Concepts & Examples
ScreenOS Reference Guide

Volume 11:
High Availability

Release 5.4.0, Rev. A

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

Part Number: 530-015778-01, Revision A

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: ScreenOS Team

Editor: Lisa Eldridge

Table of Contents

About This Volume

Volume 11: High Availability presents an overview of the NetScreen Redundancy Protocol (NSRP) and describes how to cable, configure, and manage Juniper Networks security devices in a redundant group to provide high availability (HA) services using NSRP. It also covers NSRP-Lite, which is a light-weight version of NSRP that does not support the synchronization of Run-Time Objects (RTOs).

This volume contains the following chapters:

- Chapter 1, "NetScreen Redundancy Protocol," explains how to cable, configure, and manage Juniper Networks security devices in a redundant group to provide high availability (HA) using the NetScreen Redundancy Protocol (NSRP).
- Chapter 2, "Interface Redundancy," describes the various ways in which Juniper Networks security devices provide interface redundancy.
- Chapter 3, "Failover," describes the configuration for the failover of a device, virtual security device (VSD) group, and virtual system. It also explains how to monitor certain objects to determine the failover of a device or VSD group.
- Chapter 4, "NSRP-Lite," explains how to configure Juniper Networks security devices that support NSRP-Lite.

Document Conventions

This document uses several types of conventions, which are introduced in the following sections:

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- Anything inside square brackets [ ] is optional.
- Anything inside braces **{ }** is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example:

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means "set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface."

- Variables are in *italic* type:

  ```
  set admin user name1 password xyz
  ```

In text:

- Commands are in **boldface** type.
- Variables are in *italic* type.

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u kath j12fmt54** is enough to enter the command **set admin user kathleen j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Illustration Conventions

The following figure shows the basic set of images used in illustrations throughout this manual.

Figure 1: Images in Manual Illustrations

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:

  set address trust “local LAN” 10.1.1.0/24

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, **“ local LAN ”** becomes **“local LAN”**.

- Multiple consecutive spaces are treated as a single space.

- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, **“local LAN”** is different from **“local lan”**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

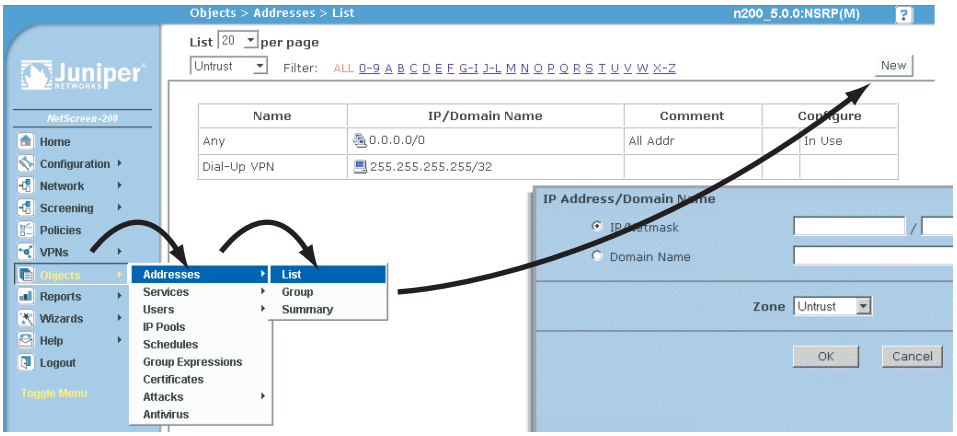
- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes (“), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

WebUI Conventions

A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

Figure 2: WebUI Navigation



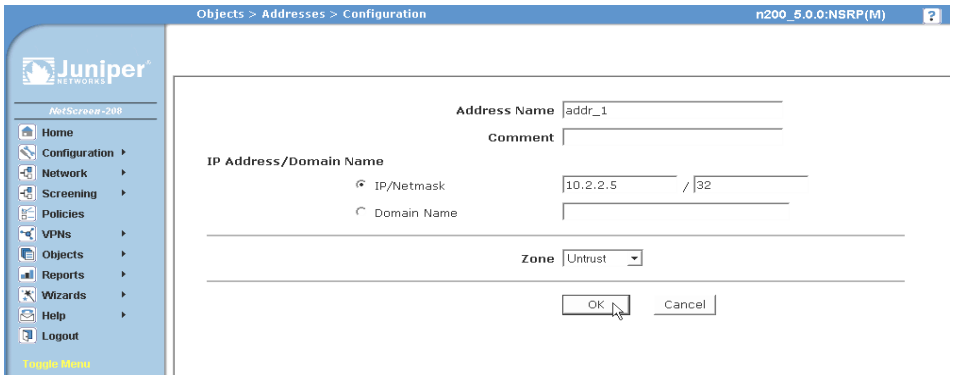
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

Figure 3: Navigational Path and Configuration Settings



Juniper Networks Documentation

To obtain technical documentation for any Juniper Networks product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

techpubs-comments@juniper.net

Chapter 1

NetScreen Redundancy Protocol

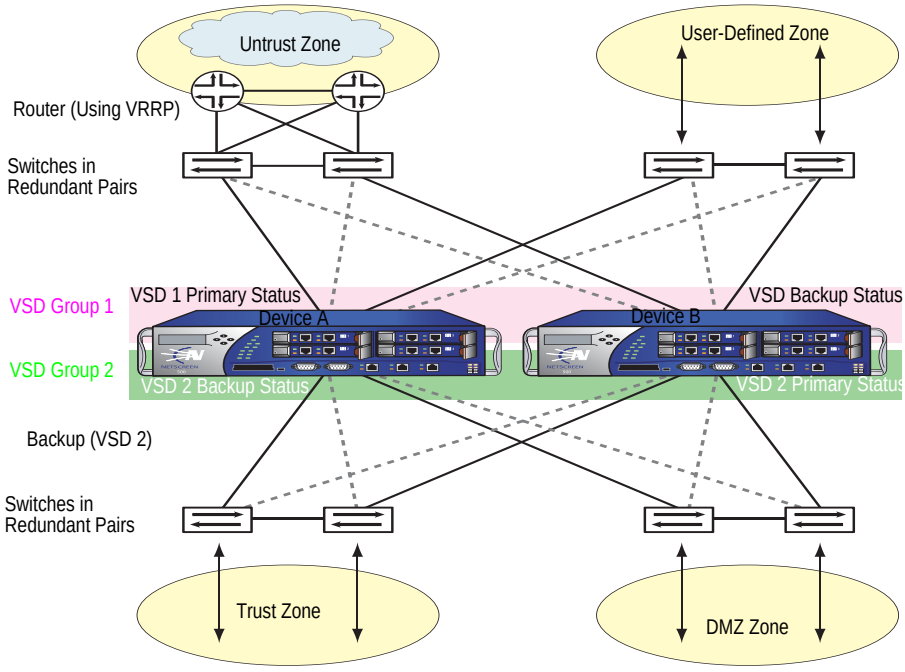
This chapter explains the components of NetScreen Redundancy Protocol (NSRP) and describes how to use NSRP to support high availability (HA). This chapter contains the following sections:

Overview

High availability provides a way to minimize the potential for device failure within a network. Because all of your network traffic passes through a Juniper Networks security device, you need to remove as many points of failure as possible from your network by ensuring that the device has a backup in case it fails.

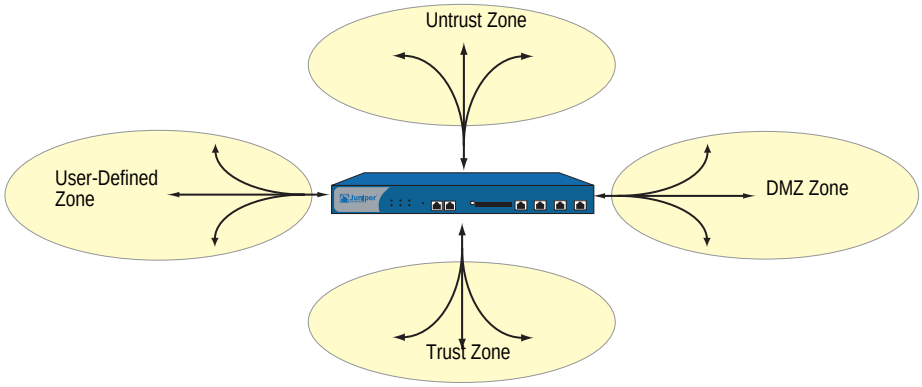
Setting up your security devices in HA pairs removes one potential point of failure from your network design. You can remove other potential points of failure by setting up redundant switches on either side of the HA pair of security devices. For a highly fault tolerant network, you can mirror the two sets of paired switches and HA pair of security devices as shown in Figure 1.

Figure 1: Introducing Fault-Tolerance into the Network



To function properly as a network firewall, a security device must be placed at the single point through which all inter-zone traffic must pass. See Figure 2.

Figure 2: All Inter-Zone Traffic Flowing Through the Firewall

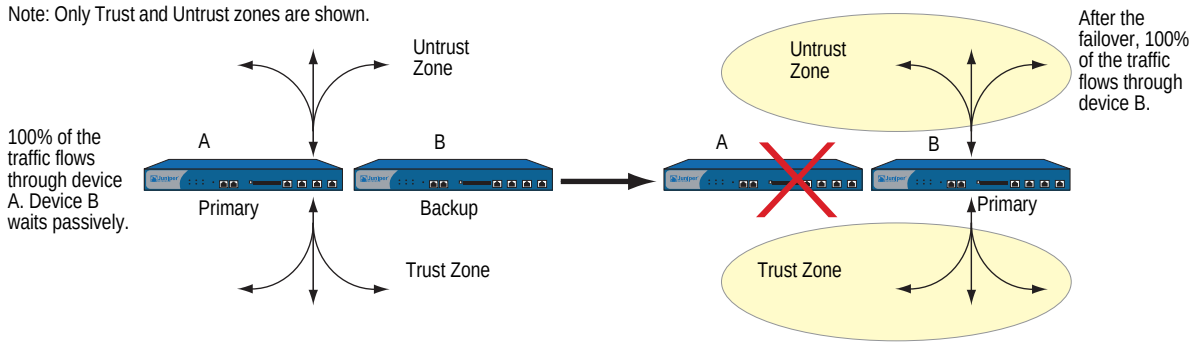


The security device is the single point through which all inter-zone traffic must pass, and, as such, traffic flow must remain uninterrupted, even in the event of a device or network failure.

To ensure a continuous traffic flow, you can cable and configure two security devices in a redundant cluster, with one device acting as a primary device and the other as its backup. The primary device propagates all its network and configuration settings and the current session information to the backup device. If the primary device fails, the backup device is promoted to primary and takes over the traffic processing.

In Figure 3, the two devices are in an active/passive configuration; that is, the primary device is active, handling all firewall and VPN activities, and the backup device is passive, waiting to take over when the primary device fails.

Figure 3: Active/Passive Failover



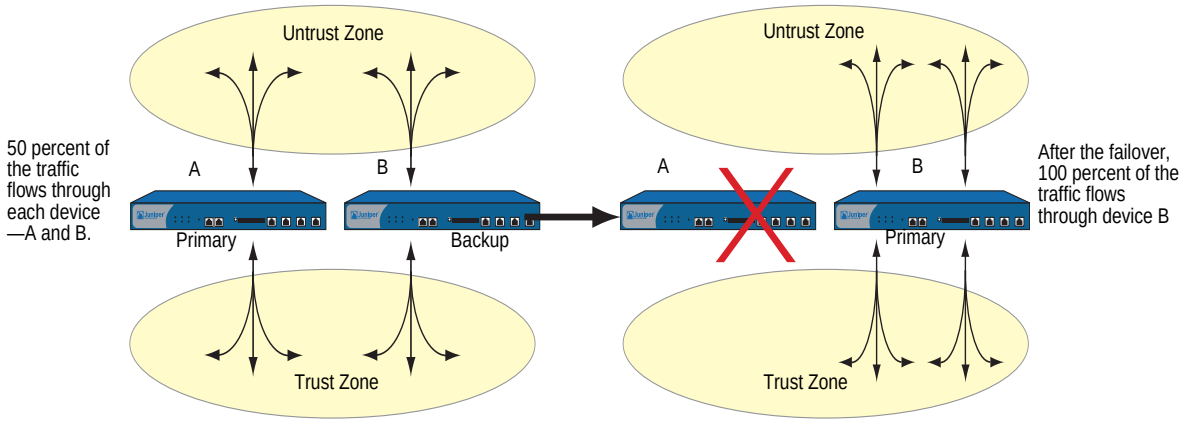
NOTE: Although the backup device is passive in the sense that it is not processing traffic, it is maintaining its synchronization with the configuration settings and session information it continuously receives from the primary device.

With the security device in Route or NAT mode, you can configure both devices in a redundant cluster to be active, sharing the traffic distributed between them by routers with load-balancing capabilities running a protocol such as the Virtual Router Redundancy Protocol (VRRP). This is accomplished using the NetScreen Redundancy Protocol (NSRP) to create two virtual security device (VSD) groups, each with its own virtual security interfaces (VSIs). Device A acts as the primary device in VSD group 1 and as the backup of VSD group 2. Device B acts as the primary device in VSD group 2 and as the backup of VSD group 1. This configuration is known as active/active (see Figure 1). No single point of failure exists in an active/active setup. Figure 1 shows an active/active setup.

Devices A and B each receive 50 percent of the network and VPN traffic. Should device A fail, device B becomes the primary device of VSD group 1, as well as continuing to be the primary device of VSD group 2, and handles 100 percent of the traffic. Traffic redirection resulting from a failover in an active/active configuration is shown in Figure 4.

Figure 4: Active/Active Failover

Note: Only Trust and Untrust zones are shown.



Although the total number of sessions divided between the two devices in an active/active configuration cannot exceed the capacity of a single security device (otherwise, in the case of a failover, the excess sessions might be lost), the addition of a second device doubles the available bandwidth potential. A second active device also guarantees that both devices have functioning network connections.

NOTE: Each device in an active/active configuration can tolerate traffic bursts exceeding 50 percent of the capacity of a single device for short periods of time; however, should a failover occur during that period, the excess traffic might be lost.

In addition to NSRP clusters, which are primarily responsible for propagating configurations among group members and advertising each member's current VSD group states, you can configure devices A and B as members in an RTO mirror group, which is responsible for maintaining the synchronicity of run-time objects (RTOs) between a pair of devices. When the primary device fails, the backup can immediately assume the primary device's role with minimal service downtime by maintaining all current sessions.

NOTE: RTOs are objects created dynamically in the security device memory during the normal operation of the device. RTOs allow the device to understand the network around it and enforce its policies. Examples of RTOs are TCP/UDP sessions, IPSec Phase 2 security associations (SAs), DHCP allocations, RSA and DSS key pairs, ARP tables, and DNS caches.

You can secure all NSRP traffic with encryption and authentication. NSRP supports the DES and MD5 algorithms. (For more information about these algorithms, see "Protocols" on page **5**-5.)

NOTE: If the HA cables run directly from one security device to another (that is, not through a switch forwarding other kinds of network traffic), it is unnecessary to use encryption and authentication.

If you want to use Simple Network Management Protocol (SNMP) to monitor the security device, private NSRP MIBs are available for download at www.juniper.net/support. (For more information about SNMP, see "Simple Network Management Protocol" on page **3**-70.)

NetScreen Redundancy Protocol

When a security device is operating at Layer 3 (NAT or Route mode) or in Layer 2 (Transparent mode), it can be in an active/active or active/passive NetScreen Redundancy Protocol (NSRP) configuration. To manage a backup device for either mode, you must use the manage IP address that you set per security zone interface.

NOTE: You cannot set a manage IP address on a VSI for any VSD group except VSD group 0.

Performing the most basic active/passive NSRP configuration is easy. You can put a device in an NSRP cluster and VSD group with a single CLI command—**set nsrp cluster id** *number*—or in the WebUI by typing a single number for the NSRP cluster ID.

You can enable automatic RTO synchronization with the CLI command **set nsrp rto sync all**, or in the WebUI by selecting the **NSRP RTO Synchronization** option on the Network > NSRP > Synchronization page and then clicking **Apply**.

Next, you must also select the ports that you want the devices to monitor, so that if they detect a loss of network connectivity on one of the monitored ports, the device fails over.

NOTE: Before NSRP can function, you must first cable two security devices together as explained in "Cabling for a Full-Mesh Configuration" on page 32. Also, if you want to maintain network connectivity for administrative traffic to one or more physical interfaces on a security device in an NSRP cluster, first set the manage IP address for those interfaces as explained in "Setting Manage IPs for Multiple Interfaces" on page **3**-29 before you enable NSRP.

Default Settings

NSRP Default Settings	Value
VSD Group Information	
■ VSD group ID:	0
■ Device priority in the VSD group:	100
■ Preempt option:	disabled
■ Preempt hold-down time:	0 seconds
■ Initial state hold-down time:	5 seconds
■ Heartbeat interval:	1000 milliseconds
■ Lost heartbeat threshold:	3
■ Master (Primary) always exist:	no
RTO Mirror Information	
■ RTO synchronization:	disabled
■ Heartbeat interval:	4 seconds
■ Lost heartbeat threshold:	16
NSRP Link Information	
■ Number of gratuitous ARPs:	4
■ NSRP encryption:	disabled
■ NSRP authentication:	disabled
■ Track IP:	none
■ Interfaces monitored:	none
■ Secondary path:	none
■ HA link probe:	none
■ Interval:	15
■ Threshold:	5

When you set a security device in an NSRP cluster, the device automatically creates VSD group 0 and transforms physical interfaces into Virtual Security Interfaces (VSIs) for VSD group 0.

NOTE: The convention for indicating a VSI is *interface_name*:*VSD_group_ID*. For example, the following indicates that the redundant interface **red1** is a VSI for VSD group 1: **red1:1**. However, if the VSD group ID is 0, no VSD group ID is specified. For example, if the redundant interface **red2** is a VSI for VSD group 0, it appears simply as **red2**.

NSRP Clusters

An NSRP cluster consists of a group of security devices that enforces the same overall security policy and share the same configuration settings. When you assign a security device to an NSRP cluster, any changes made to the configuration on one member of the cluster propagate to the other.

Members of the same NSRP cluster maintain identical settings for the following:

- Policies and policy objects (such as addresses, services, VPNs, users, and schedules)
- System parameters (such as settings for authentication servers, DNS, SNMP, syslog, URL blocking, firewall detection options, and so on)

Members of a cluster do not propagate the following configuration settings, as shown in Table 1.

Table 1: Non-Propagating Commands

NSRP	
	■ set/unset nsrp cluster id *number* ■ set/unset nsrp auth password *pswd_str* ■ set/unset nsrp encrypt password *pswd_str* ■ set/unset nsrp monitor interface *interface* ■ set/unset nsrp vsd-group id *id_num* { mode *string* | preempt | priority *number* } ■ set/unset nsrp rto-mirror …
Interface	
	■ set/unset interface *interface* manage-ip *ip_addr* ■ set/unset interface *interface* phy … ■ set/unset interface *interface* bandwidth *number* ■ set/unset interface redundant *number* phy primary *interface* ■ All commands pertaining to local interfaces
IP Tracking	
	■ All IP tracking commands (set/unset nsrp track-ip …)
Console Settings	
	■ All console commands (set/unset console …)
Hostname	
	■ set/unset hostname *name_str*
SNMP	
	■ set/unset snmp name *name_str*
Virtual Router	
	■ set/unset vrouter *name_str* router-id *ip_addr*
Clear[1]	
	■ All clear commands (clear admin, clear dhcp, …)

Debug[2]
■ All debug commands (debug alarm, debug arp, …)

1.By default, NSRP cluster members do not propagate the **clear** commands. To propagate a clear command to all devices in an NSRP cluster, insert the keyword **cluster** into the command. For example, **clear cluster admin …**, **clear cluster dhcp …**

2.By default, NSRP cluster members do not propagate the **debug** commands. To propagate a debug command to all devices in an NSRP cluster, insert the keyword **cluster** into the **debug** command. For example, **debug cluster alarm …**, **debug cluster arp …**

Before two security devices can provide redundant network connectivity, you must group them in the same NSRP cluster by assigning a cluster ID between 1 and 7. When a security device becomes a member of a cluster, it automatically becomes a member of VSD group 0, and all interfaces become VSIs for VSD group 0. If you want to retain some interfaces as local interfaces and create VSIs from select interfaces, you must do the following:

1. Remove VSD group 0.

   All the interfaces on all cluster members become local interfaces.

2. Create another VSD group, such as VSD group 1.

3. Create VSIs for that VSD group.

For more information about VSD groups, see “Virtual Security Device Groups” on page 16.

NOTE: Assigning an ID of 0 removes a device from a cluster.

Cluster members can also synchronize run-time objects (RTOs), which allows a newly elected VSD group primary device to maintain uninterrupted network and VPN services after a failover. (For more information about RTOs, see “Run-Time Objects” on page 10.)

Creating an NSRP Cluster

Because NSRP cluster members can have different host names, a failover can disrupt SNMP communication and the validity of digital certificates because SNMP communication and certificates rely on the host name of a device to function properly.

To define a single name for all cluster members, type the following CLI command:

```
set nsrp cluster name name_str
```

NOTE: On devices that do not have a dedicated HA port, you must bind the interface to the HA zone before configuring the NSRP cluster.

Use the cluster name when configuring the SNMP host name for the security device (**set snmp name** *name_str*) and when defining the common name in a PKCS10 certificate request file.

The use of a single name for all cluster members allows SNMP communication and digital certificate use to continue without interruption after a device failover.

In the example shown in Figure 5, you group devices A and B within NSRP cluster ID 1 with cluster name "cluster1." You also specify the following settings on each device:

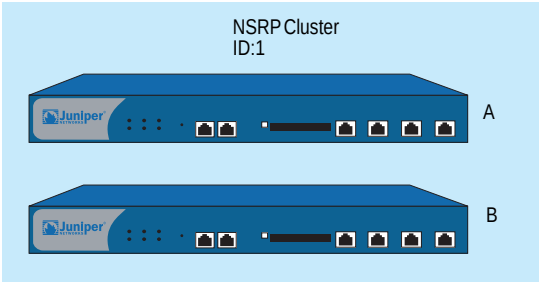
NSRP communication security: Assign passwords—725dCaIgDL and WiJoaw4177—for creating authentication and encryption keys to secure NSRP communications.

After you have grouped both devices in the same cluster and given them the same authentication and encryption passwords, you can enter the following settings on either device A or B. (Most settings entered on one device in a cluster propagate to the other device. For a list on non-propagating commands, see Table 1 on page 7.)

- **Interface monitoring:** Select the ethernet1 (bound to the Untrust zone) and ethernet2 (bound to the Trust zone) for monitoring Layer 2 network connectivity.
- **Secondary link:** Specify that the ethernet2 interface carry VSD heartbeats should both HA1 and HA2 links go down. The purpose of this feature is to prevent multiple VSD group primary devices when both HA links fail.
- **Gratuitous ARP broadcasting:** Specify the number of ARP broadcasts as 5 (the default is 4). ARP broadcasts notify surrounding network devices of the MAC address of a new primary device after a failover has occurred.

(All the interfaces on these devices become VSIs for VSD group 0. In "Virtual Security Device Groups" on page 16, you create a second VSD group for these devices.)

Figure 5: NSRP Cluster



WebUI (Device-A)

1. **NSRP Cluster and Communication Security**
   Network > NSRP > Cluster: Enter the following, then click **Apply**:

   Cluster ID: 1
   NSRP Authentication Password: (select) 725dCaIgDL
   NSRP Encryption Password: (select) WiJoaw4177

NOTE: You can only set a cluster name through the CLI.

WebUI (Device-B)

2. **NSRP Cluster and Communication Security**
   Network > NSRP > Cluster: Enter the following, then click **Apply**:

   Cluster ID: 1
   Number of Gratuitous ARPs to Resend: 5
   NSRP Authentication Password: (select) 725dCaIgDL
   NSRP Encryption Password: (select) WiJoaw4177

3. **NSRP Settings**
   Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Select **ethernet1** and **ethernet2**, then click **Apply**.

   Network > NSRP > Link: Select **ethernet2** from the Secondary Link drop-down list, then click **Apply**.

CLI (Device-A)

1. **NSRP Cluster and Communication Security**
   set nsrp cluster id 1
   set nsrp auth password 725dCaIgDL
   set nsrp encrypt password WiJoaw4177
   save

CLI (Device-B)

2. **NSRP Cluster and Communication Security**
   set nsrp cluster id 1
   set nsrp auth password 725dCaIgDL
   set nsrp encrypt password WiJoaw4177
   save

3. **NSRP Settings**
   set nsrp cluster name cluster1
   set nsrp monitor interface ethernet1
   set nsrp monitor interface ethernet2
   set nsrp secondary-path ethernet2
   set nsrp arp 5
   save

Run-Time Objects

Run-Time Objects (RTOs) are code objects created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, DHCP leases, and IPSec security associations (SAs). In the event of a failover, it is critical that the current RTOs be maintained by the new primary device to avoid service interruption.

NOTE: Using policies, you can specify which sessions to backup and which not to backup. For traffic whose sessions you do not want backed up, apply a policy with the HA session backup option disabled. In the WebUI, clear the **HA Session Backup** checkbox. In the CLI, use the **no-session-backup** argument in the **set policy** command. By default, the backing up of sessions is enabled.

To accomplish this, RTOs are backed up by the members of an NSRP cluster.

Each member backs up the RTOs from the other, which allows RTOs to be maintained if the primary device of either VSD group in an active/active HA scheme fails.

In the current ScreenOS release, you do not have to configure one or more RTO mirror groups to synchronize RTOs among members of an NSRP cluster. Defining a security device as a member of a cluster and specifying RTO synchronization automatically enables the local device to send and receive RTOs.

By default, NSRP cluster members do not synchronize RTOs. Before enabling RTO synchronization, you must first synchronize the configurations between the cluster members. Unless the configurations on both members in the cluster are identical, RTO synchronization might fail. (For examples of the synchronization procedure, see "Adding a Device to an Active NSRP Cluster" on page 25.

To enable RTO synchronization, do either of the following:

WebUI

Network > NSRP > Synchronization: Select the **NSRP RTO Synchronization** checkbox, then click **Apply**.

CLI

```
set nsrp rto-mirror sync
save
```

NOTE: In the event of a failover, the device that mirrors the primary device is the most desirable replacement—even if another VSD group member has a higher priority. In the current ScreenOS release, this precedence is irrelevant because only two devices can be present in an NSRP cluster.

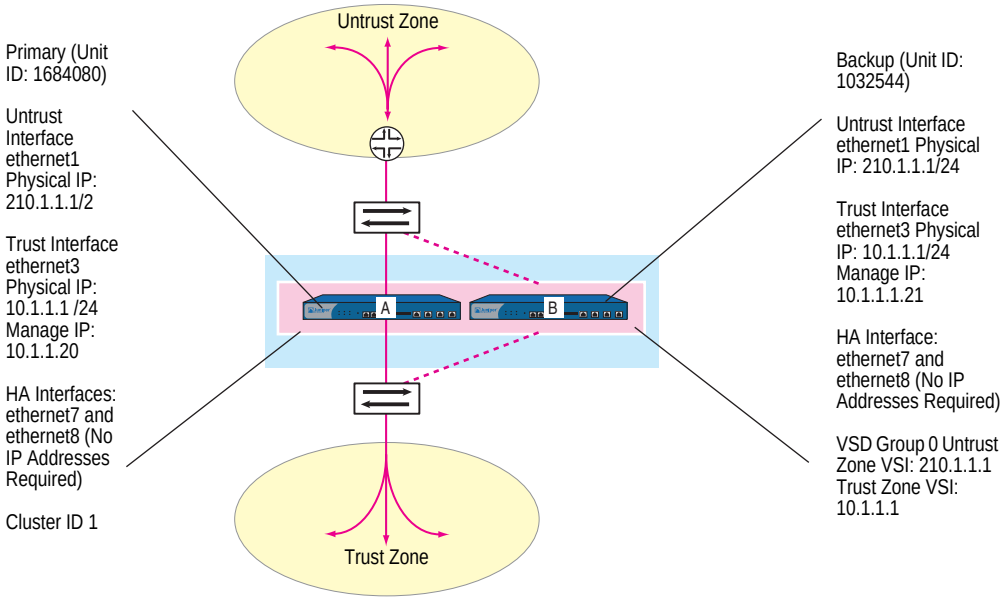
Configuring an Active/Passive NSRP Cluster

In the example shown in Figure 6, you cable ethernet7 on Device-A to ethernet7 on Device-B. You cable the ethernet8 interfaces likewise. Then you bind ethernet7 and ethernet8 to the HA zone. You set manage IP addresses for the Trust zone interfaces on both devices—10.1.1.20 for Device-A and 10.1.1.21 for Device-B. You then assign each device to NSRP cluster ID 1. When the devices become members of the NSRP cluster, the IP addresses of their physical interfaces automatically become the IP addresses of the Virtual Security Interfaces (VSIs) for VSD group ID 0. Each VSD member has a default priority of 100, the device with the higher unit ID becomes the VSD group's primary device.

NOTE: By default, ethernet8 is bound to the HA zone. Binding it to the HA zone is only necessary if you have previously bound it to a different zone. Also, on devices that do not have a dedicated HA port, you must bind the interface to the HA zone before configuring the NSRP cluster.

You configure the devices to monitor ports ethernet1 and ethernet3, so that loss of network connectivity on either of those ports triggers a device failover. You also enable the automatic synchronization of RTOs.

Figure 6: Basic Active/Passive Configuration



WebUI (Device-A)

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet7): Enter the following, then click **OK**:

   Zone Name: HA

   Network > Interfaces > Edit (for ethernet8): Enter the following, then click **OK**:

   Zone Name: HA

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 210.1.1.1/24

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.20

   Enter the following, then click **OK**:

   Interface Mode: NAT

2. **NSRP**

   Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Enter the following, then click **Apply**:

   ethernet1: (select); Weight: 255
   ethernet3: (select); Weight: 255

NOTE: The default setting for an NSRP failover threshold is 255. Therefore, if ethernet1 or ethernet3 fails with a weight of 255, its failure triggers a device failover.

Network > NSRP > Synchronization: Select **NSRP RTO Synchronization**, then click **Apply**.

NOTE: If you do not enable the automatic RTO synchronization option, you can not manually synchronize RTOs with the CLI command **exec nsrp sync rto all**. The RTO will be dropped of you do not enable synchronization.

Network > NSRP > Cluster: In the Cluster ID field enter **1**, then click **Apply**.

WebUI (Device-B)

3. **Interfaces**

   Network > Interfaces > Edit (for ethernet7): Enter the following, then click **OK**:

   Zone Name: HA

   Network > Interfaces > Edit (for ethernet8): Enter the following, then click **OK**:

   Zone Name: HA

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 210.1.1.1/24

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.21

   Enter the following, then click **OK**:

   Interface Mode: NAT

4. **NSRP**

   Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Enter the following, then click **Apply**:

   ethernet1: (select); Weight: 255
   ethernet3: (select); Weight: 255

   Network > NSRP > Synchronization: Select **NSRP RTO Synchronization**, then click **Apply**.

   Network > NSRP > Cluster: In the Cluster ID field enter **1**, then click **Apply**.

CLI (Device-A)

1. **Interfaces**

```
set interface ethernet7 zone ha
set interface ethernet8 zone ha
set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24
set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.20
set interface ethernet3 nat
```

2. **NSRP**

```
set nsrp rto-mirror sync
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set nsrp cluster id 1
save
```

NOTE: If you do not enable the automatic RTO synchronization option, you can not manually synchronize RTOs with the CLI command **exec nsrp sync rto all**.

The default weight for a monitored interface is 255 and the default NSRP failover threshold is 255. Therefore, if ethernet1 or ethernet3 fails with a weight of 255, its failure triggers a device failover. In the CLI, if you do not specify a weight for a monitored interface, the security device uses the default (255).

CLI (Device-B)

3. **Interfaces**

```
set interface ethernet7 zone ha
set interface ethernet8 zone ha
set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24
set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.21
set interface ethernet3 nat
```

4. **NSRP**

```
set nsrp rto-mirror sync
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set nsrp cluster id 1
save
```

NOTE: After performing this configuration, type the **get nsrp** command to check the default NSRP settings that the device automatically creates, which are noted on page 6.

Setting an RTO Mirror State

The procedure for two NSRP cluster members to initiate their RTO mirror relationship develops through two operational states—set and active. The devices progress through these states as follows:

1. After you add the first device to a group, its state is *set*. In the set state, the device waits for its peer to join the group. As the receiver of RTOs, it periodically transmits an r-ready message (receiver-ready), announcing its own availability. As the sender of RTOs, it waits until it gets an r-ready message from a device with the same cluster ID.

2. After you add the peer and the two devices are correctly cabled for HA (see "Cabling for a Full-Mesh Configuration" on page 32), then the following occurs:

    a. The receiver sends an r-ready message.

    b. The sender gets the r-ready message, and immediately sends a group-active message to inform its peer that its state is now *active*.

    c. The receiver then changes its state to active as well.

In addition to passing RTOs from sender to receiver, both active mirrors send RTO heartbeats at user-defined intervals to communicate their operational status. To define the interval, use the following CLI command: **set nsrp rto-mirror hb-interval** *number*.

If a device does not receive a specified number of consecutive heartbeats from its peer, it changes its state from active to set. To define the lost heartbeat threshold required to impel a state changeover, use the following CLI command: **set nsrp rto-mirror hb-threshold** *number*.

NOTE: To maintain identical RTO heartbeat settings, the **set nsrp rto-mirror hb-interval** *number* and **set nsrp rto-mirror hb-threshold** *number* are propagated.

You can use the following command to disable RTO session synchronization on the device acting as sender in an NSRP cluster: **set nsrp rto-mirror session off**. Issuing this command on a device only disables session synchronization from that device to others in the cluster. If you want to clear a session for an inactive VSI, you can use the **set nsrp rto-mirror session clear-on-inactive** command.

Virtual Security Device Groups

A Virtual Security Device (VSD) group is a pair of physical security devices that collectively make up a single VSD. One physical device acts as the primary device of the VSD group. The virtual security interface (VSI) of the VSD is bound to the physical interface of the primary device. The other physical device acts as the backup. If the primary device fails, the VSD fails over to the backup and the VSI binding is transferred to the physical interface on the backup, which is instantly promoted to primary device.

NOTE: In the current release, a VSD group can have two members. In later releases, there might be more than two members, in which case, one device acts as a primary device, another as a primary backup, and the remaining VSD group members as backups.

By grouping two security devices into two VSD groups, with each physical device being the primary device in one group and the backup in the other, both devices can actively process traffic as primary devices while backing up each other in the event of a failover.

Upon initial NSRP configuration, the VSD group member with the priority number closest to 0 becomes the primary device. (The default is 100.) If two devices have the same priority value, the device with the highest MAC address becomes primary device.

Preempt Option

You can determine whether a better priority number (closer to zero) can initiate a failover by setting the device that you want to be primary device in preempt mode. If you enable the preempt option on that device, it becomes the primary device of the VSD group if the current primary device has a lesser priority number (farther from zero). If you disable this option, a primary device with a lesser priority than a backup can keep its position (unless some other factor, such as an internal problem or faulty network connectivity, causes a failover).

Using the hold-down time to delay a failover can prevent a flurry of rapid failovers in the event of port-flickering on an adjacent switch and also ensure that surrounding network devices have sufficient time to negotiate new links before the new primary device becomes available. To enable or disable the preempt option, use the following CLI command:

```
set/unset nsrp vsd-group id number preempt
```

You can use the following CLI command to set the hold-down time—used for delaying the preempted failover—to any length from 0 to 600 seconds:

```
set nsrp vsd-group id number preempt hold-down number
```

VSD Group Member States

The members of a VSD group can be in one of six states:

- **Master**—The state of a VSD group member that processes traffic sent to the VSI. It is the primary device.
- **Primary Backup**—The state of a VSD group member that becomes the primary device if the primary device fails. The election process uses device priorities to determine which member to promote. Note that when electing a new primary device, an RTO peer has precedence over any other VSD group member, even if that member has a better priority rating.
- **Backup**—The state of a VSD group member that monitors the status of the primary backup and elects one of the backup devices to primary backup if the current one steps down.
- **Initial**—The transient state of a VSD group member while it joins a VSD group, either when the device boots up or when it is added via the **set nsrp vsd-group id** *id_num* command.

  You can specify how long a VSD group member stays in the initial state with the **set nsrp vsd-group init-hold** *number* command. The default (and minimum) setting is 5. To determine the initial state hold-down time, multiply init-hold value by the VSD heartbeat-interval (init-hold x hb-interval = initial state hold-down time). For example, if the init-hold is 5 and the hb-interval is 1000 milliseconds, then the initial state hold-down time is 5,000 milliseconds, or 5 seconds (5 x 1000 = 5000).

NOTE: If you reduce the VSD heartbeat interval, you should increase the init-hold value. For information about configuring the heartbeat interval, see "Heartbeat Messages" on page 18.

- **Ineligible**—The state that an administrator purposefully assigns to a VSD group member so that it cannot participate in the election process. To do this, use the **set nsrp vsd-group id** *id_num* **mode ineligible** command.
- **Inoperable**—The state of a VSD group member after a system check determines that the device has an internal problem (such as no processing boards) or a network connection problem (such as when an interface link fails).

NOTE: When the device returns from either the ineligible state (when you use the **exec nsrp vsd-group id** *id_num* **mode backup** command) or inoperable state (when the system or network problem has been corrected), it must first pass through the initial state.

If your platform has an HA LED, you can determine the state of a device. The meanings of the colors are as follows:

- **Dark**: The device is not enabled for NSRP.
- **Green**: The device is enabled for NSRP; it is the primary device in one or more VSD groups; and it is not in inoperable mode.
- **Yellow**: The device is enabled for NSRP; it is not the primary device in any VSD group; and it is not in inoperable mode.
- **Red**: The device is enabled for NSRP, but it is currently in inoperable mode.

Heartbeat Messages

Every VSD group member—even if it is in the initial, ineligible, or inoperable state—communicates with its group members by sending a heartbeat message every interval. These messages allow every member to know the current state of every other member. The heartbeat message includes the following information:

- Unit ID of the device
- VSD group ID
- VSD group member status (master, primary backup, or backup)
- Device priority
- RTO peer information

NOTE: If a device is in the inoperable state with all HA links down, it can neither send nor receive VSD heartbeat messages unless you have configured a secondary path for these messages.

The interval for sending VSD heartbeats is configurable (200, 600, 800, or 1000 milliseconds; 1000 ms is the default). The CLI command—which applies globally to all VSD groups—is **set nsrp vsd-group hb-interval** *number*. You can also configure the lost heartbeat threshold that is used to determine when a VSD group member is considered as missing. The CLI command, which also applies globally to all VSD groups, is **set nsrp vsd hb-threshold** *number*. The minimum value for the lost heartbeat threshold is 3.

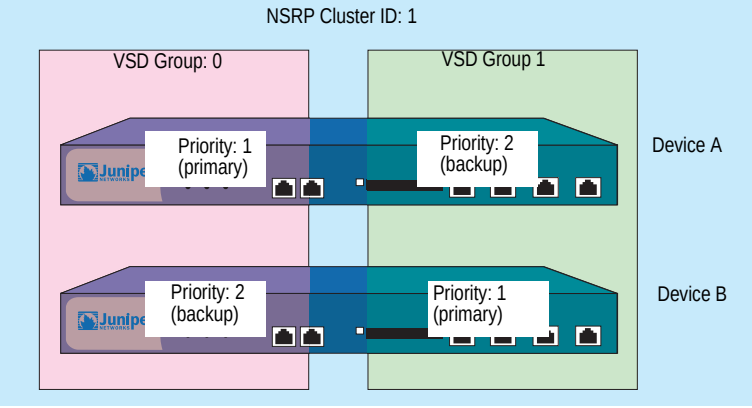
The heartbeat messages are sent over the HA1 link. For more information about the HA1 and HA2 interfaces and the kinds of messages communicated over each, see “Dual High Availability Interfaces” on page 26.

Creating Two VSD Groups

This example continues with the configuration of devices A and B, which are already members of the same NSRP cluster and VSD group 0.

In the example shown in Figure 7, you create a second VSD group—group 1. You assign device A priority 1 in group 0 and the default priority (100) in group 1. You assign device B priority 1 in group 1 and the default priority (100) in group 0. In both VSD groups, you enable the preempt option on the primary device and set the preempt hold-down time to 10 seconds. If both devices are active, device A is always the primary device of group 1, and B is always the primary device of group 2.

Figure 7: VSD Groups



WebUI

1. **Device A**

   Network > NSRP > VSD Group > Edit (for VSD group 0): Enter the following, then click **OK**:

   Priority: 1
   Enable Preempt: (select)
   Preempt Hold-Down Time (sec): 10

   Network > NSRP > VSD Group > New: In the Group ID field, type **1**, then click **OK**.

2. **Device B**

   Network > NSRP > VSD Group > Edit (for VSD group 1): Enter the following, then click **OK**:

   Priority: 1
   Enable Preempt: (select)
   Preempt Hold-Down Time (sec): 10

CLI

3. **Device A**

```
set nsrp vsd-group id 0 priority 1
set nsrp vsd-group id 0 preempt hold-down 10
set nsrp vsd-group id 0 preempt
set nsrp vsd-group id 1
save
```

4. **Device B**

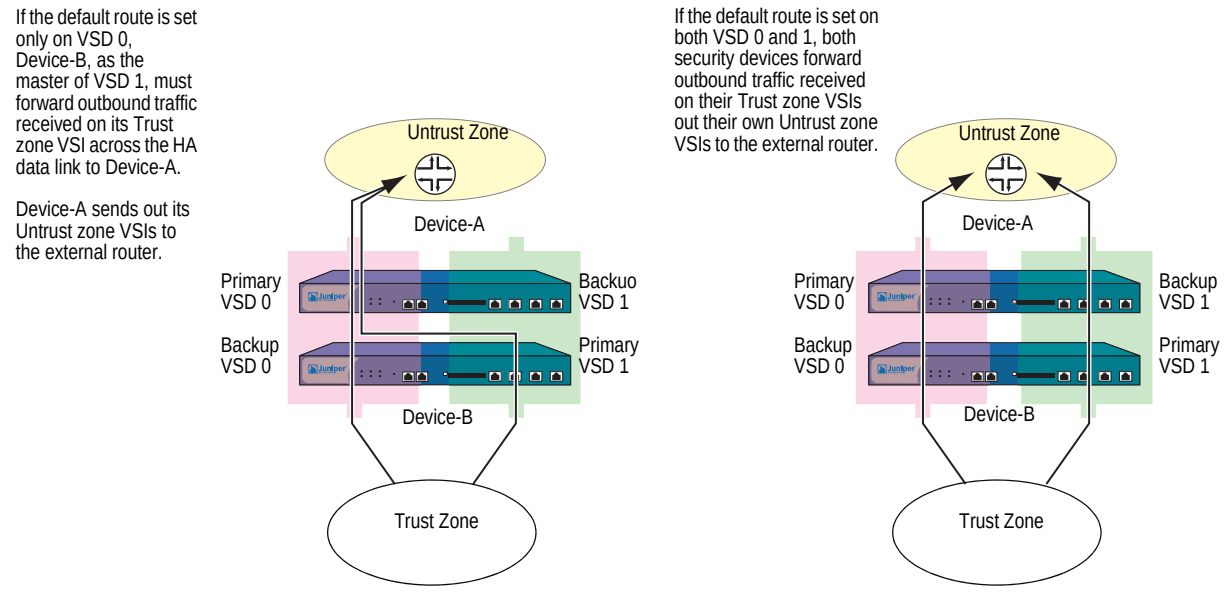
```
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
save
```

Virtual Security Interfaces and Static Routes

After you create a VSD group, you must bind Virtual Security Interfaces (VSIs) to the VSD. When you put a security device in an NSRP cluster, all the security zone interfaces become VSIs of VSD group 0. You must manually assign VSIs to VSDs with other IDs for each security zone configured on the security device.

By default, the security device adds an entry to its routing table for the immediate subnet of a VSI. For static routes to addresses beyond the immediate subnet, you must manually make route table entries for each VSI through which you want the security device to forward traffic to those addresses. For example, if you have two VSDs and you want to configure a default route to a router in the Untrust zone, you must make a routing table entry for the Untrust zone VSI of both VSDs. If you set the default route on only one VSD (for example, VSD 0), the security device acting as the primary device of the other VSD (for example, VSD 1) must pass all outbound traffic sent to it across the HA data link to the device acting as the primary device of VSD 0. See Figure 8.

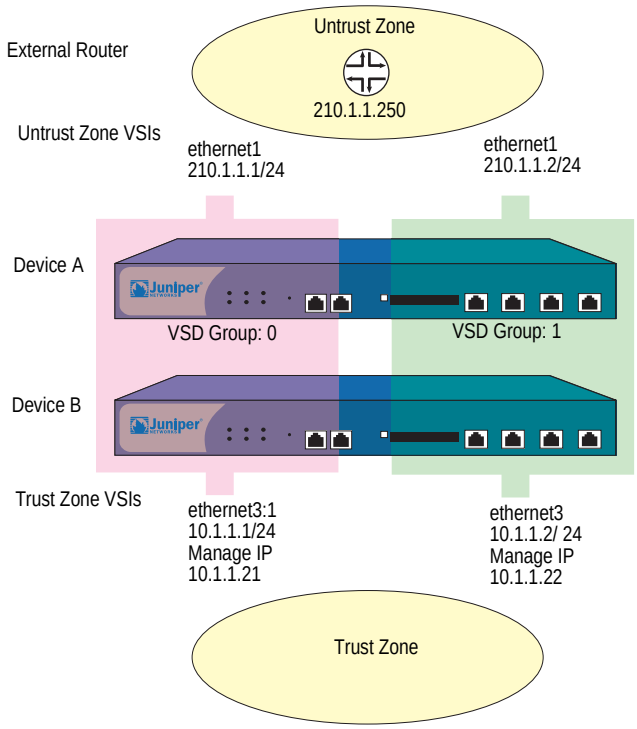
Figure 8: Forwarding Traffic Through VSIs Using Static Routes



In the example shown in Figure 9, builds on the previous example, “Creating Two VSD Groups” on page 19, and assumes that you have already done the following on devices A and B:

- Put both devices in NSRP cluster 1
- Created VSD group 1 (the security device created VSD group 0 automatically when you put the device in NSRP cluster 1)

Figure 9: Trust and Untrust Zone VSIs



You bind ethernet1 to the Untrust zone and assign it IP address 210.1.1.1/24. You bind ethernet3 to the Trust zone, put it in NAT mode, and assign it IP address 10.1.1.1/24. You define 10.1.1.21 as the manage IP on ethernet3 for device A, and 10.1.1.22 as the manage IP on ethernet3 for device B. Then you create the following VSIs for VSD group 1:

- Untrust zone VSI ethernet1:1 (210.1.1.2/24)
- Trust zone VSI ethernet3:1 (10.1.1.2/24)

The security device creates VSIs for VSD group 0 automatically, using the IP addresses already assigned to the local interfaces at the time you put the device in an NSRP cluster. In this example, the VSD group 0 Untrust zone VSI is ethernet1 with IP address 210.1.1.1/24. The VSD group 0 Trust zone VSI is ethernet3 with IP address 10.1.1.1/24.

NOTE: The VSD group ID “0” does not appear in the names of VSIs in VSD 0. Instead of *ethernet1:0,* the VSI is identified simply as *ethernet1*.

Finally, you set two default routes to the external router in the Untrust zone at 210.1.1.250—one route for the Untrust zone VSI on VSD 0 and another for the Untrust zone VSI on VSD 1. All security zones are in the trust-vr routing domain.

WebUI (Device A)

1. **Interfaces (VSIs for VSD Group 0)**
   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
   Manage IP: 10.1.1.21
   Enter the following, then click **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 210.1.1.1/24

WebUI (Device B)

2. **Manage IP Address**
   Network > Interfaces > Edit (for ethernet3): Enter **10.1.1.22** in the Manage IP field, then click **Apply**.

3. **VSIs for VSD Group 1**
   Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

   Interface Name: VSI Base: ethernet1
   VSD Group: 1
   IP Address / Netmask: 210.1.1.2/24

   Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

   Interface Name: VSI Base: ethernet3
   VSD Group: 1
   IP Address / Netmask: 10.1.1.2/24

4. **Routes**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address: 0.0.0.0
   Netmask: 0.0.0.0
   Gateway: (select)
   Interface: ethernet1:1
   Gateway IP Address: 210.1.1.250

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address: 0.0.0.0
   Netmask: 0.0.0.0
   Gateway: (select)

Interface: ethernet1:2
Gateway IP Address: 210.1.1.250

CLI (Device A)

1. **Interfaces**
   set interface ethernet3 zone trust
   set interface ethernet3 ip 10.1.1.1/24
   set interface ethernet3 manage-ip 10.1.1.21
   set interface ethernet3 nat
   set interface ethernet1 zone untrust
   set interface ethernet1 ip 210.1.1.1/24

CLI (Device B)

2. **Manage IP Address**
   set interface ethernet3 manage-ip 10.1.1.22
3. **Virtual Security Interfaces**
   set interface ethernet1:1 ip 210.1.1.2/24
   set interface ethernet3:1 ip 10.1.1.1.2/24
4. **Routes**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet1 gateway 210.1.1.250
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet1:1 gateway 210.1.1.250
   save

Synchronization

When you add a new device to an active NSRP cluster, you must synchronize the configuration and files (such as PKI public/private key files) from the primary device of the VSD group or groups to the new device. After the configurations and files are synchronized, you must then synchronize the run-time objects (RTOs). You must also synchronize configurations, files, and RTOs after a member of a cluster becomes unsynchronized for any reason.

Synchronizing Configurations

If you make any configuration changes on one device while another in the cluster reboots (or if all HA links fail), it is possible that the configuration settings can become unsynchronized. To discover if the configuration of one device is out of sync with that of another, use the **exec nsrp sync global-config check-sum** command. The output states whether the configurations of the two devices are in or out of sync and provides the checksums of the local and remote devices.

If the configurations are out of sync, use the following command to resynchronize them: **exec nsrp sync global-config save** (and then reboot the device).

NOTE: Configurations on active devices in a cluster rarely become unsynchronized because NetScreen Reliable Transport Protocol (NRTP) is a low-overhead, TCP-like protocol.

Synchronizing Files

If you need to synchronize a specific file, enter the following command on the device to which you are synchronizing the file: **exec nsrp sync file name** *name_str* **from peer**. If you need to synchronize all files, enter **exec nsrp sync file from peer**.

You can synchronize PKI objects, such as local and CA certificates, key pairs, and CRLs, with the **exec nsrp sync global-config save** command and then reboot the device.

Synchronizing Run-Time Objects

If you have enabled RTO mirror synchronization on a device in a cluster (see "Run-Time Objects" on page 10), when the device reboots, the RTOs automatically resynchronize. However, if you disable RTO mirror synchronization—perhaps to perform some debugging or maintenance on the device—when you again enable RTO synchronization, you must manually resync all the RTOs. To do that, you can use the **exec nsrp sync rto all** command. To resync only selected RTOs such as ARP, DNS, sessions, or VPNs—you can use the following CLI command: **exec nsrp sync rto { arp | auth-table | dhcp | dns | l2tp | phase1-sa | pki | rm | session | vpn }**.

To enable RTO synchronization to begin automatically when a member in an NSRP cluster detects another member in the cluster, use the **set nsrp rto-mirror sync** command.

When you need to synchronize RTOs manually, use the **exec nsrp sync rto { all | arp | auth-table | dhcp | dns | l2tp | phase1-sa | pki | rm | session | vpn }** command.

Resynchronizing RTOs Manually

In this example, devices A and B are in NSRP cluster 1 and VSD groups 1 and 2. Device A is the primary device of VSD group 1 and the backup in VSD group 2. Device B is the primary device of VSD group 2 and the backup in VSD group 1.

You want to do some troubleshooting on device B, and you do not want to disconnect it from the network. You force device B to become the backup in VSD group 2, and then you disable RTO synchronization. Device A becomes the primary device of both VSD groups. After you finish troubleshooting device B, you again enable RTO mirror synchronization and then manually resync the RTOs from device A to device B. Finally, you reassign device B as the primary device of VSD group 2.

WebUI

NOTE: The manual synchronization of RTOs is only available through the CLI.

CLI

Device B

```
exec nsrp vsd-group id 2 mode backup
unset nsrp rto-mirror sync
```

Device B is no longer processing traffic nor synchronizing RTOs with device A. At this point, you can troubleshoot device B without affecting the traffic-processing performance of device A.

```
set nsrp rto-mirror sync
exec nsrp sync rto all from peer
exec nsrp vsd-group id 2 mode master
```

Adding a Device to an Active NSRP Cluster

In this example, you add device A, which had previously been functioning as a single security appliance, to VSD groups 0 and 1 in NSRP cluster with cluster ID 1 and name "cluster1." You must unset the previous configurations on device A, reboot it, and then synchronize the configuration, files, and RTOs from the primary device of both VSD groups. You then assign device A as the primary device of VSD group 0.

WebUI

NOTE: The cold start synchronization feature is only available through the CLI.

CLI

Device A

```
unset all
```

NOTE: If you do not first use the **unset all** command, the **exec nsrp sync global-config** command appends new configuration settings to existing settings. (Note: The security device generates an error message for each duplicate setting that is synchronized.)

The following prompt appears: "Erase all system config, are you sure y / [n]?"

Press the **Y** key.

The system configuration is returned to the factory default settings.

```
reset
```

The following prompt appears: "Configuration modified, save? [y] / n"

Press the **N** key.

The following prompt appears: “System reset, are you sure? y / [n] n”

Press the **Y** key.

The system reboots.

```
set nsrp cluster id 1
set nsrp cluster name cluster1
exec nsrp sync file
exec nsrp sync global-config
set nsrp rto-mirror sync
exec nsrp vsd-group id 0 mode master
save all
```

NOTE: Using the **save all** command saves the configurations in all virtual systems as well as at the root level. Using the **save** command saves the configuration at the root level only.

Synchronizing System Clocks

NSRP contains a mechanism for synchronizing the system clocks of NSRP cluster members. When you set the system clock manually, the NSRP time synchronization mechanism keeps the members’ clocks properly synchronized. However, when you use the Network Time Protocol (NTP) to set the system clocks on all the cluster members, and then use NSRP to synchronize the time among them, the time can become unsynchronized. Although the resolution for NSRP synchronization is in seconds, NTP has sub-second resolution. Because the time on each cluster member might differ by a few seconds due to processing delays, Juniper Networks recommends that you disable NSRP time synchronization when NTP is enabled on all cluster members and each member can update its system clock from an NTP server. To disable the NSRP time synchronization function, enter the following command:

```
set ntp no-ha-sync
```

Dual High Availability Interfaces

The basic principle of NSRP is that there be no single point of failure. In addition to redundant devices, security devices either have dedicated physical, redundant, high availability (HA) interfaces (HA1 and HA2), or you can bind two generic interfaces to the HA zone to provide HA interface redundancy.

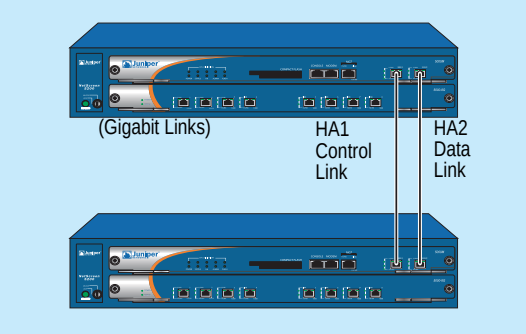
NOTE: NetScreen-1000: In addition to using the dual gigabit HA ports on the switch board, you can also use the10/100 HA port on the auxiliary board.

In addition, you can create redundant security zone interfaces.

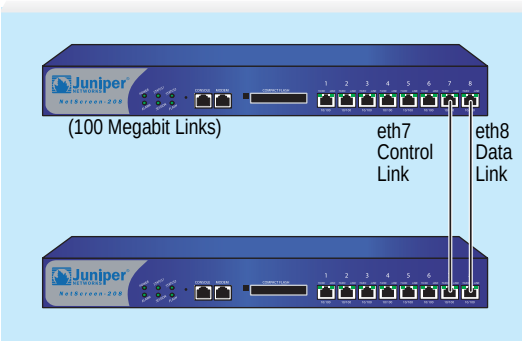
All NSRP information passes between cluster members via the two HA interfaces. To better distribute the out-of-band bandwidth, HA1 handles the NSRP control messages while HA2 handles the network data messages. If either port fails on a security device with gigabit HA1 and HA2 interfaces, the remaining active port

assumes both kinds of traffic. For security devices that must use a 100-megabit interface for the data link, a failure of the data link results in one active HA link for control messages only. If the control link fails on such devices, then the data link becomes the control link and sends and receives control messages only. See Figure 10.

Figure 10: Dedicated High Availability Links and User-Assigned High Availability Links



If either HA1 or HA2 fails, then the control and data messages are both sent over the remaining HA link.



If either ethernet7 or ethernet8 fails, then only control messages are sent over the remaining HA link.

NOTE: If you use a switch between HA ports, use port-based VLANs, which do not conflict with the VLAN tags on the forwarded packets.

On security devices that do not have dedicated HA interfaces, you must bind one or two physical ethernet interfaces to the HA zone. If you bind a single gigabit interface to the HA zone, the HA link supports both control and data messages. If you bind one 100-megabit interface to the HA zone, the HA link supports control messages only.

If you bind two interfaces (gigabit or 100-megabit) to the HA zone, the interface with the lower number becomes the control link, and the interface with the higher number becomes the data link. For example, if you bind only ethernet 8 to the HA zone, it becomes the control link. If you then bind ethernet7 to the HA zone, it becomes the control link (because it has a lower number than ethernet8), and ethernet8 changes to the data link. (For information about binding an interface to a zone, see “Binding an Interface to a Security Zone” on page **2**-53.)

The order in which you cable the HA interfaces together also affects which becomes the control and data links. If ethernet7 and ethernet8 are both bound to the HA zone, but you only cable the ethernet8 interfaces together, then ethernet8 becomes the control link. If you then cable the ethernet7 interfaces together, ethernet7 becomes the control link (because it is active and has a lower number than ethernet8) and ethernet8 becomes the data link. The same principle also applies to the HA1 and HA2 interfaces.

On security devices that do not have dedicated HA interfaces, you can also designate an interface bound to a security zone to handle HA control messages. Use the CLI command **set nsrp interface** *interface*.

NOTE: More than three interfaces can be bound to the HA zone; however, only the first three entries can be configured as an HA link.

Control Messages

There are two kinds of control messages: heartbeats and HA messages.

Heartbeats: Heartbeats are sent periodically to establish and sustain communications among the NSRP cluster members, VSD group members, and RTO mirrors. The heartbeats continually advertise the sender's member status, and the health of its system and network connectivity. The three kinds of heartbeat messages are as follows:

- HA physical link heartbeats
- VSD heartbeats
- RTO heartbeats

HA physical link heartbeats are broadcast messages from the HA1 and HA2 interfaces of each member of an NSRP cluster to the other member. The purpose of these messages is to monitor the health of the HA interfaces. If, for example, one member does not receive three consecutive heartbeats from HA1, both devices transfer transmission of the control messages to HA2.

VSD heartbeats are broadcast from the HA1 interface of each member of a VSD group. The VSD group uses these messages to monitor the membership status of all its members. If, for example, the primary device advertises that it has become inoperable, the primary backup immediately becomes the VSD group primary device.

Each member of a mirror group broadcasts RTO heartbeats from the HA1 interface. The purpose of these messages is to locate an active peer and then maintain the mirror relationship by sending group active messages. If, for example, a device does not receive 16 consecutive RTO heartbeats from its peer, it changes its state from active to set.

NOTE: If you remove a device from a mirror group, it enters the undefined state and transmits a "group detach" message to its peer. The peer immediately changes its state from active to set without waiting for the missing heartbeats to exceed the threshold.

HA Messages: The two kinds of HA messages are as follows:

- Configuration messages—The network and configuration settings that the primary device sends to the other VSD group member
- RTO messages—The RTOs that the primary device sends to the other RTO mirror

The HA messages contain the information that enables the backup to become the primary device without causing a service interruption.

Data Messages (Packet Forwarding)

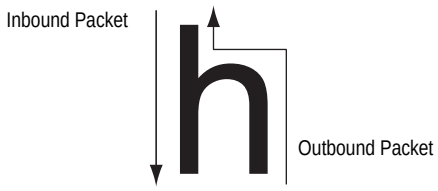
Data messages are IP packets traversing the firewall that the backup in a VSD group must forward to the device acting as primary device. When a packet arrives at the interface of a security device in an active/active configuration, the device first identifies which VSD group must process the packet. If the device that receives the packet is the primary device of the identified VSD group, it processes the packet itself. If the device is not the primary device, it forwards the packet over the HA data link to the primary device.

For example, a load-balancing router might send the first packet in a session to device A (primary device of VSD group 1), which creates an entry in its session table. If the router performs load balancing by sending packets round-robin (that is, the router sends each packet to a security device in turn), the router might send the next packet to device B (backup of VSD group 1). Because a session entry exists in device A, device B forwards the packet across the data link to device A, which processes it.

NOTE: If there is no data link, the security device that receives the packet drops it immediately.

Inbound packet forwarding across the data link occurs only when the security devices are in an active/active configuration in Route mode. When in NAT mode, the router always sends the incoming packets to the MIP, VIP, or VPN tunnel gateway, although the security device that receives the returning outbound packet might forward it across the data link to the device that has the session entry to which the packet belongs. This kind of packet forwarding produces an h-shaped path. Like the down stroke in the letter *h*, the inbound packet goes straight through one device, but the outbound packet might be sent halfway through the other device and then forwarded across the data link to the first device. See Figure 11.

Figure 11: Packet Forwarding Across the Data Link



Dynamic Routing Advisory

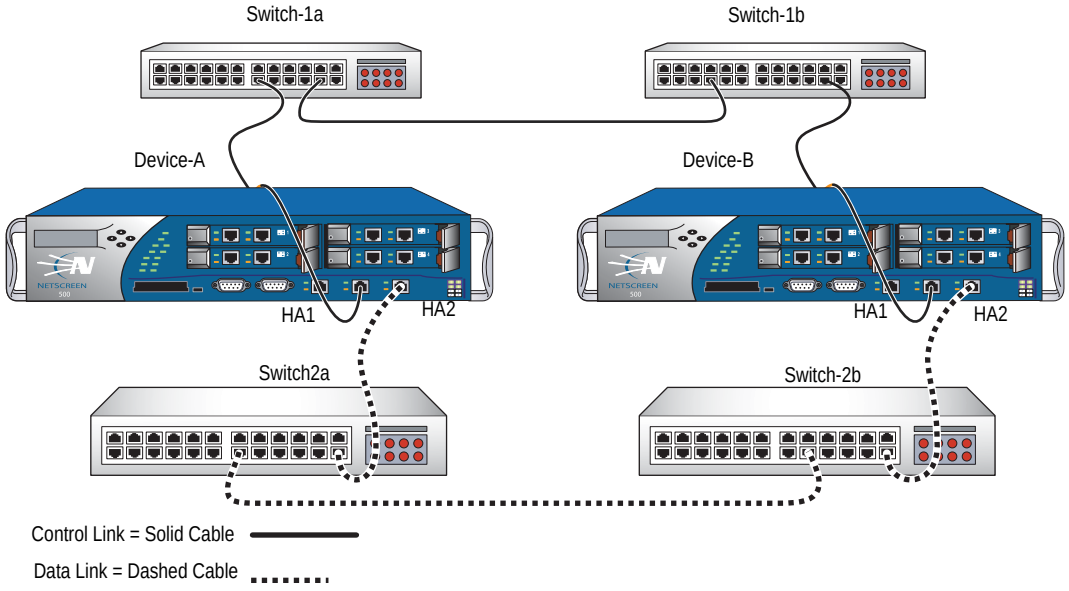
If an NSRP cluster is in a dynamic routing environment and you disable packet forwarding (**unset nsrp data-forwarding**), traffic arriving at an inactive interface can be lost. Because the security device cannot forward traffic across the data link to the security device on which the interface is active, it drops it. To avoid this when you disable packet forwarding, the security device indicates the status of interfaces belonging to a non-primary VSD on a device as “down” instead of just “inactive”. This status signals routers not to send traffic to these interfaces.

NOTE: An inactive interface is an interface belonging to a VSD that is not the primary device on that device.

Dual HA Link Probes

You can connect the redundant HA interfaces by directly cabling HA ports on one device to the HA ports on another device. Or, you can connect the HA ports on two devices through one or more switched networks. In the configuration shown in Figure 12, the HA1 port on the device Device-A is connected to the HA1 port on Device-B via two switches, Switch-1a and Switch-1b. To provide a redundant HA interface, the HA2 port on Device-A is connected to the HA2 port on Device-B via Switch-2a and Switch-2b. In this configuration, the link between the HA1 ports on Device-A and Device-B handles NSRP control messages, while the HA2 link handles network data messages. If the link between the HA1 port on Device-A and Switch-1a goes down, Device-A transfers transmission of the control messages to its HA2 port. However, Device-B does not recognize the failure of the HA1 link as its HA1 port is still active and rejects the NSRP control messages sent by Device-A on the HA2 link.

Figure 12: HA Links Connecting Through Switches



To prevent this situation, you can configure a security device to monitor the status of a HA link by sending NSRP probe requests on the HA link to its peer. If a reply is received from the peer on the HA link, the request is considered successful and the HA link is assumed to be up. If no reply is received from the peer within the constraints specified, the HA link is considered to be down. This enables security devices to switch transmission of control messages to an available HA link when necessary, even if there is no physical failure on the HA ports on either device.

There are two ways that probe requests can be sent on an HA link:

- **Manually by the administrator**—Probes are sent on a specific HA links once every second for a specified number of times. If no reply is received from the peer after the specified number of probes are sent, the HA link is considered to be down. Probes are sent out immediately after you execute the command.

- **Automatically by ScreenOS**—Probes are sent by on all HA links once every second. (You can optionally specify the HA zone interface and the interval at which probes are sent.) By default, if five consecutive probes are sent without receiving a reply from the peer, the link is considered to be down; you can specify a different threshold value for determining when the link is down. Note that even when a primary HA link is down, the security device continues to send probes on that link. If the primary HA link connection is restored and peer responses are once again received on the link, the security devices can switch transmission of control messages back to the primary HA link.

Sending Link Probes Manually

In this example, the ethernet7 and ethernet8 interfaces on the security device are bound to the HA zone. You configure 5 link probes to be sent on the ethernet8 interface to the peer's MAC address 00e02000080. (Note that if you do not specify a MAC address, the default NSRP MAC address is used.)

WebUI

NOTE: You must use the CLI to send probes manually on an HA link.

CLI

```
exec nsrp probe ethernet8 00e02000080 count 5
```

Sending Link Probes Automatically

In this example, the ethernet7 and ethernet8 interfaces on the security device are bound to the HA zone. You configure link probes to be automatically sent to both interfaces at three-second intervals. You also set the threshold value so that if there is no reply from the peer after sending four consecutive requests, the HA link is considered to be down.

WebUI

Network > NSRP > Link: Enter the following, then click **Apply**:

```
Enable HA Link Probe: (select)
Interval: 3
Threshold: 5
```

CLI

```
set nsrp ha-link probe interval 3 threshold 4
```

Setup Procedure

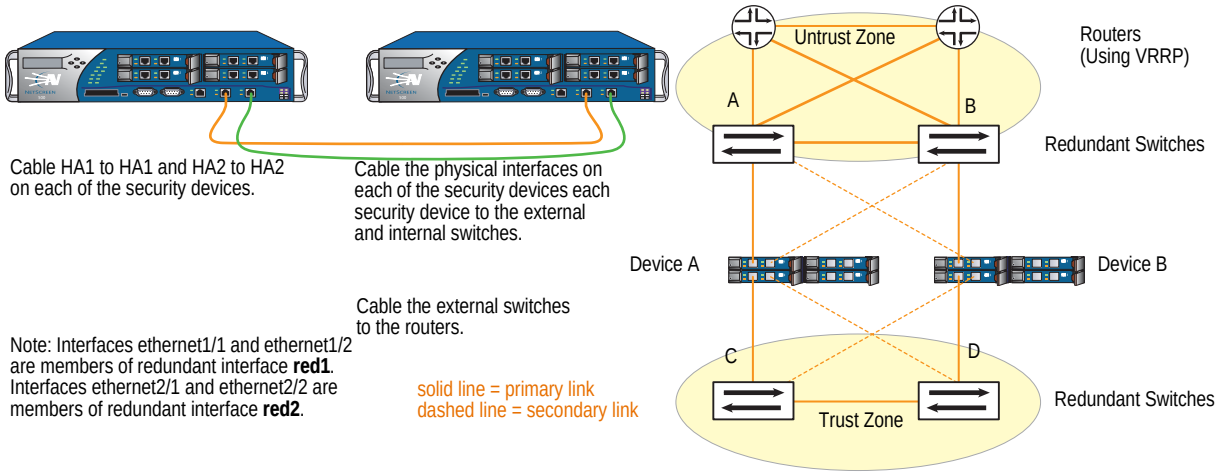
To configure two security devices for high availability, you must cable them to the network and to each other and then configure them for HA using NSRP.

Cabling for a Full-Mesh Configuration

Figure 13 and Figure 14 illustrate the cabling of two security devices to each other and to redundant pairs of internal switches and external switches. The external switches are then cabled to a pair of redundant routers running VRRP, completing the full-mesh configuration. Figure 13 shows two security devices with dedicated HA interfaces. Figure 14 shows two security devices using network interfaces for HA traffic.

NOTE: Depending on the topology in which you are deploying the security devices and the kinds of switches and routers you use, the cabling presented in Figure 13 might differ from what your network requires.

Figure 13: Cabling Security Devices with Dedicated HA Interfaces



Cable two security devices (device A and device B) for NSRP in a full-mesh configuration as follows:

Device A and Device B: HA Links

1. Cable together the HA1 interfaces on each security device.
2. Cable together the HA2 interfaces on each security device.

Device A: Redundant1 (eth1/1 and eth1/2), Untrust Zone

3. Cable ethernet1/1 to external switch A. (ethernet1/1 is one of the two physical interfaces bound to the redundant interface red1 in the Untrust zone.)
4. Cable ethernet1/2 to external switch B. (ethernet1/2 is the other physical interface bound to red1 in the Untrust zone.)

Device A: Redundant2 (eth2/1 and eth2/2), Trust Zone

5. Cable ethernet2/1 to internal switch C. (ethernet2/1 is one of the two physical interfaces bound to the redundant interface red2 in the Trust zone.)

6. Cable ethernet2/2 to internal switch D. (ethernet2/2 is the other physical interface bound to red2 in the Trust zone.)

Device B: Redundant1 (eth1/1 and eth1/2), Untrust Zone

7. Cable ethernet1/1 to external switch B. (ethernet1/1 is one of the two physical interfaces bound to the redundant interface red1 in the Untrust zone.)

8. Cable ethernet1/2 to external switch A. (ethernet1/2 is the other physical interface bound to red1 in the Untrust zone.)

Device B: Redundant2 (eth2/1 and eth2/2), Trust Zone

9. Cable ethernet2/1 to internal switch D. (ethernet2/1 is one of the two physical interfaces bound to the redundant interface red2 in the Trust zone.)

10. Cable ethernet2/2 to internal switch C. (ethernet2/2 is the other physical interface bound to red2 in the Trust zone.)

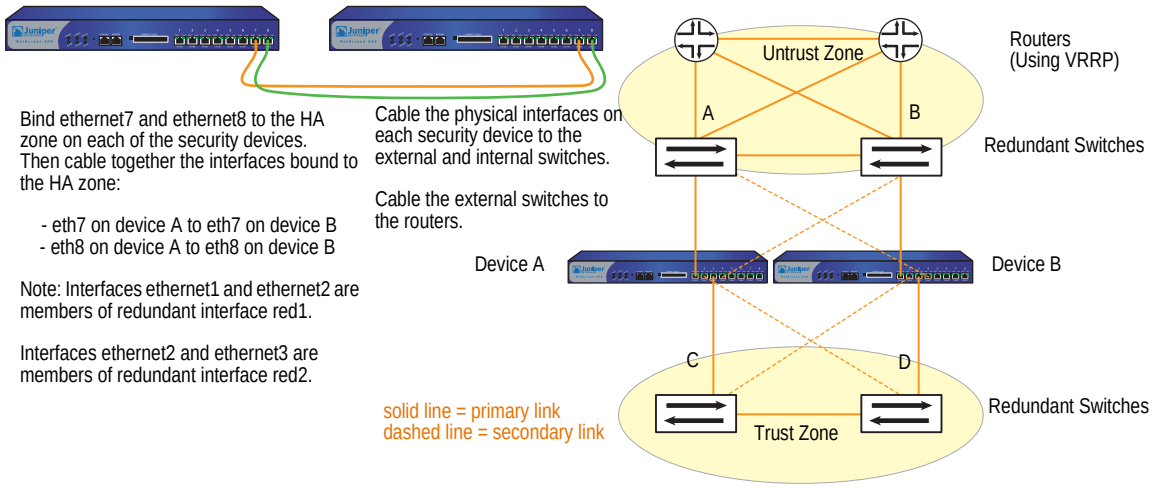
Switches and Routers

11. Cable the external redundant switches together.

12. Cable the external switches to the redundant routers in the same configuration that you used to cable the security devices to the switches.

13. Cable the internal redundant switches together.

Figure 14: Security Devices Using Network Interfaces for HA Links



After binding ethernet7 and ethernet8 to the HA zone on both security devices (device A and device B), cable the devices for NSRP in a full-mesh configuration as follows:

Device A and Device B: HA Links

1. Cable together the ethernet7 interfaces on each security device.

2. Cable together the ethernet8 interfaces on each security device.

Device A: Redundant1 (ethernet1 and ethernet2), Untrust Zone

3. Cable ethernet1 to external switch A. (ethernet1 is one of the two physical interfaces bound to the redundant interface red1 in the Untrust zone.)

4. Cable ethernet2 to external switch B. (ethernet2 is the other physical interface bound to red1 in the Untrust zone.)

Device A: Redundant2 (ethernet3 and ethernet4), Trust Zone

5. Cable ethernet3 to internal switch C. (ethernet3 is one of the two physical interfaces bound to the redundant interface red2 in the Trust zone.)

6. Cable ethernet4 to internal switch D. (ethernet4 is the other physical interface bound to red2 in the Trust zone.)

Device B: Redundant1 (ethernet1 and ethernet2), Untrust Zone

7. Cable ethernet1 to external switch B. (ethernet1 is one of the two physical interfaces bound to the redundant interface red1 in the Untrust zone.)

8. Cable ethernet2 to external switch A. (ethernet2 is the other physical interface bound to red1 in the Untrust zone.)

Device B: Redundant2 (ethernet3 and ethernet4), Trust Zone

9. Cable ethernet3 to internal switch D. (ethernet3 is one of the two physical interfaces bound to the redundant interface red2 in the Trust zone.)

10. Cable ethernet4 to internal switch C. (ethernet4 is the other physical interface bound to red2 in the Trust zone.)

Switches and Routers

11. Cable the external redundant switches together.

12. Cable the external switches to the redundant routers in the same configuration that you used to cable the security devices to the switches.

13. Cable the internal redundant switches together.

Configuring an Active/Active NSRP Cluster

After cabling the security devices together and to the surrounding network devices, you can then configure them for HA. A complete active/active configuration involves the following steps:

1. Creating an NSRP cluster, which automatically includes the creation of VSD group 0
2. Creating a second VSD group within the cluster
3. Enabling device failure tracking methods—such as interface monitoring and path monitoring

In the example shown in Figure 15, builds upon the interfaces configured in "Creating Redundant Interfaces for VSIs" on page 43, you create an NSRP cluster with ID 1 and name "cluster1" for two security devices—device A and device B—which do not have any other user-defined settings configured.

NOTE: To enable command propagation, you must first define the cluster ID number on each device. The following settings are not propagated and must be configured on each device in the cluster: VSD group, VSD priority, authentication and encryption passwords, manage IP addresses, and IP tracking settings. All other commands are propagated among devices within the cluster.

When you create the NSRP cluster, the security device automatically creates VSD group 0. You define VSD group 1. You assign device A priority 1 in VSD group 0 and priority 100 (the default) in VSD group 1. You assign device B priority 1 in VSD group 1 and leave its priority at the default (100) in VSD group 0.

NOTE: The VSD group ID "0" does not appear in the names of VSIs in VSD 0. Instead of *redundant1:0,* the VSI is identified simply as *redundant1*.

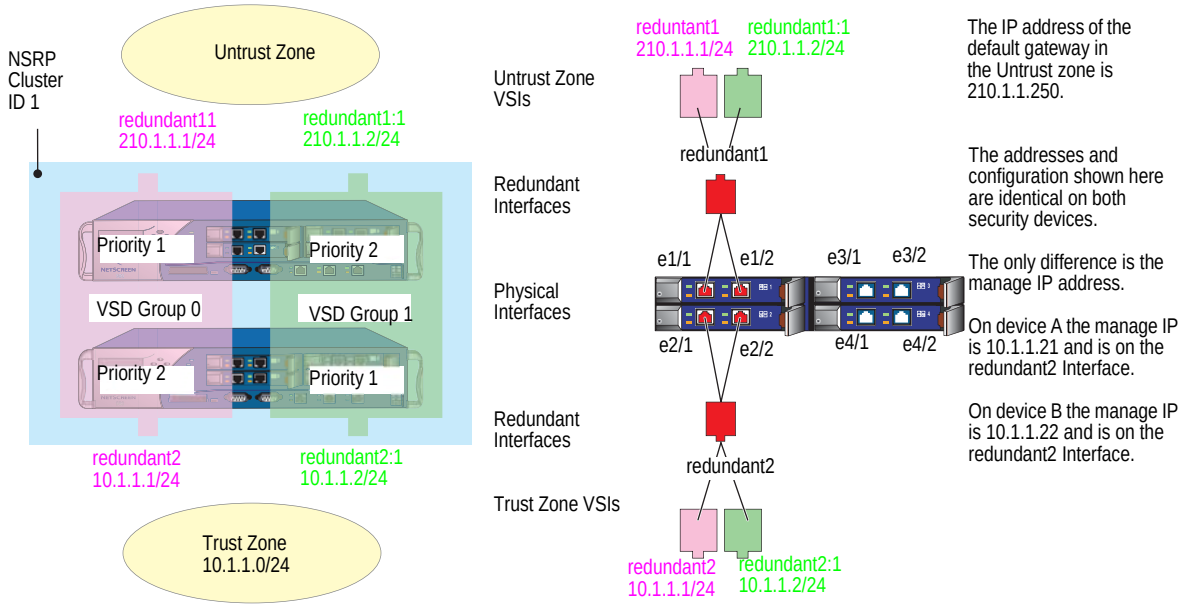
You set the interface monitoring option to monitor the two redundant interfaces—redundant1 and redundant2—for Layer 2 network connectivity. If the primary physical interface for either of the monitored interfaces fails, the device immediately fails over to the secondary interface. If both physical interfaces comprising the members of a monitored redundant interface fail, the device fails over to the other device.

You define the ethernet2/1 interface as a secondary link for VSD heartbeat messages and the number of gratuitous ARPs after a device failover has occurred to 5. Because HA cables run directly between the two security devices, communication between members of the NSRP cluster is neither authenticated nor encrypted.

You also set a route to the default gateway (210.1.1.250) for each Untrust zone VSI, and a route to the internal network for each Trust zone VSI. All security zones are in the trust-vr routing domain.

Finally, after the configurations for both devices are synchronized, you enable RTO synchronization.

Figure 15: Active/Passive NSRP Configuration



WebUI (Device A)

1. **Cluster and VSD Groups**
   Network > NSRP > Cluster: Type **1** in the Cluster ID field, then click **Apply**.

   Network > NSRP > VSD Group > Edit (for Group ID 0): Enter the following, then click **OK**:

   Priority: 1
   Enable Preempt: (select)
   Preempt Hold-Down Time (sec): 10

NOTE: The hold-down time can be any length from 0 to 255 seconds, effectively delaying the failover to prevent a flurry of rapid failovers.

Network > NSRP > VSD Group > New: Enter the following, then click **OK**:

Group ID: 1
Priority: 100
Enable Preempt: (clear)
Preempt Hold-Down Time (s): 0

WebUI (Device B)

2. **Cluster and VSD Groups**
   Network > NSRP > Cluster: Enter the following, then click **Apply**:

   Cluster ID: 1
   Number of Gratuitous ARPs to Resend: 5

NOTE: You can only set the cluster name through the CLI.

This setting specifies that after a device failover, the new VSD group primary device sends five gratuitous ARP packets announcing the association of the VSI and virtual MAC address to the new primary device.

Network > NSRP > Link: Select **ethernet2/1** from the Secondary Link drop-down list, then click **Apply**.

NOTE: If both HA1 and HA2 links are lost, the VSD heartbeat messages pass via the ethernet2/1 in the Trust zone.

Network > NSRP > Synchronization: Select **NSRP RTO Synchronization**, then click **Apply**.

Network > NSRP > VSD Group > New: Enter the following, then click **OK**:

Group ID: 1
Priority: 1
Enable Preempt: (select)
Preempt Hold-Down Time (sec): 10

3. Redundant Interfaces and Manage IP

Network > Interfaces > New Redundant IF: Enter the following, then click **OK**:

Interface Name: redundant1
Zone Name: Untrust
IP Address / Netmask: 210.1.1.1/24

Network > Interfaces > Edit (for ethernet1/1): Select **redundant1** in the "As member of" drop-down list, then click **OK**.

Network > Interfaces > Edit (for ethernet1/2): Select **redundant1** in the "As member of" drop-down list, then click **OK**.

Network > Interfaces > New Redundant IF: Enter the following, then click **Apply**:

Interface Name: redundant2
Zone Name: Trust
IP Address / Netmask: 10.1.1.1/24
> Enter **10.1.1.22** in the Manage IP field, then click **OK**.

Network > Interfaces > Edit (for ethernet2/1): Select **redundant2** in the "As member of" drop-down list, then click **OK**.

Network > Interfaces > Edit (for ethernet2/2): Select **redundant2** in the "As member of" drop-down list, then click **OK**.

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Select **redundant1** and **redundant2**, then click **Apply**.

4. **Virtual Security Interfaces**
   Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

   Interface Name: VSI Base: redundant1
   VSD Group: 1
   IP Address / Netmask: 210.1.1.2/24

   Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

   Interface Name: VSI Base: redundant2
   VSD Group: 1
   IP Address / Netmask: 10.1.1.2/24

5. **Routes**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (select)
   Interface: redundant1
   Gateway IP Address: 210.1.1.250

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address: 0.0.0.0/0
   Gateway: (select)
   Interface: redundant1:1
   Gateway IP Address: 210.1.1.250

WebUI (Device A)

6. **Manage IP Address**
   Network > Interfaces > Edit (for redundant2): Enter **10.1.1.21** in the Manage IP field, then click **OK**.

7. **RTO Synchronization**
   Network > NSRP > Synchronization: Select **NSRP RTO Mirror Synchronization**, then click **Apply**.

CLI (Device A)

1. **Cluster and VSD Groups**

```
set nsrp cluster id 1
set nsrp vsd-group id 0 preempt hold-down 10
set nsrp vsd-group id 0 preempt
set nsrp vsd-group id 0 priority 1
set nsrp vsd-group id 1
set nsrp rto-mirror sync
save
```

NOTE: The hold-down time can be any length from 0 to 255 seconds, effectively delaying the failover to prevent a flurry of rapid failovers.

CLI (Device B)

2. Cluster and VSD Groups

```
set nsrp cluster id 1
set nsrp cluster name cluster1
set nsrp rto-mirror sync
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
set nsrp secondary-path ethernet2/1
set nsrp arp 5
set arp always-on-dest
```

NOTE: Because devices A and B are both members of the same NSRP cluster, all subsequent commands (except those otherwise noted) that you enter on device B propagate to device A.

In the example, the commands **set nsrp vsd-group id 1 priority 1** and **set nsrp vsd-group id 1 preempt hold-down 10** are not propagated.

If both HA1 and HA2 links are lost, the VSD heartbeat messages pass via the ethernet2/1 in the Trust zone.

The **set nsrp arp 5** setting specifies that, after a device failover, the new VSD group primary device sends five gratuitous ARP packets announcing the association of the VSI and virtual MAC address to the new primary device.

After you enter the **set arp always-on-dest** command, the security device always does an ARP lookup to learn a destination MAC address instead of learning it from the source MAC in the originating ethernet frame. The external routers in this example are grouped as a virtual router running VRRP. Frames coming from this router use the virtual IP address as the source IP but the physical MAC address as the source MAC. If the router fails over and the security device has learned the MAC from the source MAC in the incoming frame, it would then direct return traffic to the wrong location. By doing an ARP lookup for the destination MAC, the security device can properly send traffic to the location of the new physical MAC address.

---

3. Redundant Interfaces and Manage IP

```
set interface redundant1 zone untrust
set interface redundant1 ip 210.1.1.1/24
set interface ethernet1/1 group redundant1
set interface ethernet1/2 group redundant1
set interface redundant2 zone trust
set interface redundant2 ip 10.1.1.1/24
set interface redundant2 manage-ip 10.1.1.22
set interface ethernet2/1 group redundant2
set interface ethernet2/2 group redundant2
set nsrp monitor interface redundant1
set nsrp monitor interface redundant2
```

4. Virtual Security Interfaces

```
set interface redundant1:1 ip 210.1.1.2/24
set interface redundant2:1 ip 10.1.1.2/24
```

5. **Routes**
   set vrouter trust-vr route 0.0.0.0/0 interface redundant1 gateway 210.1.1.250
   set vrouter trust-vr route 0.0.0.0/0 interface redundant1:1 gateway 210.1.1.250
   save

CLI (Device A)

6. **Manage IP Address**
   set interface redundant2 manage-ip 10.1.1.21

7. **RTO Synchronization**
   set nsrp rto-mirror sync
   save

Chapter 2

Interface Redundancy

This chapter describes the various ways in which security devices provide interface redundancy. It contains the following sections:

Redundant Interfaces and Zones

For HA interface redundancy, Juniper Networks security devices either provide dedicated physical redundant HA interfaces or allow you to bind two generic interfaces to the HA zone. See “Dual High Availability Interfaces” on page 26 for more information. You can also create redundant security zone interfaces, as described in this section.

Applying a similar kind of virtualization that allows a VSI to shift its binding from the physical interface on one device to the physical interface on another device, the redundant interface can shift its binding from one physical interface to another physical interface on the same device. For example, if the link from the primary interface to the switch becomes disconnected, the link fails over to the secondary interface, which prevents device failover from the VSD primary device to the backup device.

Creating a Redundant Interface

You can create a redundant interface with the WebUI or the CLI.

WebUI

Network > Interfaces > New Redundant IF: Enter the following, then click **OK**:

Interface Name: redundant1
Zone Name: Untrust
IP Address / Netmask: 210.1.1.1/24

CLI

```
set interface redundant1 zone untrust
```

Setting a Holddown Time Before Failover

You can also set a holddown time for a physical interface to wait before becoming the primary interface after an interface failover occurs. To set a holddown time for a member of a redundant interface, use the following command, in which the interface name is that of a physical interface: **set interface** *interface* **phy holddown** *number*. See Figure 16

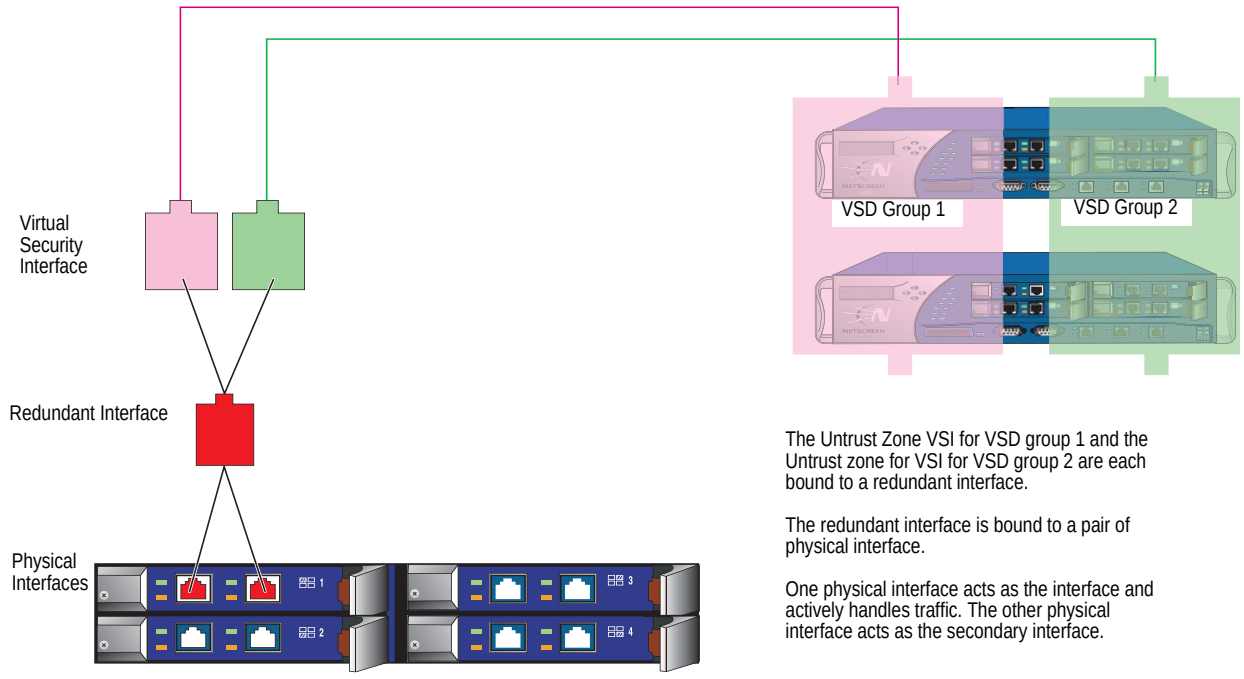
NOTE: You must enter this command before making the interface a member of a redundant group.

You can bind a VSI to any of the following interface types:

- A subinterface
- A physical interface
- A redundant interface, which in turn is bound to two physical interfaces
- A loopback interface

NOTE: You cannot group subinterfaces or a loopback interface to a redundant interface. However, you can define a VLAN on a redundant interface in the same way that you can define a VLAN on a subinterface.

Figure 16: Relationship of Physical, Redundant, and Virtual Security Interfaces



Creating Redundant Interfaces for VSIs

In the example shown in Figure 17, devices A and B are members of two VSD groups—VSD group 0 and VSD group 1—in an active/active configuration. Device A is the primary device of VSD group 0 and the backup in VSD group 1. Device B is the primary device of VSD group 1 and the backup in VSD group 0. The security devices are linked to two pairs of redundant switches—switches A and B in the Untrust zone and switches C and D in the Trust zone.

NOTE: This example only presents the creation of redundant interfaces on device A. Because devices A and B are members of the same NSRP cluster, device A propagates all interface configurations to device B except the manage IP address, which you enter on the redundant2 interface on both devices: device A 10.1.1.21, device B 10.1.1.22.

You put ethernet1/1 and ethernet1/2 in redundant1, and ethernet2/1 and ethernet2/2 in redundant2. On the redundant2 interface, you define a manage IP of 10.1.1.21 for device A and a manage IP of 10.1.1.22 for device B on this interface.

The physical interfaces that are bound to the same redundant interface connect to different switches:

- Physical interfaces bound to a redundant interface in the Untrust zone: ethernet1/1 to switch A, ethernet1/2 to switch B
- Physical interfaces bound to a redundant interface in the Trust zone: ethernet2/1 to switch C, ethernet2/2 to switch D

NOTE: The physical interfaces do not have to be in the same security zone as the redundant interface to which you bind them.

By putting ethernet1/1 and ethernet2/1 in their respective redundant interfaces first, you designate them as primary interfaces. (You can change the primary status assignments via the CLI command **set interface** *redundant1* **primary** *interface1/1*.) If the link to a primary interface becomes disconnected, the security device reroutes traffic through the secondary interface to the other switch without requiring the VSD primary device to fail over.

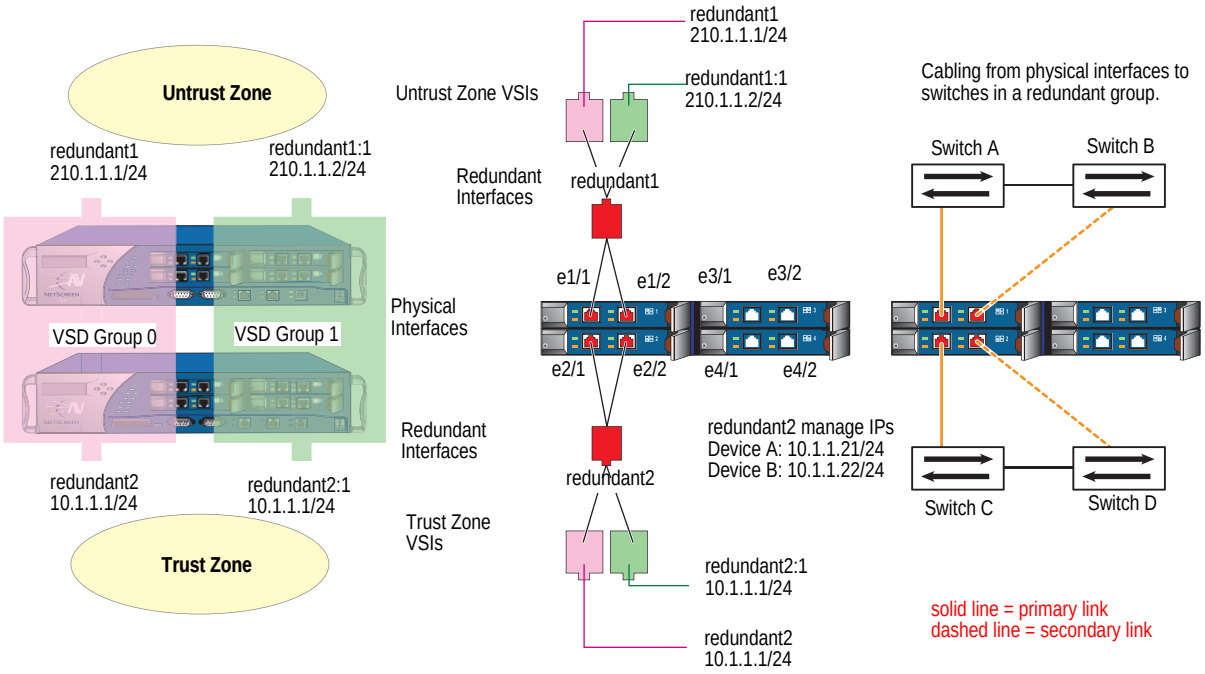
In this example, the cable from ethernet1/1 becomes disconnected, causing a port failover to ethernet1/2. Consequently, all the traffic to and from devices A and B passes through switch B. Reconnecting the cable from ethernet1/1 on device A to switch A automatically causes that interface to regain its former priority.

The IP addresses for the VSIs:

VSIs for VSD Group 0		VSIs for VSD Group 1	
redundant	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

NOTE: IP addresses for multiple VSIs can be in the same subnet or in different subnets if the VSIs are on the same redundant interface, physical interface, or subinterface. If the VSIs are on different interfaces, they must be in different subnets.

Figure 17: Redundant Interfaces for VSIs



WebUI (Device A)

Redundant Interfaces

Network > Interfaces > New Redundant IF: Enter the following, then click **OK**:

Interface Name: redundant1
Zone Name: Untrust
IP Address / Netmask: 210.1.1.1/24

Network > Interfaces > Edit (for ethernet1/1): Select **redundant1** in the "As member of" drop-down list, then click **OK**.

Network > Interfaces > Edit (for ethernet1/2): Select **redundant1** in the "As member of" drop-down list, then click **OK**.

Network > Interfaces > New Redundant IF: Enter the following, then click **Apply**:

Interface Name: redundant2
Zone Name: Trust
IP Address / Netmask: 10.1.1.1/24

Enter **10.1.1.21** in the Manage IP field, then click **OK**.

Network > Interfaces > Edit (for ethernet2/1): Select **redundant2** in the "As member of" drop-down list, then click **OK**.

Network > Interfaces > Edit (for ethernet2/2): Select **redundant2** in the "As member of" drop-down list, then click **OK**.

Virtual Security Interfaces

Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

Interface Name: VSI Base: redundant1
VSD Group: 1
IP Address / Netmask: 210.1.1.2/24

Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

Interface Name: VSI Base: redundant2
VSD Group: 1
IP Address / Netmask: 10.1.1.2/24

WebUI (Device B)

Network > Interfaces > Edit (for redundant2): Type **10.1.1.22** in the Manage IP field, then click **OK**.

NOTE: You must enter static routes to addresses beyond the immediate subnet of a VSI for each VSI in each VSD.

CLI (Device A)

Redundant Interfaces

```
set interface redundant1 zone untrust
set interface redundant1 ip 210.1.1.1/24
set interface ethernet1/1 group redundant1
set interface ethernet1/2 group redundant1
set interface redundant2 zone trust
set interface redundant2 ip 10.1.1.1/24
set interface redundant2 manage-ip 10.1.1.21
set interface redundant2 nat
set interface ethernet2/1 group redundant2
set interface ethernet2/2 group redundant2
set interface redundant1 primary ethernet1/1
set interface redundant2 primary ethernet2/1
```

Virtual Security Interfaces

```
set interface redundant1:1 ip 210.1.1.2/24
set interface redundant2:1 ip 10.1.1.2/24
save
```

CLI (Device B)

```
set interface redundant2 manage-ip 10.1.1.22
save
```

NOTE: You must enter static routes to addresses beyond the immediate subnet of a VSI for each VSI in each VSD.

Configuring Aggregate Interfaces

Some system platforms, such as the Integrated Security Gateway (ISG) systems and the NetScreen-5000 systems, allow you to combine the throughput of one or more pairs of physical ports into a single virtual port. This virtual port is known as an *aggregate interface*. Only Secure Port Modules (SPMs) support this feature, and you can only aggregate side-by-side ports that reside on the same module.

NOTE: Aggregation is not allowed across I/O modules.

You can aggregate two 2 Gigabit ports to make a single full-duplex 4 Gigabit pipe, or you can aggregate eight Fast Ethernet ports into a single full-duplex 1.6 Gigabit pipe.

You must assign one of the following names to the aggregate interface: **aggregate1**, **aggregate2**, **aggregate3**, or **aggregate4**.

NOTE: As with most other ports and interfaces, you must assign the aggregate interface an IP address so that other hosts on the network can reach it.

In the following example, you combine two Gigabit Ethernet mini-GBIC ports, each running at 1-Gbps, into an aggregate interface aggregate1 running at 2-Gbps. The aggregate interface consists of Ethernet ports 1 and 2 on a 5000-8G SPM (residing in Slot 2) and is bound to the Trust zone.

NOTE: To see the physical ports that are available on the system, go to the Network > Interfaces screen in the WebUI or enter the CLI command **get interface**.

WebUI

Network > Interfaces > Aggregate IF > New: Enter the following, then click **Apply**:

Interface Name: aggregate1
Zone Name: Trust (select)
IP Address / Netmask: 10.1.1.0/24

Enter the following, then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet2/1): Enter the following, then click **OK**:

As member of: aggregate1 (select)

Network > Interfaces > Edit (for ethernet2/2): Enter the following, then click **OK**:

As member of: aggregate1 (select)

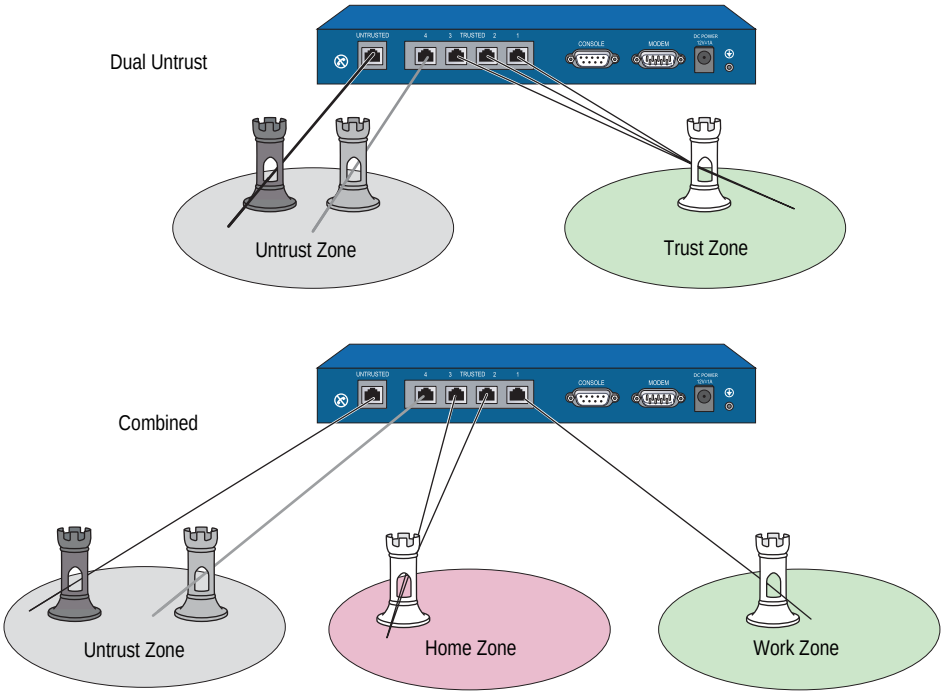
CLI

```
set interface aggregate1 zone trust
set interface aggregate1 ip 10.1.1.0/24
set interface aggregate1 nat
set interface ethernet2/1 aggregate aggregate1
set interface ethernet2/2 aggregate aggregate1
save
```

Dual Untrust Interfaces

You can select a *port mode* for some security appliances. The port mode automatically sets different port, interface, and zone bindings for the device. Certain port modes bind a second, backup interface to the Untrust zone (see "Port Modes" on page **2**-33). For these port modes, the backup interface is used only when there is a failure on the connection through the primary interface or when you manually force traffic from the primary interface to the backup. For example, on the NetScreen-5XT, the Dual Untrust and Combined port modes provide a backup interface to the Untrust zone.

Figure 18: Dual Untrust and Combined Port Modes



Interface Failover

When there are both primary and backup interfaces bound to the Untrust zone (see "Setting Port Modes" on page 2-40), you can manually force traffic from the primary interface to the backup interface through the WebUI or the CLI. You can also configure the security device to automatically forward traffic to the backup interface if ScreenOS detects a failure on the primary interface connection.

Forcing Traffic to the Backup Interface

In this example, you manually force traffic from the primary interface to the backup interface.

WebUI

Network > Untrust Failover: Select **Failover**, then click **Apply**. Then click **Force to Failover**.

CLI

```
set failover enable
save
exec failover force
```

When the primary interface is again available, you need to use the WebUI or the CLI to switch traffic from the backup to the primary interface.

Reverting Traffic to the Primary Interface

In the previous example, you forced a failover from the primary to the backup interface. In this example, you manually force traffic from the backup interface to revert to the primary interface.

WebUI

Network > Untrust Failover: Click **Force to Revert**.

CLI

```
exec failover revert
```

Automatically Failing Over Traffic

In this example, you configure the security device to fail over traffic automatically to the backup interface if the security device detects an IP tracking failure on the primary interface. When IP tracking on the primary interface again succeeds, the security device automatically reverts traffic from the backup to the primary interface.

NOTE: For information about setting IP tracking to trigger an interface failover, see "Interface Failover with IP Tracking" on page 51.

By default, there is a 30-second interval (holddown time) between the time that the IP tracking failure threshold occurs and the interface failover occurs. The purpose of the holddown time is to avoid unnecessary failovers that intermittent latency or interference in the network might cause. In this example, you shorten the holddown time to 20 seconds.

WebUI

Network > Untrust Failover: Select the following, then click **Apply**:

Track IP: (select)
Automatic Failover: (select)
Failover: (select)
Failover Holddown Time: 20

CLI

```
set failover type track-ip
set failover auto
set failover enable
set failover holddown 20
save
```

Determining Interface Failover

An interface failover can occur when ScreenOS detects a physical link problem on the primary interface connection, such as an unplugged cable. You can also define the following types of interface failover:

- When certain IP addresses become unreachable through a given interface using IP tracking
- When certain VPN tunnels on the primary Untrust interface become unreachable using VPN tunnel monitoring

The interface failover sequence occurs as follows:

1. The security device determines that interface monitoring on the primary interface has failed. The interface might be physically disconnected or there might be a failure with IP tracking or VPN monitoring.
2. The security device waits until the failover holddown time elapses.
3. When the failover holddown time has expired, the state of the primary interface changes from up to down, the state of the backup interface changes from down to up, and the security device reroutes traffic using the primary interface to the backup interface.
4. The security device connects to its ISP using DHCP or PPPoE on the now-activated backup interface.

NOTE: The security device can initiate a new PPPoE connection after it receives new outbound traffic or immediately after the failover occurs (**set pppoe name** name **auto-connect**).

The recovery sequence is essentially in reverse order from the failover sequence:

1. The security device determines that interface monitoring on the primary interface has succeeded. The interface might be physically reconnected, or IP tracking or VPN monitoring might have succeeded again.
2. The security device waits until the failover holddown time elapses.
3. When the failover holddown time has expired, the state of the backup interface changes from up to down, the state of the primary interface changes from down to up, and the security device reroutes traffic using the backup interface to the primary interface.
4. The security device connects to its ISP using DHCP or PPPoE on the now-reactivated primary interface.

NOTE: The ISP to which the security device connects on the primary interface can be the same one as or a different one from the ISP it connects to on the backup interface.

Interface Failover with IP Tracking

You can specify that when certain IP addresses become unreachable through the primary Untrust zone interface, the security device fails over to the backup Untrust zone interface even if the physical link is still active. ScreenOS uses Layer 3 path monitoring, or *IP tracking*, similar to that used for NSRP, to monitor IP addresses through the primary interface. If the IP addresses become unreachable through the primary Untrust zone interface, the security device considers the interface to be down, and all routes associated with that interface are deactivated. When the primary Untrust zone interface changes to the down state, failover to the backup Untrust zone interface occurs. You can configure IP tracking without configuring automatic interface failover.

NOTE: For information about configuring IP tracking on interfaces, see "Tracking IP Addresses" on page **2**-72.

Interface Failover

In this example, you first configure the NetScreen-5GT for Dual Untrust mode. You then configure the device for automatic failover. If automatic failover from the primary interface to the backup interface occurs, the backup interface carries all traffic to and from the Untrust zone until the primary interface is restored.

For the primary interface, the security device monitors three IP addresses to determine when failover occurs. Each tracked IP address has the following weight:

- 2.2.2.2— Weight = 6
- 3.3.3.3—Weight = 6
- 4.4.4.4— Weight = 6

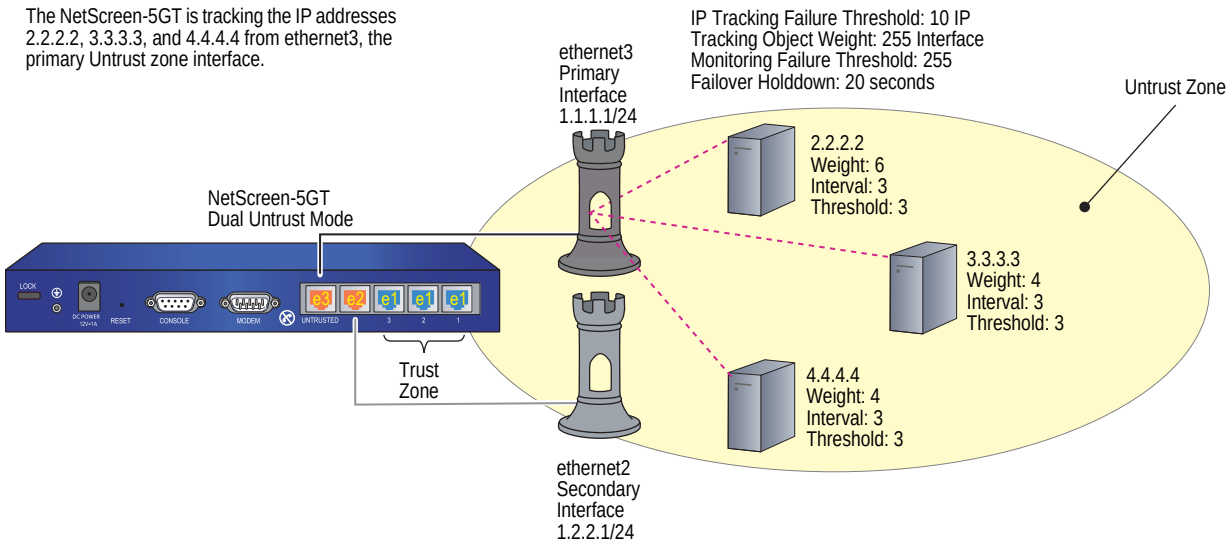
For each of the above tracked IP addresses, the failure threshold is the default value 3 and you set the interval between ICMP echo requests as 3 seconds. If the security device is unable to obtain responses from 3 consecutive ICMP requests to a tracked IP address—each request being three seconds apart—it considers the IP address unreachable through the primary interface.

When an IP tracking failure occurs, the security device adds the weight of the failed address toward a total weight for all IP tracking failures. If the total weight reaches or exceeds the IP tracking object threshold, which in this example you set at 10, then IP tracking adds its weight toward the interface monitoring failure threshold. The IP tracking object weight in this example uses the default value 255 and the interface monitoring failure threshold is also the default value 255.

Therefore, an interface failover occurs if the total weight of IP tracking failures reaches 10. For that to happen, both IP addresses 2.2.2.2 and 3.3.3.3—or 2.2.2.2 and 4.4.4.4—must become unreachable through the primary interface at the same time. If IP addresses 3.3.3.3 and 4.4.4.4 both become unreachable through the primary interface, the cumulative weight of their failures equals 8, which causes no failover to occur.

In the example shown in Figure 19, the interface monitoring failure threshold can be reached in as quickly as 9 seconds (3 failed ICMP requests with 3-second intervals). However, you set a holddown time of 20 seconds so that if the IP tracking weight (255) reaches the interface monitoring failure threshold (255), the security device waits another 20 seconds before failing over the primary interface to the backup.

Figure 19: Interface Failover



WebUI

1. **Port Mode**
   Configuration > Port Mode: Select **Dual-Untrust** from the drop-down list, then click **Apply**.

   The following prompt appears:

   Operational mode change will erase current configuration and reset the device, continue?

   Click **OK**, which causes the security device to reboot.

2. **Login and Interfaces**
   Log in again, and set the interface IP addresses. Then continue with the following configuration:

3. **Automatic Failover and IP Tracking**
   Network > Untrust Failover: Select the following, then click **Apply**:

   Track IP: (select)
   Automatic Failover: (select)
   Failover: (select)
   Failover Holddown Time: 20

   Network > Interfaces > Edit (for ethernet3) > Monitor > Monitor Track IP ADD: Enter the following, then click **Add**:

   Static: (select)
   Track IP: 2.2.2.2
   Weight: 6
   Interval: 3
   Threshold 3:

   Monitor Track IP ADD: Enter the following, then click **Add**:

   Static: (select)
   Track IP: 3.3.3.3
   Weight: 4
   Interval: 3
   Threshold 3:

   Monitor Track IP ADD: Enter the following, then click **Add**:

   Static: (select)
   Track IP: 4.4.4.4
   Weight: 4
   Interval: 3
   Threshold 3:

Network > Interface > Edit (for ethernet3) > Track IP Options: Enter the following, then click **Apply**:

Monitor Option:
Enable Track IP: (select)
Monitor Threshold: 255
Track IP Option:
Threshold: 10
Weight: 255

CLI

1. **Port Mode**

   exec port-mode dual-untrust

   The following prompt appears:

   Change port mode from <trust-untrust> to <dual-untrust> will erase system configuration and reboot box
   Are you sure y/[n] ?

   Press the **Y** key, which causes the security device to reboot.

2. **Login and Interfaces**

   Log in again, and set the interface IP addresses. Then continue with the following configuration:

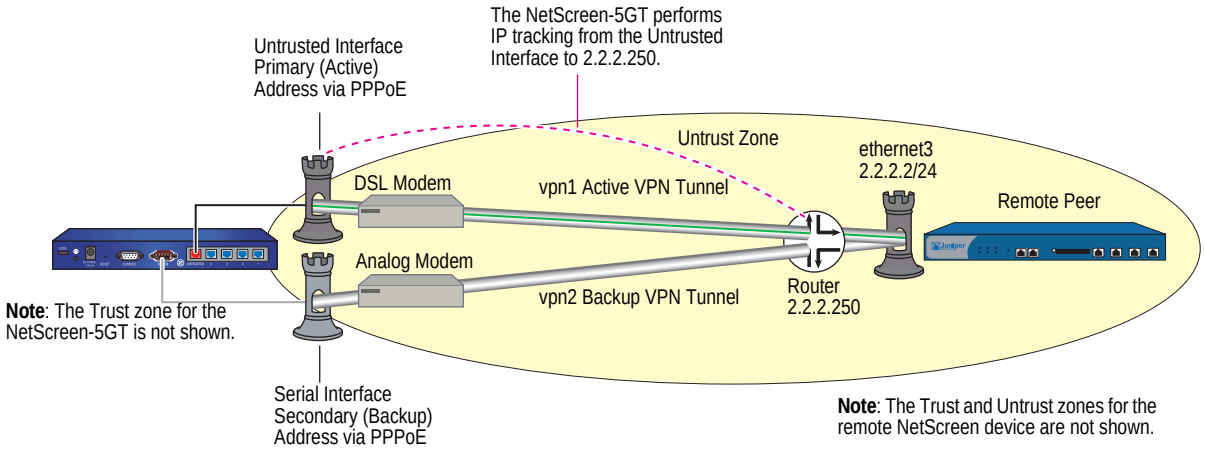
3. **Automatic Failover and IP Tracking**

```
set failover enable
set failover auto
set failover holddown 12
set failover type track-ip
set interface ethernet3 track-ip threshold 10
set interface ethernet3 track-ip ip 2.2.2.2 weight 6
set interface ethernet3 track-ip ip 2.2.2.2 interval 3
set interface ethernet3 track-ip ip 2.2.2.2 threshold 3
set interface ethernet3 track-ip ip 3.3.3.3 weight 4
set interface ethernet3 track-ip ip 3.3.3.3 interval 3
set interface ethernet3 track-ip ip 3.3.3.3 threshold 3
set interface ethernet3 track-ip ip 4.4.4.4 weight 4
set interface ethernet3 track-ip ip 4.4.4.4 interval 3
set interface ethernet3 track-ip ip 4.4.4.4 threshold 3
set interface ethernet3 track-ip
save
```

Active-to-Backup Tunnel Failover

In the example shown in Figure 20, you configure a redundant pair of bidirectional VPN tunnels on the NetScreen-5GT to a remote IKE peer. Only one tunnel is active at any given time. The VPN tunnel from the primary interface is active initially (vpn1 in this example). If the primary tunnel fails, then the security device fails over VPN traffic destined for the remote peer to the backup tunnel (vpn2 in this example).

Figure 20: Tunnel Failover from the Untrusted Interface to the Serial Interface



You configure only one VPN tunnel at the remote peer site because—from the remote peer's point of view—there is only one VPN tunnel from the NetScreen-5GT, resulting in a Y-shaped VPN configuration.

NOTE: When setting up a Y-shaped VPN configuration and the backup interface is an ethernet interface (Dual-Untrust mode for example), do not enable the VPN monitoring rekey option for any VPN tunnel using the backup interface. If you do, the security device continually tries to bring up that tunnel even though you want it to stay down. If the backup interface is a serial interface (as in this example), it does not matter if you enable VPN monitoring with the rekey option for a VPN tunnel on the backup interface.

The NetScreen-5GT is in Trust-Untrust mode. The Untrusted interface is the primary Untrust zone interface and the serial interface is its backup. Each of the Untrust zone interfaces is cabled to a modem. The Untrusted interface connects to a DSL modem (~ 1.5–8 Mbps) and the serial interface to an analog modem (~ 56–64 Kbps).

NOTE: This configuration is possible using any port mode. For a description of the different preset interface-to-zone bindings for each port mode, see "Port Modes" on page **2**-33.

After a failover, expect a considerable decrease in throughput due to the difference in modem speeds.

You use IP tracking to determine if a failover from the Untrusted interface to the serial interface ever becomes necessary. You configure IP tracking to ping the remote peer's external router at 2.2.2.250. You track that address instead of the address of the remote peer's Untrust zone interface (2.2.2.2) because the security device at the remote site is not configured to respond to ICMP echo requests arriving at its Untrust zone interface. You set the following IP tracking values:

- Track IP: 2.2.2.250
  - Weight: 255
  - Interval: 4
  - Threshold: 3
- Track IP failure threshold: 255
- Monitor failure threshold: 255
- Failover holddown: 16

Using the above settings, a failover from vpn1 to vpn2 takes about 30 seconds after IP tracking begins losing connectivity with the tracked IP address (2.2.2.250): 3 failed ICMP echo requests at 4-second intervals = 12 seconds + the 16-second holddown time. During the holddown time, the NetScreen-5GT continues to send ICMP echo requests every 4 seconds; so, in sum, a failover requires a total of 7 consecutive failed attempts to elicit replies from ICMP echo requests (the first 3 + 4 more during the holddown period).

NOTE: Because this particular example is long, only the CLI configuration is included in its entirety. The WebUI section simply lists the navigational paths to the pages where you can set the various elements of the configuration. You can see what you need to set by referring to the CLI commands.

WebUI (NetScreen-5GT)

1. **Port Mode**
   Configuration > Port Mode

2. **Login and Interfaces**
   Log back into the security device. Then continue with the following configuration:

   Network > Interfaces > Edit (for trust)

   Network > Interfaces > Edit (for serial)

   Network > Interfaces > New Tunnel IF

3. **Address**
   Objects > Addresses > List > New

4. **PPPoE**
   Network > PPPoE > New

5. **VPN Tunnels**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

6. **Asymmetric VPN**
   Network > Zones > Edit (for Trust)

7. **IP Tracking**
   Network > Interfaces > Edit (for untrust) > Monitor

   Network > Interfaces > Edit (for untrust) > Monitor > Monitor Track IP ADD

8. **Tunnel Failover**
   Network > Untrust Failover

   Network > Untrust Failover > Edit Weight

9. **Routes**
   Network > Routing > Routing Entries > trust-vr New

10. **Policies**
    Policies > (From: Trust, To: Untrust) New

    Policies > (From: Untrust, To: Trust) New

WebUI (Remote Peer)

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet1)

   Network > Interfaces > New Tunnel IF

2. **Address**
   Objects > Addresses > List > New

3. **VPN Tunnel**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

4. **Routes**
   Network > Routing > Routing Entries > trust-vr New

5. **Policies**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

CLI (NetScreen-5GT)

1. **Port Mode**

   exec port-mode trust-untrust

   The following prompt appears:

   Change port mode from <*current_port-mode*> to <trust-untrust> will erase system configuration and reboot box
   Are you sure y/[n] ?

   Press the **Y** key, which causes the security device to reboot.

2. **Login and Interfaces**

   Log back into the security device. Then continue with the following configuration:

   set interface trust ip 10.1.1.1/24
   set interface trust nat
   set interface serial zone untrust
   set interface tunnel.1 zone trust
   set interface tunnel.1 ip unnumbered interface trust
   set interface tunnel.2 zone trust
   set interface tunnel.2 ip unnumbered interface trust

3. **Address**

   set address untrust peer1 10.2.2.0/24

4. **PPPoE**

   set pppoe name isp1a
   set pppoe name isp1a username ns5gt password juniper
   set pppoe name isp1a idle 0
   set pppoe name isp1a interface untrust
   exec pppoe name isp1a connect

5. **VPN Tunnels**

   set ike gateway gw1 address 2.2.2.2 aggressive local-id ns5gt outgoing-interface untrust preshare netscreen1 sec-level compatible
   set ike gateway gw2 address 2.2.2.2 aggressive local-id ns5gt outgoing-interface serial preshare netscreen1 sec-level compatible
   set vpn vpn1 gateway gw1 sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
   set vpn vpn2 gateway gw2 sec-level compatible
   set vpn vpn2 bind interface tunnel.2
   set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

6. **Asymmetric VPN**

   set zone trust asymmetric-vpn

7. **IP Tracking**

   set interface untrust monitor track-ip ip
   set interface untrust monitor track-ip ip 2.2.2.250 interval 4
   set interface untrust monitor track-ip ip 2.2.2.250 threshold 3
   set interface untrust monitor track-ip ip 2.2.2.250 weight 255

8. **Tunnel Failover**
   set failover enable
   set failover auto
   set failover holddown 16
   set failover type track-ip
   set interface untrust track-ip threshold 255

9. **Routes**
   set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
   set vrouter trust-vr route 10.2.2.0/24 interface tunnel.2
   set vrouter trust-vr route 10.2.2.0/24 interface null metric 100

10. **Policies**
    set policy from trust to untrust any any any permit
    set policy from untrust to trust peer1 any any permit
    save

CLI (Remote Peer)

1. **Interfaces**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.2.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface tunnel.1 zone trust
   set interface tunnel.1 ip unnumbered interface ethernet1

2. **Address**
   set address untrust ns5gt 10.1.1.0/24

3. **VPN Tunnel**
   set ike gateway ns5gt dynamic ns5gt aggressive outgoing-interface ethernet3
   preshare netscreen1 sec-level compatible
   set vpn vpn1 gateway ns5gt sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

4. **Routes**
   set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
   set vrouter trust-vr route 10.1.1.0/24 interface null metric 100
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250

5. **Policy**
   set policy from untrust to trust ns5gt any any permit
   set policy from trust to untrust any ns5gt any permit
   save

Interface Failover with VPN Tunnel Monitoring

You can specify an interface failover when certain VPN tunnels on the primary interface are determined to be "down." For each VPN tunnel, you specify a failover weight, in percent. The assigned weights only come into play when the status of one or more monitored tunnels is "down". If the cumulative weight of the down VPN tunnels reaches or exceeds 100 percent, ScreenOS fails over to the backup interface.

By applying a *weight*, or a value, to a VPN tunnel, you can adjust the importance of the tunnel status in relation to other tunnels. You can assign comparatively greater weight to relatively more important tunnels, and less weight to relatively less important tunnels. The accumulated weights of *all* monitored VPN tunnels determine when interface failover occurs. For example, failure of a VPN tunnel with a weight of 50 brings the primary interface closer to a failover than would the failure of a VPN tunnel with a weight of 10. Tunnels that are in inactive, ready, or undetermined states are counted as 50 percent of the assigned weight. That is, if you assign a weight of 50 to a tunnel that is in inactive state, the tunnel's weight that is counted toward interface failover is 25.

If failover to the backup interface occurs, ScreenOS can still try to establish new VPN tunnel(s) on the primary interface if the VPN monitor rekey feature is enabled. If one or more VPN tunnels on the primary interface returns to "up" status so that the accumulated failover weight is less than 100 percent, ScreenOS can revert traffic back to the primary interface. Enable the VPN monitor rekey feature to allow ScreenOS to switch traffic from the backup interface to the primary.

Dual Active Tunnels

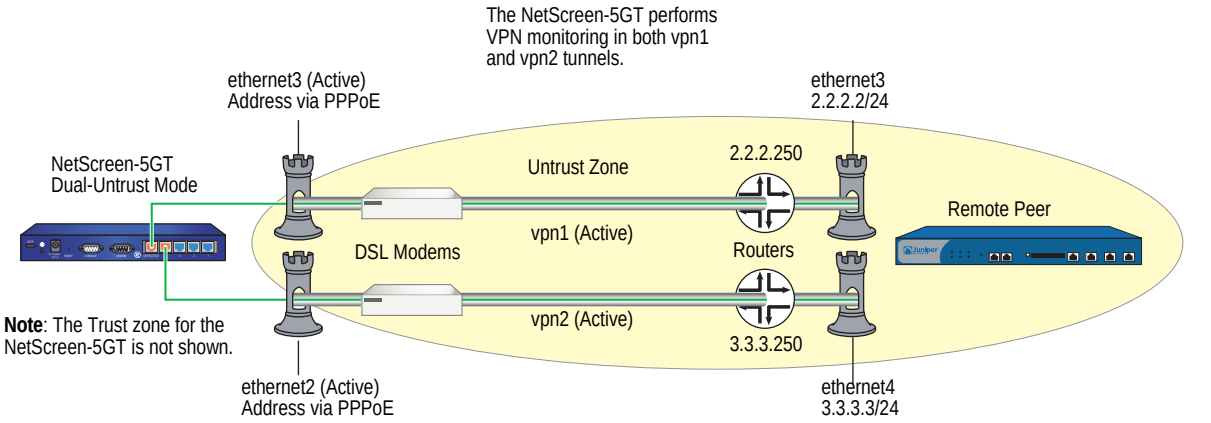
The purpose of this configuration is to support VPN traffic failover between two active VPN tunnels.

You configure a redundant pair of bidirectional VPN tunnels (vpn1 and vpn2) from the NetScreen-5GT to a remote IKE peer. Both tunnels are active at the same time, and the NetScreen-5GT performs a basic form of load-balancing, alternating sessions between the two tunnels. (This is not true load-balancing because the amount of traffic can vary greatly from one session to another, resulting in uneven "loads.") If either tunnel fails, then the NetScreen-5GT directs all VPN traffic destined for the remote peer through the other tunnel.

The NetScreen-5GT is in Dual-Untrust mode. Both ethernet3 and ethernet2 connect to DSL modems. They both become active interfaces when you disable the failover option. See Figure 21.

NOTE: This configuration is also possible using either Combined mode on the NetScreen-5XT or DMZ/Dual Untrust mode on the NetScreen-5GT Extended platform. For a description of the different preset interface-to-zone bindings for each port mode, see "Port Modes" on page **2**-33.

Figure 21: Failover Between Two Active Tunnels



You enable the asymmetric VPN option for the Trust zone at each site so that if an existing session established on one VPN tunnel transfers to another, the security device at the other end of the tunnel does not reject it.

NOTE: Because this particular example is long, only the CLI configuration is included in its entirety. The WebUI section simply lists the navigational paths to the pages where you can set the various elements of the configuration. You can see what you need to set by referring to the CLI commands.

WebUI (NetScreen-5GT)

1. **Port Mode**
   Configuration > Port Mode

2. **Login and Interfaces**
   Log back into the security device. Then continue with the following configuration:

   Network > Interfaces > Edit (for ethernet1)

   Network > Interfaces > New Tunnel IF

3. **Address**
   Objects > Addresses > List > New

4. **PPPoE**
   Network > PPPoE > New

5. **VPN Tunnels**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

6. **Dual Tunnels**
   Network > Untrust Failover

7. **Asymmetric VPN**
   Network > Zones > Edit (for Trust)

8. **Routes**
   Network > Routing > Routing Entries > trust-vr New

9. **Policies**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

WebUI (Remote Peer)

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet1)

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet4)

   Network > Interfaces > New Tunnel IF

2. **Address**
   Objects > Addresses > List > New

3. **VPN Tunnels**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

4. **Asymmetric VPN**
   Network > Zones > Edit (for Trust)

5. **Routes**
   Network > Routing > Routing Entries > trust-vr New

6. **Policies**
   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

CLI (NetScreen-5GT)

1. **Port Mode**
   exec port-mode dual-untrust

   The following prompt appears:

   ```
   Change port mode from <trust-untrust> to <dual-untrust> will erase
       system configuration and reboot box
   Are you sure y/[n] ?
   ```

   Press the **Y** key, which causes the security device to reboot.

2. **Login and Interfaces**
   Log back into the security device. Then continue with the following configuration:

   ```
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface tunnel.1 zone trust
   set interface tunnel.1 ip unnumbered interface ethernet1
   set interface tunnel.2 zone trust
   set interface tunnel.2 ip unnumbered interface ethernet1
   ```

3. **Address**
   ```
   set address untrust peer1 10.2.2.0/24
   ```

4. **PPPoE**
   ```
   set pppoe name isp1a
   set pppoe name isp1a username ns5gt1a password juniper1a
   set pppoe name isp1a idle 0
   set pppoe name isp1a interface ethernet3
   exec pppoe name isp1a connect
   set pppoe name isp1b
   set pppoe name isp1b username ns5gt1b password juniper1b
   set pppoe name isp1b idle 0
   set pppoe name isp1b interface ethernet2
   exec pppoe name isp1b connect
   ```

5. **VPN Tunnels**
   ```
   set ike gateway gw1 address 2.2.2.2 aggressive local-id 5gt-e3 outgoing-interface
       ethernet3 preshare netscreen1 sec-level compatible
   set ike gateway gw2 address 3.3.3.3 aggressive local-id 5gt-e2 outgoing-interface
       ethernet2 preshare netscreen2 sec-level compatible
   set vpn vpn1 gateway gw1 sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
   set vpn vpn1 monitor source-interface ethernet1 destination-ip 2.2.2.2 rekey
   set vpn vpn2 gateway gw2 sec-level compatible
   set vpn vpn2 bind interface tunnel.2
   set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
   set vpn vpn2 monitor source-interface ethernet1 destination-ip 3.3.3.3 rekey
   ```

6. **Dual Tunnels**
   ```
   unset failover enable
   ```

7. **Asymmetric VPN**
   ```
   set zone trust asymmetric-vpn
   ```

8. **Routes**
   ```
   set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
   set vrouter trust-vr route 10.2.2.0/24 interface tunnel.2
   set vrouter trust-vr route 10.2.2.0/24 interface null metric 100
   ```

9. **Policies**
   ```
   set policy from trust to untrust any any any permit
   set policy from untrust to trust peer1 any any permit
   save
   ```

CLI (Remote Peer)

1. **Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 3.3.3.3/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1
```

2. **Address**

```
set address untrust ns5gt 10.1.1.0/24
```

3. **VPN Tunnels**

```
set ike gateway gw1 dynamic ns5gt-e3 aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible
set ike gateway branch2 dynamic ns5gt-e2 aggressive outgoing-interface ethernet4
    preshare netscreen2 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **Asymmetric VPN**

```
set zone trust asymmetric-vpn
```

5. **Routes**

```
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.2
set vrouter trust-vr route 10.1.1.0/24 interface null metric 100
```

6. **Policies**

```
set policy from trust to untrust any any any permit
set policy from untrust to trust ns5gt any any permit
save
```

Applying Weights to Tunnel Failover

In the example shown in Figure 22, you create three pairs of unidirectional VPN tunnels, each pair consisting of a primary tunnel and a backup tunnel. The tunnels connect hosts in the Trust zone at a branch site with DNS, SMTP, and HTTP servers in the Trust zone at the corporate site. All zones at each site are in the trust-vr routing domain.

You first configure the NetScreen-5XT, which is the security device protecting the branch site, for Dual Untrust mode. You then configure three VPN tunnels with the primary Untrust zone interface (ethernet3) as the outgoing interface and three backup VPN tunnels with the backup Untrust zone interfaces (ethernet2) as the outgoing interface. The security device monitors the primary VPN tunnels to determine when a failover occurs. Each VPN tunnel has the following failover weight:

- vpn 1—Weight = 60
- vpn2—Weight = 40
- vpn3—Weight = 40

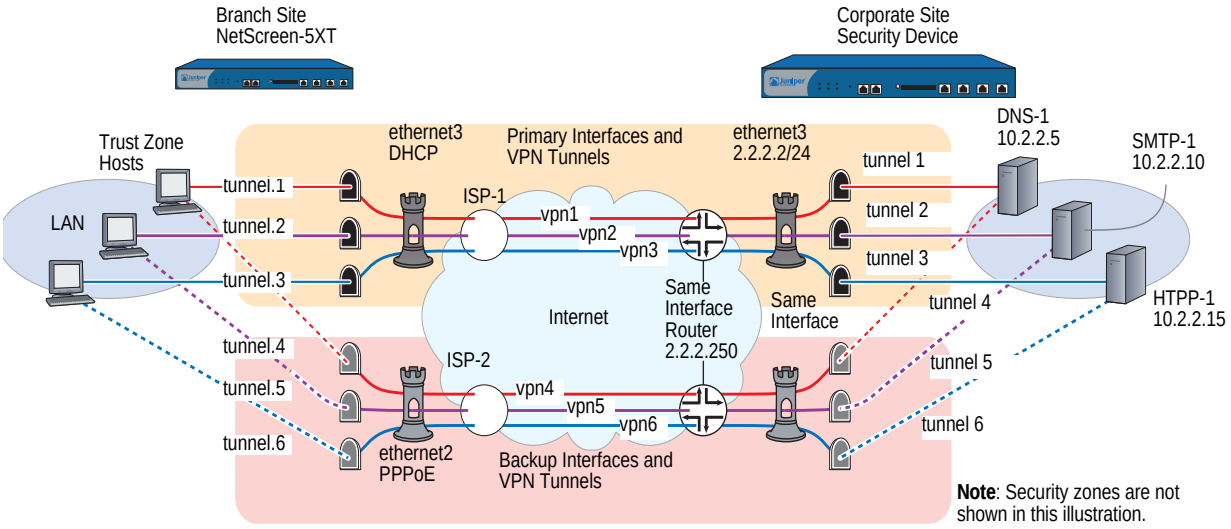
You configure the security device for automatic failover. If automatic failover from the primary interface to the backup interface occurs, the backup interface carries all traffic to and from the Untrust zone until the primary interface is restored. Primary interface failover occurs when the cumulative failover weight reaches or exceeds 100 percent. This means that if both vpn1 and vpn2 are down, the cumulative weight of the failures would be 100 percent, which would cause an automatic failover to the backup interface. If only vpn2 and vpn3 are down, the cumulative weight of the failures would be 80 percent, and no failover occurs.

You also enable the VPN monitor rekey feature. In the event of a failover, this feature allows the security device to revert traffic from the backup interface to the primary if the accumulated weight of the VPN tunnels on the primary interface becomes less than 100 percent.

Finally, you enable the asymmetric VPN option for the Trust zone at each site so that if an existing session established on one VPN tunnel fails over to another, the security device at the other end of the tunnel does not reject it.

The NetScreen-5XT receives its Untrust zone interfaces address, default gateway, and DNS server addresses dynamically from two different ISPs. Each ISP uses a different protocol. ISP-1 uses DHCP to assign an address to ethernet3, and ISP-2 uses PPPoE to assign an address to ethernet2. The security device at the corporate site has a static IP address (2.2.2.2). The IP address of its default gateway is 2.2.2.250.

Figure 22: Primary and Backup Interfaces and VPN Tunnels



The destination address for VPN monitoring is not the default—the remote gateway IP address (2.2.2.2)—but the addresses of the three servers (10.2.2.5, 10.2.2.10, 10.2.2.15). If you use the remote gateway IP address and it becomes unreachable, then all three primary tunnels always fail over to the backups together at the same time. This defeats the use of weights to cause the failover to occur only when two tunnels (vpn1 + vpn2, or vpn1 + vpn3) fail at the same time. On the other hand, if VPN monitoring targets a different destination address through each tunnel and it can no longer ping DNS-1 through vpn1, no failover occurs. If the NetScreen-5XT then cannot ping SMTP-1 through vpn2, the combined weights total 100 percent (60 + 40) and vpn1 fails over to vpn4 and vpn2 fails over to vpn5, while vpn3 remains active.

NOTE: Because this particular example is long, only the CLI configuration is included in its entirety. The WebUI section simply lists the navigational paths to the pages where you can set the various elements of the configuration. You can see what you need to set by referring to the CLI commands.

WebUI (Branch)

1. **Port Mode**
   Configuration > Port Mode

2. **Login and Interfaces**
   Log back into the security device. Then continue with the following configuration:

   Network > Interfaces > Edit (for ethernet1)

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > Edit (for ethernet2)

   Network > Interfaces > New Tunnel IF

3. **VPN Tunnels**
   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

4. **Tunnel Failover**
   Network > Untrust Failover

   Network > Untrust Failover > Edit Weight

5. **Asymmetric VPN**
   Network > Zones > Edit (for Trust)

6. **Routes**
   Network > Routing > Routing Entries > trust-vr New

7. **Policy**
   Policies > (From: Trust, To: Untrust) New

WebUI (Corp)

1. Interfaces

   Network > Interfaces > Edit (for ethernet1)

   Network > Interfaces > Edit (for ethernet3)

   Network > Interfaces > New Tunnel IF

8. **Addresses**
   Objects > Addresses > List > New

9. **Service Group**
   Objects > Services > Groups > New

10. **VPN Tunnels**
    VPNs > AutoKey Advanced > Gateway > New

    VPNs > Autokey IKE > New

11. **Asymmetric VPN**
    Network > Zones > Edit (for Trust)

12. **Route**
    Network > Routing > Routing Entries > trust-vr New

13. **Policy**
    Policies > (From: Trust, To: Untrust) New

CLI (Branch)

1. **Port Mode**
   exec port-mode dual-untrust

   The following prompt appears:

   ```
   Change port mode from <trust-untrust> to <dual-untrust> will erase
       system configuration and reboot box
   Are you sure y/[n] ?
   ```

   Press the **Y** key, which causes the security device to reboot.

2. **Login and Interfaces**
   Log back into the security device. Then continue with the following configuration:

   ```
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 dhcp client
   exec dhcp client ethernet3 renew
   set pppoe interface ethernet2
   set pppoe username ns5gt password juniper
   set interface tunnel.1 zone trust
   set interface tunnel.1 ip unnumbered interface ethernet1
   set interface tunnel.2 zone trust
   set interface tunnel.2 ip unnumbered interface ethernet1
   ```

```
set interface tunnel.3 zone trust
set interface tunnel.3 ip unnumbered interface ethernet1
set interface tunnel.4 zone trust
set interface tunnel.4 ip unnumbered interface ethernet1
set interface tunnel.5 zone trust
set interface tunnel.5 ip unnumbered interface ethernet1
set interface tunnel.6 zone trust
set interface tunnel.6 ip unnumbered interface ethernet1
```

3. **VPN Tunnels**

```
set ike gateway corp1 address 2.2.2.2 aggressive local-id 5gt-e3
    outgoing-interface ethernet3 preshare netscreen1 sec-level basic
set ike gateway corp2 address 2.2.2.2 aggressive local-id 5gt-e2
    outgoing-interface ethernet2 preshare netscreen2 sec-level basic

set vpn vpn1 gateway corp1 sec-level basic
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.2.5 rekey
set vpn vpn2 gateway corp1 sec-level basic

set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP
set vpn vpn2 monitor source-interface ethernet1 destination-ip 10.2.2.10 rekey
set vpn vpn3 gateway corp1 sec-level basic
set vpn vpn3 bind interface tunnel.3

set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
set vpn vpn3 monitor source-interface ethernet1 destination-ip 10.2.2.15 rekey
set vpn vpn4 gateway corp2 sec-level basic
set vpn vpn4 bind interface tunnel.4
set vpn vpn4 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS
set vpn vpn4 monitor source-interface ethernet1 destination-ip 10.2.2.5 rekey
set vpn vpn5 gateway corp2 sec-level basic
set vpn vpn5 bind interface tunnel.5
set vpn vpn5 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn5 monitor source-interface ethernet1 destination-ip 10.2.2.10 rekey
set vpn vpn6 gateway corp2 sec-level basic
set vpn vpn6 bind interface tunnel.6
set vpn vpn6 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
set vpn vpn6 monitor source-interface ethernet1 destination-ip 10.2.2.15 rekey
```

NOTE: Usually, the proxy ID can be "local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any". In the line **set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP** in the example above, however, the proxy ID for each tunnel must be different to distinguish one tunnel from another. If the service is the same for each proxy ID, a configuration conflict results and the security device rejects the proxy IDs for vpn2 and vpn3 (and vpn5 and vpn6).

---

4. **Tunnel Failover**

```
set failover type tunnel-if
set failover auto
set vpn vpn1 failover-weight 60
set vpn vpn2 failover-weight 40
set vpn vpn3 failover-weight 40
```

5. **Asymmetric VPN**
   set zone trust asymmetric-vpn

6. **Routes**
   set vrouter trust-vr route 10.2.2.5/32 interface tunnel.1
   set vrouter trust-vr route 10.2.2.10/32 interface tunnel.2
   set vrouter trust-vr route 10.2.2.15/32 interface tunnel.3
   set vrouter trust-vr route 10.2.2.5/32 interface tunnel.4
   set vrouter trust-vr route 10.2.2.10/32 interface tunnel.5
   set vrouter trust-vr route 10.2.2.15/32 interface tunnel.6
   set vrouter trust-vr route 10.2.2.0/24 interface null metric 100

7. **Policy**
   set policy from trust to untrust any any any permit
   save

CLI (Corp)

1. **Interfaces**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.2.2.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 2.2.2.2/24
   set interface tunnel.1 zone trust

   set interface tunnel.1 ip unnumbered interface ethernet1
   set interface tunnel.2 zone trust
   set interface tunnel.2 ip unnumbered interface ethernet1
   set interface tunnel.3 zone trust
   set interface tunnel.3 ip unnumbered interface ethernet1
   set interface tunnel.4 zone trust
   set interface tunnel.4 ip unnumbered interface ethernet1
   set interface tunnel.5 zone trust
   set interface tunnel.5 ip unnumbered interface ethernet1
   set interface tunnel.6 zone trust
   set interface tunnel.6 ip unnumbered interface ethernet1

NOTE: Instead of creating six tunnel interfaces—one for each VPN tunnel—you can also create one tunnel interface and bind multiple VPN tunnels to it. The security device uses the Next Hop Tunnel Binding (NHTB) table to differentiate each tunnel. For information about NHTB, see "Multiple Tunnels per Tunnel Interface" on page 5-251.

---

2. **Addresses**
   set address untrust branch 10.1.1.0/24
   set address trust DNS-1 10.2.2.5/32
   set address trust SMTP-1 10.2.2.10/32
   set address trust HTTP-1 10.2.2.15/32
   set group address trust servers add DNS-1
   set group address trust servers add SMTP-1
   set group address trust servers add HTTP-1

3. **Service Group**

```
set group service vpn-srv add DNS
set group service vpn-srv add SMTP
set group service vpn-srv add HTTP
set group service vpn-srv add ICMP
```

4. **VPN Tunnels**

```
set ike gateway branch1 dynamic ns5gt-e3 aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level basic
set ike gateway branch2 dynamic ns5gt-e2 aggressive outgoing-interface ethernet3
    preshare netscreen2 sec-level basic

set vpn vpn1 gateway branch1 sec-level basic
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS

set vpn vpn2 gateway branch1 sec-level basic
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn3 gateway branch1 sec-level basic
set vpn vpn3 bind interface tunnel.3
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP

set vpn vpn4 gateway branch2 sec-level basic
set vpn vpn4 bind interface tunnel.4
set vpn vpn4 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS

set vpn vpn5 gateway branch2 sec-level basic
set vpn vpn5 bind interface tunnel.5
set vpn vpn5 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn6 gateway branch2 sec-level basic
set vpn vpn6 bind interface tunnel.6
set vpn vpn6 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
```

5. **Asymmetric VPN**

```
set zone trust asymmetric-vpn
```

6. **Route**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

7. **Policy**

```
set policy from untrust to trust branch servers vpn-srv permit
save
```

Serial Interface

You can connect an external modem to the RS-232 serial port on certain security devices to allow the device to establish a PPP connection to an ISP. This provides a dial-up backup interface for traffic to the Untrust zone if there is a failure on the connection through the primary interface. The dial backup feature is enabled by default for the Trust-Untrust and Home-Work port modes (see "Port Modes" on page 2-33).

The dial backup feature allows two interfaces to the Untrust zone:

- The primary physical interface is the Untrusted Ethernet port. In ScreenOS, the primary logical interface is the Untrust interface in Trust-Untrust port mode and the ethernet3 interface in the Home-Work port mode.
- The backup physical interface is the modem port. In ScreenOS, the backup interface is the serial interface in either Trust-Untrust or Home-Work port modes. By default, the serial interface is bound to the Null zone and you need to bind it to the Untrust zone to use it as the backup interface.

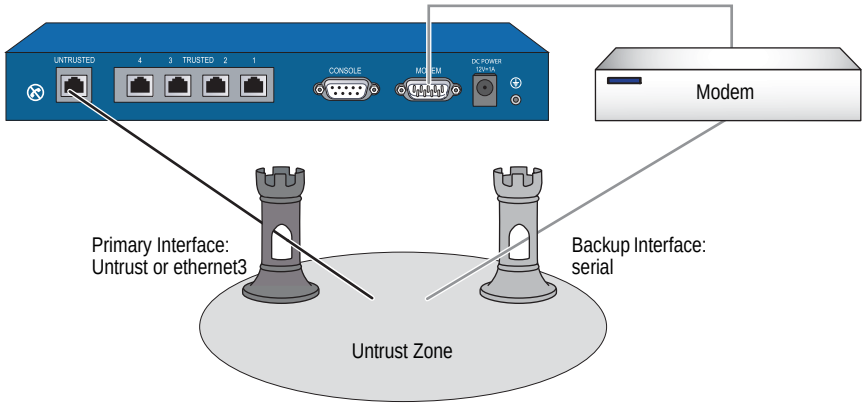
You configure ScreenOS to dial through the modem to an existing ISP account when traffic is switched to the serial interface. When a switch to the serial interface occurs, the modem does not dial unless there is traffic to be sent or the modem idle timeout is set to 0. ScreenOS can queue up to 16 packets while the dial-up link is brought up, so there is minimal data loss when traffic is switched to the serial interface.

NOTE: Only policy-enabled through (user-generated) traffic causes the modem to dial. Management or routing protocol related messages such as OSPF hellos do not cause modem dialup.

By default, interface failover on the security device is manual. With manual failover, you need to force ScreenOS to switch traffic from one interface to the other using the CLI or WebUI. When the primary interface is again available, you need to use the CLI or WebUI to direct ScreenOS to switch traffic from the backup interface to the primary interface. See Figure 24.

The security device can automatically fail over to the serial interface, including dialing and authenticating to a pre-existing ISP account. When the connection through the primary interface is restored, ScreenOS can automatically switch traffic from the serial interface back to the primary interface.

Figure 23: Dial Backup



Modem Overview

Some security devices provide an external modem to the RS-232 serial port or an internal modem to establish a point-to-point (PPP) connection to an ISP. You can configure the modem interface as a primary interface or back up interface to support interface failover.

There are two types of modem interfaces:

- V.92 — The dial-up modem specification from the International Telecommunications Union (ITU) that introduces new features providing convenience and performance for the modem user. V.92 includes Modem-On-Hold (MOH) and it uses V.44 data compression. The V.92 interface is presented as either **serial***n***1/***n***2** (used to denote devices with PIMs) or **serial0/0**. By default, this interface is bound to the Null zone.

- AUX — Auxiliary port. This is usually the same as COM 1. This interface is presented as the **serial0/0** interface. The AUX interface is used to access external networks. By default, the interface is bound to the Null zone.

The modem you use for the dial-up connection must support the following features:

- Hardware flow control: The management of transmission between two devices. Flow control enables slower-speed devices to communicate with higher-speed devices and vice versa

- Provide clear to send (CTS) signals: The signal between computers that indicates that transmission can proceed

- Able to respond to request to send (RTS) signals: An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit

- Asynchronous only:

- Support AT command set: A series of machine instructions used to activate features on a modem

Modem Configuration

You can configure the following serial link (modem) parameters in ScreenOS:

- The maximum amount of time that the serial link can be idle before ScreenOS automatically disconnects the modem (the default is 10 minutes)
- The number of times ScreenOS retries the dial-up connection if the line is busy or there is no response (the default is 3 times)
- The interval, in seconds, between dial-up retries (the default is 10 seconds)
- The maximum baud rate for the serial link (the default rate is 115200 bps)

ScreenOS uses a default modem initialization string. You can configure up to four modem initialization strings, but you can activate only one of the configured initialization strings at a time. The modem initialization string must meet the following requirements:

- Hardware flow control is recommended, but not required (you can specify no flow control)
- Software flow control is not used
- Result code must be displayed in verbal mode

In this example, you configure the modem idle time to be 20 minutes. You also define a modem initialization string for a new modem setting, *mod1*, and activate it.

WebUI

Network > Interfaces > Edit (for serial) > Modem: Enter the following, then click **OK**:

Modem Name: mod1
Init String: AT&FS7=255S32=6
Status: Enable (select)
Inactivity Timeout: 20

CLI

```
set modem idle-time 20
set modem settings mod1 init-strings AT&FS7=255S32=6
set modem settings mod1 active
save
```

If you are using a device with a V.92 modem physical interface module (PIM), do the following to set the modem connection:

WebUI

Network > Interfaces > Edit (for serial1/0) > Modem: Enter the following, then click **OK**:

Modem Name: mod1
Init String: AT&FS7=255S32=6
Status: Enable (select)
Inactivity Timeout: 20

CLI

```
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

Configuring ISP Information

You configure the security device to dial to an ISP account if a failover to the serial interface occurs and there is traffic to be sent. You can configure up to four ISP connections, assigning each a different priority number (1 is the highest priority). The priority number determines the order that ScreenOS uses in attempting the dial-up connection; ScreenOS dials up the ISP with the highest priority first. If ScreenOS is unable to log into the ISP account with the highest priority, it will dial the ISP with the next highest priority number, and so on, until there are no more ISP configurations.

NOTE: By default, ScreenOS attempts to dial to a configured ISP account up to three times (see "Modem Overview" on page 72 for information on modem parameters). If ScreenOS is not able to connect to any configured ISP account, it sends a connect fail message and waits until the primary interface is available again.

For each ISP configuration, you specify the following:

- Account login and password. (The ISP account must be a standard Point-to-Point Protocol (PPP) account that only requires a username and password for login.)
- Primary phone number and, optionally, an alternate phone number. If the modem uses pulse dial by default but you want to use tone dial, precede the phone number with a **T**. If the modem uses tone dial by default but you want to use pulse dial, precede the phone number with a **P**.
- Priority for this connection, relative to other configured ISP connections.

In this example, you configure information for two different ISP accounts: the *isp1* account has a priority value of 1, while the *isp2* account has a priority value of 2. This means that ScreenOS will always dial up the isp1 account first if failover to the serial interface occurs.

WebUI

Network > Interfaces > Edit (for serial) > ISP: Enter the following, then click **OK**:

```
ISP Name: isp1
Primary Number: 4085551111
Alternative Number: 4085552222
Login Name: kgreen
Login Password: 98765432
Priority: 1
```

Network > Interfaces > Edit (for serial) > ISP: Enter the following, then click **OK**:

ISP Name: isp2
Primary Number: 4085551212
Alternative Number:
Login Name: kgreen
Login Password: 12345678
Priority: 2

CLI

```
set modem isp isp1 account login kgreen password 98765432
set modem isp isp1 primary-number 4085551111 alternative-number
    4085552222
set modem isp isp1 priority 1
set modem isp isp2 account login kgreen password 12345678
set modem isp isp2 primary-number 4085551212
set modem isp isp2 priority 2
save
```

Serial Interface Failover

By default, you must use the WebUI or CLI to force ScreenOS to switch over to the serial interface when the primary interface (Untrust or ethernet3 interface) connection fails and to switch back to the primary interface when the primary is again available. You can configure the interface failover to be automatic. You can also configure IP tracking to monitor failure on the Untrust or ethernet3 interfaces. See "Tracking IP Addresses" on page **2**-72 for more information.

By default, policies that are enabled for traffic from the Trust zone to the Untrust zone or from the Untrust zone to the Trust zone are still active after a failover to the serial interface. But traffic through the primary interface could be so heavy that it cannot be handled by the dialup link. When you define a policy, you can specify whether or not the policy should be active if ScreenOS switches to the serial interface. See "Deactivating a Policy for Serial Interface Failover" on page 78 for information on how to configure this in the WebUI and the CLI.

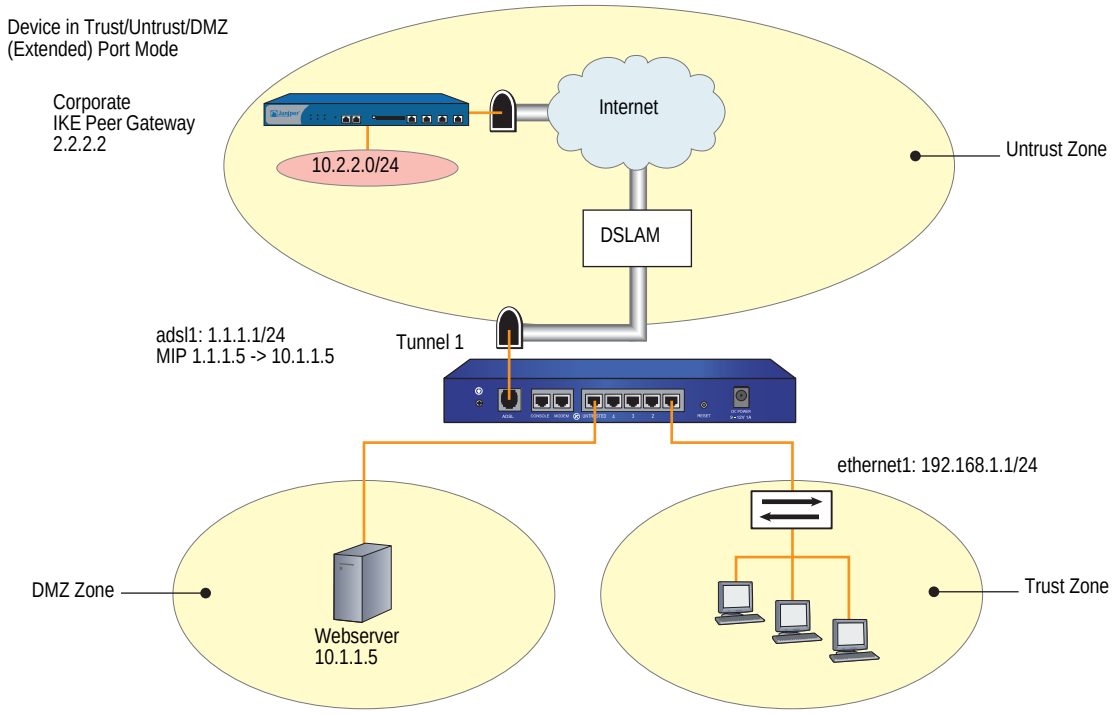
The serial interface is bound by default to the Null zone and you need to explicitly bind it to the Untrust zone to use it as a backup interface. If you bind the serial interface to the Untrust zone using the WebUI, ScreenOS automatically adds a default route for the serial interface. If you bind the serial interface to the Untrust zone using the CLI, ScreenOS does *not* add a default route to the serial interface and you must explicitly add a default route for the serial interface if traffic is to be routed through the serial interface. See "Deleting a Default Route for the Serial Interface" on page 78 for information on how to configure this in the WebUI and the CLI.

Configuring Dial Backup in Trust-Untrust Mode

In this example, you first bind the serial interface to the Untrust zone. The serial interface becomes the backup interface to the primary (the Untrust interface). You then configure ScreenOS to automatically fail over to the serial interface when the primary interface connection fails.

You configure IP tracking to determine failure of the primary interface—if IP addresses 100.100.100.100 and 200.200.200.200 become unreachable through the primary interface, ScreenOS automatically switches over to the backup interface.

Figure 24: Dial Backup in Trust-Untrust Mode



WebUI

Network > Interfaces > Edit (for serial): Enter the following, then click **OK**:

Zone Name: (select) Untrust

Network > Interfaces > Edit (for serial) > Modem: Enter the following, then click **OK**:

Modem Name: mod1
Init String: AT&FS7=255S32=6
Inactivity Timeout: 20

Network > Interfaces > Edit (for serial) > ISP: Enter the following, then click **OK**:

ISP Name: isp1
Primary Number: 4085551111
Alternative Number: 4085552222
Login Name: kgreen
Login Password: 98765432
Priority: 1

Network > Interfaces > Edit (for serial) > ISP: Enter the following, then click **OK**:

ISP Name: isp2
Primary Number: 4085551212
Alternative Number:
Login Name: kgreen

Login Password: 12345678
Priority: 2

Network > Untrust Failover > Automatic Failover: (select), then click **Apply**.

Network > Interface > Edit (for ethernet3) > Track IP: Enter the following, then click **Apply**:

Track IP: 100.100.100.100
Weight: 6
Enter the following, then click **Apply**:
Track IP: 200.200.200.200
Weight: 4
Enter the following, then click **Apply**:
Track IP: 210.210.210.210
Weight: 3

Network > Interface (ethernet3) > Edit > Track IP Options: Enter the following, then click **OK**:

Enable Track IP: (select)
Failover Threshold: 10

CLI

```
set interface serial zone untrust
set failover auto
set modem idle-time 20
set modem settings mod1 init-strings AT&FS7=255S32=6
set modem settings mod1 active
set modem isp isp1 account login kgreen password 98765432

set modem isp isp1 primary-number 4085551111 alternative-number
    4085552222
set modem isp isp1 priority 1
set modem isp isp2 account login kgreen password 12345678
set modem isp isp2 primary-number 4085551212
set modem isp isp2 priority 2
set interface ethernet3 track-ip

set interface ethernet3 track-ip threshold 10
set interface ethernet3 track-ip ip 100.100.100.100 weight 6
set interface ethernet3 track-ip ip 200.200.200.200 weight 4
set interface ethernet3 track-ip ip 210.210.210.210 weight 3
save
```

Deleting a Default Route for the Serial Interface

If you bind the serial interface to the Untrust zone using the WebUI, ScreenOS automatically adds a default route for the serial interface. In this example, you use the WebUI to bind the serial interface to the Untrust zone. You then delete the default route that has been automatically created for the serial interface.

WebUI

Network > Interfaces > Edit (for serial): Enter the following, then click **OK**:

Zone Name: (select) Untrust

Network > Routing > Routing Entries: In the Configure column, click **Remove** for the default route to 0.0.0.0/0 through the serial interface.

Adding a Default Route for the Serial Interface

If you bind the serial interface to the Untrust zone using the CLI, ScreenOS does *not* add a default route to the serial interface and you must explicitly add a default route for the serial interface if you want the security device to route traffic through the serial interface. In this example, you use the CLI to bind the serial interface to the Untrust zone. You then add a default route for the serial interface, which is bound to the Untrust zone.

CLI

```
set interface serial zone untrust
set vrouter trust-vr route 0.0.0.0/0 interface serial
save
```

Deactivating a Policy for Serial Interface Failover

In this example, normal traffic through the primary interface (ethernet3) to the Untrust zone includes large files transferred via FTP from host22 in the Trust zone to ftp_srv in the Untrust zone. If a failover to the serial interface occurs, the dialup link might drop such large FTP traffic. Whenever there is a failover to the serial interface, any policy that is configured to be inactive for the serial interface becomes invalid and the policy lookup procedure continues to the next policy.

WebUI

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), host22
Destination Address:
    Address Book Entry: (select), ftp_srv
Service: FTP
Action: Permit

> Advanced: Clear **Valid for Serial**, then click **Return** to set the advanced options and return to the basic configuration page.

CLI

```
set policy from trust to untrust host22 ftp_srv ftp permit no-session-backup
save
```

Chapter 3
Failover

This chapter explains device failover. It contains the following sections:

Device Failover

When you configure two security devices in an NSRP cluster, the primary device device synchronizes all configuration and state information with the backup device so that the backup device can become the primary device when necessary. For example, if the primary device in a cluster fails, the backup device is promoted to primary device and takes over traffic processing. If the original primary device is restored to its pre-failure status, it can resume traffic processing.

Many different conditions exist that can cause a primary device in an NSRP cluster to fail over to the backup, such as the following physical problems or administrator introduced thresholds and weights:

- **Physical problems:** system crash, loss of power, down link, or removal of CPU or memory boards from the device
- **Administrator introduced failover:** loss of connection to certain gateways or servers causes a primary device to fail over to the backup

You can configure NSRP to monitor different objects so that the failure of one or more of the monitored objects causes a failover of the primary device. For more information about these objects and how to configure them, see "Object Monitoring for Device or VSD Group Failover" on page 81.

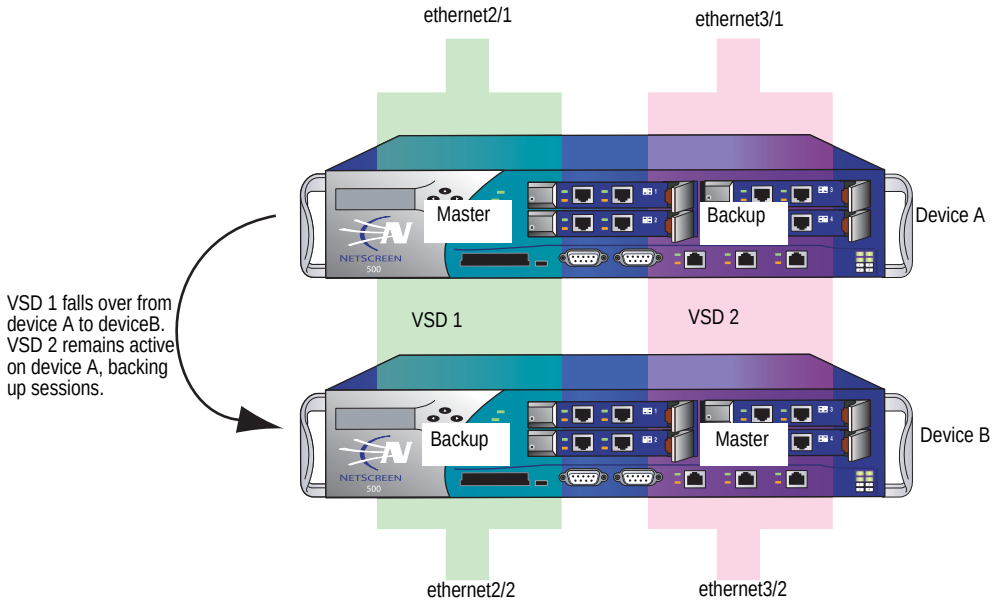
In the event of multiple failover instances within a cluster, at least one device must remain as the primary device. If a device is the last device in a cluster that has not failed or become ineligible to become primary device, that device continues to act as primary device. Under certain conditions, the failure of monitored objects can cause both devices in a cluster to become ineligible, which results in a traffic "black hole". To ensure that one device is still elected as primary device and can forward traffic, issue the CLI command **set nsrp vsd-group master-always-exist**. This allows a device in the NSRP cluster to continue to forward traffic even if all units in the cluster are deemed to have failed due to NSRP object monitoring. If all devices in a cluster simultaneously transition to a failed state, a new primary device is elected based on the preempt and priority values that you previously configured for the devices.

VSD Group Failover (NSRP)

In addition to device failover, you can configure NSRP for VSD group failover. Like device failover, failure of one or more monitored objects can cause the primary device in a VSD group to fail over to the backup device for the group. See "Object Monitoring for Device or VSD Group Failover" on page 81 for information about the objects and how to configure them. For VSD failover, you can configure the same objects to be monitored as you can for device failover.

In the example shown in Figure 25, if a port on a primary device in a VSD group fails, the entire device does not necessarily fail over to the backup device. In the following configuration, if ethernet 2/1 fails, VSD 1 fails over from the primary VSD group on device A to the backup VSD group on device B. VSD 2 remains active, backing up sessions on device A.

Figure 25: VSD Group 1 Failover



Object Monitoring for Device or VSD Group Failover

With NSRP, you can monitor certain objects to determine failover of the security device or of a VSD group. NSRP monitored objects can include:

- **Physical interfaces**—The security device uses NSRP to check that the physical ports are active and connected to other devices.
- **Zones**—The security device uses NSRP to check that all physical ports in a zone are active.
- **Specific target IP addresses**—The security device sends ping or ARP requests to up to 16 specified IP addresses per monitored object at specified intervals and then monitors responses from the targets. All the IP addresses configured on the device or for a specified VSD group constitute a single monitored object. A device can have one monitored object and each VSD group can have its own monitored object.

NOTE: A security device supports up to 32 monitored objects for use by NSRP and interface-based monitoring and up to 64 tracked IP addresses total.

Configuring device or VSD group failover with monitored objects involves setting the following:

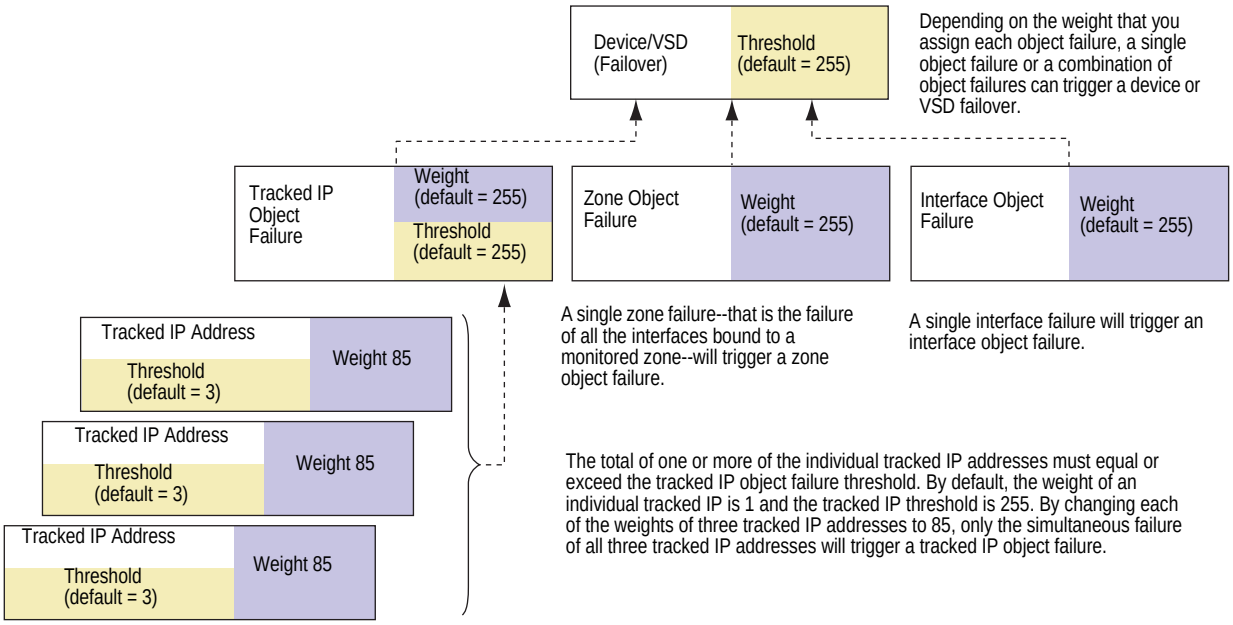
- **Device or VSD failover threshold**—The device or VSD group failover threshold is the total weight of failed monitored objects that is required to cause either a VSD group on a device or a device in an NSRP cluster to initiate a failover to the backup device. If the cumulative weight of the failures of all monitored objects exceeds the threshold, then the VSD group or the device fails over to the backup VSD group or device. You can set the device or VSD failover threshold at any value between 1 and 255. The default threshold is 255.
- **Failure weight of each object being monitored**—Each monitored object has a configurable failure weight, which is the weight that the failure of the monitored object contributes toward the device or VSD failover threshold. You can set the object failure weight at any value between 1 and 255.

For tracked IP addresses, you need to specify individual IP addresses and how they are to be monitored. You also need to define what constitutes the failure of each tracked IP address (the threshold) and the weight that the failed IP address carries. For the tracked IP object, you also specify a failure threshold. This threshold is the sum of the weights of all failed tracked IP addresses required for the tracked IP object to be considered failed.

Objects that are monitored for a VSD group are independent from the objects monitored for the device. That is, you can configure a specific set of objects, weights, and thresholds for a VSD group and a different set for a device. You can also configure independent sets of monitored objects for different VSD groups. For example, you can configure the same monitored objects for two VSD groups with different weights and thresholds specified for each VSD group for the object.

Figure 26 shows the relationship of various monitored objects to the device or VSD group failover. The weights of all failed monitored objects contribute toward the device or VSD failover threshold. If you do not change the default weight of a monitored object or the device or VSD failover threshold, failure of any monitored object can cause the device or VSD to fail over. For tracked IP addresses, the weights of all failed tracked IP addresses contribute toward the tracked IP object failure threshold. If the tracked IP object failure threshold is reached, the tracked IP object failure weight is compared to the device or VSD failover threshold.

Figure 26: Object Monitoring Weights and Failover Thresholds



Monitoring a Physical Interface Object to Trigger Failover

Layer 2 path monitoring functions by checking that the physical ports are active and connected to other network devices. Failure of a physical interface object occurs when the port is no longer active.

In this example, you enable the monitoring of ethernet2/1 for a possible device failover. You set a failure weight of 100 for the interface.

WebUI

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Enter the following, then click **Apply**:

Interface Name: ethernet2/1 (select)
Weight: 100

CLI

```
set nsrp monitor interface ethernet2/1 weight 100
save
```

Monitoring a Zone Object to Trigger Failover

Failure of a zone object occurs only when *all* interfaces in a monitored zone are down. There is no zone failure as long as there is still an active port in the zone. If a monitored zone has no interfaces bound to it, the zone object cannot not fail. The security device always perceives its state as up. If a down interface is the only interface bound to a monitored zone, the zone object fails; if you unbind the interface from the zone, the zone object is no longer failed. If you unbind an active interface from a monitored zone where the remaining interfaces are down, the zone fail.

In this example, you enable the monitoring of the Trust zone for a possible device failover. You set a failure weight of 100 for the zone.

WebUI

Network > NSRP > Monitor > Zone > VSD ID: Device Edit Zone: Enter the following, then click **Apply**:

Zone Name: Trust (select)
Weight: 100

CLI

```
set nsrp monitor zone trust weight 100
save
```

Monitoring a Tracked IP Object to Trigger Failover

IP tracking functions by sending ping or ARP requests to up to 16 specified IP addresses at user-determined intervals and then monitoring if the targets respond. When you configure IP tracking, the device sends either ping or ARP requests from a manage IP address that is bound to a physical interface, redundant interface, or subinterface. (The manage IP address must be a different IP address from the IP address of the interface.) You cannot use a VSI for IP tracking because that address can shift its bindings among multiple devices.

NOTE: When routers are grouped in a redundant cluster using the Virtual Router Redundancy Protocol (VRRP), the router functioning as the primary device cannot respond to ping requests to the virtual IP address if it is not the IP address owner (which might be the case after a failover). However, the primary device virtual router must respond to ARP requests with the virtual MAC address regardless of IP address ownership. (See RFC 2338 for details.) To use ARP when IP tracking, the polled device must be on the same physical subnet as the manage IP address.

For each tracked IP address, you specify the following:

- **Tracked IP Failure Threshold**—This is the number of consecutive failures to elicit a ping or ARP response from a specific IP address that constitutes a failed attempt. Not exceeding the threshold indicates an acceptable level of connectivity with the address; exceeding it indicates an unacceptable level. You can set the threshold to any value between 1-200. The default value is 3.
- **Tracked IP Failure Weight—**This is the weight that failure to elicit a response from the tracked IP address contributes to the tracked IP object failure weight. By applying a weight to a tracked IP address, you can adjust the importance of connectivity to that address in relation to reaching other tracked IP addresses. You can assign greater weights to relatively more important addresses, and lesser weights to relatively less important addresses. The assigned weights come into play when a tracked IP failure threshold is reached. For example, exceeding the tracked IP failure threshold for an address weighted 10 adds more to the tracked IP object failure weight than would a tracked IP failure for an address weighted 1. You can assign weights from 1 to 255. The default is 1.

You also configure a failure threshold for the tracked IP object which contributes to the device or VSD failover threshold. If one or more tracked IP addresses exceed their failure thresholds, then the weights for the individual failed addresses are totaled. If the sum reaches or exceeds the failure threshold for the tracked IP object, then the tracked IP object failure weight is applied to the device or VSD failover threshold. Only the failure weight of the tracked IP object is applied to the device or VSD failover threshold; failure weights of individual tracked IP addresses are never applied to the device or VSD failover threshold. Consider the following example:

Tracked IP Addresses	**Failure Weights**			
10.10.10.250	100	Tracked IP Object Failure Threshold	Tracked IP Object Failure Weight	Device Failover Threshold
1.1.1.30	75	125	255	255
2.2.2.40	75			

If the tracked IP address 10.10.10.250 fails, then the tracked IP failure weight (100) is compared to the tracked IP object failure threshold (125). Since the tracked IP failure weight is less than the tracked IP object failure threshold, the tracked IP object is not considered failed. If both tracked IP addresses 1.1.1.30 and 2.2.2.40 fail, then the combined failure weight (150) is compared to the tracked IP object failure threshold (125). Since the combined failure weight exceeds the tracked IP object failure weight, the tracked IP object is considered failed. The tracked IP object failure weight (255) is compared to the device failover threshold (255). Since the tracked IP object failure weight equals the device failover threshold, the device fails over.

To set a failure weight of 100 for the tracked IP address 10.10.10.250, enter the following:

WebUI

Network > NSRP > Track IP > New: Enter the following, then click **OK**:

Track IP: 10.10.10.250
Weight: 100

CLI

```
set nsrp track-ip ip 10.10.10.250 weight 100
save
```

To set a failure threshold of 125 for the tracked IP object for a possible device failover, enter the following:

WebUI

Network > NSRP > Monitor > Track IP > VSD ID: Device Edit: Enter the following, then click **Apply**:

Enable Track IP: (select)
Failover Threshold: 125

CLI

```
set nsrp monitor track-ip threshold 125
save
```

Setting Track IP for Device Failover

Two security devices are in an active/active configuration. Every 10 seconds, both devices send ARP requests to the physical IP addresses (addresses dedicated to the physical routers that comprise the VRRP cluster) of two external routers running VRRP in a redundant cluster in the Untrust zone and ping requests to two webservers in the Trust zone. The tracked IP object failure threshold is 51. The tracked IP object weight and the device failover threshold are the default values (255). The weights and failure thresholds of the tracked IP addresses are as follows:

- Redundant routers in the Untrust zone
  - 210.1.1.250—Weight: 16, threshold 5
  - 210.1.1.251—Weight: 16, threshold 5
- Webservers in the Trust zone
  - 10.1.1.30—Weight 10, threshold 3
  - 10.1.1.40—Weight 10, threshold 3

Not receiving an ARP response after 5 consecutive attempts to one of the routers is considered a failed attempt and contributes a weighted value of 16 toward the total failover threshold. Not receiving a ping response after 3 consecutive attempts to one of the webservers is considered a failed attempt and contributes a weighted value of 10 toward the total failover threshold.

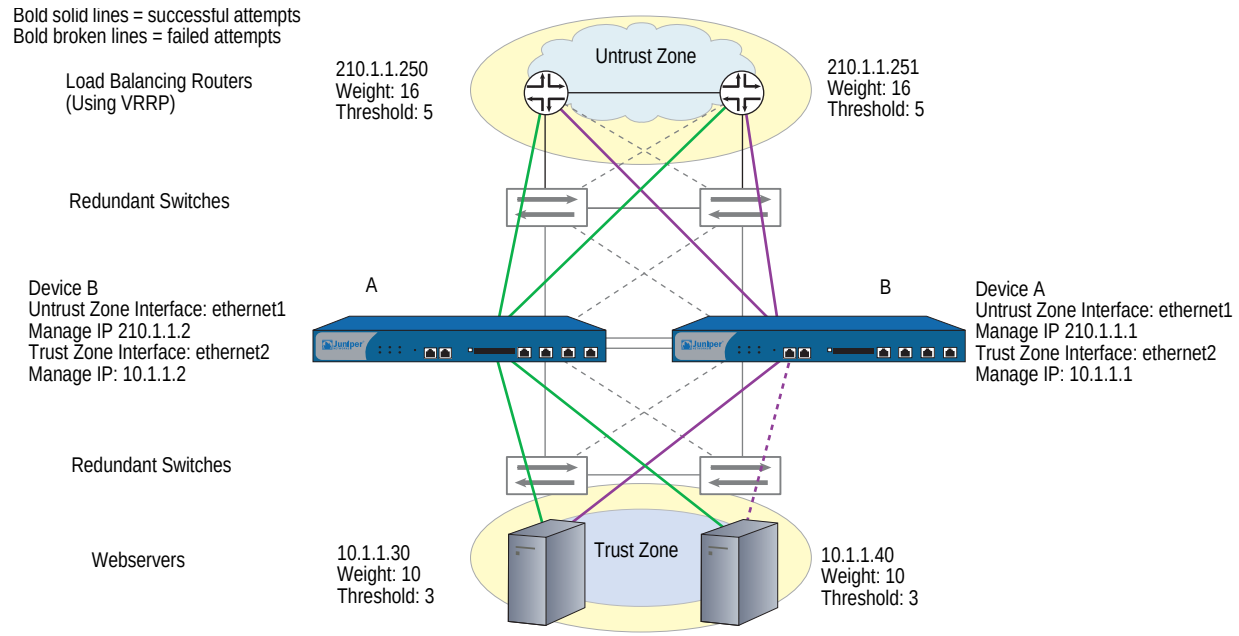
Because the device failover threshold is 51, all four tracked IP addresses must fail before a device failover occurs. If you are not willing to tolerate that amount of failure, you can lower the threshold to a more acceptable level.

Figure 27 shows device A has a 100 percent success rate, while device B has failed to receive three consecutive responses from 10.1.1.40, contributing a value of 10 toward the total failover threshold of 51.

NOTE: All NSRP monitoring settings apply to the local unit only. The IP tracking settings do not propagate to other devices in a VSD group. You must enter the same settings on all devices in the group if necessary.

The Untrust zone interface is ethernet1 and the Trust zone interface is ethernet2 on both devices. The ethernet1 manage IP address is 210.1.1.1 on device A, and 210.1.1.2 on device B. The ethernet2 manage IP address is 10.1.1.1 on device A, and 10.1.1.2 on device B. All the security zones are in the trust-vr routing domain.

Figure 27: Track IP for Device Failover



WebUI

1. **Track IP Addresses**

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 210.1.1.250
   Method: ARP
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: ethernet1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 210.1.1.251
   Method: ARP
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: ethernet1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 10.1.1.30
   Method: Ping
   Weight: 10
   Interval (sec): 10
   Threshold: 3
   Interface: ethernet2
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 10.1.1.40
   Method: Ping
   Weight: 10
   Interval (sec): 10
   Threshold: 3
   Interface: ethernet2
   VSD Group ID: Device

2. **Track IP Object Failure Threshold**

   Network > NSRP > Monitor > Track IP > Edit (for VSD: Device): Enter the following, then click **Apply**:

   Enable Track IP: (select)
   Failover Threshold: 51

CLI

1. **Track IP Addresses**

```
set nsrp track-ip ip 210.1.1.250 interface ethernet1
set nsrp track-ip ip 210.1.1.250 interval 10
set nsrp track-ip ip 210.1.1.250 method arp
set nsrp track-ip ip 210.1.1.250 threshold 5
set nsrp track-ip ip 210.1.1.250 weight 16

set nsrp track-ip ip 210.1.1.251 interface ethernet1
set nsrp track-ip ip 210.1.1.251 interval 10
set nsrp track-ip ip 210.1.1.251 method arp
set nsrp track-ip ip 210.1.1.251 threshold 5
set nsrp track-ip ip 210.1.1.251 weight 16

set nsrp track-ip ip 10.1.1.30 interface ethernet2
set nsrp track-ip ip 10.1.1.30 interval 10
set nsrp track-ip ip 10.1.1.30 method ping
set nsrp track-ip ip 10.1.1.30 threshold 3
set nsrp track-ip ip 10.1.1.30 weight 10

set nsrp track-ip ip 10.1.1.40 interface ethernet2
set nsrp track-ip ip 10.1.1.40 interval 10
set nsrp track-ip ip 10.1.1.40 method ping
set nsrp track-ip ip 10.1.1.40 threshold 3
set nsrp track-ip ip 10.1.1.40 weight 10
set nsrp track-ip
```

NOTE: By default, pinging is the method for IP tracking and a tracked IP failure threshold value is 3; therefore, you do not need to specify them. The commands **set nsrp track-ip ip 10.1.1.30** and **set nsrp track-ip ip 10.1.1.40** are sufficient.

2. **Track IP Object Failure Threshold**

```
set nsrp track-ip threshold 51
save
```

Virtual System Failover

For a virtual system to fail over, it must be in a VSD group. For a VSD group to support virtual systems, you must create VSIs for each virtual system. A virtual system has its own Trust zone VSI, and it can have its own Untrust zone VSI. A virtual system can also share the Untrust zone VSI with the root level. When virtual systems have their own Untrust zone VSIs, they must be in different subnets from each other and from the Untrust zone VSI at the root level. All Trust zone virtual system VSIs must also be in different subnets from one another.

Table 2 lists the two security devices (device A and device B) that are in an active/active full-mesh configuration. You have already configured the root system of device A as the primary device of VSD 0 and that of device B as the primary device of VSD group 1. The Trust and Untrust zone VSIs for VSDs 0 and 1 in the root system are as follows:

Table 2: VSD IP Address

VSIs for VSD Group 0		VSIs for VSD Group 1	
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

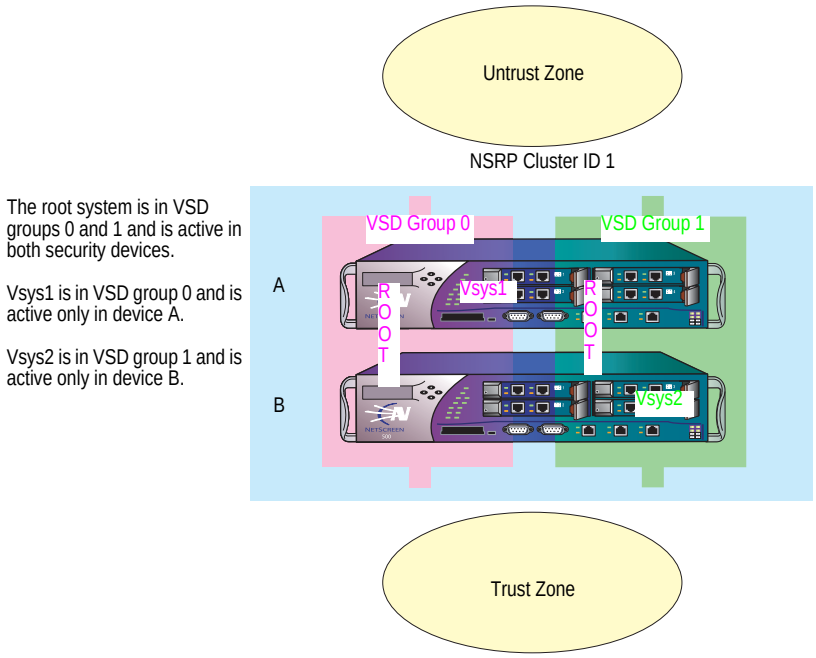
In the example shown in Figure 28, you configure two virtual systems (vsys1 and vsys2) for NSRP. To provide load sharing for incoming traffic to the virtual systems, VSD membership is apportioned as follows:

- Vsys1 is a member of VSD group 0.
- Vsys2 is a member of VSD group 1.

NOTE: In Figure 28, the load is not evenly distributed or load balanced. The two security devices share the load, with devices A and B receiving incoming traffic in dynamically shifting proportions (60/40 percent, 70/30 percent, and so on).

The security devices share the incoming traffic load by distributing the VSD groupings of the virtual systems. Because of the initial design of configuring vsys1 on device A and vsys2 on device B, incoming traffic to these virtual systems is directed to the device that contains it.

Figure 28: Virtual Systems in an NSRP Configuration

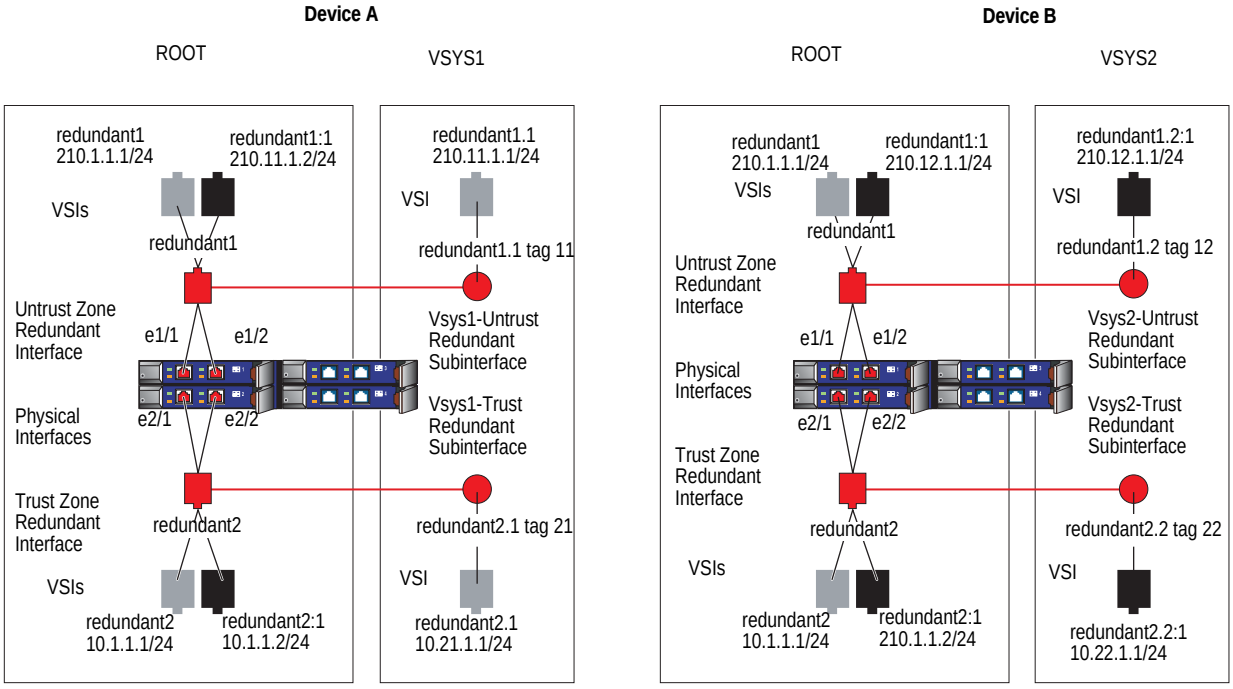


The default gateway for outbound traffic is different for the root system and each virtual system:

- Root: 210.1.1.250
- Vsys1: 210.11.1.250
- Vsys2: 210.12.1.250

Because Figure 29 builds on “Configuring an Active/Active NSRP Cluster” on page 35, in which you set up VSD groups 0 and 1 and set the devices in NSRP cluster ID 1, NSRP is already enabled. Therefore, the settings you configure on device A automatically propagate to device B.

Figure 29: Relationship of Physical Interfaces, Redundant Interfaces, Subinterfaces, and VSIs



WebUI

1. Device A: Root

NOTE: The NSRP configuration for the root system is identical to that in "Configuring an Active/Active NSRP Cluster" on page 35.

---

2. Device A: Vsys1

Vsys > New: Enter the following, then click **OK**:

VSYS Name: vsys1

NOTE: If you do not define a vsys admin, the security device automatically creates one by appending "vsys_" to the vsys name. In this example, the vsys admin for vsys1 is vsys_vsys1.

Vsys > Enter (vsys1) > Network > Interface > New Sub-IF: Enter the following, then click **OK**:

Interface Name: Redundant1.1
Zone Name: Untrust
VLAN Tag: 11

Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

VSI Base: Redundant1.1
VSD Group: 0
IP Address / Netmask: 210.11.1.1/24

Network > Interfaces > New Sub-IF: Enter the following, then click **OK**:

Interface Name: Redundant2.1
Zone Name: Trust-vsys-vsys1
VLAN Tag: 21

Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

VSD Group ID: 0
IP Address / Netmask: 10.21.1.1/24
Interface Mode: Route

NOTE: Virtual systems can be in either Route or NAT mode, independent of the mode you set at the root level.

Network > Routing > Routing Entries > untrust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (select)
    Interface: Redundant1
    Gateway IP Address: 210.11.1.250

Click **Exit Vsys** to return to the root level.

3. **Device A: Vsys2**

   Vsys > New: Enter the following, then click **OK**:

   VSYS Name: vsys2

   Vsys > Enter (vsys2) > Network > Interface > New Sub-IF: Enter the following, then click **OK**:

   Interface Name: Redundant1.2
   Zone Name: Untrust
   VLAN Tag: 12

   Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

   VSI Base: Redundant1.2
   VSD Group: 1
   IP Address / Netmask: 210.12.1.1

   Network > Interfaces > New Sub-IF: Enter the following, then click **OK**:

   Interface Name: Redundant2.2
   Zone Name: Trust-vsys-vsys2
   VLAN Tag: 22

   Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

   VSD Group ID: 1
   IP Address / Netmask: 10.22.1.1/24
   Interface Mode: Route

   Network > Routing > Routing Entries > untrust-vr New: Enter the following, then click **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (select)
   Interface: Redundant1
   Gateway IP Address: 210.12.1.250

   Click **Exit Vsys** to return to the root level.

4. **Device B**

NOTE: Because device A propagates the other configuration settings to device B, you do not need to enter them again in device B.

CLI

1. **Device A: Root**

NOTE: The NSRP configuration for the root system is identical to that in "Configuring an Active/Active NSRP Cluster" on page 35.

2. **Device A: VSYS 1**

```
set vsys vsys1
ns(vsys1)-> set interface redundant1.1 tag 11 zone untrust
ns(vsys1)-> set interface redundant1.1 ip 210.11.1.1/24
ns(vsys1)-> set interface redundant2.1 tag 21 zone trust-vsys1
ns(vsys1)-> set interface redundant2.1 ip 10.21.1.1/24
ns(vsys1)-> set interface redundant2.1 route
ns(vsys1)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway
    210.11.1.250
ns(vsys1)-> save
ns(vsys1)-> exit
```

NOTE: Virtual systems can be in either Route or NAT mode, independent of the mode you set at the root level.

3. **Device A: VSYS 2**

```
set vsys vsys2
ns(vsys2)-> set interface redundant1.2 tag 12 zone untrust
ns(vsys2)-> set interface redundant1.2:1 ip 210.12.1.1/24
ns(vsys2)-> set interface redundant2.2 tag 22 zone trust-vsys2
ns(vsys2)-> set interface redundant2.2:1 ip 10.22.1.1/24
ns(vsys2)-> set interface redundant2.2:1 route
ns(vsys2)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway
    210.12.1.250
ns(vsys2)-> save
ns(vsys2)-> exit
```

4. **Device B**

NOTE: Device A propagates the other configuration settings to device B, so you do not need to enter them again in device B.

Chapter 4

NSRP-Lite

This chapter explains the components of NSRP-Lite and describes how to configure a pair of Juniper Networks security devices to use NSRP-Lite. This chapter contains the following sections:

Introduction to NSRP-Lite

NSRP-Lite supports selected NSRP features and is supported only on some Juniper Networks security platforms running ScreenOS in Route or NAT mode. NSRP-Lite allows the following:

- Only Active/Passive configurations
- Configuration synchronization, although not by default
- User session and VPN connection disruption when failover occurs because no RTO synchronization happens.

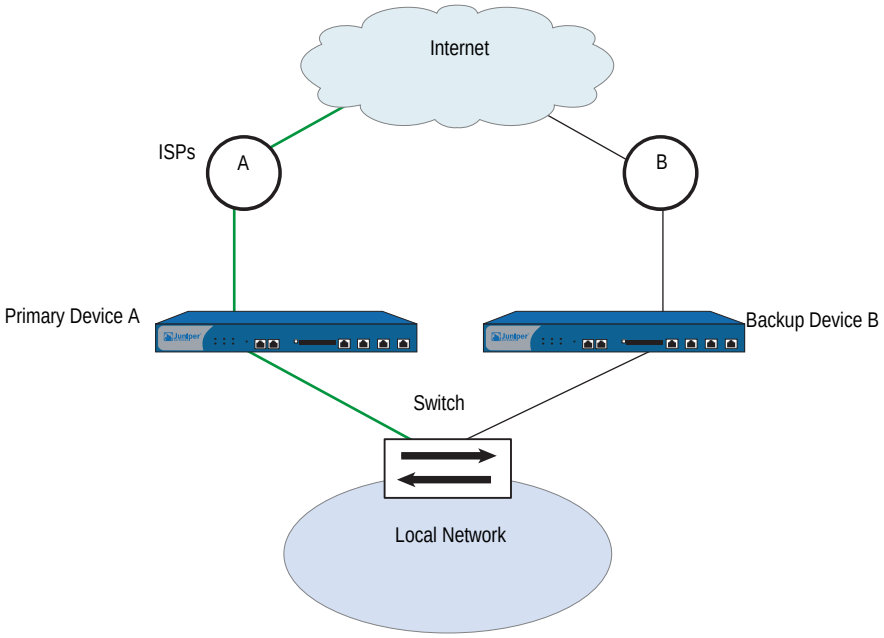
NOTE: VPN tunnels must be reestablished. We recommend that you enable VPN monitoring with the rekey option on VPN tunnels so that they automatically reestablish themselves.

NSRP-Lite is a high availability (HA) solution available for some security platforms. When you cable and configure two security devices for NSRP-Lite, one device acts as the primary device and actively processes network traffic. The other device acts as a backup, passively waiting to become primary device in the event that the primary device fails. By connecting two security devices to your local network, configuring them for NSRP-Lite, and using a different Internet service provider (ISP) for each device, you can protect the local network against both device failure and ISP failure.

NOTE: NSRP-Lite does not support RTO or session synchronization.

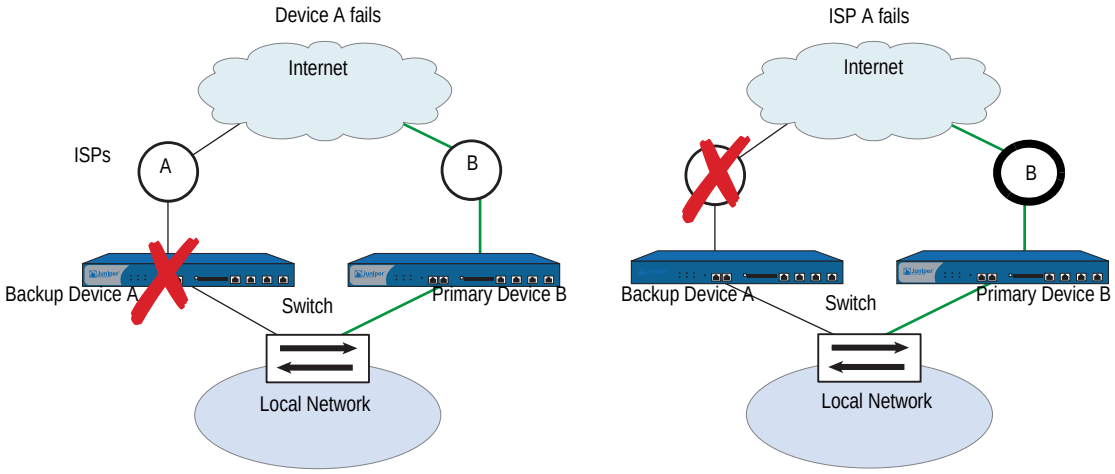
Figure 30 shows the relationship between the two security devices. The primary device (device A) actively processes traffic traversing the firewall between the local network and the Internet. The backup (device B) receives status reports from device A and remains ready to become primary device if a failover occurs. Device B, however, does not process traffic.

Figure 30: NSRP-Lite Setup



If either device A or ISP A fails, device B becomes primary device and device A becomes backup (or it becomes inoperable if it has internal system problems). See Figure 31.

Figure 31: Failover Scenarios



Clusters and VSD Groups

An NSRP-Lite cluster consists of a pair of security devices that comprise a single virtual security device (VSD) that provides redundant network connectivity. One physical device acts as the primary device of the VSD group and performs all of the network processes on traffic sent to the VSD. The other device acts as a backup to the primary device, and is ready to take over traffic processing if the current primary device fails.

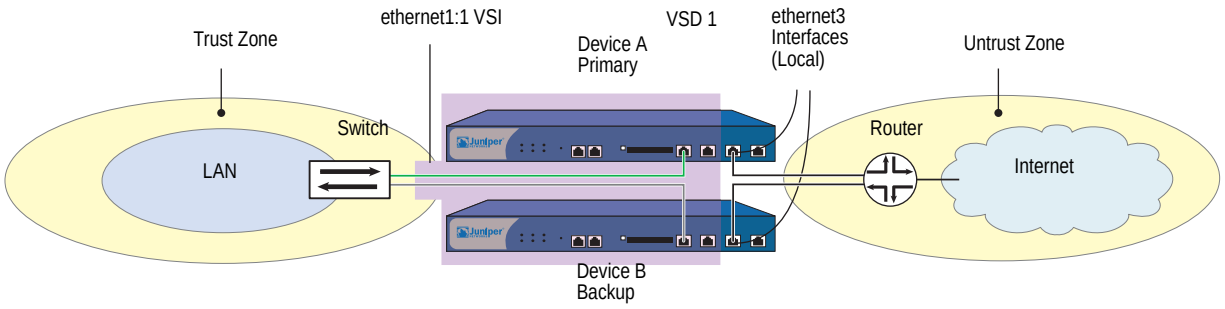
The two devices send VSD heartbeat messages to each other to provide status reports. If the backup receives a message that the primary device has experienced a network or system failure and has changed its status, the backup changes its status to primary device and begins actively processing traffic. This transition constitutes a failover.

Before two security devices can provide redundant services, you must group them in the same NSRP cluster by assigning a cluster ID between 1 and 7. When a security device becomes a member of a cluster, it automatically becomes a member of VSD group 0, and all interfaces become virtual security interfaces (VSIs) for VSD group 0.

A VSI binding can shift from one physical device to another device, as the device acting as primary device of the VSD group shifts. To return VSIs, which are virtual interfaces that all VSD members can share, to local interfaces dedicated to the physical security device that hosts them, you must unset VSD group 0. You can then selectively make local interfaces VSIs by creating a VSD group with a non-zero ID number—such as VSD 1—and defining interfaces as VSIs for that VSD.

In Figure 32 the ethernet1:1 VSI is bound to the Trust zone and form a VSI for VSD group 1, and the ethernet3 interfaces in the Untrust zone remain as local interfaces. Only the physical interface on device A is active because device A is the primary device. Each ethernet3 interface in the Untrust zone is dedicated to the physical device that hosts it.

Figure 32: VSI and Local Interfaces



Default Settings

The basic NSRP-Lite configuration uses the following default settings:

- Configure sync: disabled
- RTO sync: N/A
- VSD Group Information
  - VSD group ID: 0
  - Device priority in the VSD group: 100
  - Preempt option: disabled
  - Preempt hold-down time: 0 seconds
  - Initial state hold-down time: 5 seconds
  - Heartbeat interval: 1000 milliseconds
  - Lost heartbeat threshold: 3
- NSRP Link Information
  - Number of gratuitous ARPs: 4
  - NSRP encryption: disabled
  - NSRP authentication: disabled
  - Interfaces monitored: none
  - Secondary path: none

When you set a security device in an NSRP cluster, the device automatically creates VSD group 0 and transforms physical interfaces bound to the Trust zone into Virtual Security Interfaces (VSIs) for VSD group 0.

Clusters

An NSRP cluster consists of a group of security devices that enforce the same overall security policy and share the same configuration settings. When you assign a device to an NSRP cluster, any changes made to the configuration on one member of the cluster propagate to the other.

NOTE: You can disable configuration and file synchronization. For information, see "Automatic Configuration Synchronization" on page 111.

By default, NSRP-Lite does not propagate a complete configuration, but you can sync the configuration.

Members of the same NSRP cluster maintain identical settings for the following:

- Policies and policy objects (such as addresses, services, VPNs, users, and schedules)
- System parameters (such as settings for authentication servers, DNS, SNMP, syslog, URL blocking, firewall detection options, and so on)

Members of a cluster do not propagate the following configuration settings, as shown in Table 3.

Table 3: Non-Propagating Commands

NSRP	■ set/unset nsrp cluster id *number* ■ set/unset nsrp auth password *pswd_str* ■ set/unset nsrp encrypt password *pswd_str* ■ set/unset nsrp monitor interface *interface* ■ set/unset nsrp vsd-group id *id_num* { mode *string* | preempt | priority *number* } ■ set/unset nsrp rto-mirror …
Interface	■ set/unset interface *interface* manage-ip *ip_addr* ■ set/unset interface *interface* phy … ■ set/unset interface *interface* bandwidth *number* ■ set/unset interface redundant *number* phy primary *interface* ■ All commands pertaining to local interfaces
Monitored Objects	All IP tracking, zone monitoring, and interface monitoring commands
Console Settings	All console commands (set/unset console …)
Hostname	set/unset hostname *name_str*
SNMP	set/unset snmp name *name_str*
Virtual Router	set/unset vrouter *name_str* router-id *ip_addr*
Clear[1]	All clear commands (clear admin, clear dhcp, …)
Debug[2]	All debug commands (debug alarm, debug arp, …)

1. By default, NSRP cluster members do not propagate the **clear** commands. To propagate a clear command to all devices in an NSRP cluster, insert the keyword **cluster** into the command. For example, **clear cluster admin …**, **clear cluster dhcp …**
2. By default, NSRP cluster members do not propagate the **debug** commands. To propagate a debug command to all devices in an NSRP cluster, insert the keyword **cluster** into the **debug** command. For example, **debug cluster alarm …**, **debug cluster arp …**

Cluster Names

Because NSRP cluster members can have different host names, a failover can disrupt SNMP communication and the validity of digital certificates because SNMP communication and certificates rely on the host name of a device to function properly.

To define a single name for all cluster members, type the following CLI command:

set nsrp cluster name *name_str*

NOTE: On devices that do not have a dedicated HA port, you must bind the interface to the HA zone before configuring the NSRP cluster.

Use the cluster name when configuring the SNMP host name for the security device (**set snmp name** *name_str*) and when defining the common name in a PKCS10 certificate request file.

The use of a single name for all cluster members allows SNMP communication and digital certificate use to continue without interruption after a device failover.

Authentication and Encryption

Because of the sensitive nature of NSRP communications, you can secure all NSRP traffic through encryption and authentication. For encryption and authentication, NSRP supports the DES and MD5 algorithms respectively.

NOTE: When the devices are cabled directly to one another, there is no need to use authentication and encryption. However, if the devices are cabled through a switch to which other devices connect, you might consider implementing these additional security measures.

To enable authentication or encryption, you must provide passwords on each device in the cluster.

WebUI

Network > NSRP > Cluster: Enter the following, then click **Apply**:

NSRP Authentication Password: (select), *pswd_str*
NSRP Encryption Password: (select), *pswd_str*

CLI

set nsrp auth password *pswd_str*
set nsrp encrypt password *pswd_str*

VSD Groups

A Virtual Security Device (VSD) group is a pair of physical security devices that collectively comprise a single VSD. One physical device acts as the primary device of the VSD group. The virtual security interface (VSI) of the VSD is bound to the Trust zone physical interface of the primary device. The other physical device acts as the backup.

If the primary device fails, the VSD fails over to the backup and the VSI binding is transferred to the physical interface on the backup, which is instantly promoted to primary device.

NOTE: When using BGP and both the Trust and Untrust zones are in the same virtual routing domain, the security device advertises the subnet connected to the Trust zone VSIs of both the primary device (active) and backup (passive) VSD group members.

VSD Group Member States

The members of a VSD group can be in one of six states:

- **Master**—The state of a VSD group member that processes traffic sent to the VSI.
- **Primary Backup**—The state of a VSD group member that becomes the primary device if the current primary device fails. The election process uses device priorities to determine which member to promote.
- **Backup**—The state of a VSD group member that monitors the status of the primary backup and elects one of the backup devices to primary backup if the current one fails.
- **Initial**—The transient state of a VSD group member while it joins a VSD group, either when the device boots up or when it is added via the **set nsrp vsd-group id** *id_num* command.

  You can specify how long a VSD group member stays in the initial state with the **set nsrp vsd-group init-hold** *number* command. The default (and minimum) setting is 5. To determine the initial state hold-down time, multiply init-hold value by the VSD heartbeat-interval (init-hold x hb-interval = initial state hold-down time). For example, if the init-hold is 5 and the hb-interval is 1000 milliseconds, then the initial state hold-down time is 15,000 milliseconds, or 5 seconds (5 x 1000 = 5000).

NOTE: If you reduce the VSD heartbeat interval, you should increase the init-hold value. For information on configuring the heartbeat interval, see “Heartbeat Messages” on page 103.

- **Ineligible**—The state that an administrator purposefully assigns to a VSD group member so that it cannot participate in the election process. To do this, use the **set nsrp vsd-group id** *id_num* **mode ineligible** command.

- **Inoperable**—The state of a VSD group member after a system check determines that the device has an internal problem (such as no processing boards) or a network connection problem (such as when an interface link fails).

NOTE: When the device returns from either the ineligible state (when you use the **exec nsrp vsd-group id** id_num **mode { backup | init | master | pb }** command) or inoperable state (when the system or network problem has been corrected), it must first pass through the initial state.

Heartbeat Messages

Heartbeat messages continually advertise the sender's member status, and the health of its system and network connectivity. Every VSD group member—even if it is in the initial, ineligible, or inoperable state—communicates with its group members by sending a heartbeat message every second. These messages allow every member to know the current state of every other member. The heartbeat message includes the following information:

- Unit ID of the device
- VSD group ID
- VSD group member status
- Device priority

The interval for sending VSD heartbeats is configurable (200, 600, 800, or 1000 milliseconds; 1000ms is the default). The CLI command—which applies globally to all VSD group members—is **set nsrp vsd-group hb-interval** *number*. You can also configure the lost heartbeat threshold that is used to determine when a VSD group member is considered as missing. The CLI command, which also applies globally to all VSD group members, is **set nsrp vsd hb-threshold** *number*. The minimum value for the lost heartbeat threshold is 3.

Preempt Option

You can determine whether a better priority number (closer to zero) can initiate a failover by setting the device that you want to be primary device in preempt mode. If you enable the preempt option on that device, it becomes the primary device of the VSD group if the current primary device has a lesser priority number (farther from zero). If you disable this option, a primary device with a lesser priority than a backup can keep its position (unless some other factor, such as an internal problem or faulty network connectivity, causes a failover).

To change the priority of a device (the default value is 100) and enable or disable the preempt option, use the following CLI commands:

set nsrp vsd-group id *number* priority *number*
unset nsrp vsd-group id *number* priority
set nsrp vsd-group id *number* preempt
unset nsrp vsd-group id *number* preempt

NOTE: This returns the priority to its default value of 100.

Using the hold-down time to delay a failover can prevent a barrage of rapid failovers in the event of port-flickering on an adjacent switch and also ensure that surrounding network devices have sufficient time to negotiate new links before the new primary device becomes available. You can use the following CLI command to set the hold-down time—used for delaying the preempted failover—to any length from 0 to 600 seconds:

```
set nsrp vsd-group id number preempt hold-down number
```

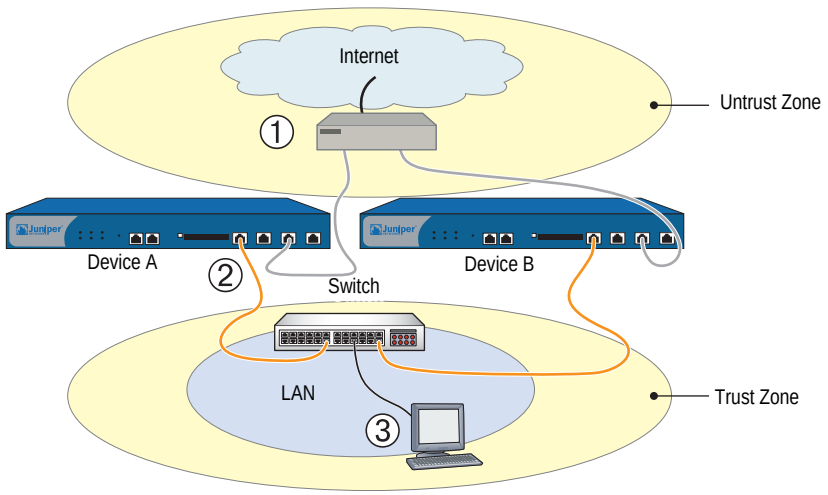
Cabling and Configuring NSRP-Lite

To set up two security devices for HA, you must cable them to the network and configure them for NSRP-Lite.

NOTE: NSRP communications used for heartbeat messages are proprietary, so these messages cannot be routed to another type of Layer 3 intermediary device. You should use only a Layer 2 switch or hub to connect the devices in the Trust zone.

- Using an RJ-45 ethernet cable, connect the Untrust zone port on each security device to the external router.
- Using another RJ-45 ethernet cable, connect the Trust zone port(s) on each security device to the internal switch on the local area network (LAN).
- Connect other hosts on the internal LAN to the switch.

Figure 33: Cabling for NSRP-Lite



In Figure 34, you configure two security devices for high availability (HA) using NSRP-Lite. The IP addresses for the interfaces are as follows:

- Device-A
  - ethernet3—Untrust zone interface, 1.1.1.1/24, manage IP: 1.1.1.2

    This is a local interface, not a VSI.
  - ethernet1:1—Trust zone interface, 10.1.1.1/24, NAT mode

    This is a VSI for VSD group 1.
  - ethernet4—HA zone interface

    This is for the control link for HA communications between the two devices. You also set ethernet1 as the secondary path interface for VSD heartbeats in the event that ethernet4 fails. (For more information about VSD heartbeats, see “Heartbeat Messages” on page 18.)
- Device-B
  - ethernet3—Untrust zone interface, 1.1.2.1/24, manage IP: 1.1.2.2

    This is a local interface, not a VSI.
  - ethernet1—Trust zone interface, 10.1.1.1/24, NAT mode

    This is a VSI for VSD group 1.
  - ethernet4—HA zone interface

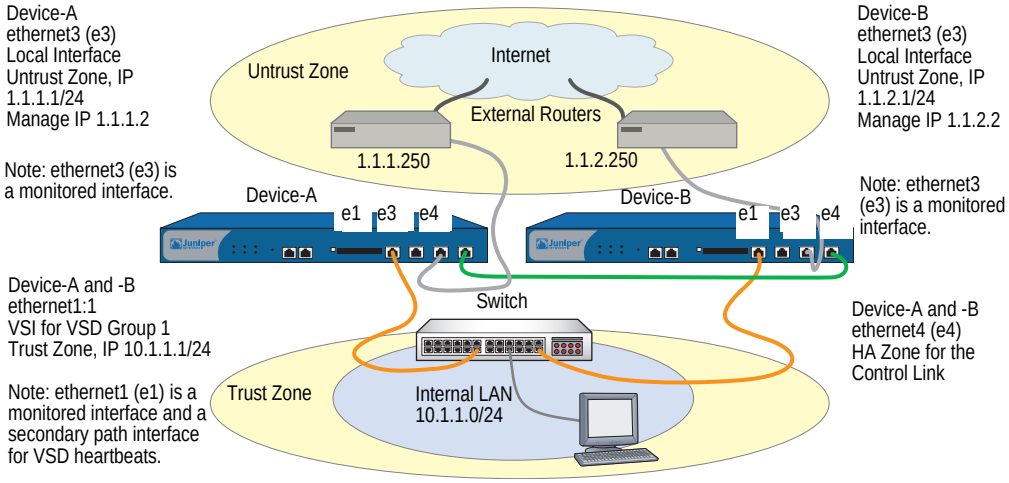
    This is for the control link for HA communications between the two devices. You also set ethernet1 as the secondary path interface for VSD heartbeats in the event that ethernet4 fails.

You want Device-A to be the primary device of VSD group 1, so you give it a priority of 1 and leave the priority for Device-B at the default value of 100. You set the preempt hold-down time for Device-A to become primary device after 10 seconds.

You set both devices to monitor interfaces ethernet1 and ethernet3, and assign each a weight of 255 (the default value). If either interface fails, a device-level failover occurs.

You define two default routes for each Untrust zone interface. For ethernet3 on Device-A, the default route points to an external router with IP address 1.1.1.250. For ethernet3 on Device-B, the default route points to an external router with IP address 1.1.2.250. All security zones are in the trust-vr routing domain.

Figure 34: NSRP-Lite Configuration



WebUI (Device-A)

1. **Interfaces (Device-A)**

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

   Zone Name: Trust

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select)
   IP Address/Netmask: 1.1.1.1/24
   Manage IP: 1.1.1.2

   Network > Interfaces > Edit (for ethernet4): Enter the following, then click **OK**:

   Zone Name: HA

2. **NSRP (Device-A)**

   Network > NSRP > Cluster: Enter the following, then click **Apply**:

   Cluster ID: (select), 1

   Network > NSRP > VSD Group: Click **Remove** for VSD group 0. When prompted to confirm the removal, click **OK**.

   Network > NSRP > VSD Group > New: Enter the following, then click **OK**:

   Group ID: 1
   Priority: 1
   Enable Preempt: (select)
   Preempt Hold-Down Time (sec): 10

Network > Interfaces > New VSI IF: Enter the following, then click **OK**:

Interface Name:
VSI Base: ethernet1
VSD Group: 1
IP Address / Netmask: 10.1.1.1/24

Network > NSRP > Link: Select **ethernet1** from the Secondary Link drop-down list, then click **Apply**.

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Enter the following, then click **Apply**:

ethernet1: (select), Weight: 255
ethernet3: (select), Weight: 255

3. **Route (Device-A)**

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, then click **OK**:

Network Address / Netmask: 0.0.0.0/0
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

WebUI (Device-B)

4. **Interfaces (Device-B)**

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select)
IP Address/Netmask: 1.1.2.1/24
Manage IP: 1.1.2.2

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **OK**:

Zone Name: HA

5. **NSRP (Device-B)**

Network > NSRP > Cluster: Enter the following, then click **Apply**:

Cluster ID: (select), 1

Network > NSRP > VSD Group: Click **Remove** for VSD group 0. When prompted to confirm the removal, click **OK**.

Network > NSRP > VSD Group > New: Enter the following, then click **OK**:

Group ID: 1
Priority: 100
Enable Preempt: (clear)
Preempt Hold-Down Time (sec): 0

NOTE: At the time of this release, you must use the following CLI command to synchronize the configuration from Device-A to Device-B: **exec nsrp sync global-config save**. Then reset the device with the **reset** command.

Network > NSRP > Link: Select **ethernet1** from the Secondary Link drop-down list, then click **Apply**.

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: Enter the following, then click **Apply**:

ethernet1: (select), Weight: 255
ethernet3: (select), Weight: 255

6. **Route (Device-B)**
   Network > Routing > Routing Entries > (trust-vr) New: Enter the following, then click **OK**:

   Network Address / Netmask: 0.0.0.0/0
   Gateway: (select)
   Interface: ethernet3
   Gateway IP Address: 1.1.2.250

CLI (Device-A)

1. **Interfaces (Device-A)**

```
set interface ethernet1 zone trust
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage-ip 1.1.1.2
set interface ethernet4 zone ha
```

2. **NSRP (Device-A)**

```
set nsrp cluster id 1
unset nsrp vsd-group id 0
set nsrp vsd-group id 1
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
set interface ethernet1:1 ip 10.1.1.1/24
set nsrp secondary-path ethernet1
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
```

3. **Route (Device-A)**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

CLI (Device-B)

4. **Interfaces (Device-B)**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.2.1/24
   set interface ethernet3 manage-ip 1.1.2.2
   set interface ethernet4 zone ha

5. **NSRP (Device-B)**
   set nsrp cluster id 1
   unset nsrp vsd-group id 0
   set nsrp vsd-group id 1
   save
   exec nsrp sync global-config save
   reset

   The following prompt appears:

   Configuration modified, save? [y] / n

   Press the **N** key.

   The following prompt appears:

   System reset, are you sure? y / [n] n

   Press the **Y** key.

   The system reboots.

   set nsrp secondary-path ethernet1
   set nsrp monitor interface ethernet1
   set nsrp monitor interface ethernet3

6. **Route (Device-B)**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.2.250
   save

Configuration and File Synchronization

When you add a new device to an active NSRP cluster, you can synchronize the configuration and files (such as PKI public/private key files) from the primary device of the VSD group or groups to the new device. By default in NSRP-Lite, two devices do not synchronize configurations and files when they first enter a cluster, begin NSRP communications, and establish the roles of primary device and backup in VSD group 0. You can manually synchronize configurations and files, or you can change the default behavior to enable automatic configuration synchronization.

Synchronizing Configurations

By default, automatic configuration synchronization is disabled in NSRP-Lite. You can change this behavior by entering the CLI command **set nsrp config sync**. However, even if you enable automatic configuration synchronization, the configuration settings can still become unsynchronized. They can become unsynchronized if, for example, you make any configuration changes to one device while another in the cluster reboots (or if either of the interfaces should fail through

which NSRP communications pass). To discover if the configuration of one device is out of sync with that of another, use the **exec nsrp sync global-config check-sum** command. The output states whether the configurations of the two devices are in or out of sync and provides the checksum of the local and remote devices.

If the configurations are out of sync, use the following command to resynchronize them: **exec nsrp sync global-config save**. If you do not use the **unset all** command on the local device before synchronizing the configurations, the local device appends the settings from the remote device to its existing settings. However, after synchronizing the configurations, every duplicate setting produces an error message. To avoid generating error messages while synchronizing configurations, you can do the following:

1. Download both the local and remote configurations to a workstation.
2. Use an application such as WinDiff to discern the differences between the files.
3. Manually enter the settings on the local device that had been added, modified, or deleted on the remote device.

NOTE: Juniper Networks security devices use the NetScreen Reliable Transport Protocol (NRTP), which is very similar to TCP and with low overhead. Configurations on active devices in a cluster rarely become unsynchronized.

Synchronizing Files

If you need to synchronize a specific file, such as a local certificate for authentication, enter the following command on the device to which you are synchronizing the file: **exec nsrp sync file name** *name_str* **from peer**. If you need to synchronize all files, enter **exec nsrp sync file from peer**.

Adding a Device to an Active NSRP Cluster

In this example, you add device A, which had previously been functioning as a single security appliance, to VSD group 0 in NSRP cluster with cluster ID 1 and name “cluster1.” You unset the previous configurations on device A, reboot it, and then synchronize the configuration and files from the primary device VSD group 0. You then assign device A as the primary device of VSD group 0.

WebUI

NOTE: The configuration synchronization feature is only available through the CLI.

CLI

Device A

```
unset all
```

NOTE: If you do not first use the **unset all** command, the **exec nsrp sync global-config** command appends new configuration settings to existing settings. (Note: The security device generates an error message for each duplicate setting that is synchronized.)

The following prompt appears:

```
Erase all system config, are you sure y / [n]?
```

Press the **Y** key.

The system configuration is returned to the factory default settings.

```
reset
```

The system reboots.

```
set nsrp cluster id 1
set nsrp cluster name cluster1
exec nsrp sync file
exec nsrp sync global-config
exec nsrp vsd-group id 0 mode master
save
```

Automatic Configuration Synchronization

By default, devices placed in an NSRP cluster do not synchronize configurations and files. This setting is useful, for example, if you want all configuration changes to originate from NetScreen-Security Manager.

You can enable the automatic synchronization of configurations with the CLI command **set nsrp config sync** (the WebUI does not support this option). Enter this command on all members in the cluster.

Before enabling automatic configuration synchronization, Juniper Networks recommends that you first manually synchronize files—such as PKI objects for example—between the cluster members. You can synchronize files with the command **exec nsrp sync file from peer**. If you synchronize the configuration, but one cluster member is missing a file that is referenced in the configuration, the configuration becomes invalid for that member. To avoid that, first synchronize files and then the configuration

Path Monitoring

Path monitoring checks the Layer 2 and Layer 3 network connections between a interface of one security device and the interface of another device. Path monitoring is a useful tool for devices within a redundant group to determine whether the network connectivity of the device is acceptable. If the connectivity is unacceptable and passes a defined threshold, a failover occurs—either at the VSD group level or at the device level. For information about the distinction between these two levels of failover, see “Failover” on page 79.

Layer 2 path monitoring functions by checking that the physical ports are active and connected to other network devices. You can monitor interfaces on a per-interface basis or on a per-zone basis. Per-interface:

- WebUI: Click Network > NSRP > Monitor > Interface > VSD ID: { Device | *number* } Edit Interface, and then select the interfaces you want the security device to monitor.
- CLI: set nsrp [vsd-group id *number*] monitor interface *interface*

Per zone (that is, the security device monitors all the interface bound to the selected zone):

- WebUI: Click Network > NSRP > Monitor > Zone > VSD ID: { Device | *number* } Edit Zone, and then select the zones you want the security device to monitor.
- CLI: set nsrp [vsd-group id *number*] monitor zone *zone*

Layer 3 path monitoring, or IP tracking, functions by sending ping or ARP requests to up to 16 specified IP addresses at user-determined intervals and then monitoring if the targets respond. If the total of tracked IP failures for a device acting as primary device (but not for the device acting as its backup) exceeds the device failover threshold, then the backup is automatically promoted to primary device, and the deposed primary device enters the inoperable state. (The inoperable VSD group member continues its IP path tracking activity. When the results no longer exceed the failover threshold, it transitions from the inoperable to initial state, and then to the backup state.)

NOTE: If the VSD group is in preempt mode and the device has a better priority than the current primary device, it transitions from the inoperable to initial to primary device state.

When routers are grouped in a redundant cluster using the Virtual Router Redundancy Protocol (VRRP), the router functioning as the primary device cannot respond to ping requests to the virtual IP address if it is not the IP address owner (which might be the case after a failover). However, the primary device virtual router must respond to ARP requests with the virtual MAC address regardless of IP address ownership. (See RFC 2338 for details.) To use ARP when IP tracking, the polled device must be on the same physical subnet as the manage IP address.

When tracking IP addresses, you can send ping or ARP requests from a manage IP address on an interface. For VSIs, the manage IP address must be different from the interface IP address and must be unique per device. For local interfaces, the manage IP address can be the same as or different from the interface IP address.

Setting Thresholds

IP path tracking involves two kinds of thresholds: a tracked IP failure threshold and a device failover threshold.

Tracked IP Failure Threshold—The number of consecutive failures to elicit a ping or ARP response from a specific IP address required to be considered a failed attempt. Not exceeding the threshold indicates an acceptable level of connectivity with that address; exceeding it indicates an unacceptable level. You can set this threshold per IP address at any value from 1 to 200. The default value is 3.

Device Failover Threshold—The total weight of the cumulative failed attempts required to cause a VSD group primary device to initiate failover to the backup device. (For information on how to assign a weight to a tracked IP address, see "Weighting Tracked IP Addresses.") You can set the device failover threshold at any value between 1 and 255. The default is 255.

Weighting Tracked IP Addresses

By applying a weight, or a value, to a tracked IP address, you can adjust the importance of connectivity to that address in relation to reaching other tracked addresses. You can assign relatively greater weights to relatively more important addresses, and lesser weights to relatively less important addresses. The assigned weights come into play when a tracked IP failure threshold is reached. For example, exceeding the tracked IP failure threshold for an address weighted 10 brings the primary device closer to device failover than would a tracked IP failure for an address weighted 1. You can assign weights from 1 to 255. The default is 255.

IP Tracking for VPN Tunnel Failover

By configuring a VPN tunnel on each device to reach the same remote network through two different remote VPN gateways and then tracking IP addresses at the remote site through the tunnels, you can protect VPN traffic from local and remote gateway device failure, tunnel failure, and ISP failure.

The primary device (device A) actively processes VPN traffic between the local and remote networks through VPN tunnel A. Device A monitors the health of its system, its network connectivity, and VPN tunnel A. The backup (device B) receives status reports from device A and remains ready to become primary device if a failover occurs. VPN tunnel B is up but inactive.

If any of the following events occur, device B becomes primary device and device A becomes backup (or device A becomes inoperable if it has internal system problems). See Figure 35.

Figure 35: Possible Points of Failure for VPN Tunnels

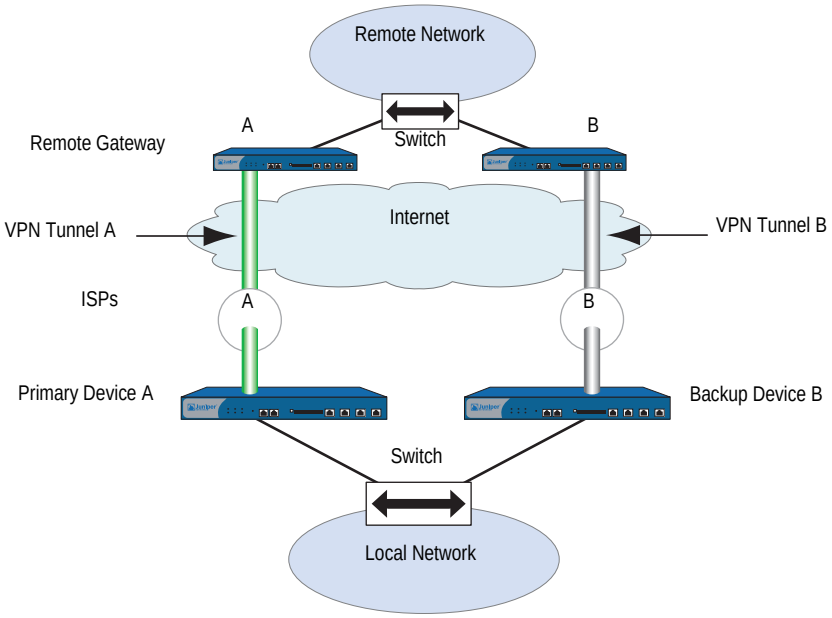
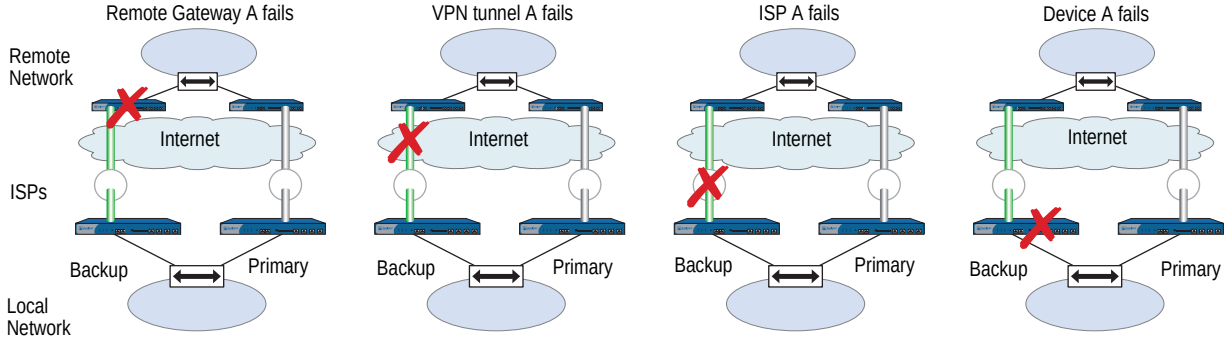


Figure 36 shows possible VPN tunnel failure scenarios.

Figure 36: VPN Tunnel Failure



In Figure 37, you configure two VPN tunnels, one for each of two security devices in an NSRP cluster. Then you configure both devices to track the IP address of two servers at the remote end of the tunnel: 10.2.2.50 and 10.2.2.60.

NOTE: The configuration of the two tunnels on the devices at the remote site is not included in this example. For more information, see "Cabling and Configuring NSRP-Lite" on page 104.

You configure each VPN tunnel as routing-based and bind it to an unnumbered tunnel interface named *tunnel.1*. Both tunnels use a preshared key (the keys are different for the two tunnels in this example, but they can also be identical). Phase 1 negotiations are in Main mode, and you enable replay protection for Phase 2 negotiations. You use the security level predefined as "Compatible" for both Phase 1 and Phase 2 proposals. You also enable VPN monitoring with the rekey option. (For more information about routing-based VPN tunnels, see *Volume 5: Virtual Private Networks*.)

NOTE: The four Phase 1-compatible security level proposals are pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5. The four Phase 2-compatible security level proposals are nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5.

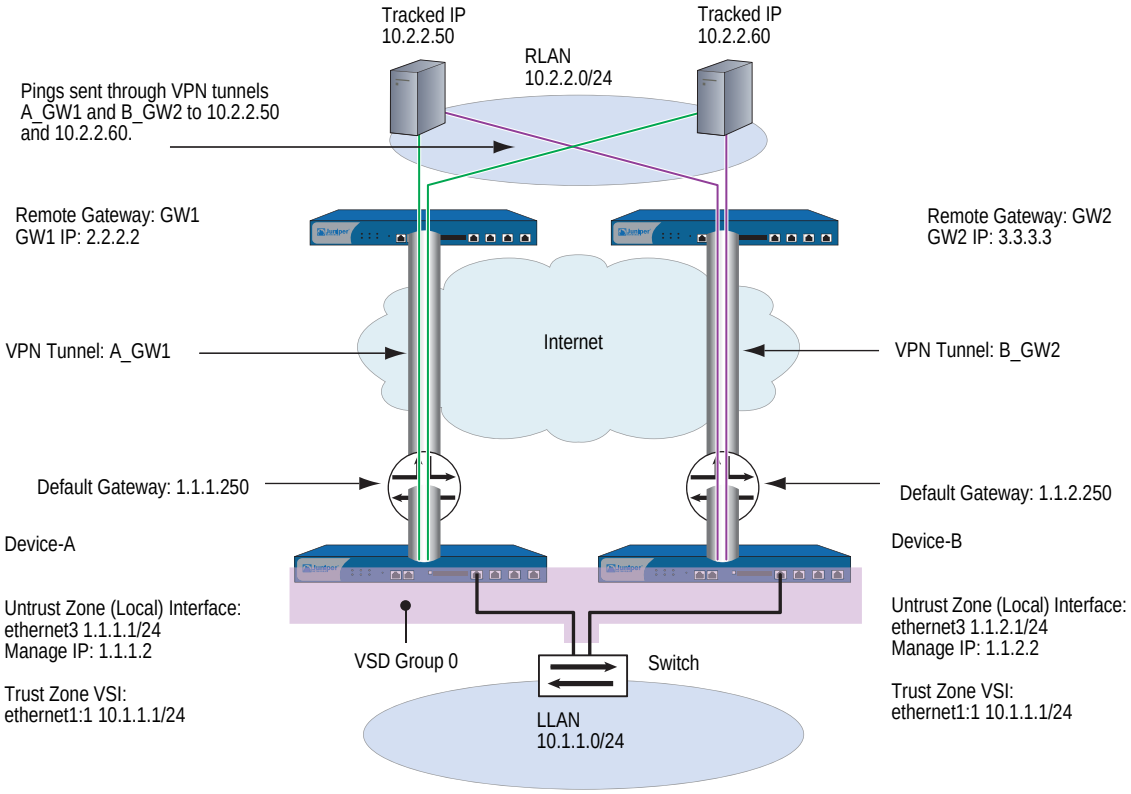
The settings you define for each tracked address are as follows:

- Server at 10.2.2.50
  - Interval: 10
  - Threshold: 5
  - Weight: 16
- Server at 10.2.2.60
  - Interval: 10
  - Threshold: 5
  - Weight: 16

Not receiving a ping response after five consecutive attempts to one of the servers is considered a failed attempt and contributes a weighted value of 16 toward the total failover threshold.

Because the device failover threshold is 31, both tracked IP addresses must fail before a device failover occurs. If you are not willing to tolerate that amount of failure, you can lower the threshold to a more acceptable level.

Figure 37: IP Tracking Through VPN Tunnels



WebUI (Device-A)

1. VPN Tunnel (Device-A)

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: LLAN
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.0/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: RLAN
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.0/24
Zone: Untrust

Network > Interfaces > Tunnel IF New: Enter the following, then click **OK**:

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (select)
Interface: ethernet3 (trust-vr)

NOTE: The source interface must be in the same virtual routing domain to which the tunnel interface is bound; in this case, the trust-vr. The unnumbered tunnel interface borrows the IP address of the specified security zone interface.

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: A_gw1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (select)
    Gateway Name: gw1
    Type: Static IP (select), Address/Hostname: 2.2.2.2
Preshared Key: h1p8A24nG5
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible
Replay Protection: (select)
Bind to: Tunnel Interface: tunnel.1
Proxy-ID: (select)
  Local IP / Netmask: 10.1.1.0/24
  Remote IP / Netmask: 10.2.2.0/24
  Service: ANY
VPN Monitor: (select)
  Source Interface: Default
  Destination IP: 2.2.2.2
  Optimization: (clear)
  Rekey: (select)

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 10.2.2.0/24
Gateway: (select)
    Interface: tunnel.1
    Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (select)
    Interface: ethernet3
    Gateway IP Address: 1.1.1.250

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), LLAN
Destination Address:
    Address Book Entry: (select), RLAN
Service: ANY
Action: Permit
Position at Top: (select)

2. **IP Tracking (Device-A)**
   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 10.2.2.50
   Method: Ping
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: tunnel.1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 10.2.2.60
   Method: Ping
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: tunnel.1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > Edit (for VSD: Device): Select **Enable Track IP**, and enter **31** in the Failover Threshold field.

3. **VPN Tunnel (Device-B)**
   Objects > Addresses > List > New: Enter the following, then click **OK**:

   Address Name: LLAN
   IP Address/Domain Name:
   IP/Netmask: (select), 10.1.1.0/24
   Zone: Trust

   Objects > Addresses > List > New: Enter the following, then click **OK**:

   Address Name: RLAN
   IP Address/Domain Name:
   IP/Netmask: (select), 10.2.2.0/24
   Zone: Untrust

   Network > Interfaces > Tunnel IF New: Enter the following, then click **OK**:

   Tunnel Interface Name: tunnel.1
   Zone (VR): Untrust (trust-vr)
   Unnumbered: (select)
   Interface: ethernet3 (trust-vr)

NOTE: The source interface must be in the same virtual routing domain to which the tunnel interface is bound; in this case, the trust-vr. The unnumbered tunnel interface borrows the IP address of the specified security zone interface.

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: B_gw2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (select)
Gateway Name: gw2
Type: Static IP (select), Address/Hostname: 3.3.3.3
Preshared Key: ih38CvE3g9
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible
Replay Protection: (select)
Bind to: Tunnel Interface: tunnel.1
Proxy-ID: (select)
Local IP / Netmask: 10.1.1.0/24
Remote IP / Netmask: 10.2.2.0/24
Service: ANY
VPN Monitor: (select)
Source Interface: Default
Destination IP: 3.3.3.3
Optimization: (clear)
Rekey: (select)

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 10.2.2.0/24
Gateway: (select)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 1.1.2.250

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), LLAN
Destination Address:
Address Book Entry: (select), RLAN
Service: ANY
Action: Permit
Position at Top: (select)

4. **IP Tracking (Device-B)**

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 10.2.2.50
   Method: Ping
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: tunnel.1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > New: Enter the following, then click **OK**:

   Track IP: 10.2.2.60
   Method: Ping
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: tunnel.1
   VSD Group ID: Device

   Network > NSRP > Monitor > Track IP > Edit (for VSD: Device): Select **Enable Track IP**, and enter **31** in the Failover Threshold field.

CLI

1. **VPN Tunnel (Device-A)**

```
set address trust LLAN 10.1.1.0/24
set address untrust RLAN 10.2.2.0/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set ike gateway gw1 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    h1p8A24nG5 sec-level compatible
set vpn A_gw1 gateway gw1 replay sec-level compatible
set vpn A_gw1 bind interface tunnel.1
set vpn A_gw1 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
set vpn A_gw1 monitor source-interface ethernet3 destination-ip 2.2.2.2 rekey
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set policy top from trust to untrust LLAN RLAN any permit
```

2. **IP Tracking (Device-A)**

```
set interface tunnel.1 track-ip ip 10.2.2.50
set interface tunnel.1 track-ip ip 10.2.2.50 interval 10
set interface tunnel.1 track-ip ip 10.2.2.50 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.50 weight 16
set interface tunnel.1 track-ip ip 10.2.2.60
set interface tunnel.1 track-ip ip 10.2.2.60 interval 10
set interface tunnel.1 track-ip ip 10.2.2.60 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.60 weight 16
set nsrp track-ip threshold 31
set nsrp track-ip
save
```

3. **VPN Tunnel (Device-B)**

```
unset nsrp config sync
set address trust LLAN 10.1.1.0/24
set address untrust RLAN 10.2.2.0/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set ike gateway gw2 ip 3.3.3.3 main outgoing-interface ethernet3 preshare
    ih38CvE3g9 sec-level compatible
set vpn B_gw2 gateway gw2 replay sec-level compatible
set vpn B_gw2 bind interface tunnel.1
set vpn B_gw2 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
set vpn B_gw2 monitor source-interface ethernet3 destination-ip 3.3.3.3 rekey
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.2.250
set policy top from trust to untrust LLAN RLAN any permit
```

4. **IP Tracking (Device-B)**

```
set interface tunnel.1 track-ip ip 10.2.2.50
set interface tunnel.1 track-ip ip 10.2.2.50 interval 10
set interface tunnel.1 track-ip ip 10.2.2.50 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.50 weight 16
set interface tunnel.1 track-ip ip 10.2.2.60
set interface tunnel.1 track-ip ip 10.2.2.60 interval 10
set interface tunnel.1 track-ip ip 10.2.2.60 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.60 weight 16
set nsrp track-ip threshold 31
set nsrp track-ip
save
```

Index

L

M

N

O

P

R

S

V