Application Note

Configure Full Mesh VPN with OSPF using Single Tunnel Interface

Version 1.0

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Contents

Contents....2
Introduction....3
Included Platforms and ScreenOS....3
Overview....4
Network Diagram....5
Configuration Overview....5
Configuration Steps....6
Step 1: Create the tunnel interface....6
Step 2: Define the IKE Gateway....9
Step 3: Define the VPN Tunnel....15
Step 4: Configuring OSPF protocol....21
Step 5: Add Static Routes and Static NHTB entries....30
Step 6: Configure policy to allow traffic between sites....38
Verifying Configuration....46
Sample configuration....49

Introduction

Full mesh VPN is used for total redundancy between the Hub and Spoke VPN. Having a Hub and Spoke VPN with a point to multipoint might have a limited redundancy because the spokes have to pass through the hub firewall in terms of reaching any other spoke sites in the network. In other words, if the hub firewall is down all the spoke sites are down.

Configuring a Hub and Spoke with point to multipoint and full mesh VPN will overcome the limited redundancy problem as every site or every firewall will be "Hub and Spoke" to each other. So if one site is down the other sites can still communicate with other sites via point to point links. So, if a VPN between any 2 sites is down, the packet can be routed through a different site because of the full mesh configuration.

Included Platforms and ScreenOS

This application note demonstrates firewall setup on ScreenOS 5.4r8. However, it also applies to following ScreenOS version:

- ScreenOS 5.1
- ScreenOS 5.2
- ScreenOS 5.3
- ScreenOS 5.4
- ScreenOS 6.0

The product list includes the following:

- NS5000
- ISG1000/2000
- NS500/200/50/25
- SSG550m/550/320/350/140
- NS5GT
- SSG5/20

Overview

With OSPF, one gets the advantage of automatic routing updates for the reach-ability for specific networks at respective sites. Manually maintaining static route entries and Next Hop Tunnel Binding (NHTB) entries for the remote sites could add administrative overhead as the network grows. Using OSPF with full mesh VPN will override the administrative overhead in maintaining the static routes and NHTB entries for each site.

However, it is worth to noting that the setup can be restricted by a firewall system limitation: maximum number of dedicated VPN tunnels allowed.

	Max no. dedicated VPN tunnels allowed
NS5GT`	10
SSG5/20	25/40*
NS25	50/125*
SSG140	250
NS50	150/500*
SSG520	500
NS204/NS208	500/1000*
SSG550	1000
NS500	1000/5000*
ISG1000	1000/2000*
ISG2000	1000/10k*
NS5200/NS5400	25k

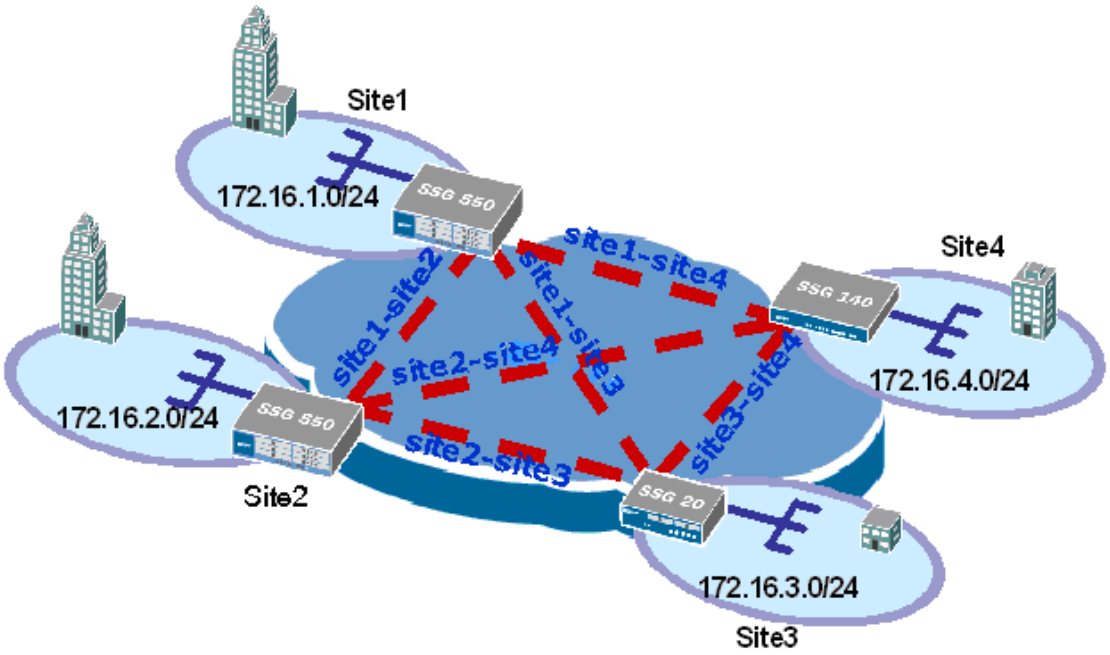
*for advanced model

The maximum number of VPN tunnels is not limited by the number of tunnel interfaces that you can create, but by either route table capacity or the maximum number of dedicated VPN tunnels allowed—whichever is lower. For instance, if your security device supports 4000 routes and 1000 dedicated VPN tunnels, you can create 1000 VPN tunnels and bind them to a single tunnel interface. If your security device supports 8192 routes and 10,000 dedicated VPN tunnels, then you can create over 8000 VPN tunnels and bind them to a single tunnel interface. To see the maximum route and tunnel capacities for your security device, refer to the relevant product data sheet at
http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/index.html

Network Diagram

Refer to Figure 1 below for Network Topology used for this configuration example.

Figure 1.



Configuration Overview

- Configure one tunnel interface on each firewall. This will be bound to multiple VPNs.
- The tunnel interface is required to assign a unique IP address, which is used in NHTB entries to find the specific gateways to reach specific networks.
- In this example, there will be 6 VPNs created:
  - site1-site2
  - site1-site3
  - site1-site4
  - site2-site3
  - site2-site4
  - site3-site4
- Enable OSPF on the VR, containing the interface connecting to the down stream router and the tunnel interface.
- Configure p2mp OSPF on the tunnel interface for populating the NHTB entries automatically.
- Enable VPN Monitor with Rekey option for remote VPN connectivity detection.
- Configure a policy to control traffic entering or pumping out to the remote sites, as well as transit traffic between different sites over the VPN network.

Note: Starting with ScreenOS 5.1, OSPF point to multipoint is supported, which is required for automatic population of the NHTB entries between firewalls as this is a full mesh VPN.

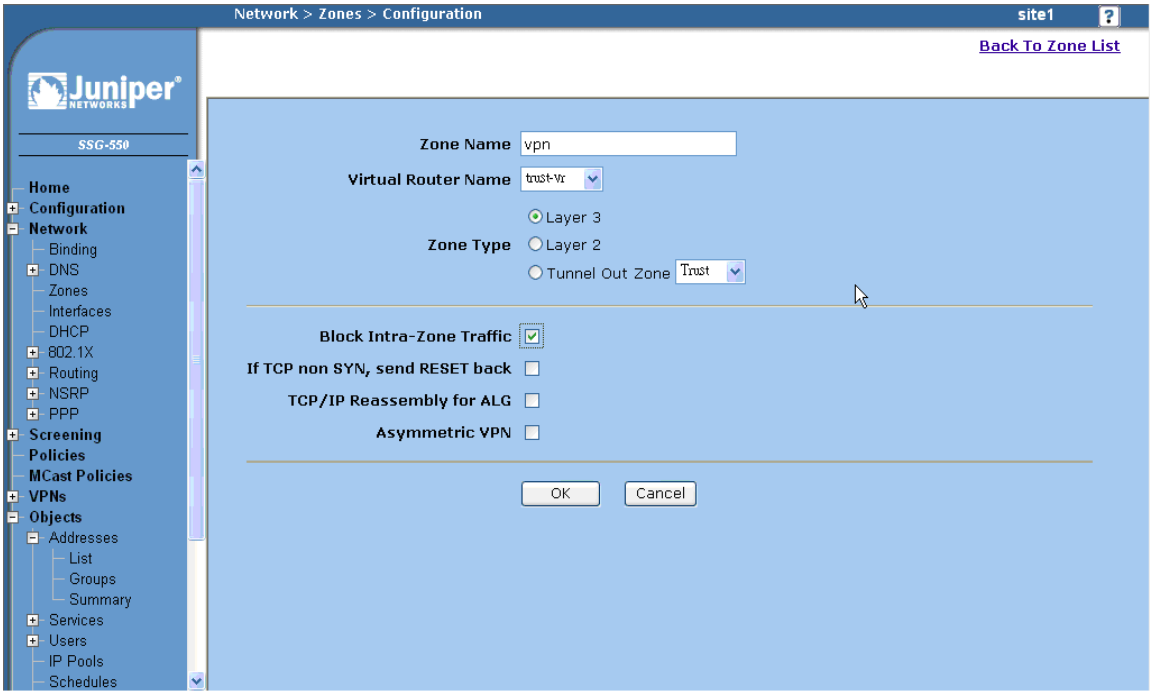
Configuration Steps

Step 1: Create the tunnel interface

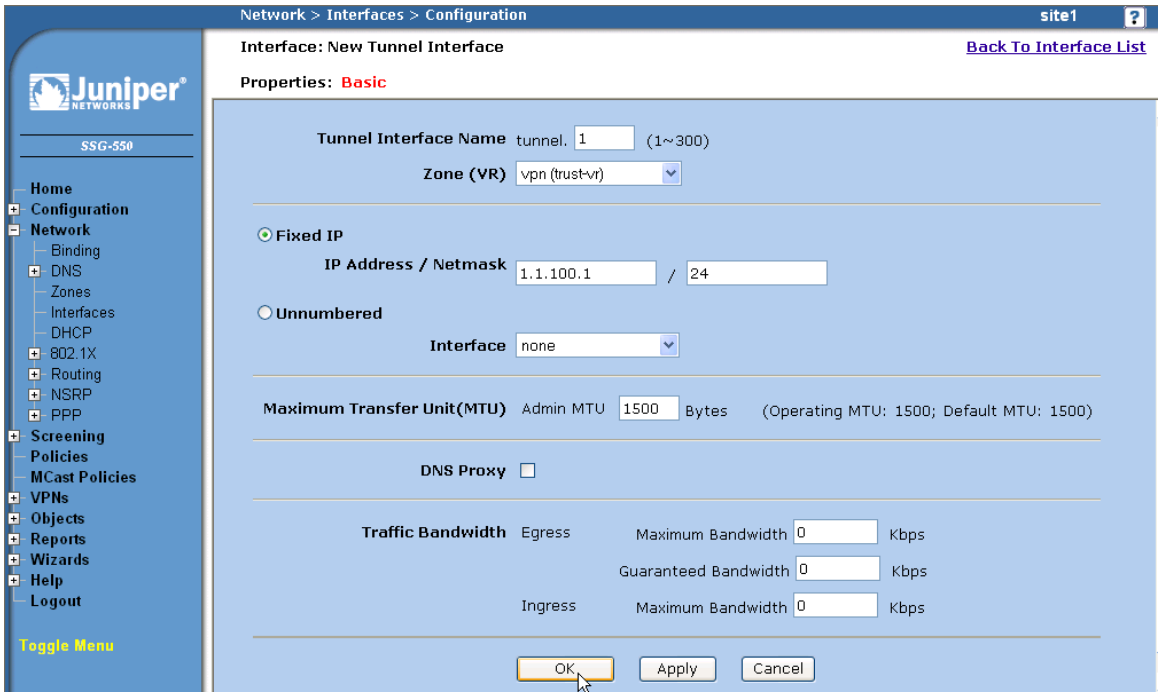
In configuring the tunnel interface the administrator selects the zone to which the tunnel interface will be bound and the IP address to use.

When a tunnel terminates in the *vpn* zone and the target network is in the *trust* zone, a permit or deny policy will be required to move the traffic from the *vpn* zone to the *trust* zone. If the tunnel is terminated on the trust side (i.e. the tunnel interface is created in the trust zone), traffic to/from the trust zone is allowed without a policy, unless an intra-zone policy is defined specifying another action.

Before creating the tunnel interface, create the *vpn* zone:



Then create the tunnel interface:



The WebUI and CLI 'Step 1' instructions for each firewall are as follows:

<u>WebUI:</u>

Site1 firewall

VPN zone:
- Select Network > Zones, select New
- Zone Name: vpn
- Block Intra-Zone Traffic: (selected)

Interface tunnel.1:
- Select Network > Interface
- Choose "Tunnel IF" and click New
- Tunnel Interface Name: tunnel.1
- Zone (VR): vpn (trust-vr)
- Fixed IP: (select), 1.1.100.1/24

Site2 firewall

VPN zone:
- Select Network > Zones, select New
- Zone Name: vpn
- Block Intra-Zone Traffic: (selected)

Interface tunnel.1:

Select Network > Interface
Choose "Tunnel IF" and click New
Tunnel Interface Name: tunnel.1
Zone (VR): vpn (trust-vr)
Fixed IP: (select), 1.1.100.2/24

Site3 firewall

VPN zone:
Select Network > Zones, select New
Zone Name: vpn
Block Intra-Zone Traffic: (selected)
Interface tunnel.1:
Select Network > Interface
Choose "Tunnel IF" and click New
Tunnel Interface Name: tunnel.1
Zone (VR): vpn (trust-vr)
Fixed IP: (select), 1.1.100.3/24

Site4 firewall

VPN zone:
Select Network > Zones, select New
Zone Name: vpn
Block Intra-Zone Traffic: (selected)
Interface tunnel.1:
Select Network > Interface
Choose "Tunnel IF" and click New
Tunnel Interface Name: tunnel.1
Zone (VR): vpn (trust-vr)
Fixed IP: (select), 1.1.100.4/24

CLI:

Site1 firewall

```
set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 1.1.100.1/24
```

Site2 firewall

```
set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 1.1.100.2/24
```

Site3 firewall

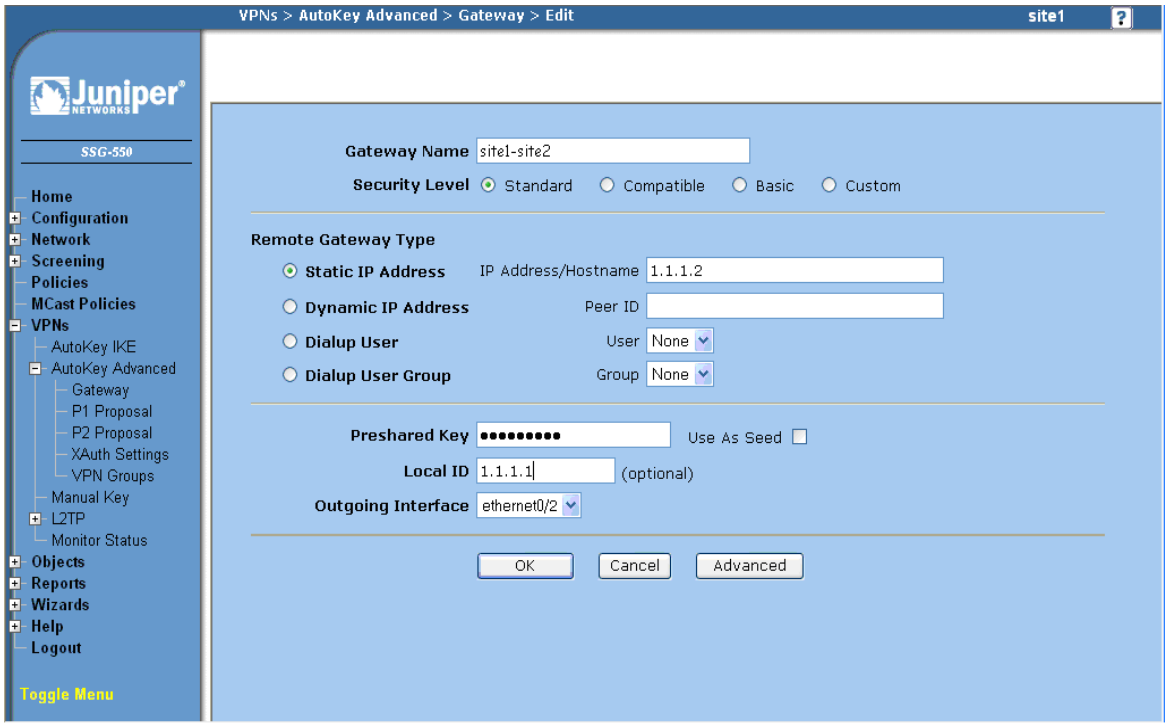
```
set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 1.1.100.3/24
```

Site4 firewall

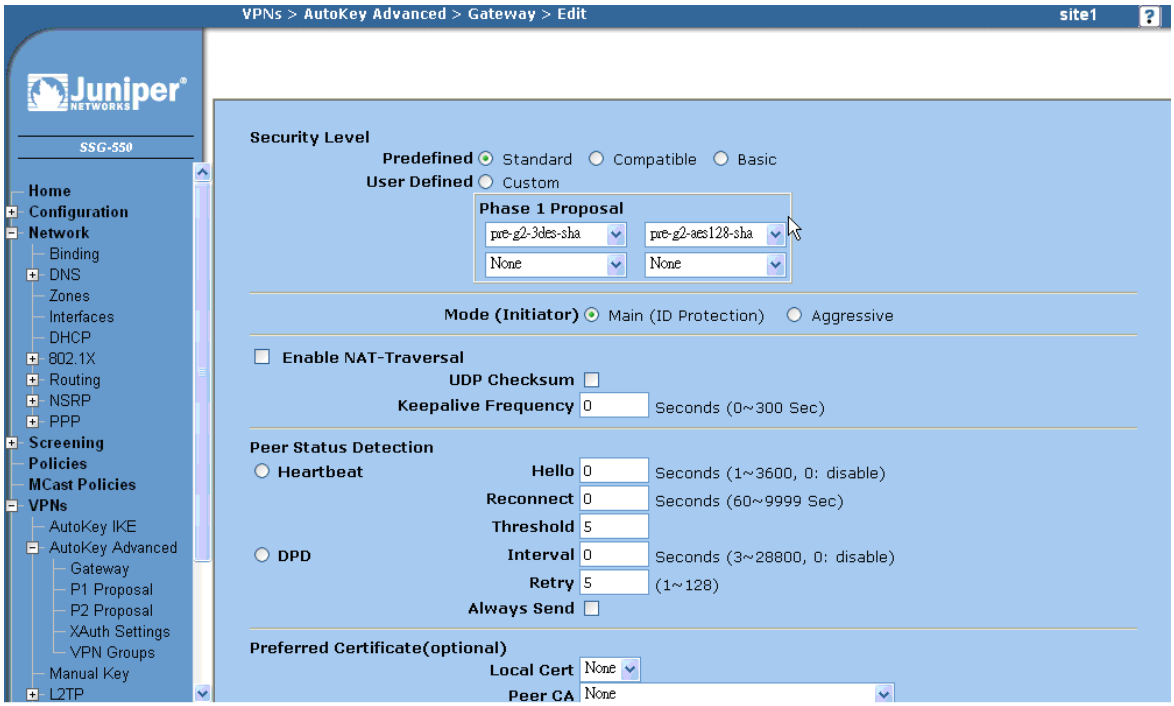
```
set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 1.1.100.4/24
```

Step 2: Define the IKE Gateway

The IKE gateway defines the type of tunnel at the peer location, the outgoing interface to use, the Phase 1 proposals to use, and the key-exchange method. An IKE gateway is configured for each VPN tunnel.



Click the Advanced button to see more configuration options.



When the configuration of the Proposals and Mode is completed, select Return button of the screen. Then select OK or Apply to save the information.

In creating the IKE Gateway, the following options were selected:

- Remote Gateway Type of “Static IP Address” was chosen since this is a LAN-to LAN VPN and both ends of the tunnel have statically assigned addresses.
- Preshared key of “netscreen” was configured at both ends of the tunnel.
- The “Outgoing Interface” is that interface used in order to gain access to the other end of the tunnel. In this application note, the interface in the untrust zone was used for the full mesh VPNs.
- Main Mode was selected as the key-exchange method. In a LAN-to-LAN VPN, Main Mode is the preferred method since it conceals the identities of the parties during the key exchange. In a dynamically assigned IP environment, Aggressive mode is used. In aggressive mode, IKE key exchanges are initiated without ID protection.

The WebUI and CLI 'Step 2' instructions for each firewall are as follows:

WebUI:

Site1 firewall

Site1 to Site2:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site1-site2
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.2
Preshare Key: netscreen
Local ID: 1.1.1.1
Outgoing Interface: ethernet0/2*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site1 to Site3:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site1-site3
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.3
Preshare Key: netscreen
Local ID: 1.1.1.1
Outgoing Interface: ethernet0/2*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site1 to Site4:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site1-site4
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.4
Preshare Key: netscreen
Local ID: 1.1.1.1
Outgoing Interface: ethernet0/2*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site2 firewall

Site2 to Site1:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site1-site2 (name was chosen to be same name of VPN configured on Site 1)
Seccurity Level: Standard

Static IP Address: (selected)
IP Address/Hostname: 1.1.1.1
Preshare Key: netscreen
Local ID: 1.1.1.2
Outgoing Interface: ethernet0/2*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site2 to Site3:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site2-site3
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.3
Preshare Key: netscreen
Local ID: 1.1.1.2
Outgoing Interface: ethernet0/2*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site2 to Site4:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site2-site4
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.4
Preshare Key: netscreen
Local ID: 1.1.1.2
Outgoing Interface: ethernet0/2*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site3 firewall

Site3 to Site1:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site1-site3 (name was chosen to be same name of VPN configured on Site 1)
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.1
Preshare Key: netscreen
Local ID: 1.1.1.3
Outgoing Interface: ethernet0/0*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site3 to Site2:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site2-site3 (name was chosen to be same name of VPN configured on Site 2)
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.2
Preshare Key: netscreen
Local ID: 1.1.1.3
Outgoing Interface: ethernet0/0*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site3 to Site4:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site3-site4
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.4
Preshare Key: netscreen
Local ID: 1.1.1.3
Outgoing Interface: ethernet0/0*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site4 firewall

Site4 to Site1:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site1-site4 (name was chosen to be same name of VPN configured on Site 1)
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.1
Preshare Key: netscreen
Local ID: 1.1.1.4
Outgoing Interface: ethernet0/0*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

Site4 to Site2:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site2-site4 (name was chosen to be same name of VPN configured on Site 2)
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.2
Preshare Key: netscreen
Local ID: 1.1.1.4
Outgoing Interface: ethernet0/0*
Select Advanced:
Mode (Initiator): Main (ID Protection)

Select Return and OK

Site4 to Site3:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:
Gateway Name: site3-site4 (name was chosen to be same name of VPN configured on Site 3)
Seccurity Level: Standard
Static IP Address: (selected)
IP Address/Hostname: 1.1.1.3
Preshare Key: netscreen
Local ID: 1.1.1.4
Outgoing Interface: ethernet0/0*
Select Advanced:
Mode (Initiator): Main (ID Protection)
Select Return and OK

CLI:

Site1 firewall

```
set ike gateway site1-site2 address 1.1.1.2 main local-id 1.1.1.1 outgoing-
interface ethernet0/2* preshare netscreen sec-level standard
set ike gateway site1-site3 address 1.1.1.3 main local-id 1.1.1.1 outgoing-
interface ethernet0/2* preshare netscreen sec-level standard
set ike gateway site1-site4 address 1.1.1.4 main local-id 1.1.1.1 outgoing-
interface ethernet0/2* preshare netscreen sec-level standard
```

Site2 firewall

```
set ike gateway site1-site2 address 1.1.1.1 main local-id 1.1.1.2 outgoing-
interface ethernet0/2* preshare netscreen sec-level standard
set ike gateway site2-site3 address 1.1.1.3 main local-id 1.1.1.2 outgoing-
interface ethernet0/2* preshare netscreen sec-level standard
set ike gateway site2-site4 address 1.1.1.4 main local-id 1.1.1.2 outgoing-
interface ethernet0/2* preshare netscreen sec-level standard
```

Site3 firewall

```
set ike gateway site1-site3 address 1.1.1.1 main local-id 1.1.1.3 outgoing-
interface ethernet0/0* preshare netscreen sec-level standard
set ike gateway site2-site3 address 1.1.1.2 main local-id 1.1.1.3 outgoing-
interface ethernet0/0* preshare netscreen sec-level standard
set ike gateway site3-site4 address 1.1.1.4 main local-id 1.1.1.3 outgoing-
interface ethernet0/0* preshare netscreen sec-level standard
```

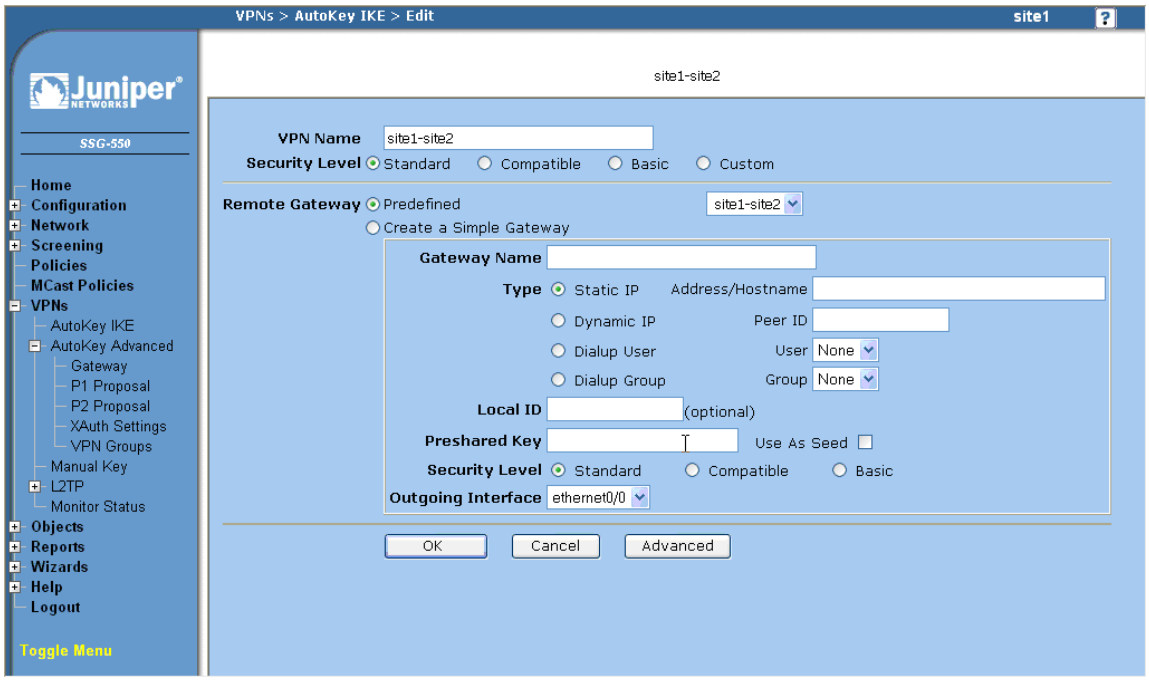
Site4 firewall

```
set ike gateway site1-site4 address 1.1.1.1 main local-id 1.1.1.4 outgoing-
interface ethernet0/0* preshare netscreen sec-level standard
set ike gateway site2-site4 address 1.1.1.2 main local-id 1.1.1.4 outgoing-
interface ethernet0/0* preshare netscreen sec-level standard
set ike gateway site3-site4 address 1.1.1.3 main local-id 1.1.1.4 outgoing-
interface ethernet0/0* preshare netscreen sec-level standard
```

*note interface name may varies depends on the assignment of interface for untrust zone.

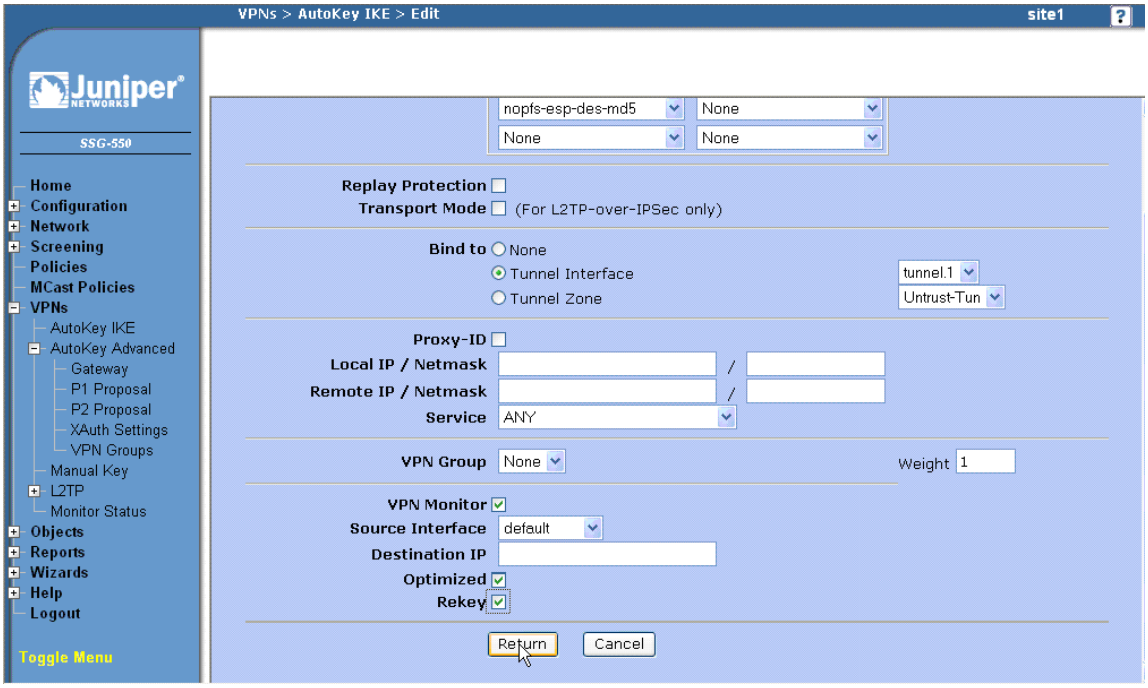
Step 3: Define the VPN Tunnel

The VPN Tunnel (or AutoKey IKE as it is called in Screen OS) defines the Phase 2 proposals, how the tunnel is to be bound, proxy ids, and the IKE Gateway to be associated with the VPN Tunnel.



In the example, site1-site2 is the name given to the tunnel from the Site1 device to the Site2 device. In the Remote Gateway section, use the pull down tab to select the predefined gateway created in the previous step.

Clicking the Advanced button displays more configuration options.



In the LAN-to-LAN VPN route-based tunnel, the Tunnel is bound to the tunnel interface created in step 1. In addition, VPN Monitor, Optimized, and Rekey are recommended to set up the tunnel without having to wait for user-originated VPN traffic.

The WebUI and CLI 'Step 3' instructions for each firewall are as follows:

<u>WebUI:</u>

Site1 firewall

Site1 to Site2:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site1-site2
Security Level: Standard
Remote Gateway: Predefined (selected), site1-site2 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site1 to Site3:

Select VPNs > AutoKey IKE, select New and enter following:

VPN Name: site1-site3
Security Level: Standard
Remote Gateway: Predefined (selected), site1-site3 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site1 to Site4:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site1-site4
Security Level: Standard
Remote Gateway: Predefined (selected), site1-site4 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site2 firewall

Site2 to Site1:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site1-site2
Security Level: Standard
Remote Gateway: Predefined (selected), site1-site2 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site2 to Site3:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site2-site3
Security Level: Standard
Remote Gateway: Predefined (selected), site2-site3 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site2 to Site4:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site2-site4

Security Level: Standard
Remote Gateway: Predefined (selected), site2-site4 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site3 firewall

Site3 to Site1:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site1-site3
Security Level: Standard
Remote Gateway: Predefined (selected), site1-site3 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site3 to Site2:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site2-site3
Security Level: Standard
Remote Gateway: Predefined (selected), site2-site3 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site3 to Site4:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site3-site4
Security Level: Standard
Remote Gateway: Predefined (selected), site3-site4 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site4 firewall

Site4 to Site1:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site1-site4
Security Level: Standard
Remote Gateway: Predefined (selected), site1-site4 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site4 to Site2:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site2-site4
Security Level: Standard
Remote Gateway: Predefined (selected), site2-site4 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

Site4 to Site3:

Select VPNs > AutoKey IKE, select New and enter following:
VPN Name: site3-site4
Security Level: Standard
Remote Gateway: Predefined (selected), site3-site4 (select from pull down menu)
Select Advanced
Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)
VPN Monitor: (checked)
Optimized: (checked)
Rekey: (checked)
Select Return and OK

CLI:

Site1 firewall

Site1 to Site2:

```
set vpn site1-site2 gateway site1-site2 sec-level standard
set vpn site1-site2 bind interface tunnel.1
set vpn site1-site2 monitor optimized rekey
```

Site1 to Site3:

```
set vpn site1-site3 gateway site1-site3 sec-level standard
set vpn site1-site3 bind interface tunnel.1
set vpn site1-site3 monitor optimized rekey
```

Site1 to Site4:

```
set vpn site1-site4 gateway site1-site4 sec-level standard
set vpn site1-site4 bind interface tunnel.1
set vpn site1-site4 monitor optimized rekey
```


Site2 firewall

Site2 to Site1:

```
set vpn site1-site2 gateway site1-site2 sec-level standard
set vpn site1-site2 bind interface tunnel.1
set vpn site1-site2 monitor optimized rekey
```

Site2 to Site3:

```
set vpn site2-site3 gateway site2-site3 sec-level standard
set vpn site2-site3 bind interface tunnel.1
set vpn site2-site3 monitor optimized rekey
```

Site2 to Site4:

```
set vpn site2-site4 gateway site2-site4 sec-level standard
set vpn site2-site4 bind interface tunnel.1
set vpn site2-site4 monitor optimized rekey
```

Site3 firewall

Site3 to Site1:

```
set vpn site1-site3 gateway site1-site3 sec-level standard
set vpn site1-site3 bind interface tunnel.1
set vpn site1-site3 monitor optimized rekey
```

Site3 to Site2:

```
set vpn site2-site3 gateway site2-site3 sec-level standard
set vpn site2-site3 bind interface tunnel.1
set vpn site2-site3 monitor optimized rekey
```

Site3 to Site4:

```
set vpn site3-site4 gateway site3-site4 sec-level standard
set vpn site3-site4 bind interface tunnel.1
set vpn site3-site4 monitor optimized rekey
```

Site4 firewall

Site4 to Site1:

```
set vpn site1-site4 gateway site1-site4 sec-level standard
set vpn site1-site4 bind interface tunnel.1
set vpn site1-site4 monitor optimized rekey
```

Site4 to Site2:

```
set vpn site2-site4 gateway site2-site4 sec-level standard
set vpn site2-site4 bind interface tunnel.1
set vpn site2-site4 monitor optimized rekey
```

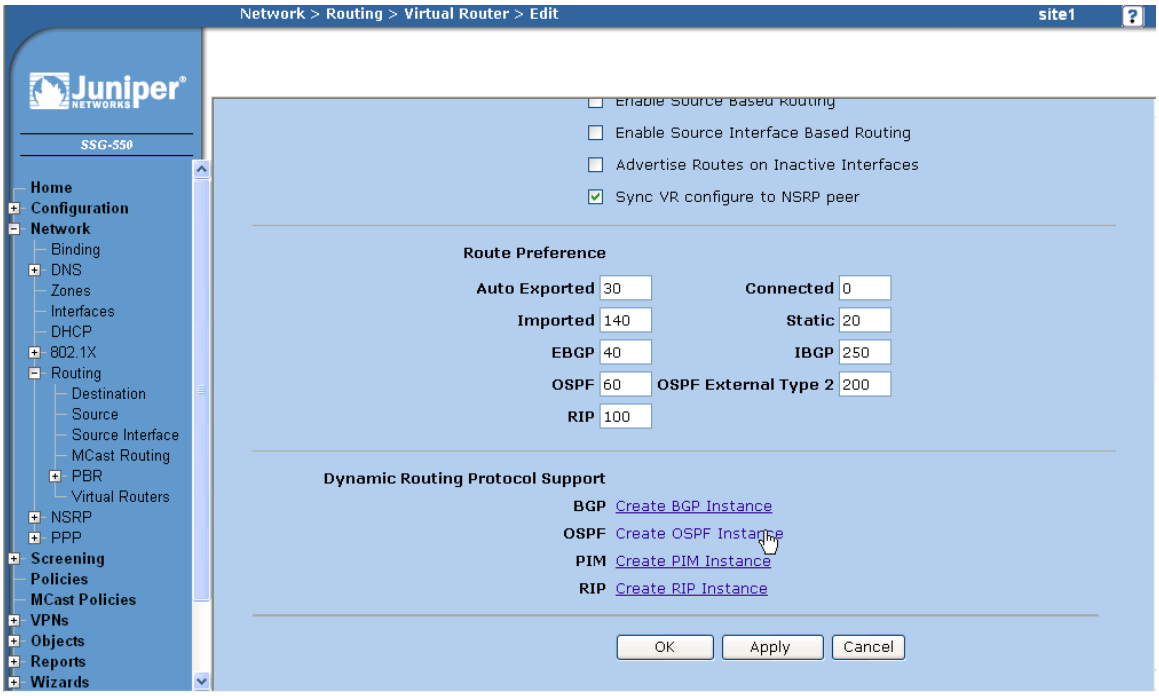
Site4 to Site3:

```
set vpn site3-site4 gateway site3-site4 sec-level standard
set vpn site3-site4 bind interface tunnel.1
set vpn site3-site4 monitor optimized rekey
```

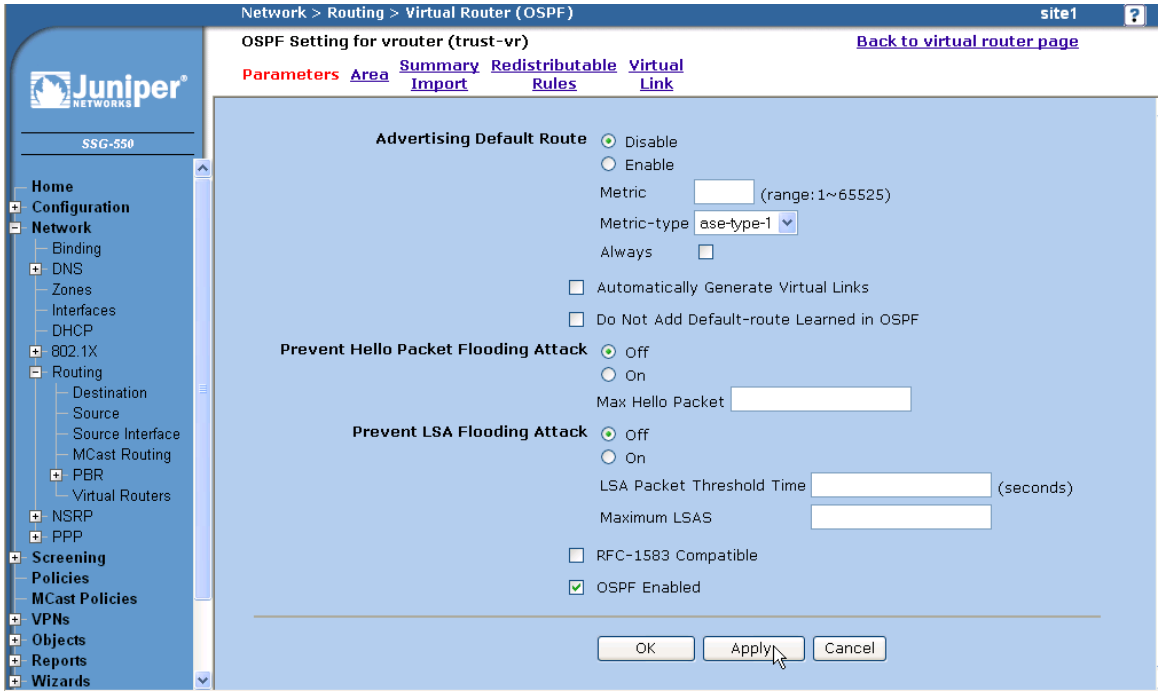
Step 4: Configuring OSPF protocol

OSPF is the routing protocol that used in this application note to demonstrate how routing information can be integrated in the Full Mesh VPN scenario. With OSPF, the local routes will be automatically learned by remote gateways. This is a way to minimize administrative overhead in maintaining large VPN network.

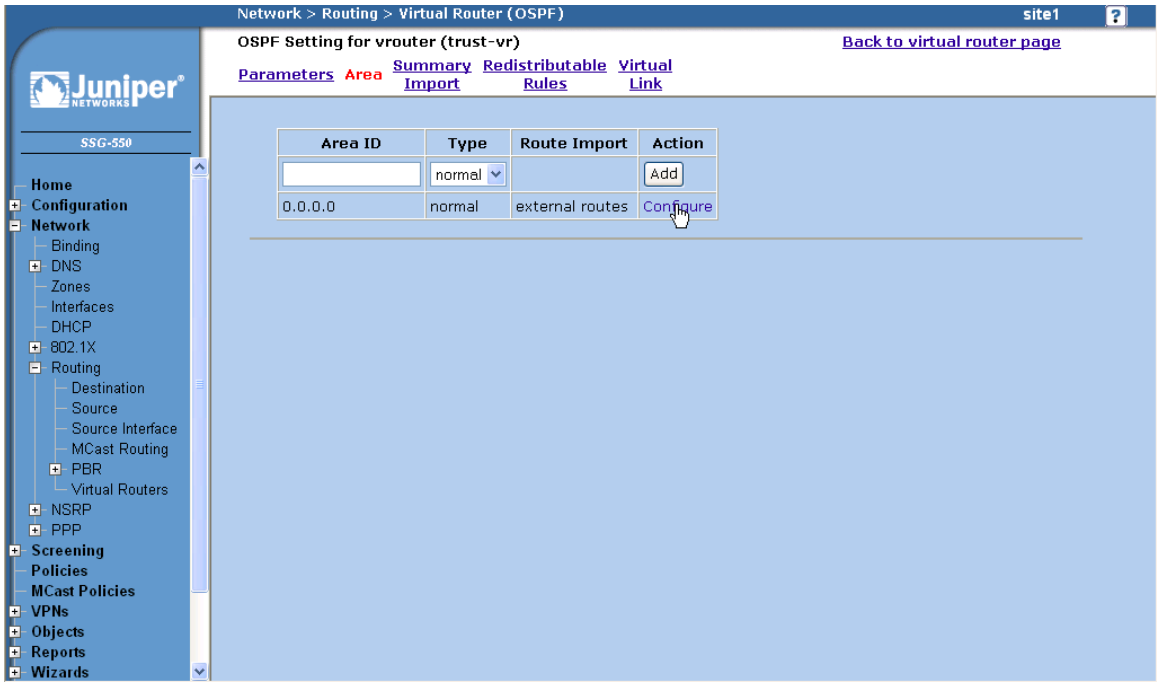
Create OSPF routing instance:



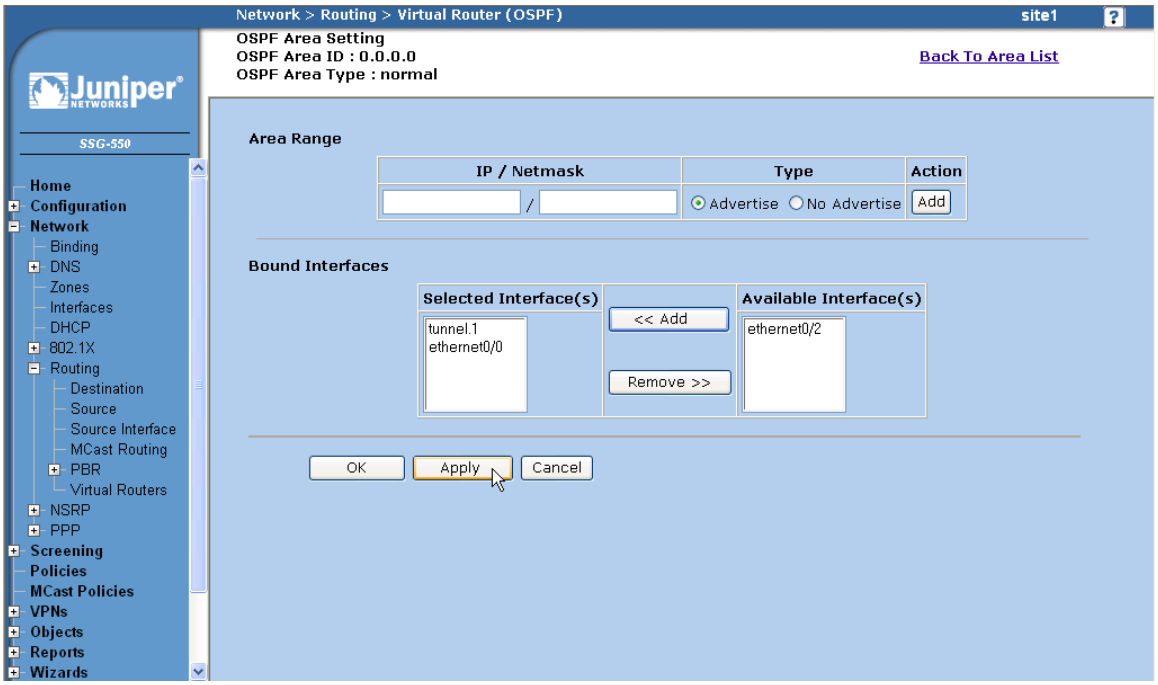
Enable OSPF and select Apply.



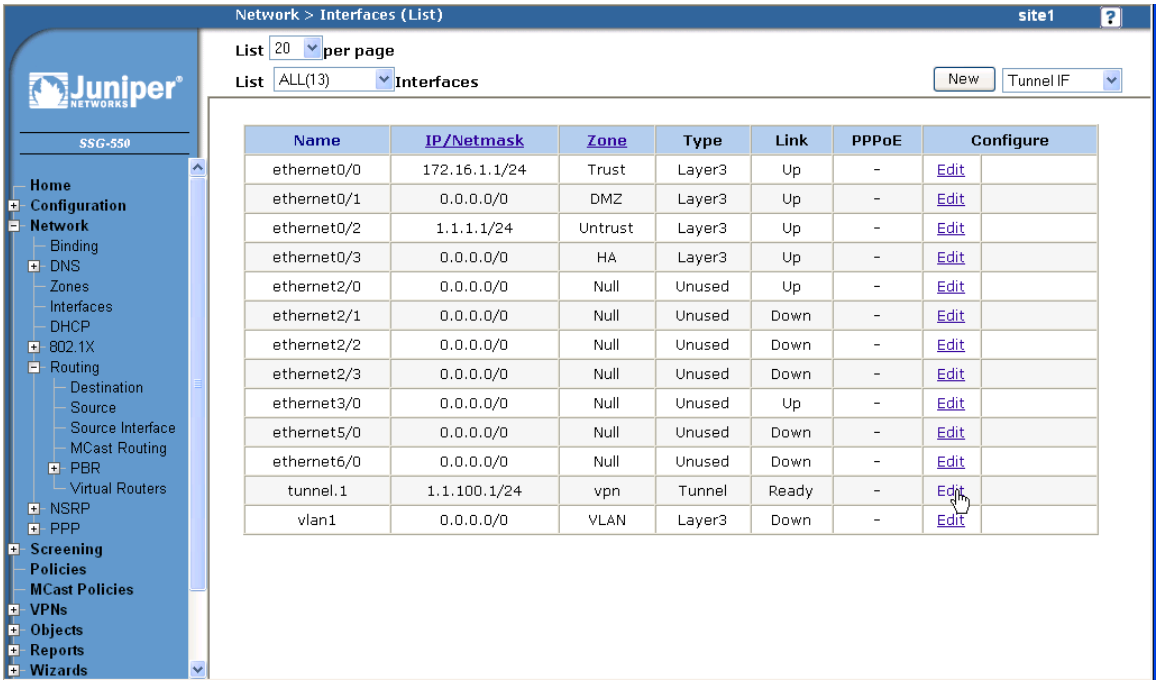
Select Area and configure area “0.0.0.0”.



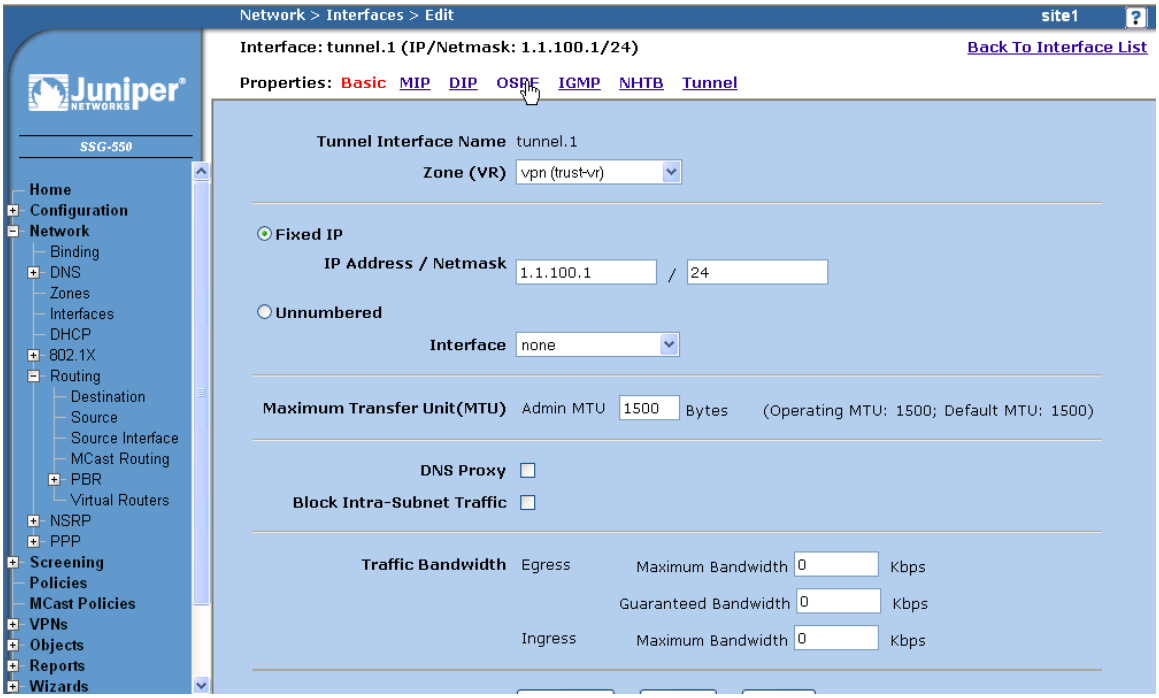
Select interfaces that participate on area “0.0.0.0” and Apply.



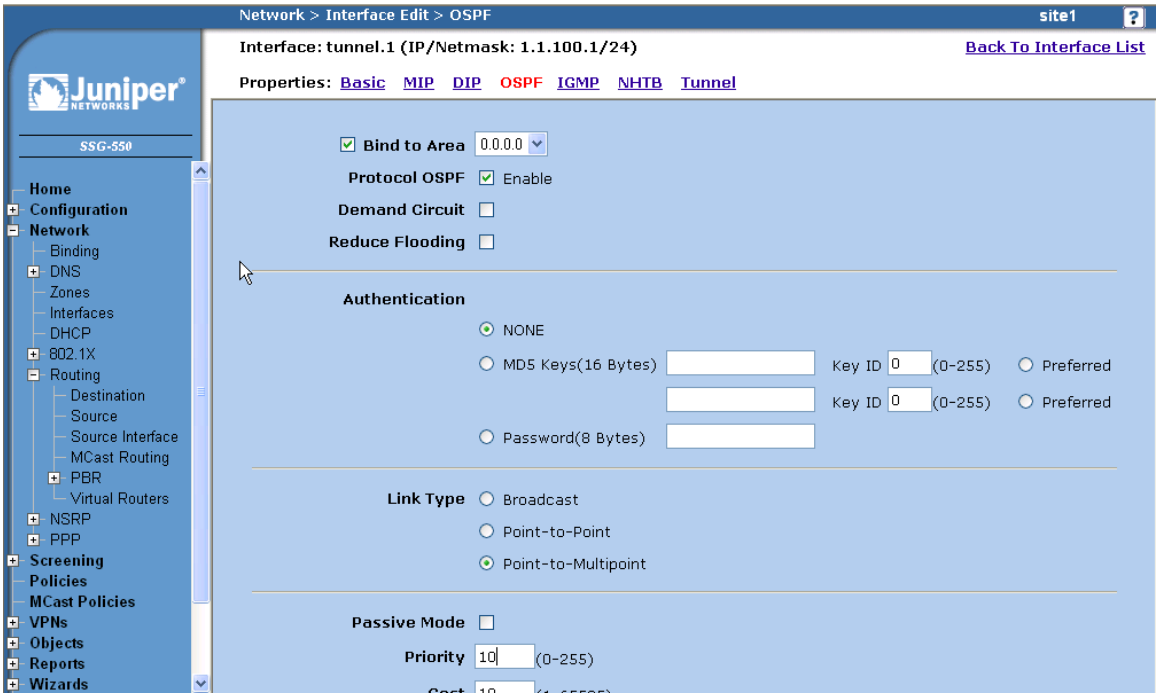
Then select OK back to the virtual router page. Select OK.
Select Interface > tunnel.1.



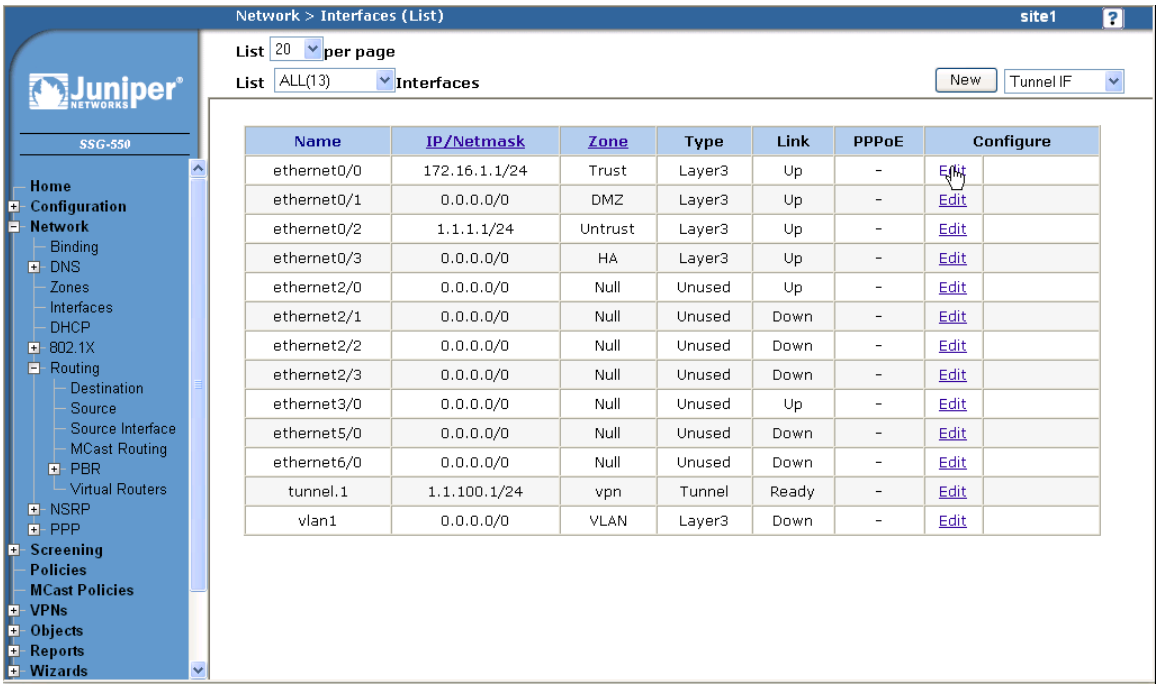
Select OSPF.



Enable OSPF and select Point-to-Multipoint link type. Edit Priority and Cost, if needed. Then select Apply.

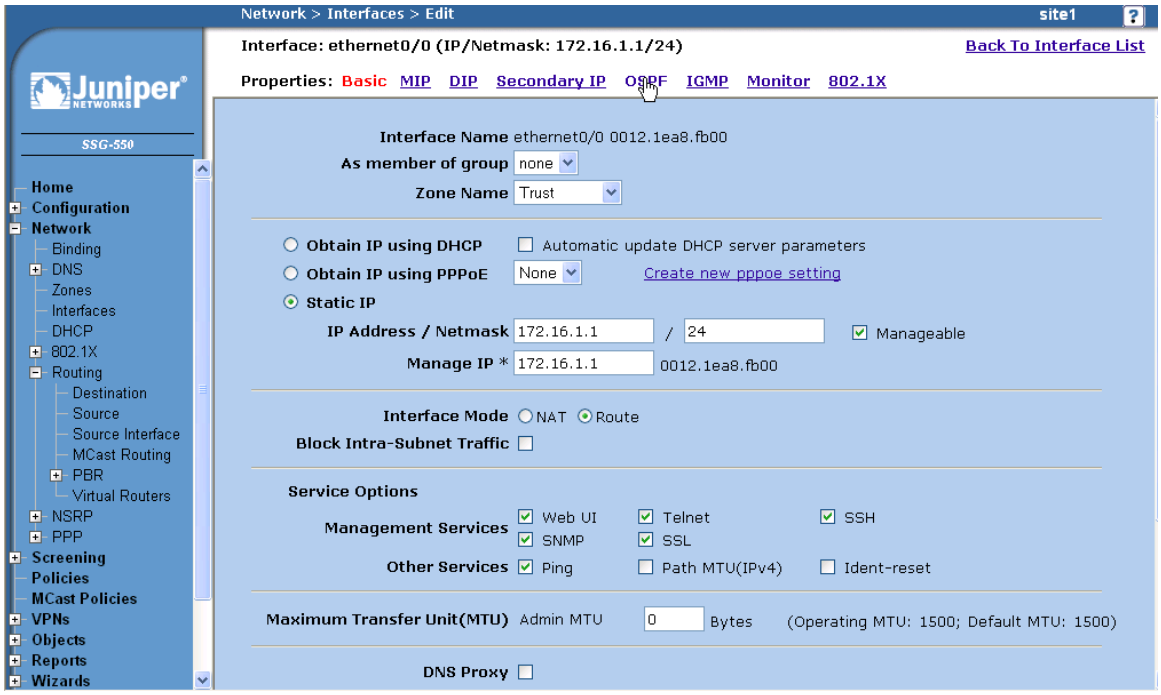


Select interface and edit interface connecting to local OSPF network.

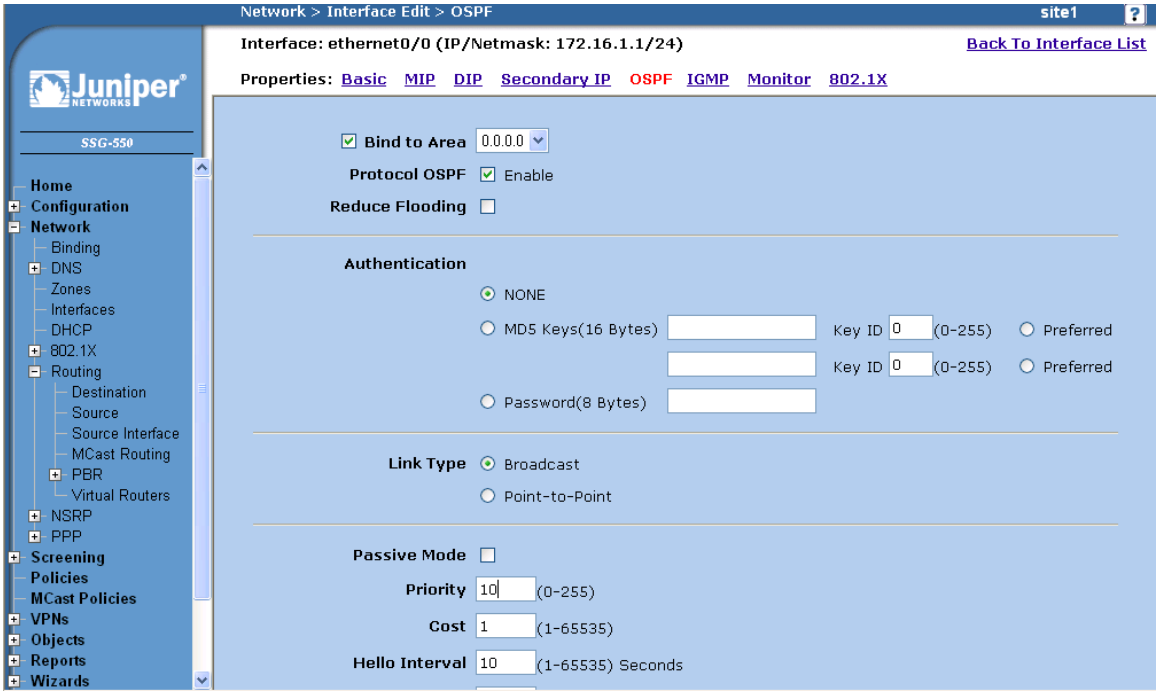


Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ethernet0/0	172.16.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Up	-	Edit
ethernet0/2	1.1.1.1/24	Untrust	Layer3	Up	-	Edit
ethernet0/3	0.0.0.0/0	HA	Layer3	Up	-	Edit
ethernet2/0	0.0.0.0/0	Null	Unused	Up	-	Edit
ethernet2/1	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet2/2	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet2/3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet3/0	0.0.0.0/0	Null	Unused	Up	-	Edit
ethernet5/0	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet6/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	1.1.100.1/24	vpn	Tunnel	Ready	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Select OSPF.



Enable OSPF and edit priority and cost (if needed), then Apply.



The WebUI and CLI 'Step 4' instructions for each firewall are as follows:

<u>WebUI:</u>

Site1 firewall

Enable OSPF Instance:

Select Network > Routing > Virtual Routers, select trust-vr and then Edit.
Select Create OSPF Instance.
Select OSPF Enable and then Apply.
Choose Area ID "0.0.0.0", then Configure.
Select interface "tunnel.1" and "ethernet0/0" to add to Bound Interfaces list, then Apply and OK to exit.

Enable OSPF on tunnel interface:

Select Network > Interfaces, the select tunnel.1 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Link Type: Point-to-Multipoint (selected)
Priority: 10
Cost: 1

Enable OSPF on interface connecting to local OSPF network:

Select Network > Interfaces, the select ethernet0/0 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Priority: 10
Cost: 1

Site2 firewall

Enable OSPF Instance:

Select Network > Routing > Virtual Routers, select trust-vr and then Edit.
Select Create OSPF Instance.
Select OSPF Enable and then Apply.
Choose Area ID "0.0.0.0", then Configure.
Select interface "tunnel.1" and "ethernet0/0" to add to Bound Interfaces list, then Apply and OK to exit.

Enable OSPF on tunnel interface:

Select Network > Interfaces, the select tunnel.1 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Link Type: Point-to-Multipoint (selected)
Priority: 10
Cost: 1

Enable OSPF on interface connecting to local OSPF network:

Select Network > Interfaces, the select ethernet0/0 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Priority: 10
Cost: 1

Site3 firewall

Enable OSPF Instance:

Select Network > Routing > Virtual Routers, select trust-vr and then Edit.
Select Create OSPF Instance.
Select OSPF Enable and then Apply.
Choose Area ID "0.0.0.0", then Configure.
Select interface "tunnel.1" and "bgroup0" to add to Bound Interfaces list, then Apply and OK to exit.

Enable OSPF on tunnel interface:

Select Network > Interfaces, the select tunnel.1 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Link Type: Point-to-Multipoint (selected)
Priority: 10

Cost: 1

Enable OSPF on interface connecting to local OSPF network:

Select Network > Interfaces, the select bgroup0 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Priority: 10
Cost: 1

Site4 firewall

Enable OSPF Instance:

Select Network > Routing > Virtual Routers, select trust-vr and then Edit.
Select Create OSPF Instance.
Select OSPF Enable and then Apply.
Choose Area ID "0.0.0.0", then Configure.
Select interface "tunnel.1" and "ethernet0/2" to add to Bound Interfaces list, then Apply and OK to exit.

Enable OSPF on tunnel interface:

Select Network > Interfaces, the select tunnel.1 and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Link Type: Point-to-Multipoint (selected)
Priority: 10
Cost: 1

Enable OSPF on interface connecting to local OSPF network:

Select Network > Interfaces, the select ethernet0/2and Edit.
Select OSPF.
Enter the following, then select Apply.
Protocol OSPF: Enable (selected)
Priority: 10
Cost: 1

<u>CLI:</u>

Site1 firewall

Enable OSPF instance:

```
set vrouter trust-vr protocol ospf
set vrouter trust-vr protocol ospf enable
```

Enable OSPF on tunnel interface:

```
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
```

Enable OSPF on interface connecting local OSPF network:

```
set interface ethernet0/0 protocol ospf area 0.0.0.0
set interface ethernet0/0 protocol ospf enable
set interface ethernet0/0 protocol ospf priority 10
set interface ethernet0/0 protocol ospf cost 1
```

Site2 firewall

Enable OSPF instance:

```
set vrouter trust-vr protocol ospf
set vrouter trust-vr protocol ospf enable
```

Enable OSPF on tunnel interface:

```
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
```

Enable OSPF on interface connecting local OSPF network:

```
set interface ethernet0/0 protocol ospf area 0.0.0.0
set interface ethernet0/0 protocol ospf enable
set interface ethernet0/0 protocol ospf priority 10
set interface ethernet0/0 protocol ospf cost 1
```

Sit3 firewall

Enable OSPF instance:

```
set vrouter trust-vr protocol ospf
set vrouter trust-vr protocol ospf enable
```

Enable OSPF on tunnel interface:

```
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
```

Enable OSPF on interface connecting local OSPF network:

```
set interface bgroup0 protocol ospf area 0.0.0.0
set interface bgroup0 protocol ospf enable
set interface bgroup0 protocol ospf priority 10
set interface bgroup0 protocol ospf cost 1
```

Site4 firewall

Enable OSPF instance:

```
set vrouter trust-vr protocol ospf
set vrouter trust-vr protocol ospf enable
```

Enable OSPF on tunnel interface:

```
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
```

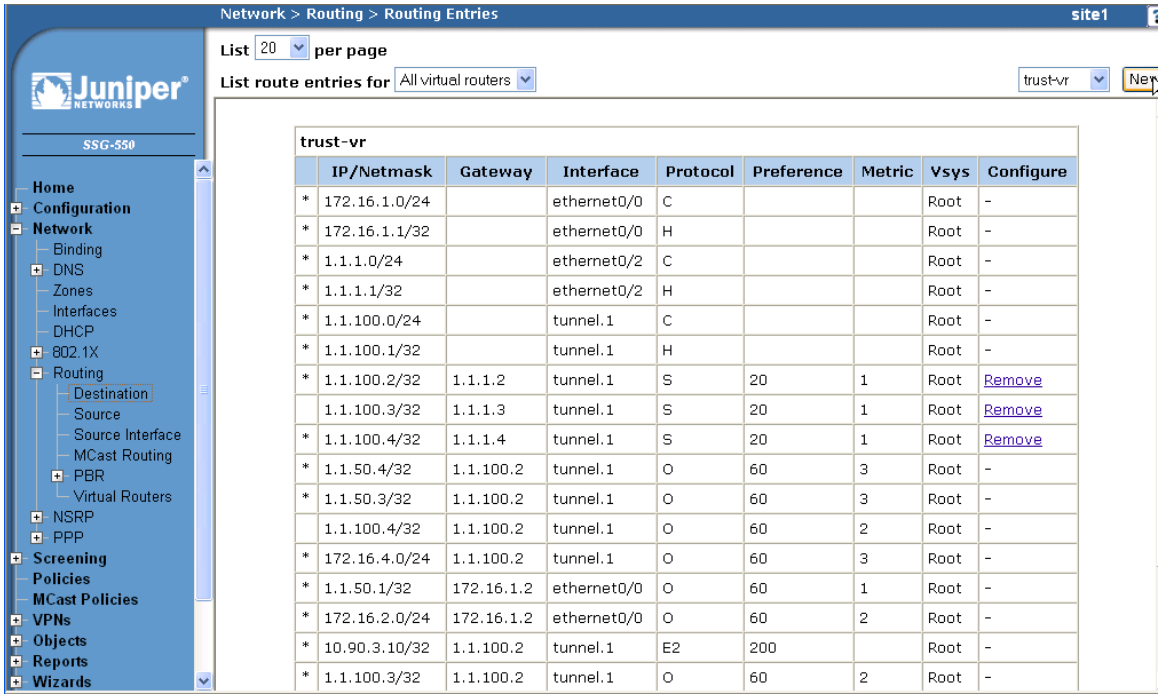
Enable OSPF on interface connecting local OSPF network:

```
set interface ethernet0/2 protocol ospf area 0.0.0.0
set interface ethernet0/2 protocol ospf enable
set interface ethernet0/2 protocol ospf priority 10
set interface ethernet0/2 protocol ospf cost 1
```

Step 5: Add Static Routes and Static NHTB entries

Static route is required to maintain the reachability between tunnel interfaces among firewalls. In addition, to ensure multicast OSPF traffic is using the correct tunnel, static NHTB entries are required. (Otherwise, the OSPF neighbor state may get stuck in "Exstart" as the multicast OSPF traffic may use the incorrect tunnel.)

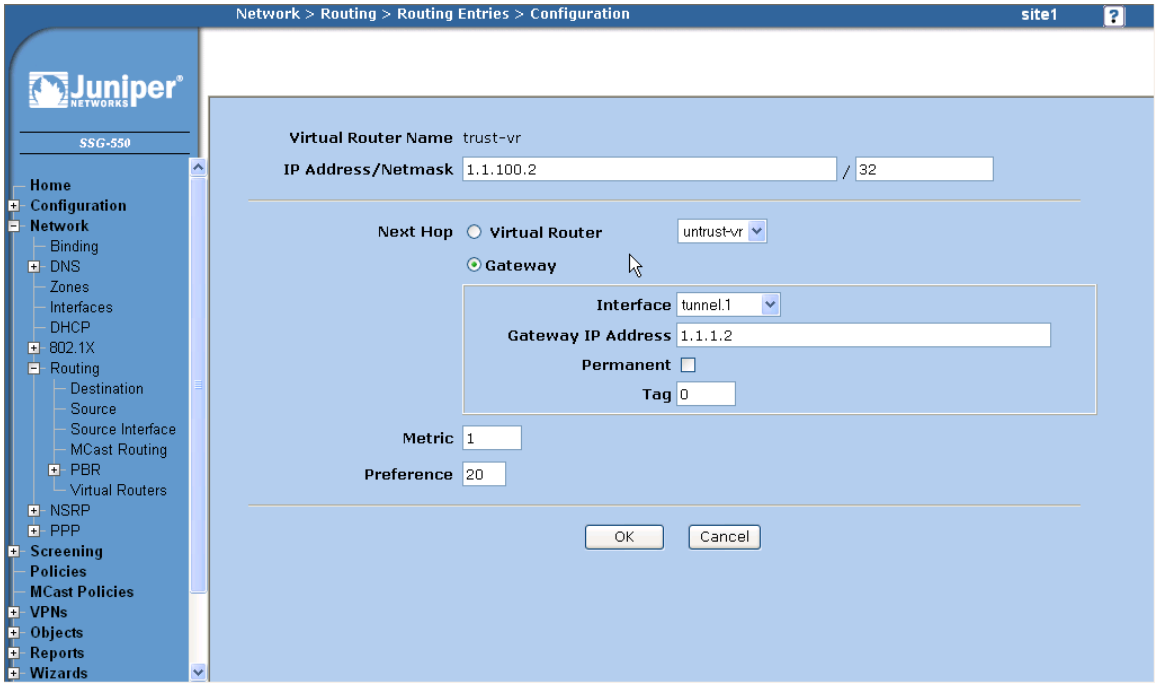
Configure static route entries, select New from trust-vr.



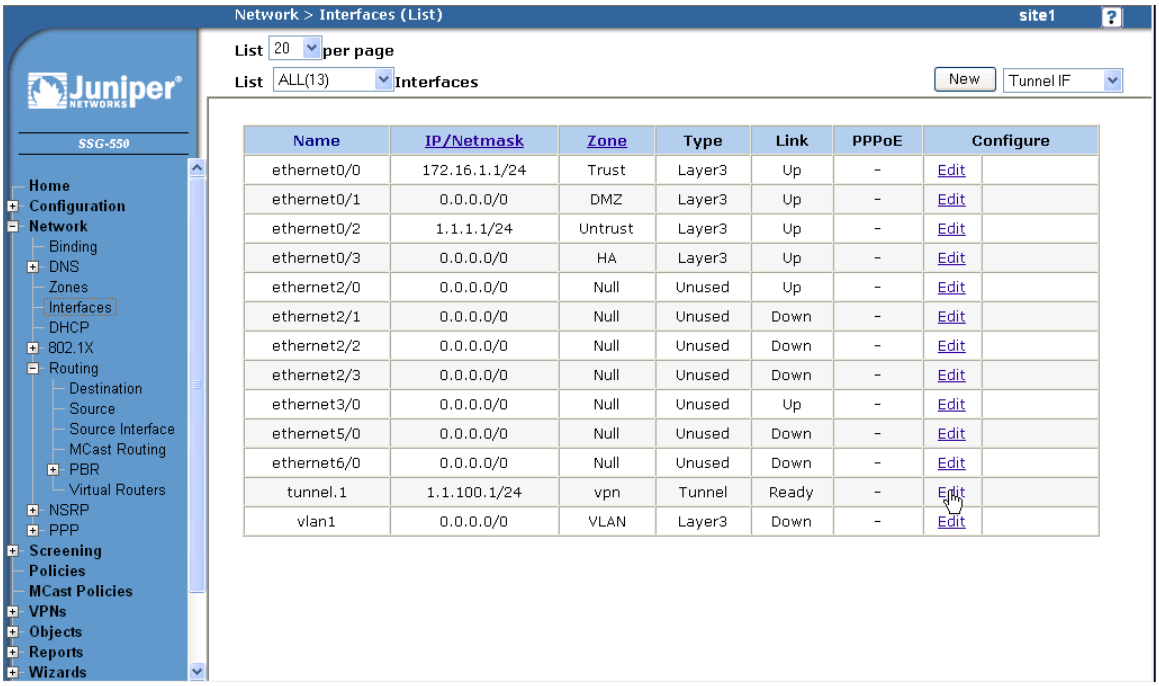
trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Configure
*	172.16.1.0/24		ethernet0/0	C			Root	-
*	172.16.1.1/32		ethernet0/0	H			Root	-
*	1.1.1.0/24		ethernet0/2	C			Root	-
*	1.1.1.1/32		ethernet0/2	H			Root	-
*	1.1.100.0/24		tunnel.1	C			Root	-
*	1.1.100.1/32		tunnel.1	H			Root	-
*	1.1.100.2/32	1.1.1.2	tunnel.1	S	20	1	Root	Remove
	1.1.100.3/32	1.1.1.3	tunnel.1	S	20	1	Root	Remove
*	1.1.100.4/32	1.1.1.4	tunnel.1	S	20	1	Root	Remove
*	1.1.50.4/32	1.1.100.2	tunnel.1	O	60	3	Root	-
*	1.1.50.3/32	1.1.100.2	tunnel.1	O	60	3	Root	-
	1.1.100.4/32	1.1.100.2	tunnel.1	O	60	2	Root	-
*	172.16.4.0/24	1.1.100.2	tunnel.1	O	60	3	Root	-
*	1.1.50.1/32	172.16.1.2	ethernet0/0	O	60	1	Root	-
*	172.16.2.0/24	172.16.1.2	ethernet0/0	O	60	2	Root	-
*	10.90.3.10/32	1.1.100.2	tunnel.1	E2	200		Root	-
*	1.1.100.3/32	1.1.100.2	tunnel.1	O	60	2	Root	-

Enter address of remote tunnel interface, then enters correct interface and gateway IP. Select OK when done.

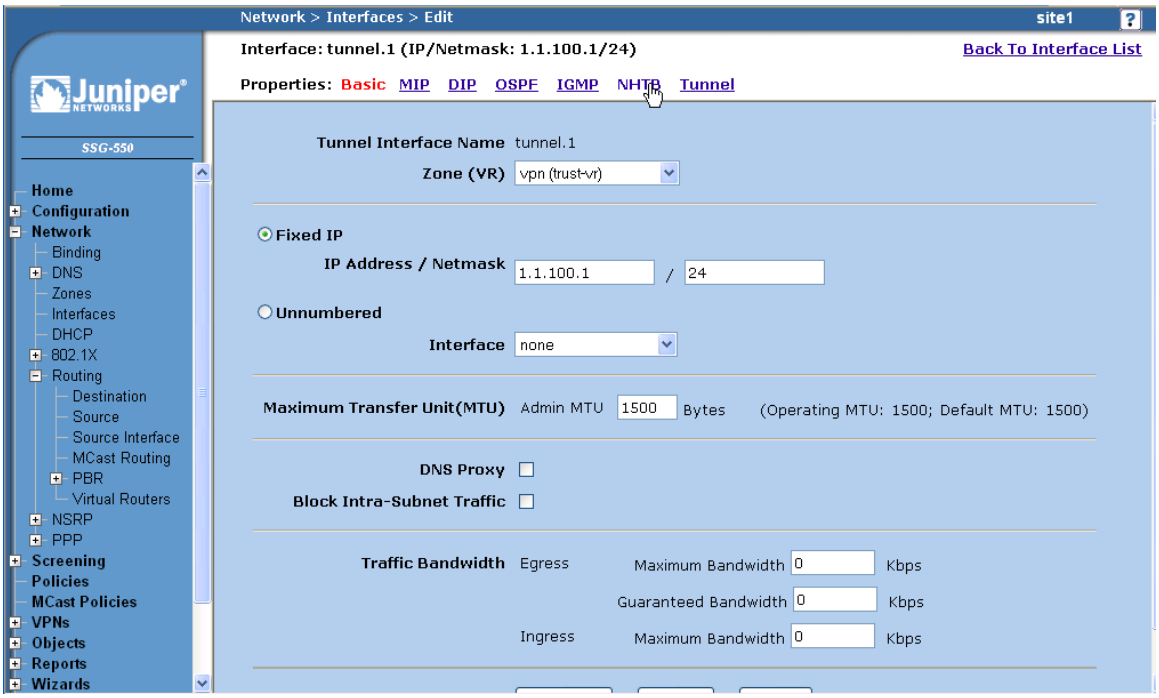


To configure static NHTB entries, select edit on tunnel interface.

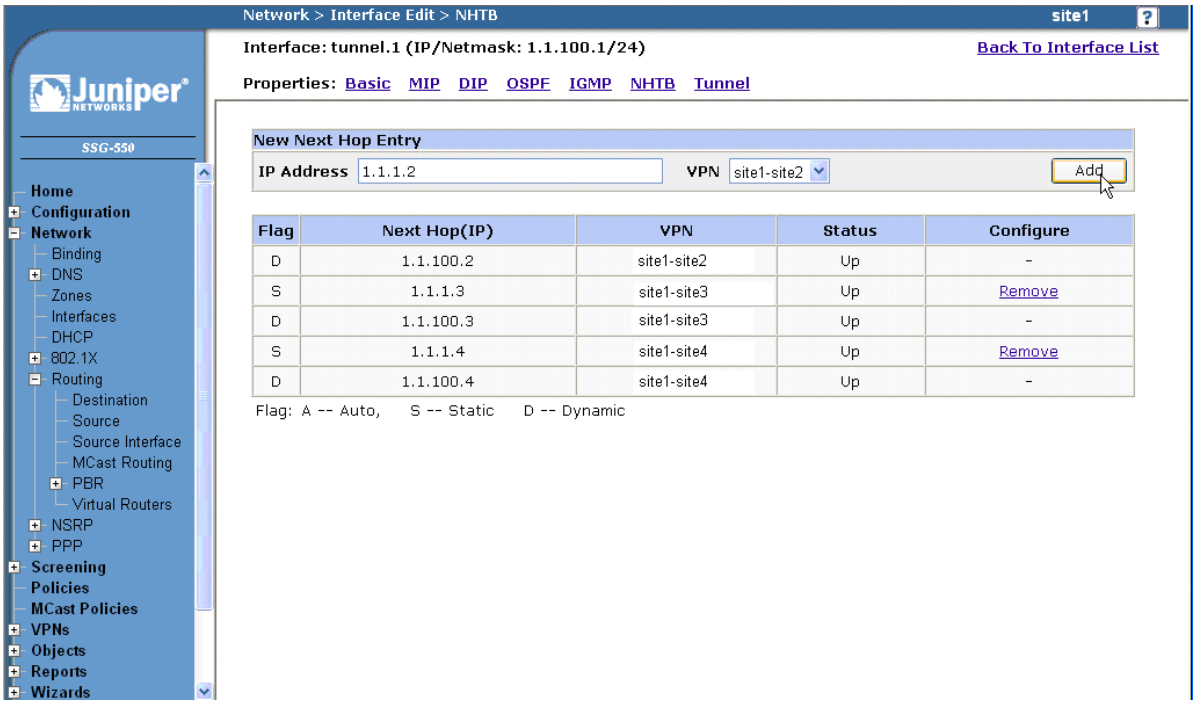


Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ethernet0/0	172.16.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Up	-	Edit
ethernet0/2	1.1.1.1/24	Untrust	Layer3	Up	-	Edit
ethernet0/3	0.0.0.0/0	HA	Layer3	Up	-	Edit
ethernet2/0	0.0.0.0/0	Null	Unused	Up	-	Edit
ethernet2/1	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet2/2	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet2/3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet3/0	0.0.0.0/0	Null	Unused	Up	-	Edit
ethernet5/0	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet6/0	0.0.0.0/0	Null	Unused	Down	-	Edit
tunnel.1	1.1.100.1/24	vpn	Tunnel	Ready	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Select NHTB (which allows one to bind multiple VPNs to one tunnel interface):



Enter remote gateway IP address and corresponding vpn tunnel name, then select Add.



The WebUI and CLI 'Step 5' instructions for each firewall are as follows:

WebUI:

Site1 firewall

Static route to tunnel interface of Site2:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.2 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.2
Select OK

Static route to tunnel interface of Site3:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.3 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.3
Select OK

Static route to tunnel interface of Site4:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.4 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.4
Select OK

Static NHTB entry to Site2 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.2
VPN: site1-site2
Select Add

Static NHTB entry to Site3 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.3
VPN: site1-site3
Select Add

Static NHTB entry to Site4 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:

IP Address: 1.1.1.4
VPN: site1-site4
Select Add

Site2 firewall

Static route to tunnel interface of Site1:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.1 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.1
Select OK

Static route to tunnel interface of Site3:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.3 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.3
Select OK

Static route to tunnel interface of Site4:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.4 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.4
Select OK

Static NHTB entry to Site1 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.1
VPN: site1-site2
Select Add

Static NHTB entry to Site3 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.3
VPN: site2-site3
Select Add

Static NHTB entry to Site4 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.4

VPN: site2-site4
Select Add

Site3 firewall

Static route to tunnel interface of Site1:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.1 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.1
Select OK

Static route to tunnel interface of Site2:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.2 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.2
Select OK

Static route to tunnel interface of Site4:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.4 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.4
Select OK

Static NHTB entry to Site1 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.1
VPN: site1-site3
Select Add

Static NHTB entry to Site2 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.2
VPN: site2-site3
Select Add

Static NHTB entry to Site4 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.4

VPN: site3-site4
Select Add

Site4 firewall

Static route to tunnel interface of Site1:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.1 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.1
Select OK

Static route to tunnel interface of Site2:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.2 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.2
Select OK

Static route to tunnel interface of Site3:

Select Network > Routing > Destination, select New and enter following:
IP Address / Netmask: 1.1.100.3 / 32
Next Hop: Gateway (selected)
Interface: tunnel.1 (select from pull down menu)
Gateway IP Address: 1.1.1.3
Select OK

Static NHTB entry to Site1 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.1
VPN: site1-site4
Select Add

Static NHTB entry to Site2 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.2
VPN: site2-site4
Select Add

Static NHTB entry to Site3 firewall:

Select Network > Interfaces, select Edit on tunnel.1.
Select NHTB and enter the following:
IP Address: 1.1.1.3
VPN: site3-site4

Select Add

CLI:

Site1 firewall

```
set route 1.1.100.2/32 interface tunnel.1 gateway 1.1.1.2
set route 1.1.100.3/32 interface tunnel.1 gateway 1.1.1.3
set route 1.1.100.4/32 interface tunnel.1 gateway 1.1.1.4
set interface tunnel.1 nhtb 1.1.1.2 vpn site1-site2
set interface tunnel.1 nhtb 1.1.1.3 vpn site1-site3
set interface tunnel.1 nhtb 1.1.1.4 vpn site1-site4
```

Site2 firewall

```
set route 1.1.100.1/32 interface tunnel.1 gateway 1.1.1.1
set route 1.1.100.3/32 interface tunnel.1 gateway 1.1.1.3
set route 1.1.100.4/32 interface tunnel.1 gateway 1.1.1.4
set interface tunnel.1 nhtb 1.1.1.1 vpn site1-site2
set interface tunnel.1 nhtb 1.1.1.3 vpn site2-site3
set interface tunnel.1 nhtb 1.1.1.4 vpn site2-site4
```

Site3 firewall

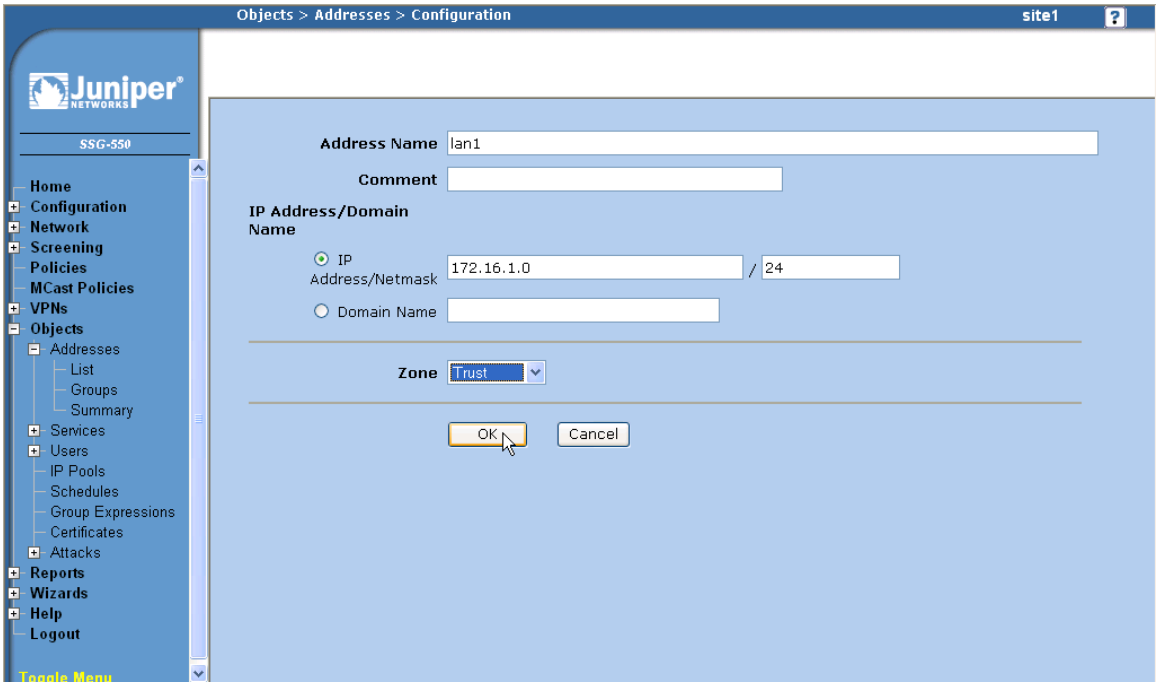
```
set route 1.1.100.1/32 interface tunnel.1 gateway 1.1.1.1
set route 1.1.100.2/32 interface tunnel.1 gateway 1.1.1.2
set route 1.1.100.4/32 interface tunnel.1 gateway 1.1.1.4
set interface tunnel.1 nhtb 1.1.1.1 vpn site1-site3
set interface tunnel.1 nhtb 1.1.1.2 vpn twp2three
set interface tunnel.1 nhtb 1.1.1.4 vpn site3-site4
```

Site4 firewall

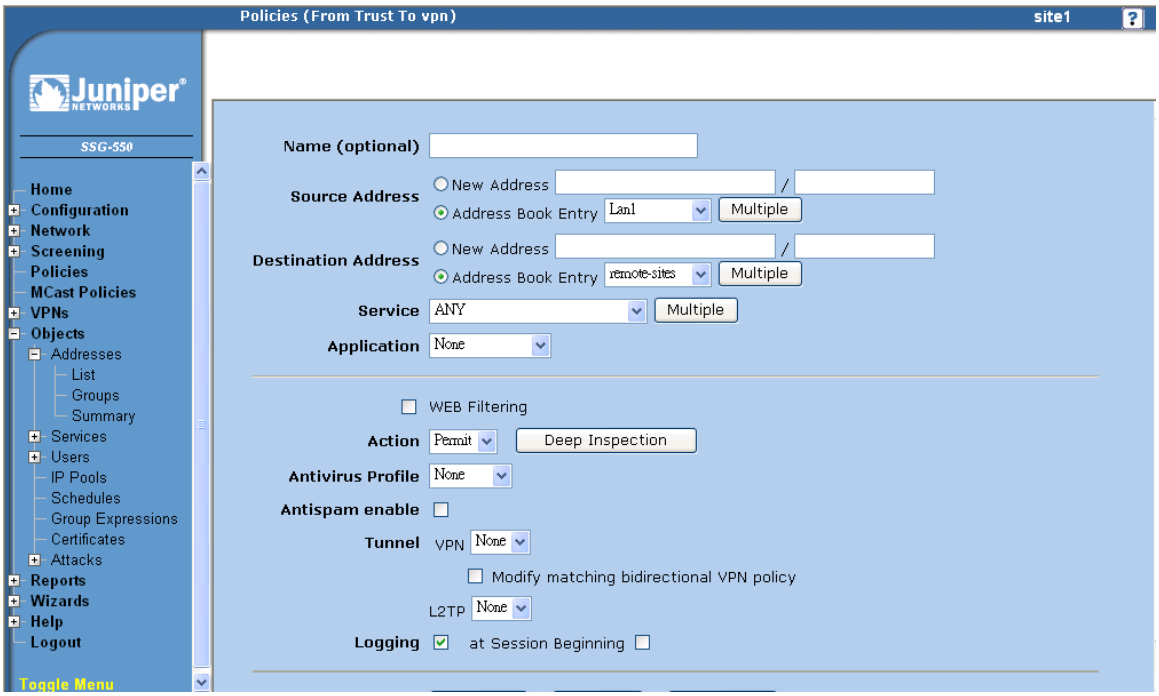
```
set route 1.1.100.1/32 interface tunnel.1 gateway 1.1.1.1
set route 1.1.100.2/32 interface tunnel.1 gateway 1.1.1.2
set route 1.1.100.3/32 interface tunnel.1 gateway 1.1.1.3
set interface tunnel.1 nhtb 1.1.1.1 vpn site1-site4
set interface tunnel.1 nhtb 1.1.1.2 vpn site2-site4
set interface tunnel.1 nhtb 1.1.1.3 vpn site3-site4
```

Step 6: Configure policy to allow traffic between sites

To create policy, firstly we need to define address objects. Then, define policies to allow traffic from and to spokes.



After all the required address objects are defined, select Policies to define policies.



The WebUI and CLI 'Step 6' instructions for each firewall are as follows:

<u>WebUI:</u>

Site1 firewall

Define address objects:

Select Objects > Addresses > List > vpn (pull down menu).
Select New then enter following:
Address Name: Site2
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.2.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site3
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.3.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site4
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.4.0/24
Select OK

Select Objects > Addresses > Groups > vpn (pull down menu)
Select New then enter following:
Group Name: Remote-sites
Group Members: Site2, Site3, Site4

Select OK

Select Objects > Addresses > List > trust (pull down menu)
Select New then enter following:
Address Name: Lan1
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.1.0/24
Select OK

Define policy: (Lan to remote)

Select Policies
From: Trust (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Lan1 (pull down menu)
Destination Address: Address Book Entry: Remote-sites2 (pull down menu)
Select OK

Define policy: (remote to Lan)

Select Policies
From: vpn (pull down menu)
To: Trust (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Lan1 (pull down menu)
Select OK

Define policy: (interconnect between remote sites)

Select Policies
From: vpn (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Remote-sites (pull down menu)
Select OK

Site2 firewall

Define address objects:

Select Objects > Addresses > List > vpn (pull down menu).
Select New then enter following:
Address Name: Site1
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.1.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site3
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.3.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site4
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.4.0/24
Select OK

Select Objects > Addresses > Groups > vpn (pull down menu)
Select New then enter following:
Group Name: Remote-sites
Group Members: Site1, Site3, Site4
Select OK

Select Objects > Addresses > List > trust (pull down menu)
Select New then enter following:
Address Name: Lan2
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.2.0/24
Select OK

Define policy: (Lan to remote)

Select Policies
From: Trust (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Lan2 (pull down menu)
Destination Address: Address Book Entry: Remote-sites2 (pull down menu)
Select OK

Define policy: (remote to Lan)

Select Policies
From: vpn (pull down menu)
To: Trust (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Lan2 (pull down menu)
Select OK

Define policy: (interconnect between remote sites)

Select Policies
From: vpn (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Remote-sites (pull down menu)
Select OK

Site3 firewall

Define address objects:

Select Objects > Addresses > List > vpn (pull down menu).
Select New then enter following:

Address Name: Site1
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.1.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site2
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.2.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site4
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.4.0/24
Select OK

Select Objects > Addresses > Groups > vpn (pull down menu)
Select New then enter following:
Group Name: Remote-sites
Group Members: Site1, Site2, Site4
Select OK

Select Objects > Addresses > List > trust (pull down menu)
Select New then enter following:
Address Name: Lan3
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.3.0/24
Select OK

Define policy: (Lan to remote)

Select Policies
From: Trust (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Lan3 (pull down menu)
Destination Address: Address Book Entry: Remote-sites2 (pull down menu)
Select OK

Define policy: (remote to Lan)

Select Policies
From: vpn (pull down menu)
To: Trust (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Lan3 (pull down menu)
Select OK

Define policy: (interconnect between remote sites)

Select Policies
From: vpn (pull down menu)
To: vpn (pull down menu)

Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Remote-sites (pull down menu)
Select OK

Site4 firewall

Define address objects:

Select Objects > Addresses > List > vpn (pull down menu).
Select New then enter following:
Address Name: Site1
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.1.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site2
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.2.0/24
Select OK

Select Objects > Addresses > List > vpn (pull down menu)
Select New then enter following:
Address Name: Site3
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.3.0/24
Select OK

Select Objects > Addresses > Groups > vpn (pull down menu)
Select New then enter following:
Group Name: Remote-sites
Group Members: Site1, Site2, Site3
Select OK

Select Objects > Addresses > List > trust (pull down menu)
Select New then enter following:
Address Name: Lan4
IP Address/Domain Name: IP Address/Netmask (checked), 172.16.4.0/24
Select OK

Define policy: (Lan to remote)

Select Policies
From: Trust (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Lan4 (pull down menu)
Destination Address: Address Book Entry: Remote-sites2 (pull down menu)
Select OK

Define policy: (remote to Lan)

Select Policies
From: vpn (pull down menu)

To: Trust (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Lan4 (pull down menu)
Select OK

Define policy: (interconnect between remote sites)

Select Policies
From: vpn (pull down menu)
To: vpn (pull down menu)
Select New
Source Address: Address Book Entry: Remote-sites (pull down menu)
Destination Address: Address Book Entry: Remote-sites (pull down menu)
Select OK

CLI:

Site1 firewall

```
set address vpn site2 172.16.2.0/24
set address vpn site3 172.16.3.0/24
set address vpn site4 172.16.4.0/24
set address trust lan1 172.16.1.0/24
set group address vpn remote-sites add site2
set group address vpn remote-sites add site3
set group address vpn remote-sites add site4
set policy from trust to vpn lan1 remote-sites any permit
set policy from vpn to trust remote-sites lan1 any permit
set policy from vpn to vpn remote-sites remote-sites any permit
```

Site2 firewall

```
set address vpn site1 172.16.1.0/24
set address vpn site3 172.16.3.0/24
set address vpn site4 172.16.4.0/24
set address trust lan2 172.16.2.0/24
set group address vpn remote-sites add site1
set group address vpn remote-sites add site3
set group address vpn remote-sites add site4
set policy from trust to vpn lan2 remote-sites any permit
set policy from vpn to trust remote-sites lan2 any permit
set policy from vpn to vpn remote-sites remote-sites any permit
```

Site3 firewall

```
set address vpn site1 172.16.1.0/24
set address vpn site2 172.16.2.0/24
set address vpn site4 172.16.4.0/24
set address trust lan3 172.16.3.0/24
set group address vpn remote-sites add site1
set group address vpn remote-sites add site2
set group address vpn remote-sites add site4
```

```
set policy from trust to vpn lan3 remote-sites any permit
set policy from vpn to trust remote-sites lan3 any permit
set policy from vpn to vpn remote-sites remote-sites any permit
```

Site4 firewall

```
set address vpn site1 172.16.1.0/24
set address vpn site2 172.16.2.0/24
set address vpn site3 172.16.3.0/24
set address trust lan4 172.16.4.0/24
set group address vpn remote-sites add site1
set group address vpn remote-sites add site2
set group address vpn remote-sites add site3
set policy from trust to vpn lan4 remote-sites any permit
set policy from vpn to trust remote-sites lan4 any permit
set policy from vpn to vpn remote-sites remote-sites any permit
```

Verifying Configuration

To check connectivity over the VPN between the different sites, use traffic to test it. Normally, if ICMP is permitted by policy to go through tunnel, it is most convenient to use "ping" as a tool to verify the configuration. Here we use ping to test the vpn between the following sites:

(Remember to specify the source interface by using "from" option in the ping, otherwise ping traffic will be source from interface nearest to the next hop interface.)

- Site1 and Site2

```
site1-> ping 172.16.2.1 from e0/0
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 1 seconds from
ethernet0/0
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=1/1/2 ms
```

- Site2 and Site3

```
site2-> ping 172.16.3.1 from e0/0
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 1 seconds from
ethernet0/0
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=2/2/3 ms
```

- Site3 and Site4

```
site3-> ping 172.16.4.1 from bgroup0
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 172.16.4.1, timeout is 1 seconds from bgroup0
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=3/3/4 ms
```

In addition, check with Security Association (SA) to ensure the VPNs are in good status:

```
site3-> get sa
total configured sa: 3
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<         1.1.1.1  500 esp:3des/sha1 b42415ca  2781 unlim A/U    -1 0
00000001>         1.1.1.1  500 esp:3des/sha1 94568c36  2781 unlim A/U    -1 0
00000002<         1.1.1.2  500 esp:3des/sha1 b42415cc  3310 unlim A/U    -1 0
00000002>         1.1.1.2  500 esp:3des/sha1 0523a7e5  3310 unlim A/U    -1 0
00000003<         1.1.1.4  500 esp:3des/sha1 b42415cd  3311 unlim A/U    -1 0
00000003>         1.1.1.4  500 esp:3des/sha1 9356ab4b  3311 unlim A/U    -1 0
```

Check with SA for the corresponding gateway (reference by IP address) , status A/U means the VPN is Active and VPN Monitor is Up.

Furthermore, you can check with "get interface tunnel.1" the NHTB entries and VPN binding.

```
site3-> get int t.1
Interface tunnel.1:
  description tunnel.1
  number 20, if_info 8168, if_index 1, mode route
  link ready
  vsys Root, zone vpn, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
```

```
  *ip 1.1.100.3/24
  *manage ip 1.1.100.3
  route-deny disable
  bound vpn:
    site1-site3
    site2-site3
    site3-site4

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN
   S    U    1.1.1.1 0x00000001 site1-site3
        U    1.1.100.1 0x00000001 site1-site3
   S    U    1.1.1.2 0x00000002 site2-site3
        U    1.1.100.2 0x00000002 site2-site3
   S    U    1.1.1.4 0x00000003 site3-site4
        U    1.1.100.4 0x00000003 site3-site4

  pmtu-v4 disabled
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled
  DNS Proxy disabled
  OSPF enabled  BGP disabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
Number of SW session: 8043, hw sess err cnt 0
```

When checking the OSPF neighbor status, make sure all of them are in “Full” state.

```
site3-> get vrouter trust-vr protocol ospf neighbor
VR: trust-vr RouterId: 172.16.3.1
----------------------------------
                Neighbor(s) on interface tunnel.1 (Area 0.0.0.0)
IpAddr/IfIndex  RouterId        Pri State    Opt  Up           StateChg
-------------------------------------------------------------------------------
1.1.100.1       172.16.1.1       10 Full     E    00:10:16     (+14 -2)
1.1.100.4       172.16.4.1       10 Full     E    02:00:00     (+6 -0)
1.1.100.2       172.16.2.1       10 Full     E    02:00:02     (+6 -0)

                Neighbor(s) on interface bgroup0 (Area 0.0.0.0)
IpAddr/IfIndex  RouterId        Pri State    Opt  Up           StateChg
-------------------------------------------------------------------------------
172.16.3.2      172.16.3.2      128 Full     E    01:59:58     (+7 -0)
```

Also, check with session table for the multicast OSPF traffic, make sure the correct tunnel is used.

```
site3-> get sess src-ip 1.1.100.1
alloc 23/max 8064, alloc failed 0, mcast alloc 0, di alloc failed 0
total reserved 0, free sessions in shared pool 8041
Total 2 sessions according filtering criteria.
id 8047/s**,vsys 0,flag 00000040/0080/0021,policy 320002,time 5, dip 0 module 0
 if 20(nspflag 800601):1.1.100.1/1->1.1.100.3/1,89,00121ea8fb06,sess token 27,vlan
0,tun 40000001,vsd 0,route 7
 if 3(nspflag 0010):1.1.100.1/1<-1.1.100.3/1,89,000000000000,sess token 8,vlan
0,tun 0,vsd 0,route 0

site3-> get sess src-ip 1.1.100.2
alloc 23/max 8064, alloc failed 0, mcast alloc 0, di alloc failed 0
total reserved 0, free sessions in shared pool 8041
Total 2 sessions according filtering criteria.
id 8045/s**,vsys 0,flag 00000040/0080/0021,policy 320002,time 6, dip 0 module 0
 if 20(nspflag 800601):1.1.100.2/1->1.1.100.3/1,89,00121ea82b86,sess token 27,vlan
0,tun 40000002,vsd 0,route 8
 if 3(nspflag 0010):1.1.100.2/1<-1.1.100.3/1,89,000000000000,sess token 8,vlan
0,tun 0,vsd 0,route 0

site3-> get sess src-ip 1.1.100.4
alloc 23/max 8064, alloc failed 0, mcast alloc 0, di alloc failed 0
```

```
total reserved 0, free sessions in shared pool 8041
Total 2 sessions according filtering criteria.
id 8046/s**,vsys 0,flag 00000040/0080/0021,policy 320002,time 5, dip 0 module 0
 if 20(nspflag 800601):1.1.100.4/1->1.1.100.3/1,89,0017cb404680,sess token 27,vlan
0,tun 40000003,vsd 0,route 9
 if 3(nspflag 0010):1.1.100.4/1<-1.1.100.3/1,89,000000000000,sess token 8,vlan
0,tun 0,vsd 0,route 0
```

Finally, check with routing table, verify that remote network is learned from OSPF.

```
site3-> get route


IPv4 Dest-Routes for <untrust-vr> (0 entries)
-------------------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2


IPv4 Dest-Routes for <trust-vr> (18 entries)
-------------------------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref    Mtr     Vsys
-------------------------------------------------------------------------------
*   2         1.1.1.3/32         eth0/0         0.0.0.0   H    0      0     Root
*  22        1.1.50.3/32        bgroup0      172.16.3.2   O   60      1     Root
*  10        1.1.50.4/32          tun.1       1.1.100.4   O   60      2     Root
*   3      172.16.3.0/24        bgroup0         0.0.0.0   C    0      0     Root
*  21      172.16.2.0/24          tun.1       1.1.100.2   O   60      2     Root
*  20      172.16.1.0/24          tun.1       1.1.100.1   O   60      2     Root
*  14      172.16.4.0/24          tun.1       1.1.100.4   O   60      2     Root
*  17      10.90.3.10/32          tun.1       1.1.100.4  E2  200      0     Root
*   9       1.1.100.4/32          tun.1         1.1.1.4   S   20      1     Root
   11       1.1.100.4/32          tun.1       1.1.100.4   O   60      1     Root
*   7       1.1.100.1/32          tun.1         1.1.1.1   S   20      1     Root
   18       1.1.100.1/32          tun.1       1.1.100.1   O   60      1     Root
*   8       1.1.100.2/32          tun.1         1.1.1.2   S   20      1     Root
   19       1.1.100.2/32          tun.1       1.1.100.2   O   60      1     Root
*   6       1.1.100.3/32          tun.1         0.0.0.0   H    0      0     Root
*   5       1.1.100.0/24          tun.1         0.0.0.0   C    0      0     Root
*   4      172.16.3.1/32        bgroup0         0.0.0.0   H    0      0     Root
*   1         1.1.1.0/24         eth0/0         0.0.0.0   C    0      0     Root
```

Sample configuration

- Site1 Firewall

```
site1-> get config
Total Config size 5509:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
set protocol ospf
set enable
exit
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 27911
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone id 100 "vpn"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "vpn" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface "tunnel.1" zone "vpn"
unset interface vlan1 ip
set interface ethernet0/0 ip 172.16.1.1/24
set interface ethernet0/0 route
set interface ethernet0/2 ip 1.1.1.1/24
set interface ethernet0/2 route
set interface tunnel.1 ip 1.1.100.1/24
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/2 ip manageable
set interface ethernet0/2 manage ping
set interface ethernet0/2 manage web
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set console page 0
set hostname site1
```



```
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "Lan1" 172.16.1.0 255.255.255.0
set address "vpn" "Site2" 172.16.2.0 255.255.255.0
set address "vpn" "Site3" 172.16.3.0 255.255.255.0
set address "vpn" "Site4" 172.16.4.0 255.255.255.0
set group address "vpn" "remote-sites"
set group address "vpn" "remote-sites" add "Site2"
set group address "vpn" "remote-sites" add "Site3"
set group address "vpn" "remote-sites" add "Site4"
set ike gateway "site1-site2" address 1.1.1.2 id "1.1.1.2" Main local-id "1.1.1.1"
outgoing-interface "ethernet0/2" preshare "LJELr7HpNMyc4fsb5DCbws1TGinb+SLR1A=="
sec-level standard
set ike gateway "site1-site3" address 1.1.1.3 id "1.1.1.3" Main local-id "1.1.1.1"
outgoing-interface "ethernet0/2" preshare "5PGwAcISNORUohsKtWCLXY5OYinTvj/9eQ=="
sec-level standard
set ike gateway "site1-site4" address 1.1.1.4 id "1.1.1.4" Main local-id "1.1.1.1"
outgoing-interface "ethernet0/2" preshare "EUPgEFrlNlqTHzsjTWC5JMymlRngAveEWA=="
sec-level standard
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "site1-site2" gateway "site1-site2" no-replay tunnel idletime 0 sec-level
standard
set vpn "site1-site2" monitor optimized rekey
set vpn "site1-site2" id 1 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.2 vpn "site1-site2"
set vpn "site1-site3" gateway "site1-site3" no-replay tunnel idletime 0 sec-level
standard
set vpn "site1-site3" monitor optimized rekey
set vpn "site1-site3" id 2 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.3 vpn "site1-site3"
set vpn "site1-site4" gateway "site1-site4" no-replay tunnel idletime 0 sec-level
standard
set vpn "site1-site4" monitor optimized rekey
set vpn "site1-site4" id 3 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.4 vpn "site1-site4"
set url protocol websense
exit
set anti-spam profile ns-profile
 set sbl default-server enable
exit
set policy id 4 from "vpn" to "Trust"  "remote-sites" "Lan1" "ANY" permit log
set policy id 4
exit
set policy id 3 from "Trust" to "vpn"  "Lan1" "remote-sites" "ANY" permit log
set policy id 3
exit
set policy id 5 from "vpn" to "vpn"  "remote-sites" "remote-sites" "ANY" permit
log
set policy id 5
exit
set nsmgmt bulkcli reboot-timeout 60
set nsmgmt bulkcli reboot-wait 0
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 1.1.100.2/32 interface tunnel.1 gateway 1.1.1.2
set route 1.1.100.3/32 interface tunnel.1 gateway 1.1.1.3
set route 1.1.100.4/32 interface tunnel.1 gateway 1.1.1.4
```

```
exit
set interface ethernet0/0 protocol ospf area 0.0.0.0
set interface ethernet0/0 protocol ospf enable
set interface ethernet0/0 protocol ospf priority 10
set interface ethernet0/0 protocol ospf cost 1
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
site1->
```

- Site2 Firewall

```
site2-> get config
Total Config size 5491:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
set protocol ospf
set enable
exit
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 27911
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone id 100 "vpn"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "vpn" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Trust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Untrust"
set interface "tunnel.1" zone "vpn"
unset interface vlan1 ip
set interface ethernet0/0 ip 172.16.2.1/24
set interface ethernet0/0 route
set interface ethernet0/2 ip 1.1.1.2/24
set interface ethernet0/2 route
set interface tunnel.1 ip 1.1.100.2/24
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/2 ip manageable
set interface ethernet0/0 manage mtrace
set interface ethernet0/2 manage web
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set console page 0
set hostname site2
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "lan2" 172.16.2.0 255.255.255.0
set address "vpn" "site1" 172.16.1.0 255.255.255.0
set address "vpn" "site3" 172.16.3.0 255.255.255.0
```

```
set address "vpn" "site4" 172.16.4.0 255.255.255.0
set group address "vpn" "remote-sites"
set group address "vpn" "remote-sites" add "site1"
set group address "vpn" "remote-sites" add "site3"
set group address "vpn" "remote-sites" add "site4"
set ike gateway "site1-site2" address 1.1.1.1 id "1.1.1.1" Main outgoing-interface
"ethernet0/2" preshare "cxFqOrojNJAgnHsoOpCSux2nwUnTwDyE5Q==" sec-level standard
set ike gateway "site2-site3" address 1.1.1.3 id "1.1.1.3" Main outgoing-interface
"ethernet0/2" preshare "Um6JUY0XNhh9Izs5iiCr1Lfg0jnezYidpw==" sec-level standard
set ike gateway "site2-site4" address 1.1.1.4 id "1.1.1.4" Main outgoing-interface
"ethernet0/2" preshare "xr+6GzjqNHXfjMsQgZCq47sWn7nges/1OA==" sec-level standard
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "site1-site2" gateway "site1-site2" no-replay tunnel idletime 0 sec-level
standard
set vpn "site1-site2" monitor optimized rekey
set vpn "site1-site2" id 1 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.1 vpn "site1-site2"
set vpn "site2-site3" gateway "site2-site3" no-replay tunnel idletime 0 sec-level
standard
set vpn "site2-site3" monitor optimized rekey
set vpn "site2-site3" id 2 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.3 vpn "site2-site3"
set vpn "site2-site4" gateway "site2-site4" no-replay tunnel idletime 0 sec-level
standard
set vpn "site2-site4" monitor optimized rekey
set vpn "site2-site4" id 3 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.4 vpn "site2-site4"
set url protocol websense
exit
set anti-spam profile ns-profile
set sbl default-server enable
exit
set policy id 1 from "Trust" to "vpn"  "lan2" "remote-sites" "ANY" permit
set policy id 1
exit
set policy id 2 from "vpn" to "Trust"  "remote-sites" "lan2" "ANY" permit
set policy id 2
exit
set policy id 3 from "vpn" to "vpn"  "remote-sites" "remote-sites" "ANY" permit
set policy id 3
exit
set nsmgmt bulkcli reboot-timeout 60
set nsmgmt bulkcli reboot-wait 0
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 1.1.100.1/32 interface tunnel.1 gateway 1.1.1.1
set route 1.1.100.3/32 interface tunnel.1 gateway 1.1.1.3
set route 1.1.100.4/32 interface tunnel.1 gateway 1.1.1.4
exit
set interface ethernet0/0 protocol ospf area 0.0.0.0
set interface ethernet0/0 protocol ospf enable
set interface ethernet0/0 protocol ospf priority 10
set interface ethernet0/0 protocol ospf cost 1
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf ignore-mtu
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
```



```
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
site2->
```

Site3 Firewall

```
site3-> get config
Total Config size 6163:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
set protocol ospf
set enable
exit
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone id 100 "vpn"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "vpn" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface adsl2/0 phy operating-mode auto
set interface "ethernet0/0" zone "Untrust"
set interface "ethernet0/1" zone "DMZ"
set interface "wireless0/0" zone "Null"
set interface "bgroup0" zone "Trust"
set interface "adsl2/0" pvc 8 35 mux llc protocol bridged qos ubr zone "Untrust"
set interface "tunnel.1" zone "vpn"
set interface bgroup0 port ethernet0/2
set interface bgroup0 port ethernet0/3
set interface bgroup0 port ethernet0/4
unset interface vlan1 ip
set interface ethernet0/0 ip 1.1.1.3/24
set interface ethernet0/0 route
set interface bgroup0 ip 172.16.3.1/24
set interface bgroup0 nat
set interface tunnel.1 ip 1.1.100.3/24
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface bgroup0 ip manageable
set interface ethernet0/0 manage ping
set interface ethernet0/0 manage web
set interface "serial0/0" modem settings "USR" init "AT&F"
set interface "serial0/0" modem settings "USR" active
set interface "serial0/0" modem speed 115200
set interface "serial0/0" modem retry 3
set interface "serial0/0" modem interval 10
set interface "serial0/0" modem idle-time 10
```

```
set flow tcp-mss
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set console page 0
set hostname site3
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "lan3" 172.16.3.0 255.255.255.0
set address "vpn" "site1" 172.16.1.0 255.255.255.0
set address "vpn" "site2" 172.16.2.0 255.255.255.0
set address "vpn" "site4" 172.16.4.0 255.255.255.0
set group address "vpn" "remote-sites"
set group address "vpn" "remote-sites" add "site1"
set group address "vpn" "remote-sites" add "site2"
set group address "vpn" "remote-sites" add "site4"
set ike gateway "site1-site3" address 1.1.1.1 id "1.1.1.1" Main local-id "1.1.1.3"
outgoing-interface "ethernet0/0" preshare "50bS1H7KNuZWNZssdxCNOxhO3ln9OYV2yA=="
sec-level standard
set ike gateway "site2-site3" address 1.1.1.2 id "1.1.1.2" Main local-id "1.1.1.3"
outgoing-interface "ethernet0/0" preshare "2WqMVUWdNtHKARsvaRC8BTeZi5nh5rtQ5w=="
sec-level standard
set ike gateway "site3-site4" address 1.1.1.4 id "1.1.1.4" Main local-id "1.1.1.3"
outgoing-interface "ethernet0/0" preshare "jdYSWfgONVsLYxstKdCAdcTIZMn6ZZnNcg=="
sec-level standard
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "site1-site3" gateway "site1-site3" no-replay tunnel idletime 0 sec-level
standard
set vpn "site1-site3" monitor optimized rekey
set vpn "site1-site3" id 1 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.1 vpn "site1-site3"
set vpn "site2-site3" gateway "site2-site3" no-replay tunnel idletime 0 sec-level
standard
set vpn "site2-site3" monitor optimized rekey
set vpn "site2-site3" id 2 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.2 vpn "site2-site3"
set vpn "site3-site4" gateway "site3-site4" no-replay tunnel idletime 0 sec-level
standard
set vpn "site3-site4" monitor optimized rekey
set vpn "site3-site4" id 3 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.4 vpn "site3-site4"
set url protocol websense
exit
set anti-spam profile ns-profile
 set sbl default-server enable
exit
set policy id 1 from "Trust" to "vpn"  "lan3" "remote-sites" "ANY" permit
set policy id 1
exit
set policy id 2 from "vpn" to "Trust"  "remote-sites" "lan3" "ANY" permit
set policy id 2
exit
set policy id 3 from "vpn" to "vpn"  "remote-sites" "remote-sites" "ANY" permit
set policy id 3
exit
set nsmgmt bulkcli reboot-timeout 60
set nsmgmt bulkcli reboot-wait 0
set ssh version v2
set config lock timeout 5
set wlan 0 channel auto
set wlan 1 channel auto
set snmp port listen 161
set snmp port trap 162
```

```
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 1.1.100.1/32 interface tunnel.1 gateway 1.1.1.1
set route 1.1.100.2/32 interface tunnel.1 gateway 1.1.1.2
set route 1.1.100.4/32 interface tunnel.1 gateway 1.1.1.4
exit
set interface bgroup0 protocol ospf area 0.0.0.0
set interface bgroup0 protocol ospf enable
set interface bgroup0 protocol ospf priority 10
set interface bgroup0 protocol ospf cost 1
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf ignore-mtu
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
site3->
```

- Site4 Firewall

```
site4-> get config
Total Config size 5522:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
set protocol ospf
set enable
exit
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone id 100 "vpn"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "vpn" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Untrust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Trust"
set interface "bri1/0" zone "Untrust"
set interface "tunnel.1" zone "vpn"
set interface ethernet0/0 ip 1.1.1.4/24
set interface ethernet0/0 route
unset interface vlan1 ip
set interface ethernet0/2 ip 172.16.4.1/24
set interface ethernet0/2 nat
set interface tunnel.1 ip 1.1.100.4/24
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/2 ip manageable
set interface ethernet0/0 manage ping
set interface ethernet0/0 manage web
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set console page 0
set hostname site4
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "lan4" 172.16.4.0 255.255.255.0
set address "vpn" "site1" 172.16.1.0 255.255.255.0
```

```
set address "vpn" "site2" 172.16.2.0 255.255.255.0
set address "vpn" "site3" 172.16.3.0 255.255.255.0
set group address "vpn" "remote-sites"
set group address "vpn" "remote-sites" add "site1"
set group address "vpn" "remote-sites" add "site2"
set group address "vpn" "remote-sites" add "site3"
set ike gateway "site1-site4" address 1.1.1.1 id "1.1.1.1" Main local-id "1.1.1.4"
outgoing-interface "ethernet0/0" preshare "hja8q3MjNUesMns7DgCGLwWJmpnlHcbw9w=="
sec-level standard
set ike gateway "site2-site4" address 1.1.1.2 id "1.1.1.2" Main local-id "1.1.1.4"
outgoing-interface "ethernet0/0" preshare "p7Kypti9NYiJIRs4X2CqOn3BERn2q+H8wA=="
sec-level standard
set ike gateway "site3-site4" address 1.1.1.3 id "1.1.1.3" Main local-id "1.1.1.4"
outgoing-interface "ethernet0/0" preshare "MqBQaajGNcAqmjsP9PC6V/6c2Bn6yiGMCQ=="
sec-level standard
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vpn "site1-site4" gateway "site1-site4" no-replay tunnel idletime 0 sec-level
standard
set vpn "site1-site4" monitor optimized rekey
set vpn "site1-site4" id 1 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.1 vpn "site1-site4"
set vpn "site2-site4" gateway "site2-site4" no-replay tunnel idletime 0 sec-level
standard
set vpn "site2-site4" monitor optimized rekey
set vpn "site2-site4" id 2 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.2 vpn "site2-site4"
set vpn "site3-site4" gateway "site3-site4" no-replay tunnel idletime 0 sec-level
standard
set vpn "site3-site4" monitor optimized rekey
set vpn "site3-site4" id 3 bind interface tunnel.1
set interface tunnel.1 nhtb 1.1.1.3 vpn "site3-site4"
set url protocol websense
exit
set policy id 1 from "Trust" to "vpn"  "lan4" "remote-sites" "ANY" permit
set policy id 1
exit
set policy id 2 from "vpn" to "Trust"  "remote-sites" "lan4" "ANY" permit
set policy id 2
exit
set policy id 3 from "vpn" to "vpn"  "remote-sites" "remote-sites" "ANY" permit
set policy id 3
exit
set nsmgmt bulkcli reboot-timeout 60
set nsmgmt bulkcli reboot-wait 0
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 1.1.100.1/32 interface tunnel.1 gateway 1.1.1.1
set route 1.1.100.2/32 interface tunnel.1 gateway 1.1.1.2
set route 1.1.100.3/32 interface tunnel.1 gateway 1.1.1.3
exit
set interface ethernet0/2 protocol ospf area 0.0.0.0
set interface ethernet0/2 protocol ospf enable
set interface ethernet0/2 protocol ospf priority 10
set interface ethernet0/2 protocol ospf cost 1
set interface tunnel.1 protocol ospf area 0.0.0.0
set interface tunnel.1 protocol ospf ignore-mtu
set interface tunnel.1 protocol ospf link-type p2mp
```



```
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf priority 10
set interface tunnel.1 protocol ospf cost 1
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
site4->
```