Definition Videoconferencing in a Small Office

Small office, home office (SOHO) is a residence or small site connected to the Internet using standard broadband technology such as DSL or cable. SOHO has gained popularity due to the advent of high-speed broadband connectivity, low- cost computing equipment, and innovations in secure remote access and visual communication infrastructure.

Enterprises and large corporations are encouraging employees who telecommute and employees with extreme daily commutes to utilize video as a telecommunications tool because it allows enterprises to save on physical infrastructure costs and address environmental factors. To enhance the productivity of teleworkers, a small office with reliable and cost-effective high-definition videoconferencing functionality is essential. A high-definition videoconference requires a network that can respond dynamically to the needs of the service, allocating network resources and providing a feedback loop between applications, users, and network infrastructure.

The Juniper Networks intelligent network infrastructure, in combination with Polycom high-definition videoconferencing, provides a solution that:

- Enables the delivery of high-definition video over a single converged network, significantly lowering service provider costs and improving return on investment (ROI).
- Enhances consistent customer experience by providing high-quality visual communications that are secure, scalable and cost effective.
- Provides scalable bandwidth on optimal hardware.
- Delivers predictable quality of service (QoS) performance and a rich set of security and service functions simultaneously.
- Provides a trustworthy network security perimeter for secure applications.
- Accelerates time to market as service providers deliver compelling video services faster with network convergence.
- Allows different service models, enabling service providers to offer managed video services that can be easily administered.

The joint solution takes advantage of network intelligence to ensure quality of experience for high-definition videoconferencing services from the desktop to the boardroom. By leveraging an intelligent infrastructure from Juniper Networks, service providers can deliver greater customer value through assured video experiences that are consistent, scalable, secure, and easy for end users to access.

Related Documentation

- Understanding the Small Office Videoconferencing Reference Architecture on page 2
- Example: Configuring a Small Office for High-Definition Videoconferencing on page 4

Understanding the Small Office Videoconferencing Reference Architecture

This topic provides the details of the SOHO reference architecture for deploying high-definition videoconferencing in a small office.

The SOHO reference architecture connects PCs and teleconferencing equipment to the high-speed broadband network using the residential network and Internet. The SRX Series Services Gateway connects to the broadband network, using either an integrated DSL modem or an external gateway.

NOTE: The reference architecture is dependent on the speed and latency of the telecommuter's broadband provider network. Unless an enterprise is willing to provide a dedicated circuit or virtual private network, and dedicated connection to the teleworker, the video quality is handled as *best effort* and is difficult to guarantee.

Figure 1 on page 2 shows the SOHO broadband reference architecture for a DSL connection.

Figure 1: SOHO Broadband Reference Architecture Using DSL

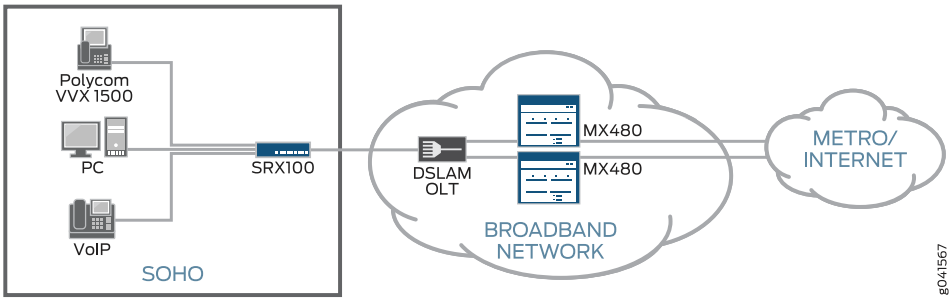
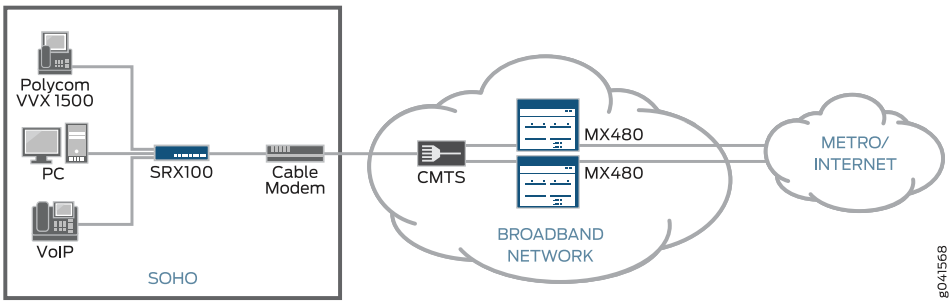


Figure 2 on page 3 shows the SOHO broadband reference architecture for a cable network.

Figure 2: SOHO Broadband Reference Architecture Using Cable Modem



In addition to PCs and voice over IP (VOIP) phones, the infrastructure at the SOHO network consists of the following devices:

- Polycom videoconferencing equipment— Polycom personal video solutions seamlessly extend clear, high-definition video to small offices, mobile users, and branch sites. Polycom VVX 1500 business media phones unify voice, video, and applications capabilities into simple-to-use unified communication (UC) devices, providing a dynamic, real-time meeting experience in a compact format with features that are easy to use in a small office environment and operate over an IP network. The Polycom VVX 1500 connects to the SRX Series Services Gateways.
- Juniper Networks SRX Series Services Gateways—Provide the security WAN routing and gateway functionality and offer the essential capabilities to connect, secure, and manage enterprise and service provider networks. The SRX Series Services Gateways offer service expandability as well as flexible processing and I/O scalability. Major features include:
  - Tightly integrated networking and security capabilities that include firewall, intrusion prevention system (IPS), distributed denial of service (DDoS) and denial of service (DoS), routing, quality of service (QoS), Network Address Translation (NAT), and other capabilities.
  - Dynamic services architecture that allows the SRX Series devices to quickly enable new services and capabilities.

  The SRX Series Services Gateway connects to the broadband network, using either an integrated DSL modem or an external gateway.
- Cable modem—The connection to the customer premise equipment (CPE) is provided through a cable modem using an Ethernet interface. The modem connects to a Cable Modem Termination Device (CMTS) on the residential network. In Figure 2 on page 3, an SRX100 Services Gateway serves as the secure router between the customer premises LAN segment and the Internet.
- DSL modem—The connection to the customer premises equipment is provided through a DSL modem, either using an Ethernet interface, in the case of a provider-supplied DSL modem, or through the SRX WAN interface option (ADSL2 Annex-A Mini-PIM). In Figure 1 on page 2, an SRX100 customer premises device with a WAN interface option (ADSL2 Annex-A Mini-PIM port) serves as the residential gateway device. This allows the SRX Series device to serve as both a DSL modem and a security router in the SOHO

site and helps to boost security while avoiding the associated dual NAT complexities. The ISP's residential network terminates the DSL modem on to a Digital Subscriber Line Access Multiplexer (DSLAM).

NOTE: When you configure an Ethernet interface, you must configure Point-to-Point Protocol over ATM (PPPoA) with login credentials to negotiate and set up IP connectivity to the public Internet.

The videoconferencing infrastructure in the data center consists of the following products:

- Juniper Networks SRX Series Services Gateways provide the security WAN routing and gateway functionality in the data center and offer the essential capabilities to connect, secure, and manage enterprise and service provider networks.
- Polycom Distributed Media Application (DMA) server is a network-based application for managing and distributing multipoint calls across conference platforms. It also performs the role of a Session Initiation Protocol (SIP) server and H.323 gatekeeper. The DMA that serves as the call control engine is the gatekeeper, which is contacted by the endpoints during call setup. The DMA is pre-provisioned with information about endpoints, their capabilities, and the site topology.
- Polycom Real-Time Media Conferencing Platform (RMX) is a real-time media conference platform that provides the multipoint conferencing facility to the endpoints by mixing the video and audio streams from multiple calls. When a conference call setup request is received, the DMA selects an RMX device based on the current load and communicates the call setup information to the appropriate RMX media server.
- Converged Management Application (CMA) helps by centrally managing and deploying visual communication across the enterprise organization—from large conference rooms to individual desktops.
- Juniper Networks Session and Resource Control (SRC) software is a dynamic policy and network resource allocation system that enables network resources to be dynamically reconfigured based on the requirements. The SRC connects the service layer with the network layer of service provider networks by providing a feedback loop between applications, users, and the network. Its open interfaces allow it to integrate with any network and any service offering, regardless of where the demand is generated. The SRC allows service providers to generate additional revenue on their existing network infrastructure by adding dynamically activated services.

Related Documentation

- Advantages of Using High-Definition Videoconferencing in a Small Office on page 1
- Example: Configuring a Small Office for High-Definition Videoconferencing on page 4

Example: Configuring a Small Office for High-Definition Videoconferencing

This example provides step-by-step procedures to configure the SRX100 Services Gateway to support broadband access with high-definition videoconferencing terminals. It shows how to establish secure connectivity using IP security (IPsec), implement a local

Dynamic Host Configuration Protocol (DHCP) server with NAT, set up security zones, provision QoS, and define the interface maximum transmission unit (MTU).

The topic includes the following sections:

Requirements

This example uses the following hardware and software components:

- Two Juniper Networks SRX Series Services Gateways (SRX100 and SRX3600) running Junos OS Release 11.4 or later.
- Two Juniper Networks MX Series 3D Universal Edge Routers running Junos OS Release 11.4 or later.

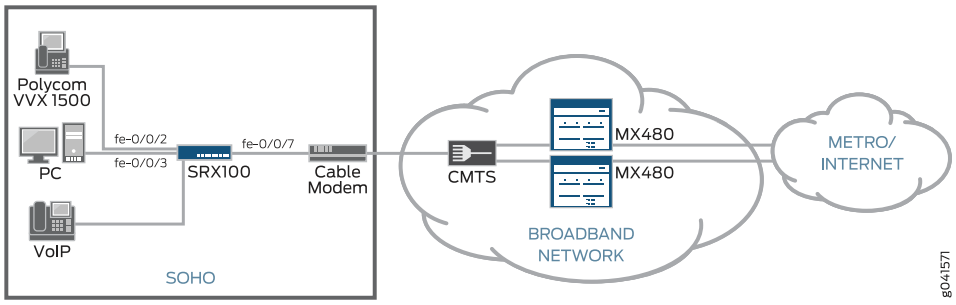
NOTE: This configuration example has been tested using the software release listed and is assumed to work on all later releases.

Overview

In this example, a cable-based SOHO is used as a reference model. This example assumes that the WAN link is represented with an Ethernet interface, and all configurations in the example reflect this.

Figure 3 on page 5 shows the physical topology.

Figure 3: SOHO Broadband Network Physical Topology



SOHO deployments are designed for desktop endpoint equipment whose bandwidth needs are less than 768 Kbps. An example is Polycom's VVX series device. In this example, the videoconferencing call is treated as best-effort traffic. No special resources or admission control provisioning is required by the service provider, and therefore the

high-definition videoconferencing service is provided with enhanced but not assured call experience.

The topology includes the following configurations:

- A small videoconferencing system such as Polycom's VVX1500 connects to the SRX100 Services Gateway over a 100 Mbps Fast-Ethernet link. The Polycom VVX device is configured to receive an IP address automatically using DHCP from a local server running on the SRX Series Services Gateway. The Polycom VVX device uses the interface IP address of the SRX Series Services Gateway as its gateway. The configuration for Polycom's VVX1500 is beyond the scope of this document.
- In the SOHO, the SRX Series Services Gateway provides secure IPsec virtual private network (VPN) connectivity for the video endpoint to communicate with the video data center as well as with endpoints at other sites during a point-to-point call. Additionally, the SRX100 device also acts as a security router protecting the SOHO equipment connected to its interfaces from the threats of the Internet.

  The SRX Series Services Gateway is also configured to protect devices in the trust zones from attacks originating from the unsecure Internet. These options help combat attacks, such as IP address sweeps, port scans, DOS attacks, Internet Control Message Protocol (ICMP) floods, User Datagram Protocol (UDP) floods, and many others.
- Security zones are configured on the SRX Series device to permit all traffic to and from the physical port to which the Polycom VVX1500 is connected. This ensures that the video endpoint can communicate (register, call signaling) with the centralized SIP proxy/ H.323 gateway that resides in the video data center, as well as with other endpoints at other sites. In this example, you configure two security zones: Trust and Untrust. The Trust security zone is used for all customer premises devices including PCs and videoconferencing endpoints, while the Untrust zone is used on the WAN interface. Because the SOHO devices are regarded as trustworthy, the Trust security zone is used for all customer premises devices.
- The SRX Series device serves as a DHCP server and NAT gateway for the video endpoints. It receives a public IP address from the ISP and in turn provides NAT to all traffic from the video endpoint to this IP address. The DHCP server is configured to match the device hardware address of the video endpoint with a pre-defined IP address. This is important because the Polycom DMA controller in the data center is provisioned to recognize endpoints using the IP address. The SRX Series device translates all traffic from the video endpoint's private IP address to the DHCP-assigned public IP address on the egress interface and vice versa.
- Although it is challenging to guarantee service-level agreements (SLAs) for calls over the public Internet, as a best practice, provision the SRX Series device to apply static QoS on the video endpoint traffic. You can achieve this by attaching a filter on the interface to which the endpoint is connected and marking ingress traffic on this interface with an assured forwarding Differentiated Services code point (DSCP). Since the traffic is traversing the Internet, only best-effort delivery is guaranteed.

NOTE: Ideally, QoS must be used across the end-to-end connection. However, since the last mile might not be QoS-enabled, a congestion-free metro access network cannot be guaranteed.

- Configure the MTU to ensure minimal packet loss and transit delays for videoconferencing traffic. You must consider the size of the entire network's MTU and configure the video endpoints accordingly.

Configuration

To configure a small office for high-definition videoconferencing, perform the following procedures on your SRX100 Services Gateway:

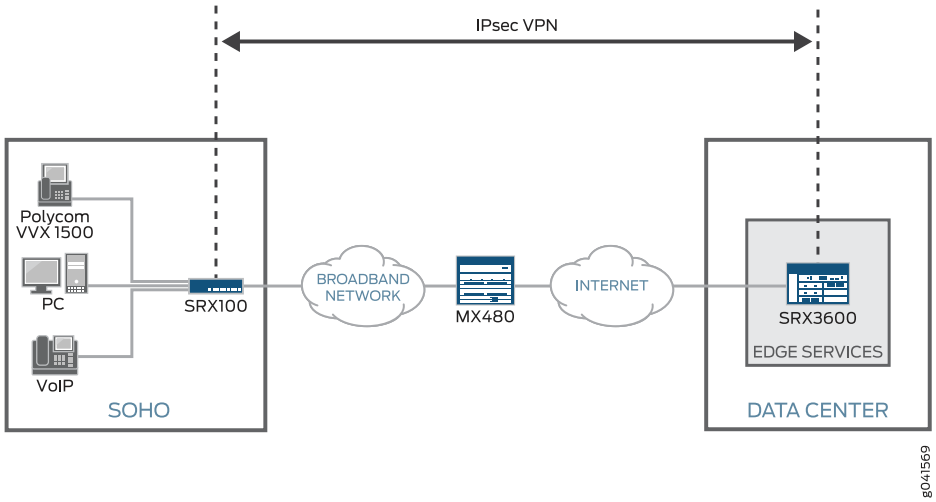
BEST PRACTICE: In any configuration session, it is a good practice to periodically use the **commit check** command to verify that the configuration can be committed.

Establishing Secure Connectivity Using IPsec

Step-by-Step Procedure

In this section, you configure the SRX Series device to provide IPsec VPN connectivity for the video endpoint to communicate with the video data center as well as with endpoints at other sites during a point-to-point call. Figure 4 on page 8 shows the IPsec connectivity between the video endpoint and the video data center.

Figure 4: IPsec Connectivity



To configure the IPsec VPN:

1. Configure the Internet key protocol (IKE) proposal.

   The IKE proposal must match with the IPsec tunnel termination proposal at the SRX3600 device in the video data center and at all other sites that this site communicates with. You define the authentication method, Diffie-Hellman group, authentication algorithm, encryption algorithm, and lifetime seconds.

   ```
   [edit]
   user@srx# set security ike proposal hdvc-ike-proposal authentication-method
     pre-shared-keys
   user@srx# set security ike proposal hdvc-ike-proposal dh-group group1
   user@srx# set security ike proposal hdvc-ike-proposal authentication-algorithm
     md5
   user@srx# set security ike proposal hdvc-ike-proposal encryption-algorithm
     aes-128-cbc
   user@srx# set security ike proposal hdvc-ike-proposal lifetime-seconds 86400
   ```

2. Configure the IKE policy that references the IKE proposal.

   Specify the IKE authentication method as **hdvc-ike-proposal**, and specify the mode as **main** for negotiating the IPsec security association.

   ```
   [edit]
   user@srx# set security ike policy ike-policy1 mode main
   user@srx# set security ike policy ike-policy1 proposals hdvc-ike-proposal
   ```

```
user@srx# set security ike policy ike-policy1 pre-shared-key ascii-text
  "$9$/2i.AuBcyKxNbIENbs2GU/CtuIESre"
```

3. Configure the IKE gateway that references the IKE policy.

   Specify the IKE IDs for the local and remote devices and the IP address of the SRX3600 device at the data center as the IPsec tunnel endpoint.

```
[edit]
user@srx# set security ike gateway hdvc-dc-Site-1 ike-policy ike-policy1
user@srx# set security ike gateway hdvc-dc-Site-1 address 10.10.10.1
user@srx# set security ike gateway hdvc-dc-Site-1 external-interface fe-0/0/7.0
```

4. Define the IPsec proposal by specifying the protocol, authentication algorithm, and encryption algorithm.

```
[edit]
user@srx# set security ipsec proposal hdvc-ipsec-proposal protocol esp
user@srx# set security ipsec proposal hdvc-ipsec-proposal authentication-algorithm
  hmac-md5-96
user@srx# set security ipsec proposal hdvc-ipsec-proposal encryption-algorithm
  aes-128-cbc
```

5. Configure an IPsec policy that references the IPsec proposal.

```
[edit]
user@srx# set security ipsec policy hdvc-ipsec-policy1 proposals hdvc-ipsec-proposal
```

6. Configure an IPsec VPN tunnel that references both the IKE gateway and the IPsec policy.

```
[edit]
user@srx# set security ipsec vpn hdvc-steer-VPN ike gateway hdvc-dc-Site-1
user@srx# set security ipsec vpn hdvc-steer-VPN ike ipsec-policy hdvc-ipsec-policy1
user@srx# set security ipsec vpn hdvc-steer-VPN establish-tunnels immediately
```

Configuring the Security Zones for the Endpoints

Step-by-Step Procedure

In this section, you configure **trust** and **untrust** security zones to permit all traffic to and from the physical port to which the Polycom VVX is connected.

To configure security zones:

1. Configure the Ethernet interface that serves as the default gateway for the video endpoint.

   Optionally, specify the description.

```
[edit]
user@srx# set interfaces fe-0/0/2 description "connected to V700-1"
user@srx# set interfaces fe-0/0/2 unit 0 family inet address 192.168.40.1/24
```

2. Configure the **trust** security zone.

   Include the TCP reset (**tcp-rst**) statement at the **[edit security zones security-zone trust]** hierarchy level. Specify **vvx-devices** as the address book address name and **192.168.40.0/24** as the address book IPv4 address. Specify **all** as the allowed host-inbound-traffic system services for the security zone. Specify **all** as the allowed host-inbound-traffic protocols.

```
[edit]
user@srx# set security zones security-zone trust tcp-rst
user@srx# set security zones security-zone trust address-book address vvx-devices
  192.168.40.0/24
user@srx# set security zones security-zone trust host-inbound-traffic
  system-services all
user@srx# set security zones security-zone trust host-inbound-traffic protocols all
```

3. Configure the **untrust** security zone.

   Assign an interface to the security zone and allow all system services for the security zone. Configure the address book entry for the untrust security zone. Specify an address set that includes all video endpoints and devices that the site has to communicate with.

```
[edit]
user@srx# set security zones security-zone untrust screen untrust-screen
user@srx# set security zones security-zone untrust address-book address
  managed-hdvc-at-dc 10.12.12.0/24
user@srx# set security zones security-zone untrust address-book address
  BigCo-remote-site-1 192.168.41.0/24
user@srx# set security zones security-zone untrust address-book address
  BigCo-remote-site-2 192.168.44.0/24
user@srx# set security zones security-zone untrust address-book address-set
  managed-hdvc-devices address managed-hdvc-at-dc
user@srx# set security zones security-zone untrust address-book address-set
  managed-hdvc-devices address BigCo-remote-site-1
user@srx# set security zones security-zone untrust address-book address-set
  managed-hdvc-devices address BigCo-remote-site-2
user@srx# set security zones security-zone untrust interfaces fe-0/0/7.0
  host-inbound-traffic system-services dhcp
user@srx# set security zones security-zone untrust interfaces fe-0/0/7.0
  host-inbound-traffic system-services ike
user@srx# set security zones security-zone untrust interfaces fe-0/0/7.0
  host-inbound-traffic protocols all
```

4. Configure the security policy to permit traffic from the **trust** zone to the **trust** zone.

```
[edit]
user@srx# set security policies from-zone trust to-zone trust policy default-permit
  match source-address any
user@srx# set security policies from-zone trust to-zone trust policy default-permit
  match destination-address any
user@srx# set security policies from-zone trust to-zone trust policy default-permit
  match application any
user@srx# set security policies from-zone trust to-zone trust policy default-permit
  then permit
```

5. Configure the security policy to permit traffic from the **trust** zone to the **untrust** zone.

```
[edit]
user@srx# set security policies from-zone trust to-zone untrust policy
  hdvc-endpoint-steer match source-address vvx-devices
user@srx# set security policies from-zone trust to-zone untrust policy
  hdvc-endpoint-steer match destination-address managed-hdvc-devices
user@srx# set security policies from-zone trust to-zone untrust policy
  hdvc-endpoint-steer match application any
```

```
user@srx# set security policies from-zone trust to-zone untrust policy
  hdvc-endpoint-steer then permit tunnel ipsec-vpn hdvc-steer-VPN
user@srx# set security policies from-zone trust to-zone untrust policy
  hdvc-endpoint-steer then permit tunnel pair-policy steer-to-hdvc-endpoint
user@srx# set security policies from-zone trust to-zone untrust policy default-permit
  match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy default-permit
  match destination-address any
user@srx# set security policies from-zone trust to-zone untrust policy default-permit
  match application any
user@srx# set security policies from-zone trust to-zone untrust policy default-permit
  then permit
```

6. Configure the security policy to permit traffic from the **untrust** zone to the **trust** zone.

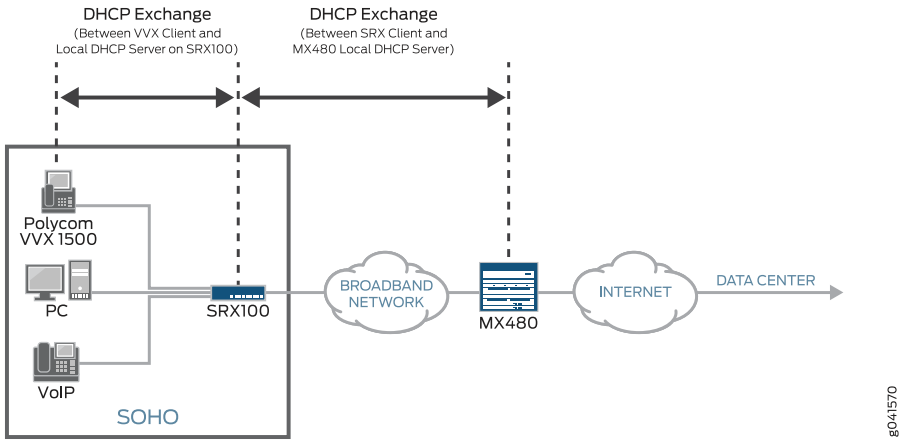
```
[edit]
user@srx# set security policies from-zone untrust to-zone trust policy
  steer-to-hdvc-endpoint match source-address managed-hdvc-devices
user@srx# set security policies from-zone untrust to-zone trust policy
  steer-to-hdvc-endpoint match destination-address vvx-devices
user@srx# set security policies from-zone untrust to-zone trust policy
  steer-to-hdvc-endpoint match application any
user@srx# set security policies from-zone untrust to-zone trust policy
  steer-to-hdvc-endpoint then permit tunnel ipsec-vpn hdvc-steer-VPN
user@srx# set security policies from-zone untrust to-zone trust policy
  steer-to-hdvc-endpoint then permit tunnel pair-policy hdvc-endpoint-steer
user@srx# set security policies from-zone untrust to-zone trust policy default-permit
  match source-address any
user@srx# set security policies from-zone untrust to-zone trust policy default-permit
  match destination-address any
user@srx# set security policies from-zone untrust to-zone trust policy default-permit
  match application any
user@srx# set security policies from-zone untrust to-zone trust policy default-permit
  then permit
```

Configuring the Local DHCP Server

Step-by-Step Procedure

This section describes how to configure an SRX Series device as a local DHCP server and a DHCP client. Figure 5 on page 12 illustrates the DHCP address assignment mechanism.

Figure 5: DHCP Address Assignment



To configure DHCP:

1. Configure the DHCP server.

   Specify the static binding for the DHCP client and bind the hardware address of the Polycom VVX device to a static IP address on the local network.

   ```
   [edit]
   user@srx# set system services dhcp router 192.168.40.1
   user@srx# set system services dhcp static-binding 00:e0:db:07:e3:df fixed-address
     192.168.40.228
   ```

2. Specify fe-0/0/7 as the interface on which the DHCP client has to be enabled.

   Optionally specify the description.

   ```
   [edit]
   user@srx# set interfaces fe-0/0/7 description "Connected to the WAN-Edge layer"
   user@srx# set interfaces fe-0/0/7 unit 0 family inet dhcp
   ```

3. Specify DHCP as a host-inbound service for the **untrust** security zone to which the interface is bound.

   ```
   [edit]
   user@srx# set security zones security-zone untrust interfaces fe-0/0/7.0
     host-inbound-traffic system-services dhcp
   ```

4. Define the number of attempts allowed to retransmit a DHCP packet.

   ```
   [edit]
   user@srx# set interfaces fe-0/0/7 unit 0 family inet dhcp retransmission-attempt
     3
   ```

5. Define the interval, in seconds, allowed between retransmission attempts.

```
[edit]
user@srx# set interfaces fe-0/0/7 unit 0 family inet dhcp retransmission-interval
  6
```

Configuring Source NAT

Step-by-Step Procedure

In this section, you configure the SRX100 Services Gateway to translate all traffic from the private IP address of the video endpoint to the DHCP-assigned public IP address on the egress interface and vice versa.

To configure NAT:

1. Create a source NAT rule set called **VVX-Interface-NAT**.

```
[edit]
user@srx# set security nat source rule-set VVX-Interface-NAT from zone trust
user@srx# set security nat source rule-set VVX-Interface-NAT to zone untrust
```

2. Create a rule called **private_net** and assign it to the rule set. Specify the range of private IP addresses that require NAT translation.

```
[edit]
user@srx# set security nat source rule-set VVX-Interface-NAT rule private_net
  match source-address 192.168.40.0/24
```

3. Specify the action to translate the source address to the address of the egress interface.

   The SRX100 device uses the specified source-nat interface, and translates the source IP address and port for outgoing traffic, using the IP address of the egress interface as the source IP address and a random higher port for the source port.

```
[edit]
user@srx# set security nat source rule-set VVX-Interface-NAT rule private_net then
  source-nat interface
```

Configuring Screens

Step-by-Step Procedure

In this section, you configure an intrusion detection service (IDS) profile and attach it to the **untrust** zone. You configure the SRX100 Services Gateway to protect devices in the trust zone from attacks originating from the unsecure Internet. The screening options help combat attacks, such as IP address sweeps, port scans, DOS attacks, ICMP floods, and UDP floods.

To configure the IDS profile and attach it to a zone:

1. Create an IDS profile called **untrust-screen** and configure the ICMP screening options.

```
[edit]
user@srx# set security screen ids-option untrust-screen icmp ping-death
```

2. Configure the IP screening options.

```
[edit]
user@srx# set security screen ids-option untrust-screen ip source-route-option
```

```
user@srx# set security screen ids-option untrust-screen ip tear-drop
```

3. Configure the TCP screening options.

```
[edit]
user@srx# set security screen ids-option untrust-screen tcp syn-flood
  alarm-threshold 1024
user@srx# set security screen ids-option untrust-screen tcp syn-flood
  attack-threshold 200
user@srx# set security screen ids-option untrust-screen tcp syn-flood
  source-threshold 1024
user@srx# set security screen ids-option untrust-screen tcp syn-flood
  destination-threshold 2048
user@srx# set security screen ids-option untrust-screen tcp syn-flood timeout 20
user@srx# set security screen ids-option untrust-screen tcp land
```

4. Attach the IDS profile **untrust-screen** to the **untrust** zone.

```
[edit]
user@srx# set security zones security-zone untrust screen untrust-screen
```

Provisioning QoS on the Video Endpoint and Configuring the Interface MTU

Step-by-Step Procedure

In this section, the SRX100 Services Gateway is provisioned to apply static QoS on the video endpoint traffic.

To ensure minimal packet loss and transit delays for video conferencing traffic, you must consider the size of the entire network's MTU and configure the video endpoints accordingly. By default, on the Polycom V700 device, the MTU is set to 1260 bytes. The end-to-end MTU assessment must account for overhead added by IPsec VPN (~52 bytes), VLAN header (4 bytes), and Layer 3 VPN (4 bytes). If the packet size exceeds that MTU of any network link, it is fragmented into two or more fragments. This must be avoided for high-definition videoconferencing traffic because it results in degraded quality. In the case of IPsec tunnels, packet fragmentation is absolutely not permissible.

The default value for the MTU on the Fast Ethernet interface of the SRX Series device is 1500 bytes. Based on the end-to-end MTU calculation, this must be changed on both the interface connecting the video endpoint and the WAN uplink, if required. Typically, the MTU size in cable and asymmetric digital subscriber line (ADSL) networks is even shorter, so ensure that the length of the transmitted packets does not exceed the link's MTU.

To provision QoS and reset the MTU:

1. Create a firewall filter called **V700-MC-Bronze-Tier**, and specify the term as **All-VVX-Traffic** and the forwarding class as **MC-BRONZE** to select the traffic.

```
[edit]
user@srx# set firewall filter V700-MC-Bronze-Tier term All-VVX-Traffic then
  forwarding-class MC-BRONZE
user@srx# set firewall filter V700-MC-Bronze-Tier term All-VVX-Traffic then accept
```

2. Apply the firewall filter to the fe-0/0/2 interface, which connects the video endpoint.

   Optionally, specify the description.

```
[edit]
user@srx#  set interfaces fe-0/0/2 description "connected to V700-1"
user@srx# set interfaces fe-0/0/2 unit 0 family inet filter input VVX-Bronze-Tier
user@srx# set interfaces fe-0/0/2 unit 0 family inet address 192.168.40.1/24
```

3. Reset the MTU size to 1492 at the fe-0/0/2 interface.

```
[edit]
user@srx# set interfaces fe-0/0/2 unit 0 family inet mtu 1492
```

Verification

After configuring the SRX Series Services Gateway, ensure the connectivity to the essential elements in the network. The following steps illustrate debugging examples at various network elements in the path.

Ping the DHCP server from the SRX Series Services Gateway, If the DHCP IP address is not assigned to the SRX Series Services Gateway, perform the following steps:

1. Re-initiate the DHCP request.

   The video endpoint device acquires an IP address through DHCP.

2. If an IP address is acquired at the video endpoint device, check the end-to-end connectivity between the video endpoint and the video signaling equipment (Polycom's DMA, RMX) in the data center.

   Video endpoints provide a connectivity test that is accessible using the Web interface of the endpoint. If problems still exist, troubleshoot the routers.

3. If connectivity to the video signaling equipment in the data center has not yet been established, verify the connectivity to the public Internet.

   You can verify the connectivity by pinging the default gateway that was assigned to the SRX Series Services Gateway by the ISP's DHCP server.

4. If there are no connectivity issues, then inspect the IPsec VPN configuration on the SRX Series Services Gateway, and the tunnel termination configuration in the SRX cluster at the video data center.

5. If there are any MTU-related problems, ping from the video endpoint using the ICMP packets with the packet length set to the size of the MTU configured on the SRX Series Services Gateway.

Confirm that the configuration is working properly.

Re-Initiating DHCP IP Address Assignment on SRX Series Services Gateway

Purpose Re-initiate the DHCP client IP address assignment on the SRX Series Services Gateway.

Action From operational mode on the SRX Series Services Gateway, enter the **request system services dhcp renew fe-0/0/7** command.

```
user@srx> request system services dhcp renew fe-0/0/7
```

Meaning If the IP address of the interface is renewed, then this command produces no output.

Verifying the DHCP Client Information

Purpose Verify the DHCP client information on the SRX Series Services Gateway.

Action From operational mode on the SRX Series Services Gateway, enter the **show system services dhcp client fe-0/0/7.0** command.

```
user@srx> show system services dhcp client fe-0/0/7.0
```

```
user@srx> show system services dhcp client fe-0/0/7.0
Logical Interface name         fe-0/0/7.0
Hardware address        00:12:1e:a9:7b:81
Client status           bound
Address obtained        30.1.1.20
Update server           disabled
Lease obtained at       2013-05-10 18:16:18 UTC
Lease expires at        2013-05-11 18:16:18 UTC
DHCP options:
    Name: server-identifier, Value: 30.1.1.2
Code: 1, Type: ip-address, Value: 255.255.255.0
Name: name-server, Value: [ 77.77.77.77, 55.55.55.55 ]
Name: domain-name, Value: testlab.test.net
```

Meaning Verify the hardware address is correct, the client status is **bound**, and that the address obtained is correct.

Verifying the DHCP Statistics

Purpose Verify the DHCP statistics on the SRX Series Services Gateway are incrementing.

Action From operational mode on the SRX Series Services Gateway, enter the **show system services dhcp client statistics** command.

```
user@srx> show system services dhcp client statistics
```

```
Packets dropped:
    Total                     0

Messages received:
    DHCPOFFER                 0
    DHCPACK                   8
    DHCPNAK                   0

Messages sent:
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPREQUEST               1
    DHCPINFORM                0
    DHCPRELEASE               0
```

```
DHCPRENEW                   7
DHCPREBIND                  0
```

Meaning Verify that the **DHCPACK**, **DHCPRENEW**, and **DHCPACK** statistics are all incrementing.

Verifying the Connectivity from SRX Series Services Gateway

Purpose Verify that you have end-to-end connectivity between the video endpoint and the video signaling equipment at the data center.

Action From operational mode, enter the **ping** command on the SRX Series Services Gateway to verify connectivity to the video endpoint.

```
user@srx> ping 192.168.40.228
PING 192.168.40.228 (192.168.40.228): 56 data bytes
...
–192.168.40.228 ping statistics –
15 packets transmitted, 15 packets received, 0% packet loss
```

From operational mode, enter the **ping** command on the SRX Series Services Gateway to verify connectivity to the video signaling equipment (DMA) at the data center.

```
user@srx> ping 10.12.12.248
PING 10.12.12.248 (10.12.12.248): 56 data bytes
...
–10.12.12.248 ping statistics –
20 packets transmitted, 20 packets received, 0% packet loss
```

Meaning Verify the number of packets transmitted, packets received, and packets lost. If **0% packet loss** is displayed, it indicates that the connectivity is working.

Related Documentation

- Advantages of Using High-Definition Videoconferencing in a Small Office on page 1
- Understanding the Small Office Videoconferencing Reference Architecture on page 2