

Juniper SSG 5 (ScreenOS 6) Site2Site-VPN Howto

David Rupprechter / rupprechter@dotlike.net / www.dotlike.net / 2011

First of all open the menu item „Gateway“ in „VPNs“.

Create a gateway like this on Site A:

The screenshot shows the configuration window for a gateway on Site B. The 'Gateway Name' field is set to 'SSG5 - Site B'. The 'Version' is set to 'IKEv1'. Under the 'Remote Gateway' section, 'Static IP Address' is selected, and the 'IP Address/Hostname' is set to 'External IP- Site B'. Other options like 'Dynamic IP Address', 'Dialup User', 'Dialup User Group', 'ACVPN-Dynamic', and 'ACVPN-Profile' are unselected. The 'Local ID' field contains '[DistinguishedName]'. The 'Peer ID', 'User', and 'Group' fields are empty or set to 'None'. At the bottom, there are 'OK', 'Cancel', and 'Advanced' buttons.

Create a gateway like this on Site B:

The screenshot shows the configuration window for a gateway on Site A. The 'Gateway Name' field is set to 'SSG5 - Site A'. The 'Version' is set to 'IKEv1'. Under the 'Remote Gateway' section, 'Static IP Address' is selected, and the 'IP Address/Hostname' is set to 'External IP- Site A'. Other options like 'Dynamic IP Address', 'Dialup User', 'Dialup User Group', 'ACVPN-Dynamic', and 'ACVPN-Profile' are unselected. The 'Local ID' field contains '[DistinguishedName]'. The 'Peer ID', 'User', and 'Group' fields are empty or set to 'None'. At the bottom, there are 'OK', 'Cancel', and 'Advanced' buttons.

Advanced details are nearly the same on both sites. Define identical “preshared key” and “Phase 1 Proposal”. For outgoing interface please select the port which is connected to the internet. If you have multiple internet uplinks select the interface with the IP address which was specified as VPN-gateway-IP on the other site.

IKEv2 Auth Method

Self

Peer

Preshared Key Use As Seed

Local ID (optional)

Outgoing Interface

Security Level

Predefined Standard Compatible Basic

User Defined Custom

Phase 1 Proposal

Mode (Initiator) Main (ID Protection) Aggressive

Go to "Network" -> "Interfaces" -> "List" and choose New (Tunnel IF):

Tunnel Interface Name tunnel. (1~10)

Zone (VR)

Fixed IP

IP Address / Netmask /

Unnumbered

Interface

Select the same interface as before when creating the gateway. Create the tunnel.

These steps are identical on both sites

Choose "AutoKey IKE" and select "New":

As gateway select the created gateway. Click on "Advanced". Choose a "Phase 2 Proposal" and select the before create "Tunnel Interface".

Security Level

Predefined Standard Compatible Basic

User Defined Custom

Phase 2 Proposal

Replay Protection

Transport Mode

Bind to None Tunnel Interface Tunnel Zone

Now open the menu item "Destination" in "Network" -> "Routing". Add a new "trust-vr"-Route by clicking on "New".

On both Juniper SSG5 create a route:

| | | |
|-----------------------|---------------------|-----------------------------------|
| <u>SSG5 – Site A:</u> | IP Address/Netmask: | Site-B-External IP / 32 |
| | Gateway IP Address: | Site-A-External IP |
| | Interface: | Interface of "Site-A-External IP" |
| | | |
| <u>SSG5 – Site B:</u> | IP Address/Netmask: | Site-A-External IP / 32 |
| | Gateway IP Address: | Site-B-External IP |
| | Interface: | Interface of "Site-B-External IP" |

If you want to route the private network to the other site of the vpn you have to create a new route on both sites. Select the appropriate tunnel-interface when creating the rule. Leave Gateway-IP empty.

| | | |
|-----------------------|---------------------|---|
| <u>SSG5 – Site A:</u> | IP Address/Netmask: | 192.168.0.0 / 24 |
| | Gateway IP Address: | 0.0.0.0 |
| | Interface: | <i>Tunnel Interface for VPN to Site B</i> |
| | | |
| <u>SSG5 – Site B:</u> | IP Address/Netmask: | 192.168.0.0 / 24 |
| | Gateway IP Address: | 0.0.0.0 |
| | Interface: | <i>Tunnel Interface for VPN to Site A</i> |

You are done! Check the event log for errors.