Application Note

High Availability at the Central Site Edge

Daniel Backman

Alan Sardella
Contents

Contents ..................................................................................................................................................2
Executive Summary ..............................................................................................................................3
Overview of Benefits .............................................................................................................................4
Traditional Switch Block Mesh ...........................................................................................................4
Routed Edge Resiliency .........................................................................................................................6
  Configuration Checklist ......................................................................................................................8
  Virtual Security Interface Configuration ...........................................................................................8
  Enable VSD-Less Clusters ..................................................................................................................8
  Ensure Correct Next-Hop Information ..............................................................................................8
  Directly Connect Inter-Router Links ..................................................................................................9
  Configure Link Costs ..........................................................................................................................9
  Prevent Asymmetric Routing in Stateful Devices ..............................................................................10
  Mixing Failover Protocols ................................................................................................................11
Conclusion ............................................................................................................................................11
Appendix A: Background on NSRP Technology and Terminology ......................................................12
  Virtual Security Domain ....................................................................................................................12
  Virtual Security Interface ..................................................................................................................13
  Synchronization ................................................................................................................................13
  VSD-Less Clusters .............................................................................................................................13
Appendix B: Configuration for Routed Edge Resiliency ......................................................................14
  Netscreen-1 (ScreenOS) .....................................................................................................................14
  Netscreen-2 (ScreenOS) .....................................................................................................................15
  External Router A (JUNOS) ..............................................................................................................16
  External Router B (JUNOS) ..............................................................................................................16
  Internal Router A (JUNOS) ...............................................................................................................16
  Internal Router B (JUNOS) ...............................................................................................................17
Executive Summary

The Central Site Edge, where the enterprise meets the WAN or Internet, contains critical requirements, in terms of both security (from intrusion and denial of service, among other concerns) and high availability. Juniper Networks provides this area with a variety of high-availability solutions. The two most common ones are as follows:

- Traditional Switch Block Mesh
- Routed Edge Resiliency

This application note briefly describes the Traditional Switch Block Mesh and then details the Routed Edge Resiliency solution. The Traditional Switch Block Mesh will be familiar to most network engineers in the enterprise, since network architects have often used Layer 2 switches in this way, allowing the multitude of links to provide fault protection in case of failure.

Routed Edge Resiliency is a newer option, specific to Juniper Networks, that has some unique advantages. This solution employs routers and security systems in a configuration that eliminates the layer of Ethernet switches commonly used in the edge, and enhances availability and security at a lower TCO by fostering a simplified design and operation.

Routed Edge Resiliency takes advantage of the routing functionality within Juniper Networks NetScreen firewalls, and simplifies the design by providing routed connectivity instead of a switched mesh. It uses Open Shortest Path First (OSPF) between the security gateways and the Customer Edge (CE) routers, and NetScreen Redundancy Protocol (NSRP) to ensure that hosts can always reach the routers. Juniper Networks firewalls support this solution with OSPF.

Both of these high-availability options provide stateful failover on the order of 1 to 4 seconds; the main difference between them lies in the operational costs. The pros and cons of these solutions are discussed here. Of course, Juniper Networks supports both solutions, as well as other high-availability configurations that can be adapted to any customer topology at the Central Site Edge.
Overview of Benefits

The WAN module in the Central Site Edge has critical requirements for enforcement of security (from both intrusion and denial of service) and availability, as well as high performance. Two high-availability solutions for the edge are discussed in this application note:

- Traditional Switch Block Mesh
- Routed Edge Resiliency

The main goal of a redundant network topology is to continue to forward user traffic, despite the failure of one or more links or nodes in the network. Both solutions address this requirement with failover on the order of 1 to 4 seconds.

The Traditional Switch Block Mesh is familiar to many network administrators and has been in use for some time. In some cases, this solution may allow you to utilize a switched infrastructure that is already in place at the Central Site Edge.

Routed Edge Resiliency does not require switches or corresponding rack space (if you have switches in your existing Central Site Edge, you can redeploy them). There are several potential operational savings to be derived from lower heat and power requirements, less complex management considerations, and the fact that there’s no switch software to configure, maintain, or upgrade. There are fewer nodes to maintain and thus fewer troubleshooting errors - the most common single cause of network downtime. The simplicity of Routed Edge Resiliency ultimately means a lower mean time to repair (MTTR), which naturally results in greater uptime.

By pushing failure detection and correction into a domain that is solely routed, Routed Edge Resiliency allows more intelligent use of network resources through direct routing protocol interaction between routers without intervening switches. It also moves the security intelligence closer to the provider edge, which decreases the number of devices that hackers can potentially compromise, especially with denial of service (DoS) attacks. In addition, by eliminating the Layer 2 switches, this solution presents fewer potential points of failure (eliminating two devices and several links in a single connection domain) and a simplified logical topology (no Spanning Tree Protocol).

Although the Routed Edge Resiliency model clearly has operational advantages over the Traditional Switch Block Mesh, the performance of Juniper Networks J-series and M-series routers will allow for security configurations that improve uptime, no matter which configuration is chosen. The perimeter M-series router is the first layer of defense in a layered security approach or “defense in depth.” Firewall, VPN, intrusion detection and prevention, and antivirus provide additional layers of security.

Traditional Switch Block Mesh

At the Central Site Edge, network architects have often used Layer 2 switches to form a hierarchical mesh, with the intention of letting the multitude of links provide fault protection in case of failure. For this basic high-availability solution, consider the configuration shown in Figure 1.
The capital expenditures for this solution would be as follows:

- 2 routers
- 2 Juniper Networks NetScreen security systems
- 4 switches

The operational expense is potentially higher, since there are extra devices and links to maintain.

This configuration is traditional and familiar, and there is no potential for asymmetric routing\(^1\) since only one of the NetScreen security devices is active at a time. There is no dynamic routing involved. There are potentially few extra switches to maintain, and there

---

\(^1\) This is a phenomenon in which traffic in one direction of a TCP connection travels through one firewall, and traffic in the other direction travels through the other firewall.
are extra links tied up on the firewall.

While this solution does provide some degree of physical redundancy, it does so at a high cost, in terms of both capital equipment (for the links and the switches themselves) and operational expense (for the rack space, power, and maintenance of the equipment). Even discounting the cost, a switched solution is suboptimal: it can actually hamper the rapid detection and correction of failures by insulating Ethernet link failures from detection by the routers.

**Routed Edge Resiliency**

With Routed Edge Resiliency, the NetScreen firewalls seamlessly integrate into your routed mesh. OSPF manages path calculation through the network topology, and advertises routes between the WAN routers and the internal network. The firewalls are seamlessly integrated into the routing domain; if there is a topology change, OSPF dynamically changes the forwarding path from the primary to the secondary firewall.

In this configuration, the routing protocol handles the fault detection and correction. On the host side of the network, NetScreen Redundancy Protocol (NSRP) provides a service similar to Virtual Router Redundancy Protocol (VRRP) for keeping hosts connected to their gateways in case of link or gateway failure. NSRP also provides mechanisms for path failure detection, runtime state, and security policy synchronization.

The Routed Edge Resiliency solution allows more intelligent use of network resources than a switching-only switch solution, because it pushes failure detection and correction into a domain that is solely routed, and allows direct routing protocol interaction without intervening switches. It also moves the security intelligence closer to the provider edge, which decreases the number of devices available for hackers to attack.

Each of the routers outside the firewall is a member of an OSPF area; failure detection and rerouting are controlled by OSPF. The firewalls run the NSRP protocol to replicate sessions between devices, and a VSD-Less cluster configuration (see Appendix A) for Active/Active NSRP operation. In this configuration, OSPF calculates path routes around failures, and NSRP is used for redundancy and to synchronize firewall state and security policies.

By eliminating the switches, this solution also offers fewer potential points of failure (eliminating two devices and several links in a single connection domain), and a simplified logical topology and control plane (no need for Spanning Tree Protocol). The link shown at the top of Figure 2 (between the edge routers) would make the cross links optional, since there would be a backup path without them. However, if the routers are customer premises equipment (CPE) devices, provided by two separate service providers (A and B), then the service providers might object to this connection.

---

2 In a VSD-Less cluster mode, all members of the firewall cluster in NSRP keep their interfaces up, and all OSPF adjacencies remain in FULL state during normal operation. For more information on the VSD-Less configuration, see Appendix A: Background on NSRP Technology and Terminology.
High Availability at the Central Site Edge

Figure 2: Routed Edge Resiliency

Note: The security policies in this application note are kept as simple as possible: basic traffic policies are configured between the “trust” and “untrust” zones. If you need to perform Network Address Translation (NAT) operations or terminate VPNs on the firewall, there are additional complexities due to the routing of return traffic. To support these features, you need a “mixed mode NSRP” environment. Details on how to configure for NAT and VPN termination are beyond the scope of this application note.

It is important to recognize the stateful nature of this rapid failover. Firewalls need up-to-date state information; without a stateful synchronization protocol between the two firewalls, a topology change would result in the loss of existing connections through the firewalls. To support seamless failover, the backup device maintains correct session state information, so it can correctly forward user streams without interruption. If user sessions were not synchronized, users would have to reinitiate Transmission Control Protocol (TCP) sessions or User Datagram Protocol (UDP) flows, and the failover would cause service interruption.

Juniper Networks supports this type of session replication using the NetScreen Redundancy Protocol (NSRP) on its NetScreen 200, 500, ISG 2000, and NetScreen 5000 firewall products. While a complete discussion of NSRP is outside the scope of this document, there are a few important concepts to understand when configuring a redundant environment with NetScreen firewalls. For further information on NSRP and related concepts, see Appendix A: Background on NSRP Technology and Terminology.
High Availability at the Central Site Edge

Configuration Checklist

The following table provides a checklist for both the NSRP and OSPF configuration for Routed Edge Resiliency.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Checklist Options</th>
</tr>
</thead>
</table>
| **NSRP** | Do not use Virtual Security Interfaces (VSIs) for OSPF adjacencies.  
|          | Do not use Virtual Security Domains (VSDs); use VSD-Less cluster.  
|          | Configure a VSD-Less cluster with Non-VSI Real-Time Object Sync.  
|          | Use `set arp always-on-dest` to ensure correct next-hop information. |
| **OSPF** | There is no routed link between firewalls (not in OSPF topology).  
|          | Do not allow asymmetric routing.  
|          | Do not enable equal-cost multipath routing (ECMP).  
|          | Configure OSPF links as /30 subnets in point-to-point mode.  
|          | Configure link costs as appropriate, with same cost on both sides of each link. |

Virtual Security Interface Configuration

OSPF neighbor relationships should not be run on a VSI. OSPF assumes that the interface IP addresses of neighboring routers are fixed, and are mapped to specific router IDs. Running an OSPF neighbor relationship on a virtual address can cause problems (such as interrupting the neighbor state machine) on a failover. To advertise the VSI’s subnet to the routing domain, add the VSI to OSPF as a passive interface.

Enable VSD-Less Clusters

To enable NSRP in a VSD-Less cluster mode, issue the following ScreenOS commands.

```plaintext
*** SET CLUSTER ID ***
set nsrp cluster id 1
set nsrp rto-mirror sync
*** KEY TO VSD-LESS STATE SYNCHRONIZATION ***
set nsrp rto-mirror session non-vsi
unset nsrp vsd-group id 0
```

Unsetting VSD 0 and setting `rto-mirror sync` and `rto-mirror session vsi` will put the firewall into a mode wherein you can keep all your routing protocol adjacencies active, while still synchronizing state (sessions).

Ensure Correct Next-Hop Information

When using VSD-Less clusters in a routed environment, next-hop Message Authentication Code (MAC) addresses on a given session will be different on each NSRP node. Some MAC
addresses can be replicated with session information. The command-line interface (CLI) command `set arp always-on-dest` forces the device to update next-hop MAC addresses for new sessions. Without this command, traffic can be sent to the wrong MAC address and may be blackholed.

Directly Connect Inter-Router Links

On all routers and NetScreen security systems, each link between devices should be configured as a separate IP network. A 30-bit or 31-bit subnet mask can be used to minimize address usage. This allows OSPF to see each link between routers as a separate network, and provides a topology with multiple Layer 3 failover paths. It also speeds failure detection, because a link failure will immediately tear down an OSPF neighbor relationship and force the protocol to reroute around the failure without delay. This requires that links between devices be directly connected and that they do not traverse an intermediary device (such as an Ethernet switch). Without this configuration, OSPF may not recover from a failure until the neighbor dead interval expires (default 40 seconds).

Cross links (for example, links between Router-A and Firewall-2 in the example) may or may not be used, depending on customer needs. Using them will ensure that traffic stays on the same firewall after a link-based topological change. Keeping traffic on the same firewall is desirable for the following reasons:

- Screening (e.g., for DoS attacks) is preserved.
- Application-level gateway (ALG) state is preserved.
- The full TCP handshake is not interrupted when new sessions are started.

When using the additional cross links, however, the interfaces should be added as separate point-to-point links in OSPF, and should be a member of the Trust or Untrust zones. NetScreen’s zone model for security policy makes this multiple interface failover possible, allowing a traffic path to switch to a new interface without impacting existing security policy configuration.

In keeping with OSPF best practices, each OSPF router must have a unique router ID. It can also be useful to configure a loopback interface with a unique host IP address (32-bit subnet mask). This should be the OSPF router ID, which can then be added as a passive interface in the OSPF area. This technique makes it easy to locate a router generating a link-state advertisement (LSA) into the OSPF topology.

Configure Link Costs

OSPF link costs must be used to control routing paths in a deterministic manner, so as to eliminate the possibility of asymmetric routing. Asymmetric routing is not supported through an NSRP environment.

As already described, it is important to guarantee that traffic will not be forwarded asymmetrically in this OSPF environment. OSPF costs can be used to control routing paths.

---

3 However, route paths to different zones will impact policy and will interrupt traffic.

4 In asymmetric routing, a connection’s traffic in one direction may be flowing through a different firewall than the traffic going the other direction. This can cause several major problems, including interference with the TCP handshake, incorrectly blocked traffic, and interference with ALG operation.
in a deterministic manner. Figure 3 shows two topologies with appropriate OSPF costs, which guarantee that traffic will traverse the same path in both directions. The advantage of using cross-links is that traffic will stay within the same firewall in the case of a single link failure.

Figure 3: OSPF Link Costs (With and Without Cross Links)

Costs are calculated on each link as traffic would logically exit that router. It is very important to configure the link cost on both sides of each link. Also, because default OSPF link costs can vary when using different equipment from multiple vendors (and sometimes even different equipment from the same vendor), Juniper Networks recommends that all OSPF link costs within the area that contains the NetScreen firewall cluster be manually configured.

Note: The High Availability (HA) link between the two firewalls in the cluster is used only for NSRP communication. The HA link is not part of the OSPF topology, does not have an IP subnet, and is not used for IP forwarding. In some NSRP scenarios, it will be used for data path forwarding,\(^5\) but not in a VSD-Less cluster.

Prevent Asymmetric Routing in Stateful Devices

---

\(^5\) Data path forwarding is a processor-based technique to forward traffic received on a backup device to the master device over an HA link.
IP routers are traditionally stateless devices, which forward all traffic according to the same criteria. However, as a network security device, a NetScreen security system performs stateful forwarding; state information such as the TCP connection is maintained. In a stateful device, a data-plane forwarding decision on a packet depends on that of previous related packets (for example, a SYN-A CK must follow a SYN in the opposite direction).

In a NetScreen security system, all traffic is characterized into a bidirectional flow. Each flow represents a specific protocol connection between two endpoints. In standard traffic handling, Layer 2-4 criteria define the traffic flow; in higher level processing (such as in application-level gateways or Deep Inspection), additional protocol state is tracked.

In order to correctly forward traffic, all protocol state must match a given flow in the firewall. In most cases, traffic will flow bidirectionally through the same device, and all flow information will match the protocol state tracked by the firewall.

NSRP is designed to maintain symmetric forwarding paths. In an HA pair, the primary device will be responsible for forwarding traffic in two directions, while the backup device will not actively forward traffic. However, interior gateway routing protocols like OSPF are designed for path calculation in a standard routed environment. Since most routers process IP traffic in a stateless fashion, these protocols are designed to allow asymmetric forwarding paths and equal cost multipath (ECMP) routing.

**Note:** A symmetric traffic flows can interfere with normal traffic inspection within the firewalls, and user traffic will be impaired. **When using OSPF, it is particularly important to verify that link costs are set symmetrically, so that traffic always flows on the same path, through the same firewall, in both directions. In addition, Juniper Networks recommends that ECMP not be used in conjunction with stateful devices.**

**Mixing Failover Protocols**

Using multiple redundancy protocols and configurations (e.g., using redundant interfaces for link failover between two separate paths) in the same environment is not recommended. This practice could conflict with standard OSPF failover. However, using aggregate interfaces (802.3ad link aggregation, or Fast/ Gig EtherChannel) between two OSPF neighbors is supported, and will protect adjacencies from a single link failure.

**Conclusion**

The Juniper Networks Routed Edge Resiliency solution addresses the requirements of customers with critical network connectivity requirements in these areas:

- **Economy:** The solution saves multiple tens of thousands of dollars over competing solutions, with increased savings in operational costs over time.
- **Security:** Purpose-built security systems offer a broad set of firewall and DoS protection, IPsec VPN, and traffic-management capabilities.
- **High Availability:** The intelligence and speed of directly connected routing protocol interaction are combined with the broad capabilities of the NSRP protocol.
- **Multiservice Capability:** The solution provides high-performance, standards-based quality of service (QoS) features, and the richest set of VPN offerings in the industry.

By eliminating unnecessary redundancy while enhancing network availability, this solution improves customer control and decreases costs. This solution has been proven in the Juniper...
Appendix A: Background on NSRP Technology and Terminology

NSRP is designed to make a firewall pair (or cluster) appear to operate as a single device. A master/backup protocol, NSRP allows two devices to synchronize their configurations and operations. In the event of a failover, the backup device seamlessly picks up where the master device left off, without disrupting transit traffic or services (like VPNs) terminating on the device.

To support this seamless failover, NSRP must coordinate multiple functions within each firewall. This includes virtual IP support, as well as the synchronization of real-time objects (RTO) such as the following:

- Layer 3/4 session information
- IPsec Security Associations
- Cryptographic data (session keys, digital certificates, private keys)

As a redundancy protocol for firewalls, NSRP must support firewall/VPN functions, as well as standard IP routing. Since Juniper Networks NetScreen firewalls provide stateful inspection and VPN service termination, NSRP synchronizes this information to provide stateful failover within the cluster.

There are three important components within NSRP:

- The Virtual Security Interface (VSI)
- The Virtual Security Domain (VSD)
- Synchronization

These are discussed in the following sections, along with a fourth component, the VSD-Less cluster, which enables the Routed Edge Resiliency solution described in this application note.

Virtual Security Domain

A VSD is a collection of objects within ScreenOS that are replicated from a master to a backup node within an NSRP cluster. High-end NetScreen security systems (such as the NetScreen 500, NetScreen 5000 and ISG 2000) can support multiple VSDs. This allows more than one collection of real-time objects (RTO) to be synchronized within the same firewall cluster.

By default, all interfaces are in VSD 0. However, when using multiple VSDs, interfaces (logical or physical) are configured to be part of a specific VSD. Each VSI is mapped to a specific VSD. Then, all configuration, session, or security objects that reference that interface or VSI are considered part of that VSD.

In each Virtual Security Domain, a separate master/backup state machine is run. RTOs are replicated from the master to backup cluster members. This “multiple VSD” support allows Active/Active load-sharing configurations to be supported on high-end security systems, effectively partitioning objects into separate failover domains. In most implementations, however, an NSRP cluster will have a single VSD with one master and one primary backup node.
Virtual Security Interface

The VSI provides the virtual IP component to NSRP. To external devices, the VSI works much like the virtual IP support in Hot Standby Routing Protocol (HSRP) or VRRP.

To ensure failover between Layers 2 and 3, the VSI is mapped to a logical MAC address. Upon failover, traffic is rerouted through the new master device. In the ScreenOS CLI, a VSI is denoted with a colon (e.g., Ethernet2/1:1 is a VSI that maps traffic into VSD 1 on the interface Ethernet2/1).

The VSI provides additional functions. Since real-time objects (such as user sessions) in a VSD cluster must be associated with the appropriate domain, a VSI is located within a specific VSD, but any objects that reference the VSI are then associated with the appropriate failover domain. In the above example of a VSI (Ethernet2/1:1), any sessions that reference this virtual interface are a part of VSD id 1.

In a redundant NSRP configuration, VSI usage is analogous to what you would expect from VRRP or HSRP. The VSI should be deployed at the edge of a routing domain, where the firewall is a redundant first-hop router for end nodes.

Synchronization

NSRP ensures stateful failover (for active user traffic, and services between VPNs) by continuously replicating (synchronizing) RTOs and configuration information between firewalls in a cluster. This information is sent across special HA links between firewalls.

The synchronization function is defined within the VSD, and is governed by a state machine that elects a master device. Within each VSD, NSRP monitors tracking and health information between all members of a cluster, and determines the master. Once elected, the master node replicates relevant RTOs and configuration information to the backup nodes.

Actual failover is controlled by OSPF, and has no dependencies or visibility into NSRP. Although NSRP supports failover control, its failover model would interfere with the HA solution described in this application note. Thus, a new mode was introduced into NSRP, where there is no VSD, and (as a result) no master/backup state machine. This is known as a VSD-Less cluster.

VSD-Less Clusters

When NSRP uses a standard VSD cluster, it can only replicate objects from a master to a backup node. But when running OSPF, both nodes must be active, as OSPF may choose to change the active traffic path without notifying NSRP to failover to a different master node.

In a standard Active/Passive NSRP configuration, interfaces on the backup NetScreen node are down, and thus the backup node cannot maintain active OSPF adjacencies. In an NSRP failover, the backup node must first transition to NSRP master state and then establish OSPF neighbor adjacencies and recalculate routes, before it can begin forwarding traffic.

While session objects may be pre-replicated to the backup node, the node will not actively forward traffic until OSPF has successfully converged. Using default timers in standard broadcast mode, this can take over 40 seconds due to Designated Router (DR) election – an unacceptable failover time.
Using VSD-Less cluster mode, NSRP allows all cluster members to keep interfaces up and replicate RTOs in both directions. Since neither device is in backup mode, all interfaces remain active, and OSPF adjacencies are all in full state during normal operation.

It's important to note that, in a VSD-Less mode, NSRP is only replicating RTOs, not operating in a standard master/backup fashion. This special NSRP mode is designed to support session replication for transit traffic in an OSPF environment. It does not support all NSRP functions, like redundant termination of VPN tunnels, as in normal NSRP VSD modes.

Appendix B: Configuration for Routed Edge Resiliency

Configurations for Routed Edge Resiliency follow. Figure 4 shows the topology as tested, which will match these configurations.

Figure 4: Topology as Tested

```
set hostname NetScreen-1
set interface "ethernet2/1" zone "untrust"
set interface "ethernet2/5" zone "trust"
set interface "loopback.1" zone "trust"
set interface ethernet2/1 ip 10.1.4.2/24
set interface ethernet2/5 ip 10.2.4.1/24
```
set interface loopback.1 ip 10.3.255.1/32
set nsrp cluster id 1
set nsrp rto-mirror sync
set nsrp rto-mirror session non-vsi
unset nsrp vsd-group id 0
set arp always-on-dest
set router-id 10.3.255.1
set vrouter trust-vr protocol ospf
set interface ethernet2/1 protocol ospf area 0.0.0.0
set interface ethernet2/1 protocol ospf enable
set interface ethernet2/5 protocol ospf area 0.0.0.0
set interface ethernet2/5 protocol ospf enable
set interface ethernet2/5 protocol ospf cost 10
set interface loopback.1 protocol ospf area 0.0.0.0
set interface loopback.1 protocol ospf passive
set interface loopback.1 protocol ospf enable
set vrouter trust-vr protocol ospf enable
set policy id 1 from Trust to Untrust any any any permit

Netscreen-2 (ScreenOS)

set hostname NetScreen-2
set interface "ethernet2/1" zone "untrust"
set interface "ethernet2/5" zone "trust"
set interface "loopback.1" zone "trust"
set interface ethernet2/1 ip 10.1.5.2/24
set interface ethernet2/5 ip 10.2.5.1/24
set interface loopback.1 ip 10.3.255.2/32
set nsrp cluster id 1
set nsrp rto-mirror sync
set nsrp rto-mirror session non-vsi
unset nsrp vsd-group id 0
set arp always-on-dest
set router-id 10.3.255.2
set vrouter trust-vr protocol ospf
set interface ethernet2/1 protocol ospf area 0.0.0.0
set interface ethernet2/1 protocol ospf enable
set interface ethernet2/1 protocol ospf cost 25
set interface ethernet2/5 protocol ospf area 0.0.0.0
set interface ethernet2/5 protocol ospf enable
set interface ethernet2/5 protocol ospf cost 25
set interface loopback.1 protocol ospf area 0.0.0.0
set interface loopback.1 protocol ospf passive
set interface loopback.1 protocol ospf enable
set vrouter trust-vr protocol ospf enable
set policy id 1 from Trust to Untrust any any any permit
**External Router A (JUNOS)**

*Note: The original commands are seen with the `show | display set` command.*

```plaintext
set system host-name External-Router-A
set interfaces fe-0/0/1 unit 0 family inet address 10.1.1.2/24
set interfaces fe-0/0/2 unit 0 family inet address 10.1.3.1/24
set interfaces fe-0/0/3 unit 0 family inet address 10.1.4.1/24
set interfaces lo0 unit 0 family inet address 10.1.255.2/32
set routing-options static route 0.0.0.0/0 next-hop 172.19.116.1
set routing-options router-id 10.1.255.2
set protocols ospf area 0.0.0.0 interface fe-0/0/1.0 metric 10
set protocols ospf area 0.0.0.0 interface fe-0/0/2.0 metric 5
set protocols ospf area 0.0.0.0 interface fe-0/0/3.0 metric 10
set protocols ospf area 0.0.0.0 interface fe-0/0/0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0 passive
```

**External Router B (JUNOS)**

*Note: The original commands are seen with the `show | display set` command.*

```plaintext
set system host-name External-Router-B
set interfaces fe-0/0/1 unit 0 family inet address 10.1.2.2/24
set interfaces fe-0/0/2 unit 0 family inet address 10.1.3.2/24
set interfaces fe-0/0/3 unit 0 family inet address 10.1.5.1/24
set interfaces lo0 unit 0 family inet address 10.1.255.3/32
set routing-options router-id 10.1.255.3
set protocols ospf area 0.0.0.0 interface fe-0/0/1.0 metric 10
set protocols ospf area 0.0.0.0 interface fe-0/0/2.0 metric 5
set protocols ospf area 0.0.0.0 interface fe-0/0/3.0 metric 25
set protocols ospf area 0.0.0.0 interface fe-0/0/0.0 disable
set protocols ospf area 0.0.0.0 interface lo0.0 passive
```

**Internal Router A (JUNOS)**

*Note: The original commands are seen with the `show | display set` command.*

```plaintext
set system host-name Internal-Router-A
set interfaces fe-0/0/1 unit 0 family inet address 10.2.1.1/24
set interfaces fe-0/0/2 unit 0 family inet address 10.2.3.1/24
set interfaces fe-0/0/3 unit 0 family inet address 10.2.4.2/24
set interfaces lo0 unit 0 family inet address 10.2.255.2/32
set protocols ospf area 0.0.0.0 interface fe-0/0/0.0 disable
set protocols ospf area 0.0.0.0 interface fe-0/0/1.0 metric 10
set protocols ospf area 0.0.0.0 interface fe-0/0/2.0 metric 5
set protocols ospf area 0.0.0.0 interface fe-0/0/3.0 metric 10
```
Internal Router B (JUNOS)

**Note:** The original commands are seen with the `show | display set` command.

```plaintext
set system host-name Internal-Router-B
set interfaces fe-0/0/1 unit 0 family inet address 10.2.2.1/24
set interfaces fe-0/0/2 unit 0 family inet address 10.2.3.2/24
set interfaces fe-0/0/3 unit 0 family inet address 10.2.5.2/24
set interfaces lo0 unit 0 family inet address 10.2.255.3/32
set routing-options router-id 10.2.255.3
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface fe-0/0/0.0 disable
set protocols ospf area 0.0.0.0 interface fe-0/0/1.0 metric 10
set protocols ospf area 0.0.0.0 interface fe-0/0/2.0 metric 5
set protocols ospf area 0.0.0.0 interface fe-0/0/3.0 metric 25
```