Application Note

Configure Route-based Hub and Spoke VPN

Version 1.3

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

Contents

Introduction

When connecting multiple sites via VPNs, it is important to consider the overall layout of the tunnel interconnections. One option is a full mesh of VPNs. In a full mesh, every site has a VPN to every other site in the network. While interconnectivity is available, this approach has significant disadvantages when it comes to performance and manageability, and in some cases isn't even possible due to system limitations.

Initially, most VPNs are deployed in a configuration allowing remote users to reach a central site to access key resources. However, as networks grow, individuals might need to create tunnels to more than just the central network site.

A hub-and-spoke design addresses this by allowing a central, powerful site to act as a hub with a series of VPN tunnels branching out from it like spokes to perimeter sites. Consequently, each remote site need only maintain a single tunnel for all VPN communications.

The Hub and Spoke system allows the firewall to act as a relay for VPN sessions established between the hub and spoke firewalls. The Hub firewall actually encrypts and decrypts the data, allowing the Hub firewall to further apply security rules, which enhance the flexibility to apply security policy.

Included Platforms and ScreenOS

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

- ScreenOS 5.x
- 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

Why Route-Based VPNs

There are several key benefits to using Route-based VPNs over Policy-based VPNs. In addition to being simpler to configure, with Route-based VPNs, network functions are separated from policy functions. Changes can be made to a permit or deny policy on one end of a tunnel without effecting the other end of the tunnel. Additionally, in a Route-based VPN, with the implementation of routing update protocols (such as OSPF), changes in the network architecture behind the tunnel end points will not affect the tunnel. In a dynamic implementation, it is possible to configure parallel tunnels across separate service providers, thus allowing for reliable failover. How to setup dynamic routing protocols with VPNs is beyond the scope of this document but should be taken into design consideration when planning the VPN network; consult the application note http://kb.juniper.net/kb/documents/public/ApplicationNotes/Technical/ScreenOS%204.0.0/VPN-400-001.htm for dynamic routing protocols with VPNs.

Packet handling

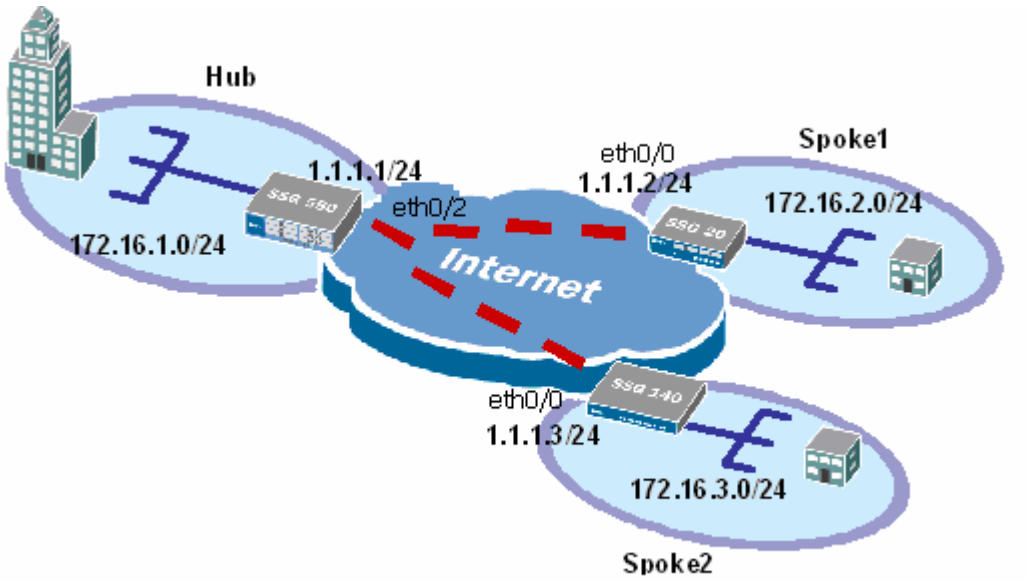
With Route-based VPNs, the routing table is used to determine where the packet is sent; not the policy. As a packet arrives at the Juniper firewall device, the interface module determines the zone in which it arrived. If there is not an existing session, a route look-up is performed. Before the Juniper firewall routes the packet, in accordance with the route table, a policy look-up is conducted. If a policy match is found, the specified action is taken. Note, the action is either permit or deny in the case of route-based VPNs; not tunnel.

Recall, policies are used when communicating from one zone to a different zone or when intrazone policies are activated. This is an important note to consider when designing Route-based VPNs. If the tunnel interface is created in the trust zone and intrazone policies are not defined, policies are not needed if the data is traversing to/from the same zone, i.e. trust. Another option is to create a custom "*vpn* zone" and create the tunnel interface in the *vpn* zone. Then policies are needed between the Trust and *vpn* zones to allow data to traverse.

Network Diagram

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

Figure 1.



Configuration Overview

Configuring the Hub and Spoke VPN environment; although there are many variations of a Hub and Spoke VPN this document addresses the most basic.

In this setup, SSG550 is acting as a Hub firewall, whereas SSG20 and SSG140 are the Spokes. Each Spoke will have only one VPN connection which is terminated on the Hub. With Hub and Spoke VPN configurations, VPN traffic between Spokes will use the same tunnel to the Hub.

The setup for this application note consisted of

- Three SSG firewalls, with SSG550 to be the Hub, SSG5 and SSG20 are the Spokes, that are connected via the Internet
- Tunnels are created between the Hub and each Spoke (shown as a dotted red line). The Hub firewall will have 2 tunnels created via one interface, eth0/2.
- Pre-Shared keys are configured
- Additional routes are added to the firewalls to provide communication to each of the trusted networks .

Configuration Steps

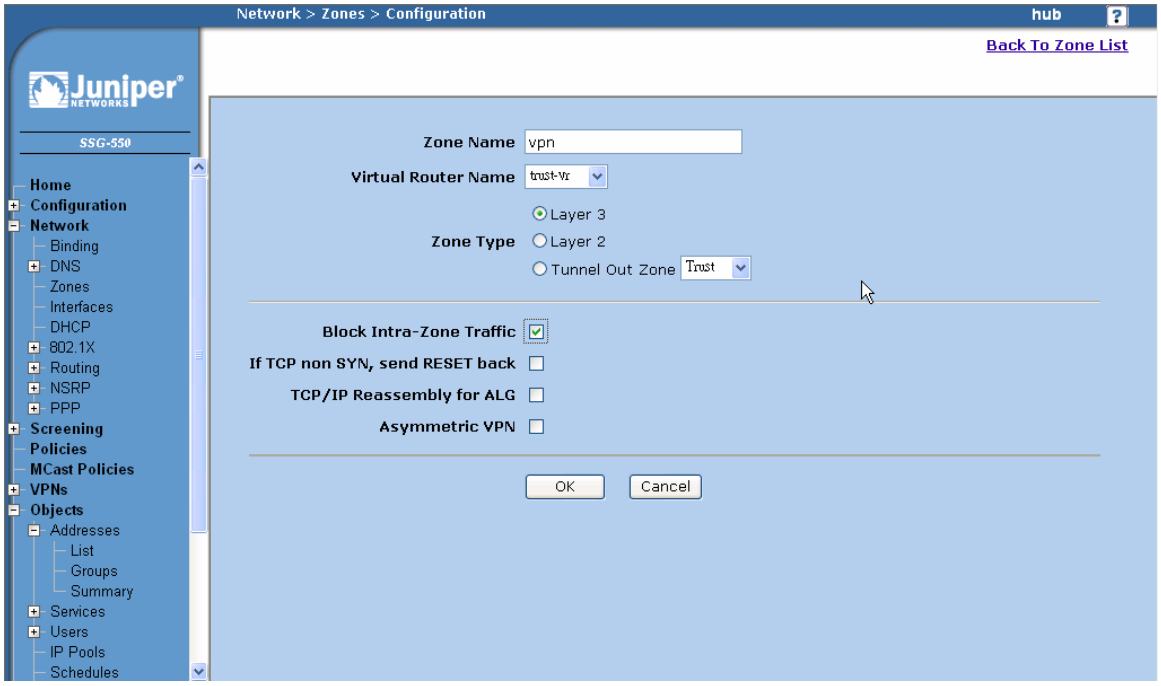
Step 1: Create the tunnel interface

In configuring the tunnel interface the administrator selects the zone to which the tunnel interface will bound and the IP address to use. In this document, the tunnel interface is assigned to custom zone -- *vpn* zone, and therefore the tunnel will terminate in the *vpn* zone.

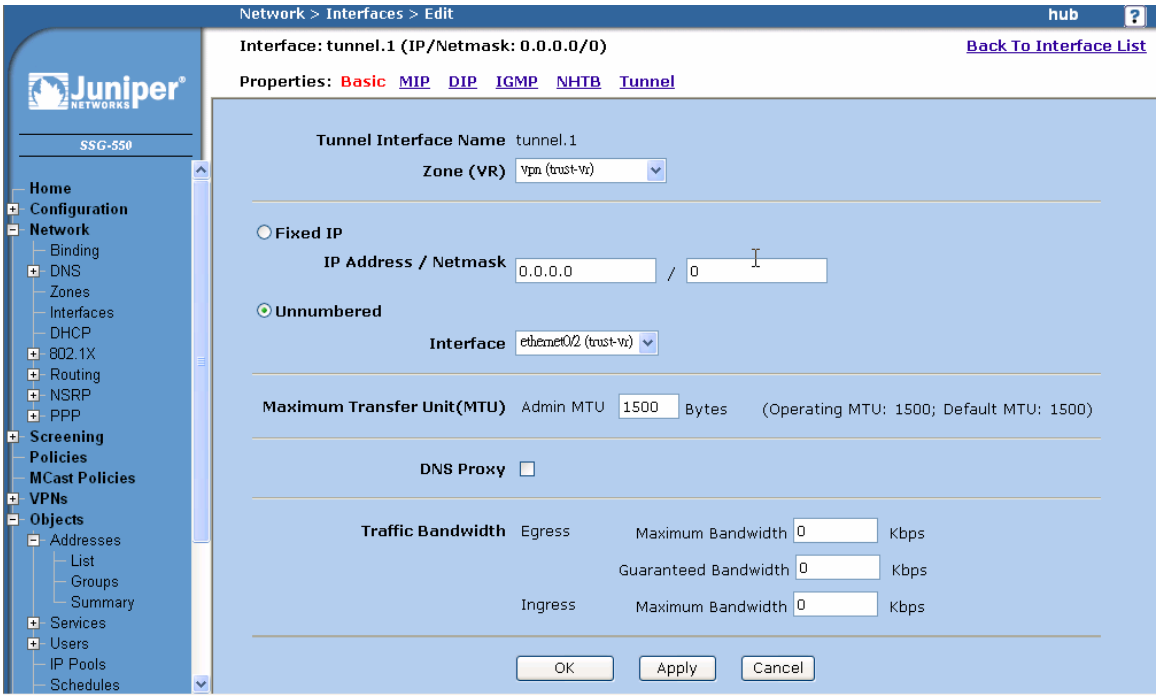
When a tunnel terminates in the *vpn* zone and the target network is in the *trust* zone, a permit or deny policy will be required to move the traffic from the *vpn* zone to the *trust* zone. If the tunnel is terminated on the trust side (i.e. the tunnel interface is created in the trust zone), traffic is allowed unless an intra-zone policy defined specifying another action.

The IP address can either be fixed IP or unnumbered. An unnumbered assignment borrows the IP address of the selected interface. If a fixed IP address is selected, the address must be accessible (at minimum via ping) from the other tunnel end-point.

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:

WebUI:

Hub 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)

Unnumbered: (select)

Interface: ethernet0/2(trust/vr)*

Interface tunnel.2:

Choose "Tunnel IF" and click New

Tunnel Interface Name: tunnel.2

Zone (VR): vpn (trust-vr)

Select Network > Interface

Unnumbered: (select)

Interface: ethernet0/2(trust/vr)*

Spoke1 and Spoke2 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)

Unnumbered: (select)

Interface: ethernet0/0(trust/vr)*

CLI:

Hub firewall

```
set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip unnumbered interface ethernet0/2*
set interface tunnel.2 zone vpn
set interface tunnel.2 ip unnumbered interface ethernet0/2*
```

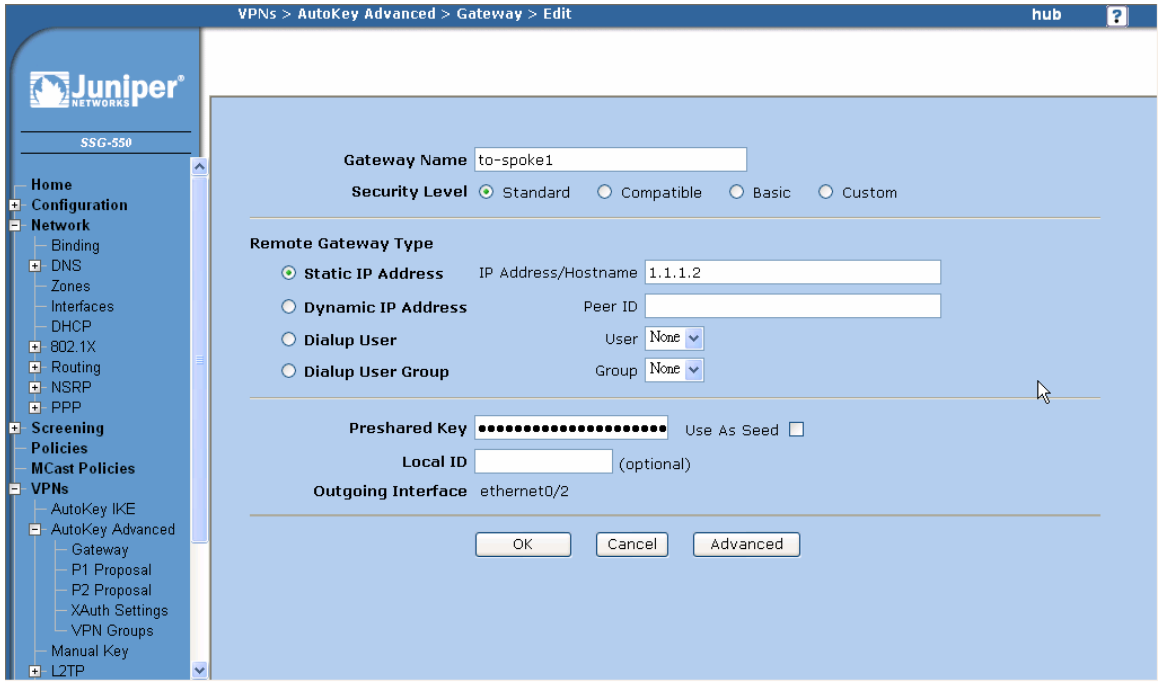
Spoke1 and Spoke2 firewall

```
set zone name vpn
set interface tunnel1.zone vpn
set interface tunnel.1 ip unnumbered interface ethernet0/0*
```

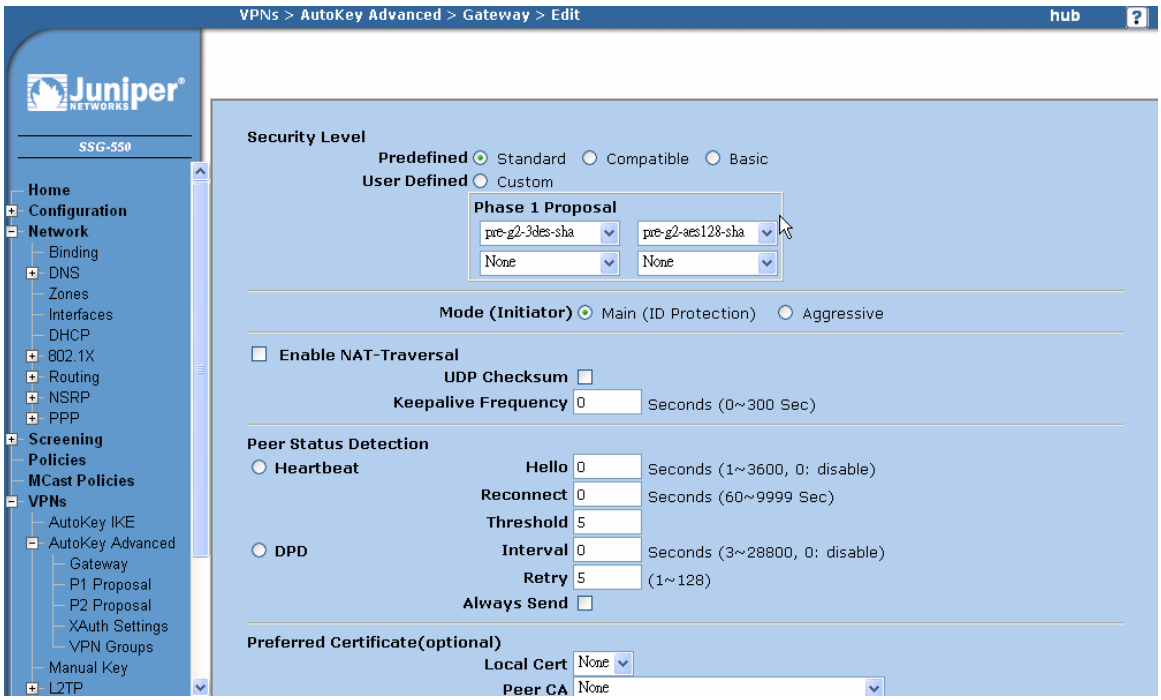
*note interface name may varies depends on the assignment of untrust interface.

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. On the hub firewall, an IKE gateway is configured for each Hub to Spoke tunnel. In this example, there will be 2 tunnels created: vpn-spoke1 and vpn-spoke2. On each spoke firewall, the peer tunnel from each Spoke back to the Hub is also created.



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 the test lab, the untrust interface was used for both VPN tunnels from the Hub to Spoke1 and Hub to Spoke2.
- 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:

Hub firewall

To Spoke1:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:

Gateway Name: to-spoke1

Seccurity Level: Standard

Static IP Address: (selected)

IP Address/Hostname: 1.1.1.2

Preshare Key: netscreen

Outgoing Interface: ethernet0/2*

Select Advanced:

Mode (Initiator): Main (ID Protection)

Select Return and OK

To Spoke2:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:

Gateway Name: to-spoke2

Security Level: Standard

Static IP Address: (selected)

IP Address/Hostname: 1.1.1.3

Preshare Key: netscreen

Outgoing Interface: ethernet0/2*

Select Advanced:

Mode (Initiator): Main (ID Protection)

Select Return and OK

Spoke1 and Spoke2 firewall

To Hub:

Select VPNs > AutoKey Advanced > Gateway, select New and enter following:

Gateway Name: to-hub

Security Level: Standard

Static IP Address: (selected)

IP Address/Hostname: 1.1.1.1

Preshare Key: netscreen

Outgoing Interface: ethernet0/0 (** see Note)

Select Advanced:

Mode (Initiator): Main (ID Protection)

Select Return and OK

CLI:

Hub firewall

```
set ike gateway to-spoke1 address 1.1.1.2 main outgoing-interface ethernet0/2**
preshare netscreen sec-level standard

set ike gateway to-spoke2 address 1.1.1.3 main outgoing-interface ethernet0/2**
preshare netscreen sec-level standard
```

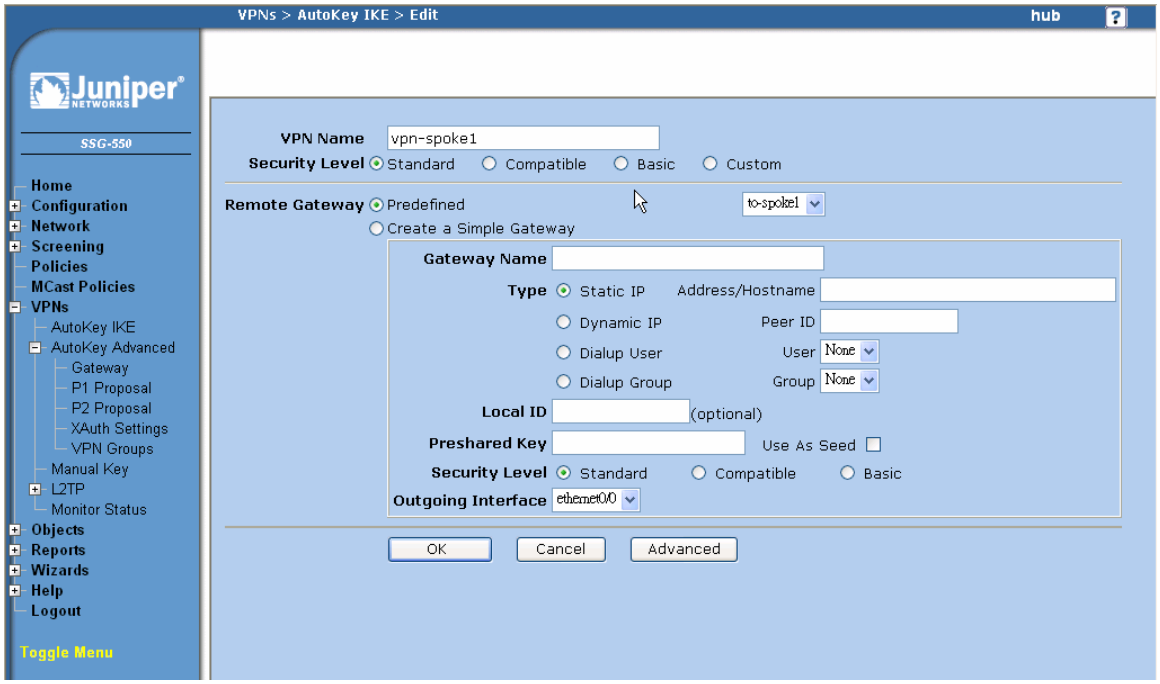
Spoke1 and Spoke2 firewall

```
set ike gateway to-hub address 1.1.1.1 main outgoing-interface ethernet0/0*
preshare netscreen sec-level stand
```

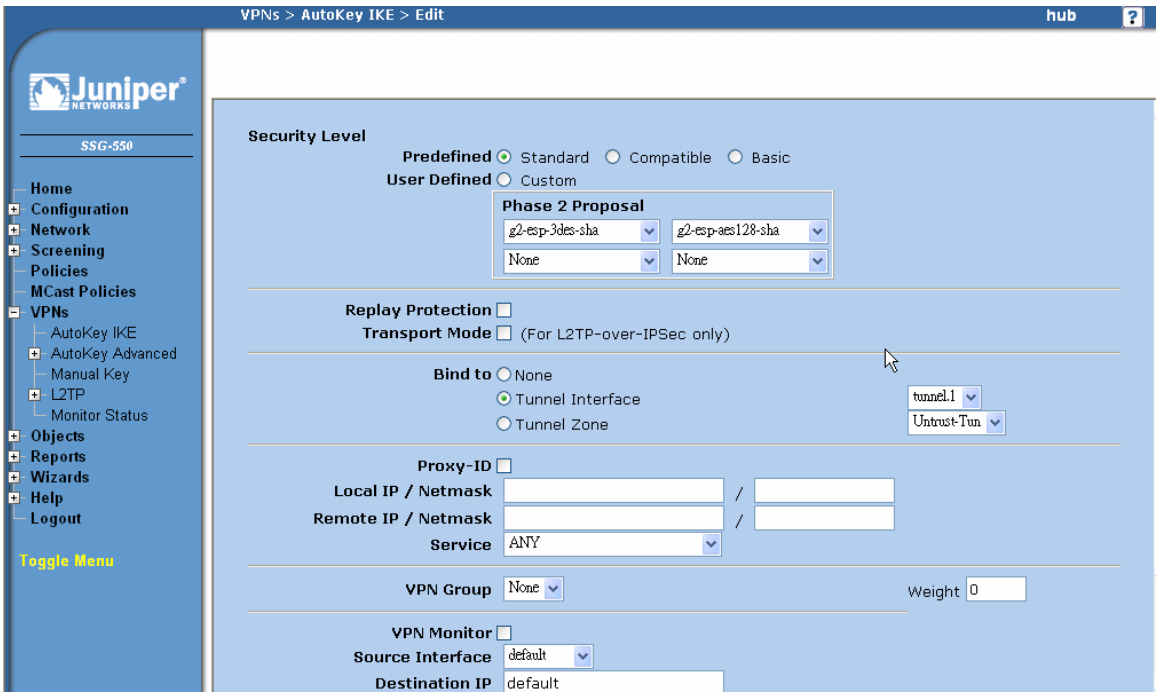
**Note: interface name may varies depends on the assignment of untrust interface.

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 and the IKE Gateway to be associated with the VPN Tunnel.



In the example, vpn-spoke1 is the name given to the tunnel from the Hub device to the Spoke1 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 VPN is bound to the tunnel interface created in step 1.

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

WebUI:

Hub firewall

To Spoke1:

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

VPN Name: vpn-spoke1

Security Level: Standard

Remote Gateway: Predefined (selected), to-spoke1 (select from pull down menu)

Select Advanced

Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)

Select Return and OK

To Spoke2:

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

VPN Name: vpn-spoke2

Security Level: Standard

Remote Gateway: Predefined (selected), to-spoke1 (select from pull down menu)

Select Advanced

Bind to: Tunnel Interface (checked), tunnel.2 (select from pull down menu)

Select Return and OK

Spoke1 firewall

To Hub:

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

VPN Name: vpn-spoke1

Security Level: Standard

Remote Gateway: Predefined (selected), to-spoke1 (select from pull down menu)

Select Advanced

Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)

Select Return and OK

Spoke2 firewall

To Hub:

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

VPN Name: vpn-spoke2

Security Level: Standard

Remote Gateway: Predefined (selected), to-spoke1 (select from pull down menu)

Select Advanced

Bind to: Tunnel Interface (checked), tunnel.1 (select from pull down menu)

Select Return and OK

CLI:

Hub firewall

To Spoke1:

```
set vpn vpn-spoke1 gateway to-spoke1 sec-level standard
set vpn vpn-spoke1 bind interface tunnel.1
```

To Spoke2:

```
set vpn vpn-spoke2 gateway to-spoke2 sec-level standard
set vpn vpn-spoke2 bind interface tunnel.2
```

Spoke1 firewall

```
set vpn vpn-spoke1 gateway to-hub sec-level standard

set vpn vpn-spoke1 bind interface tunnel.1
```

Spoke2 firewall

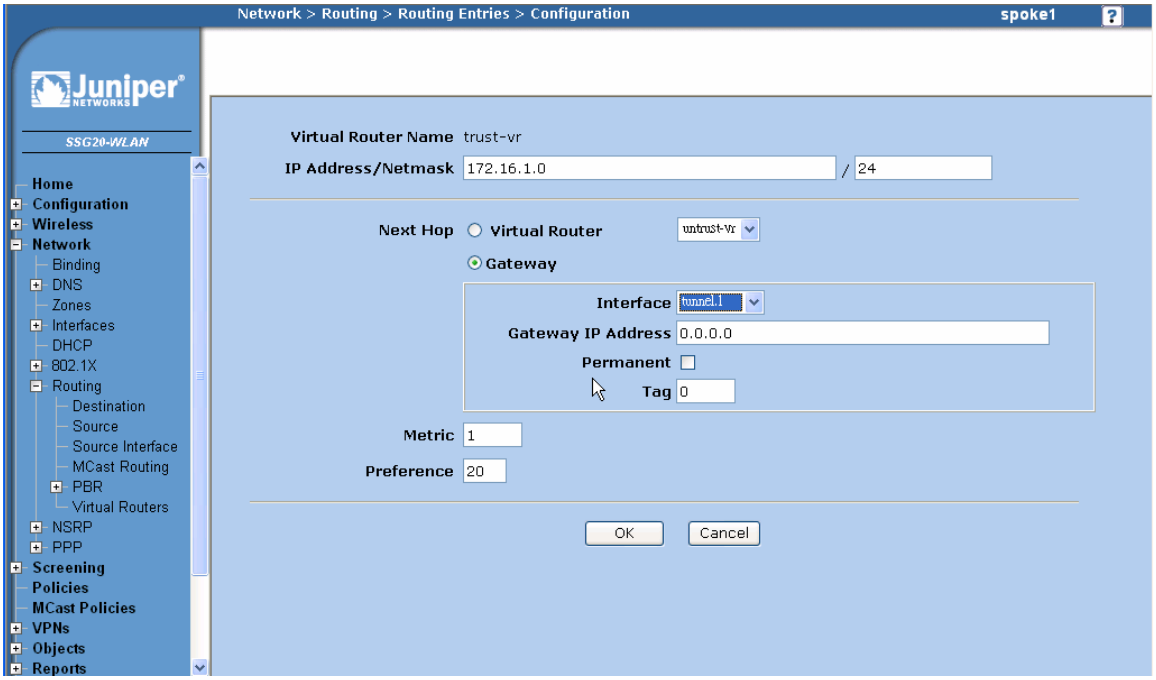
```
set vpn vpn-spoke2 gateway to-hub sec-level standard

set vpn vpn-spoke2 bind interface tunnel.1
```

Step 4: Add Routes

The routes determine the direction the traffic should take. On each Hub and Spoke, add the networks or devices that are accessible via the specified tunnel.

For example, to reach the 172.16.1.0/24 from Spoke1, the traffic is sent through the tunnel.1 interface with the following route entry. (A specific address or network range can be entered for each route entry.)



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

WebUI:

Hub firewall

To Spoke1:

Select Network > Routing > Destination, select New and enter following:

IP Address / Netmask: 172.16.2.0 / 24

Next Hop: Gateway (selected)

Interface: tunnel.1 (select from pull down menu)

Select OK

To Spoke2:

Select Network > Routing > Destination, select New and enter following:

IP Address / Netmask: 172.16.3.0 / 24

Next Hop: Gateway (selected)

Interface: tunnel.2 (select from pull down menu)

Select OK

Spoke1 firewall

To Hub:

Select Network > Routing > Destination, select New and enter following:

IP Address / Netmask: 172.16.1.0/ 24

Next Hop: Gateway (selected)

Interface: tunnel.1 (select from pull down menu)

Select OK

To Spoke2:

Select Network > Routing > Destination, select New and enter following:

IP Address / Netmask: 172.16.3.0/ 24

Next Hop: Gateway (selected)

Interface: tunnel.1 (select from pull down menu)

Select OK

Spoke2 firewall

To Hub:

Select Network > Routing > Destination, select New and enter following:

IP Address / Netmask: 172.16.1.0/ 24

Next Hop: Gateway (selected)

Interface: tunnel.1 (select from pull down menu)

Select OK

To spoke1:

Select Network > Routing > Destination, select New and enter following:

IP Address / Netmask: 172.16.2.0/ 24

Next Hop: Gateway (selected)

Interface: tunnel.1 (select from pull down menu)

Select OK

CLI:

Hub firewall

To spoke1:

```
set route 172.16.2.0/24 interface tunnel.1
```

To spoke2:

```
set route 172.16.3.0/24 interface tunnel.2
```

Spoke1 firewall

To Hub:

```
set route 172.16.1.0/24 interface tunnel.1
```

To Spoke2:

```
set route 172.16.3.0/24 interface tunnel.1
```

Spoke1 firewall

To Hub:

```
set route 172.16.1.0/24 interface tunnel.1
```

To Spoke1:

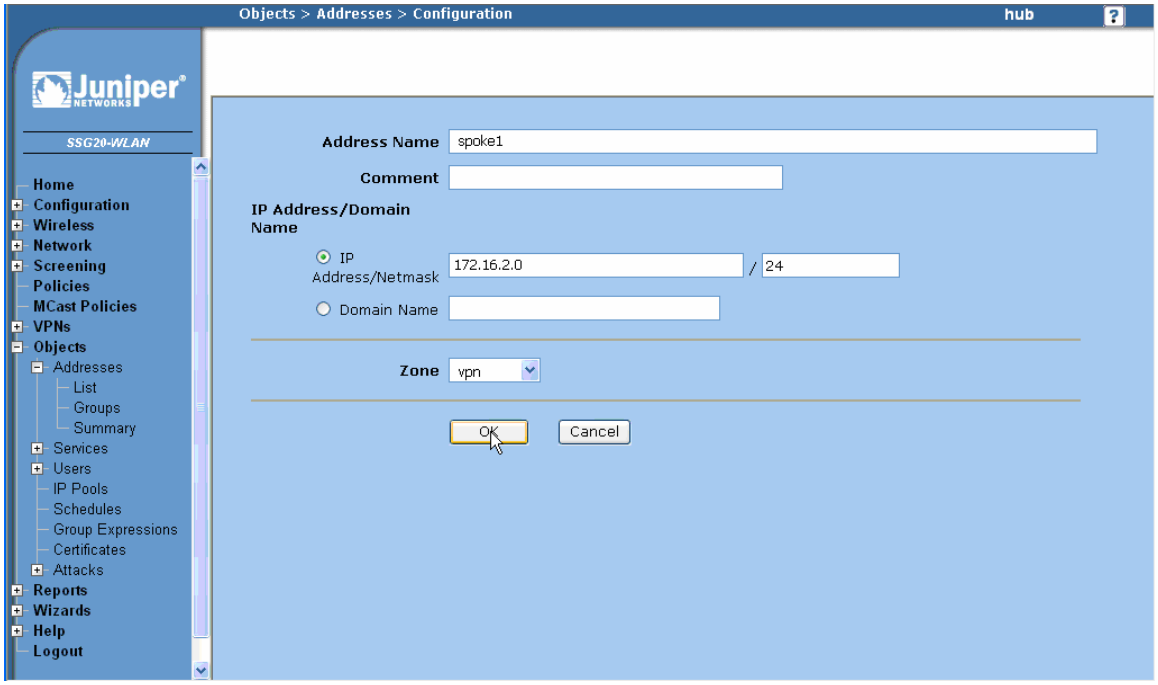
```
set route 172.16.2.0/24 interface tunnel.1
```

Step 5: Configure policy to allow traffic between spokes

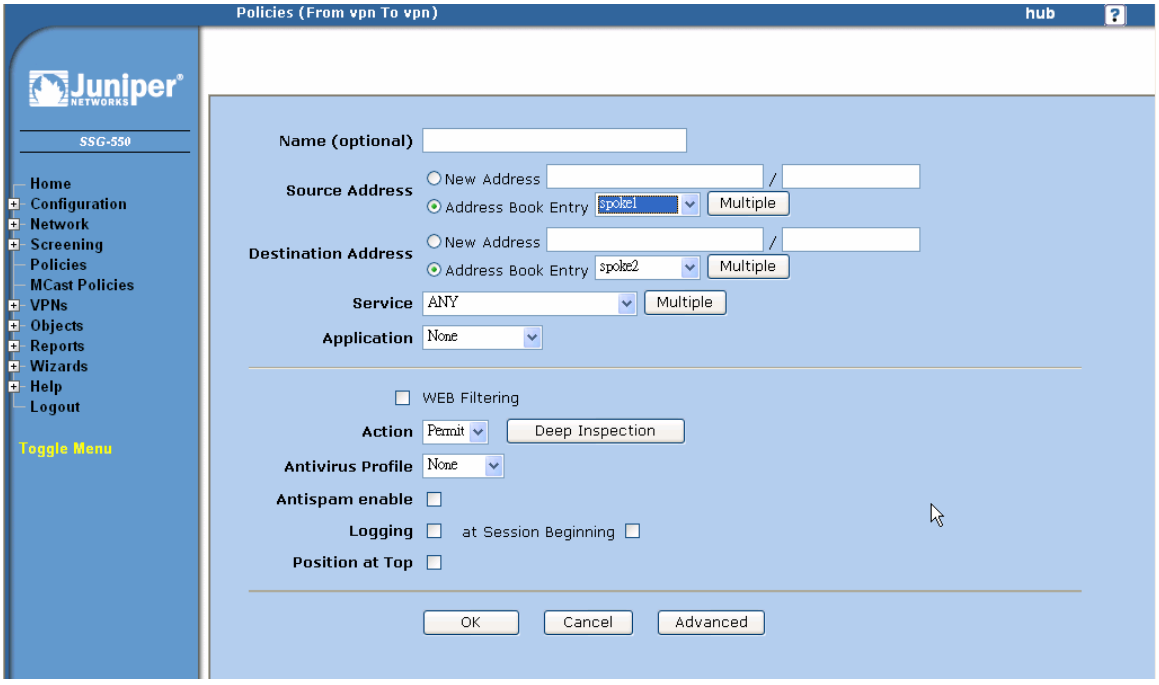
Because the tunnel interface was created in the *vpn* zone and it is configured to block intra-zone traffic, the firewall does require a policy to permit the traffic between spokes on the Hub firewall.

In addition, a policy (to and from the *vpn* and trust zone) on the spoke firewalls is required to permit traffic between the spoke firewalls.

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.



WebUI:

Hub firewall

Define address objects:

Select Objects > Addresses > List > vpn (pull down menu).

Select New then enter following:

Address Name: spoke1

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: spoke2

IP Address/Domain Name: IP Address/Netmask (checked), 172.16.3.0/24

Define policy: (Spoke1 to Spoke2)

Select Policies

From: vpn (pull down menu)

To: vpn (pull down menu)

Select New

Source Address: Address Book Entry: spoke1 (pull down menu)

Destination Address: Address Book Entry: spoke2 (pull down menu)

Select OK

Define policy: (Spoke2 to Spoke1)

Select Policies

From: vpn (pull down menu)

To: vpn (pull down menu)

Select New

Source Address: Address Book Entry: spoke2 (pull down menu)

Destination Address: Address Book Entry: spoke1 (pull down menu)

Select OK

Spoke1 firewall

Define address objects:

Select Objects > Addresses > List > Trust (pull down menu).

Select New then enter following:

Address Name: spoke1

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: spoke2

IP Address/Domain Name: IP Address/Netmask (checked), 172.16.3.0/24

Define policy: (Spoke1 to Spoke2)

Select Policies

From: Trust (pull down menu)

To: vpn (pull down menu)

Select New

Source Address: Address Book Entry: spoke1 (pull down menu)

Destination Address: Address Book Entry: spoke2 (pull down menu)

Select OK

Define policy: (Spoke2 to Spoke1)

Select Policies

From: vpn (pull down menu)

To: Trust (pull down menu)

Select New

Source Address: Address Book Entry: spoke2 (pull down menu)

Destination Address: Address Book Entry: spoke1 (pull down menu)

Select OK

Spoke2 firewall

Define address objects:

Select Objects > Addresses > List > Trust (pull down menu).

Select New then enter following:

Address Name: spoke2

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: spoke1

IP Address/Domain Name: IP Address/Netmask (checked), 172.16.2.0/24

Define policy: (Spoke1 to Spoke2)

Select Policies

From: Trust (pull down menu)

To: vpn (pull down menu)

Select New

Source Address: Address Book Entry: spoke2 (pull down menu)

Destination Address: Address Book Entry: spoke1 (pull down menu)

Select OK

Define policy: (Spoke2 to Spoke1)

Select Policies

From: vpn (pull down menu)

To: Trust (pull down menu)

Select New

Source Address: Address Book Entry: spoke1 (pull down menu)

Destination Address: Address Book Entry: spoke2 (pull down menu)

Select OK

CLI:

Hub firewall

```
set address vpn spoke1 172.16.2.0/24
set address vpn spoke2 172.16.3.0/24
set policy from vpn to vpn spoke1 spoke2 any permit
set policy from vpn to vpn spoke2 spoke1 any permit
```

Spoke1 firewall

```
set address trust spoke1 172.16.2.0/24
set address vpn spoke2 172.16.3.0/24
set policy from trust to vpn spoke1 spoke2 any permit
set policy from vpn to trust spoke2 spoke1 any permit
```

Spoke2 firewall

```
set address trust spoke1 172.16.3.0/24
set address vpn spoke2 172.16.2.0/24
set policy from trust to vpn spoke2 spoke1 any permit
set policy from vpn to trust spoke1 spoke2 any permit
```

Verifying Configuration

To check with VPN between spokes, 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 vpn between:

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

- Spoke1 and Hub

```
spoke1-> ping 172.16.1.1 from bgroup0
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 1 seconds from bgroup0
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=2/2/3 ms
```

- Spoke2 and Hub

```
spoke2-> ping 172.16.1.1 from e0/3
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 1 seconds from
ethernet0/3
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=1/1/4 ms
```

- Spoke1 and Spoke2

```
spoke1-> ping 172.16.3.1 from bgroup0
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 172.16.3.1, 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:

```
hub-> get sa
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<         1.1.1.2  500 esp:3des/sha1 5b0d6a9c  3053 unlim A/-    -1 0
00000001>         1.1.1.2  500 esp:3des/sha1 c69306ed  3053 unlim A/-    -1 0
00000002<         1.1.1.3  500 esp:3des/sha1 5c0d6a9c  3054 unlim A/-    -1 0
00000002>         1.1.1.3  500 esp:3des/sha1 f629a51c  3054 unlim A/-    -1 0
```

Check with SA for the corresponding gateway (reference by IP address) , status A means Active, which means the tunnel is ready for traffic.

Sample configuration

- Hub firewall

```
hub-> get config
Total Config size 4403:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
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"
set interface "tunnel.2" zone "vpn"
unset interface vlan1 ip
set interface ethernet0/0 ip 172.16.1.1/24
set interface ethernet0/0 nat
set interface ethernet0/2 ip 1.1.1.1/24
set interface ethernet0/2 route
set interface tunnel.1 ip unnumbered interface ethernet0/2
set interface tunnel.2 ip unnumbered interface ethernet0/2
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 hostname hub
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "hub" 172.16.1.0 255.255.255.0
set address "vpn" "spoke1" 172.16.2.0 255.255.255.0
set address "vpn" "spoke2" 172.16.3.0 255.255.255.0
set ike gateway "to-spoke1" address 1.1.1.2 Main outgoing-interface "ethernet0/2"
preshare "EfKJtytrNVpN80s66UC7IrHSO/ni+RtujA==" sec-level standard
set ike gateway "to-spoke2" address 1.1.1.3 Main outgoing-interface "ethernet0/2"
preshare "iT2eNR36NCzE4YsbhBCBOieTuYnh3ya5Vg==" 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 "vpn-spoke1" gateway "to-spoke1" no-replay tunnel idletime 0 sec-level
standard
set vpn "vpn-spoke1" id 3 bind interface tunnel.1
set vpn "vpn-spoke2" gateway "to-spoke2" no-replay tunnel idletime 0 sec-level
standard
set vpn "vpn-spoke2" id 4 bind interface tunnel.2
set url protocol websense
exit
set anti-spam profile ns-profile
 set sbl default-server enable
exit
set policy id 7 from "vpn" to "Trust"  "spoke1" "hub" "ANY" permit
set policy id 7
exit
set policy id 8 from "Trust" to "vpn"  "hub" "spoke1" "ANY" permit
set policy id 8
exit
set policy id 10 from "Trust" to "vpn"  "hub" "spoke2" "ANY" permit
set policy id 10
exit
set policy id 11 from "vpn" to "Trust"  "spoke2" "hub" "ANY" permit
set policy id 11
exit
set policy id 12 from "vpn" to "vpn"  "spoke1" "spoke2" "ANY" permit
set policy id 12
exit
set policy id 13 from "vpn" to "vpn"  "spoke2" "spoke1" "ANY" permit
set policy id 13
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 172.16.2.0/24 interface tunnel.1
set route 172.16.3.0/24 interface tunnel.2
exit
set vrouter "untrust-vr"
```

```
exit
set vrouter "trust-vr"
exit
```

Spoke1 firewall

```
spoke1-> get config
Total Config size 4723:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
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 1.1.1.2/24
set interface ethernet0/0 route
set interface bgroup0 ip 172.16.2.1/24
set interface bgroup0 nat
set interface tunnel.1 ip unnumbered interface ethernet0/0
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 interface wireless0/0 shutdown
set interface wireless0/1 shutdown
set interface wireless0/2 shutdown
set interface wireless0/3 shutdown
set flow tcp-mss
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set hostname spoke1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "spoke1" 172.16.2.0 255.255.255.0
set address "vpn" "hub" 172.16.1.0 255.255.255.0
set address "vpn" "spoke2" 172.16.3.0 255.255.255.0
set ike gateway "to-hub" address 1.1.1.1 Main outgoing-interface "ethernet0/0"
preshare "ynAFDfcYNBb6U+s+ZFCWwZ2X4vnjyp7s/A==" 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 "vpn-spoke1" gateway "to-hub" no-replay tunnel idletime 0 sec-level
standard
set vpn "vpn-spoke1" id 3 bind interface tunnel.1
set url protocol websense
exit
set anti-spam profile ns-profile
 set sbl default-server enable
exit
set policy id 5 from "vpn" to "Trust"  "hub" "spoke1" "ANY" permit
set policy id 5
exit
set policy id 6 from "Trust" to "vpn"  "spoke1" "hub" "ANY" permit
set policy id 6
exit
set policy id 7 from "Trust" to "vpn"  "spoke1" "spoke2" "ANY" permit
set policy id 7
exit
set policy id 8 from "vpn" to "Trust"  "spoke2" "spoke1" "ANY" permit
set policy id 8
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 172.16.1.0/24 interface tunnel.1
set route 172.16.3.0/24 interface tunnel.1
```

```
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
spoke1->
```

- Spoke2 firewall

```
spoke2-> get config
Total Config size 3985:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
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 "Untrust"
set interface "ethernet0/3" zone "Trust"
set interface "bri1/0" zone "Untrust"
set interface "tunnel.1" zone "vpn"
set interface ethernet0/0 ip 1.1.1.3/24
set interface ethernet0/0 route
unset interface vlan1 ip
set interface ethernet0/3 ip 172.16.3.1/24
set interface ethernet0/3 nat
set interface tunnel.1 ip unnumbered interface ethernet0/0
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/3 ip manageable
set interface ethernet0/0 manage web
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set hostname spoke2
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "spoke2" 172.16.3.0 255.255.255.0
set address "vpn" "hub" 172.16.1.0 255.255.255.0
set address "vpn" "spoke1" 172.16.2.0 255.255.255.0
set ike gateway "to-hub" address 1.1.1.1 Main outgoing-interface "ethernet0/0"
preshare "KIMOqV10NA6Zc0sGCvCrvFE0hInJILlrig==" 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 "vpn-spoke2" gateway "to-hub" no-replay tunnel idletime 0 sec-level
standard
set vpn "vpn-spoke2" id 1 bind interface tunnel.1
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"  "spoke2" "hub" "ANY" permit
set policy id 1
exit
set policy id 2 from "vpn" to "Trust"  "hub" "spoke2" "ANY" permit
set policy id 2
exit
set policy id 3 from "Trust" to "vpn"  "spoke2" "spoke1" "ANY" permit
set policy id 3
exit
set policy id 4 from "vpn" to "Trust"  "spoke1" "spoke2" "ANY" permit
set policy id 4
exit
set nsmgmt bulkcli reboot-timeout 60
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 172.16.1.0/24 interface tunnel.1
set route 172.16.2.0/24 interface tunnel.1
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
spoke2->
```