Site-to-Site VPN with SonicWall Firewalls

6300-CX

Site-to-Site VPN with SonicWall Firewalls

Skill level: ***Expert*** (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's WAN internet connection, and use that IPSec tunnel to access endpoints inside a VPN.

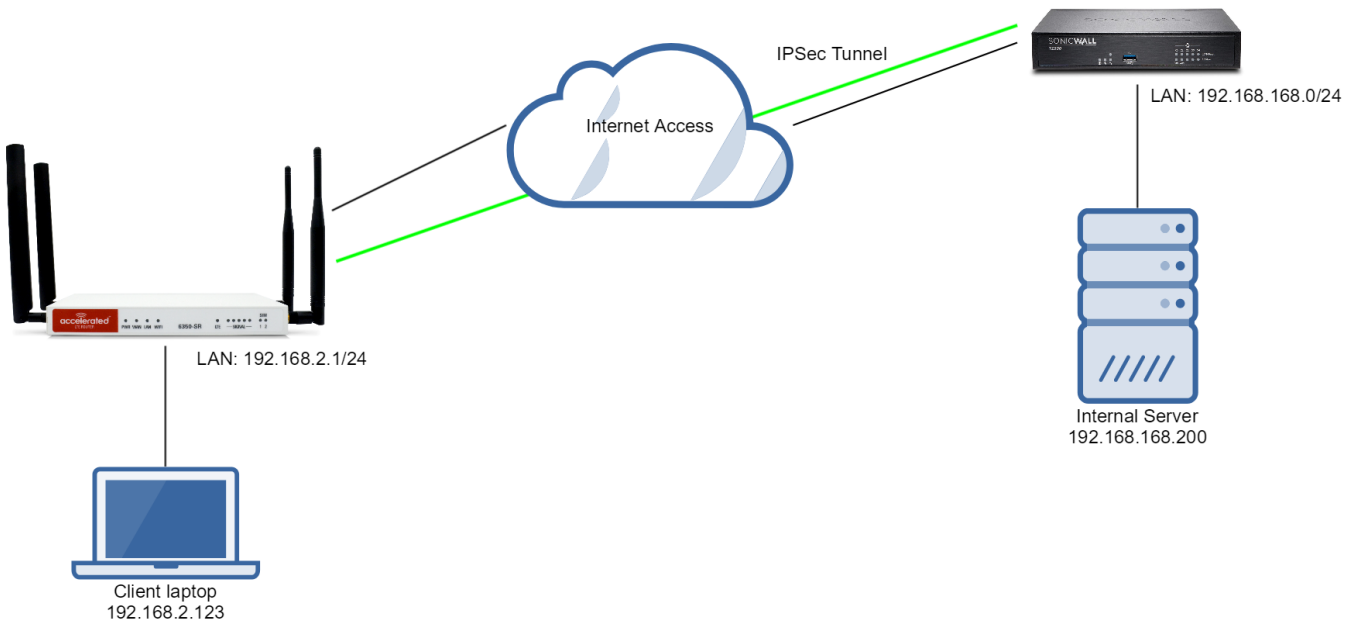
Setup

For this setup the Accelerated router will need an active WAN Internet connection (cellular for the CX series, cellular or wireline broadband for the SR and MX series). This connection must have a publicly reachable IP address.

Similarly, the SonicWall firewall must have an active Internet connection with a publicly reachable IP address.

Sample

The sample configuration below shows a 6350-SR building a tunnel to a SonicWall TZ300 through its cellular modem. A client laptop connected to the LAN Ethernet port of the 6350-SR will be able to access the SonicWall's LAN (and vice versa).



Sample Configuration: 6350-SR

Open the configuration profile for the 6350-SR. Under IPSec, create a new entry with the following settings:

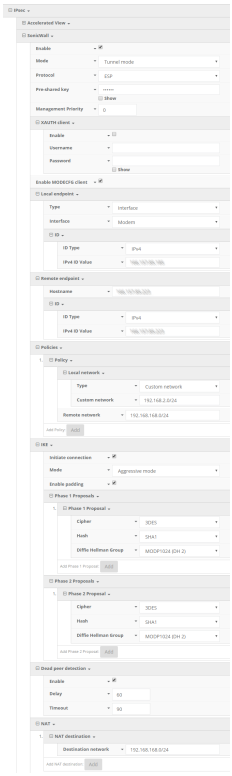
1. Enter in a PSK into the ***Pre-shared key***. This must match what is ultimately entered as the SonicWall's "Shared Secret."
2. Check the ***Enable MODECFG client*** box.
3. Change ***Local endpoint*** to ***Interface*** and select the intended route for the IPSec tunnel: "Modem" to leverage a cellular connection or "WAN" for a wireline ISP.
4. Set ***Local Endpoint -> ID -> ID type*** to "IPv4"
5. Set the local ID in ***Local endpoint -> ID -> IPv4 ID Value*** to the publicly reachable IP address associated with the selected Interface in step 3.

> NOTE: Leaving ***Local endpoint -> type*** to ***Interface*** as ***Default route*** will allow the tunnel to be built through any available WAN interface.

6. The ***Remote endpoint Hostname*** is the publicly reachable IP address of the SonicWall.
7. Change ***Remote endpoint -> ID -> ID type*** to ***IPv4***
8. Set the IP address of the SonicWall device in ***Remote endpoint -> ID -> IPv4 ID Value*** (same value as step 6).
9. Set ***IKE -> Mode*** to ***Aggressive mode***.
10. Set ***IKE -> Phase 1 Proposals*** and ***IKE -> Phase 2 Proposals*** to match the IKE settings required by the SonicWall. In this example, both proposals are set to 3DES, SHA1, MODP1024 (DH 2).
11. Under ***NAT*** click the ***Add*** button and specify the ***Destination network***. This will be the same value entered in the remote policy specified below.

Under IPSec -> Policies, click "Add" to create a new policy, and enter the following settings:

1. Set ***Policy -> Local network -> Type*** to ***Custom network.***
2. Enter the local subnet of the Accelerated router in the ***Custom network*** field (192.168.2.0/24 by default).
3. Set ***Policy -> Remote network*** to the IPv4 network you wish to access through the tunnel. (The local subnet of the SonicWall.)



Under Firewall -> Packet filtering, create a new entry by clicking Add and enter the following settings:

Action: Accept

IP Version: IPv4

Protocol: UDP

Secure zone: IPsec

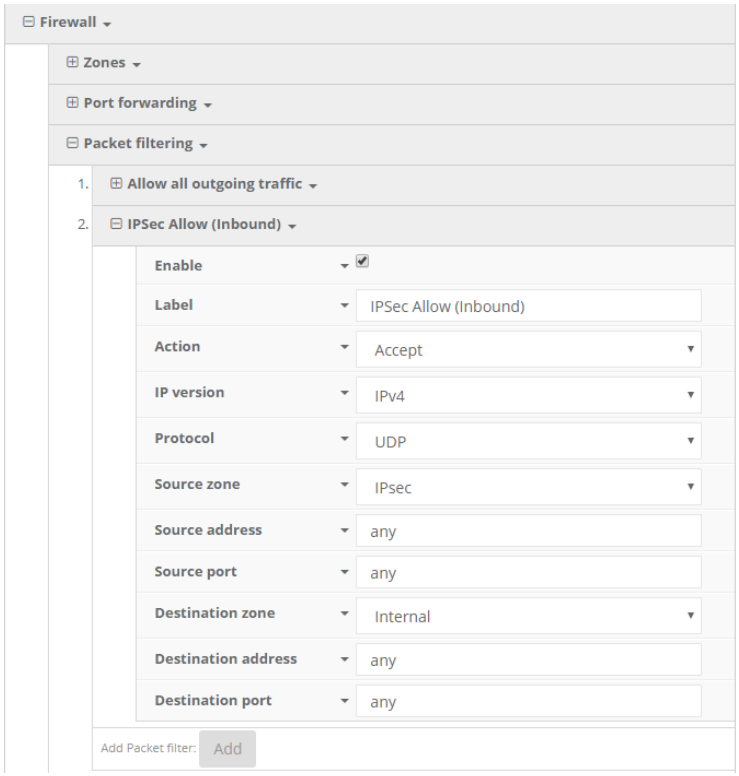
Source address: any

Source port: any

Destination zone: Internal

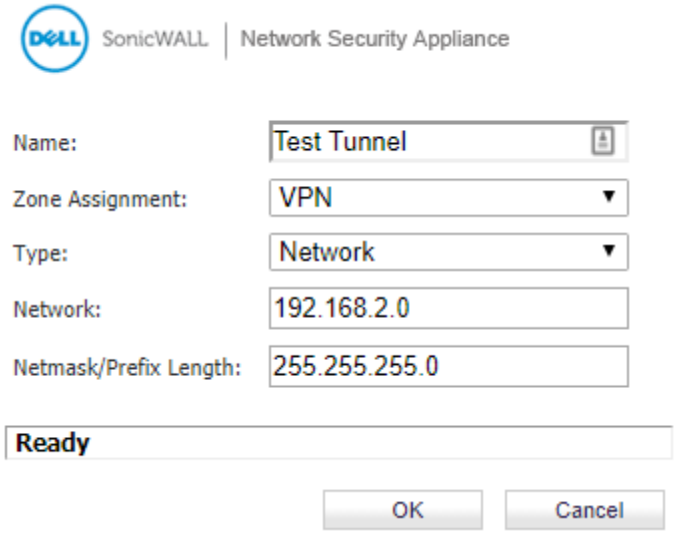
Destination address: any

Destination port: any



Sample Configuration: SonicWall TZ300

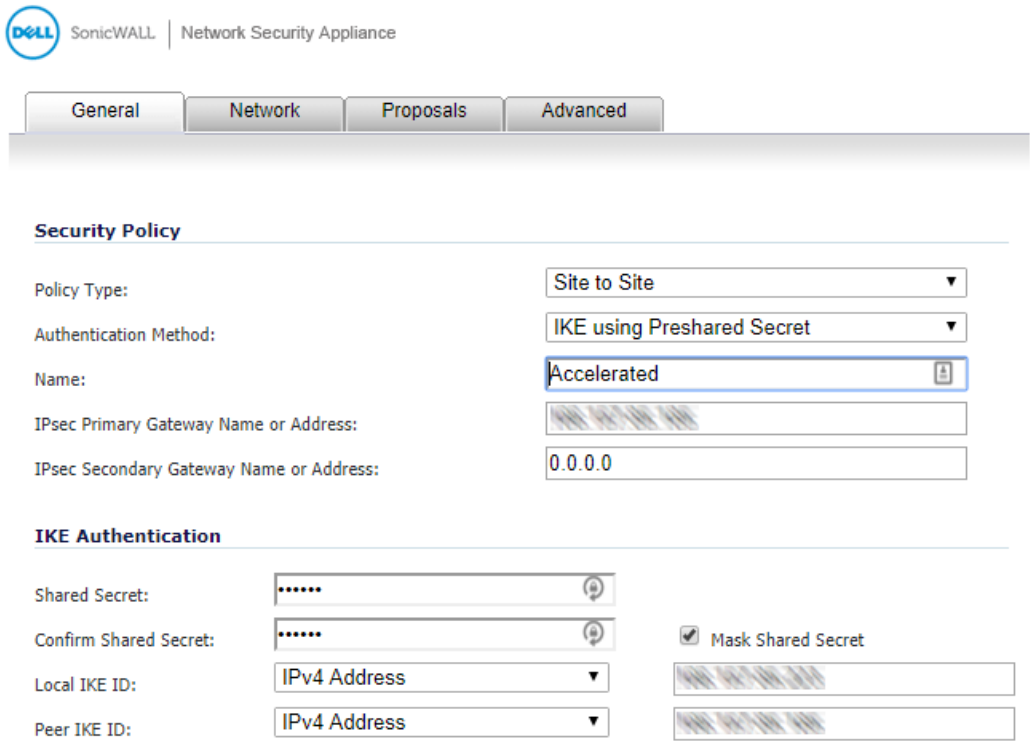
Step 1: Create a new Address Object for VPN Subnets



1. Log in to the SonicWall Management Interface
2. Navigate to ***Network > Address Objects***, click on ***ADD*** button.
3. Configure the Address Object as depicted above, click ***Add*** and click ***Close*** when finished.

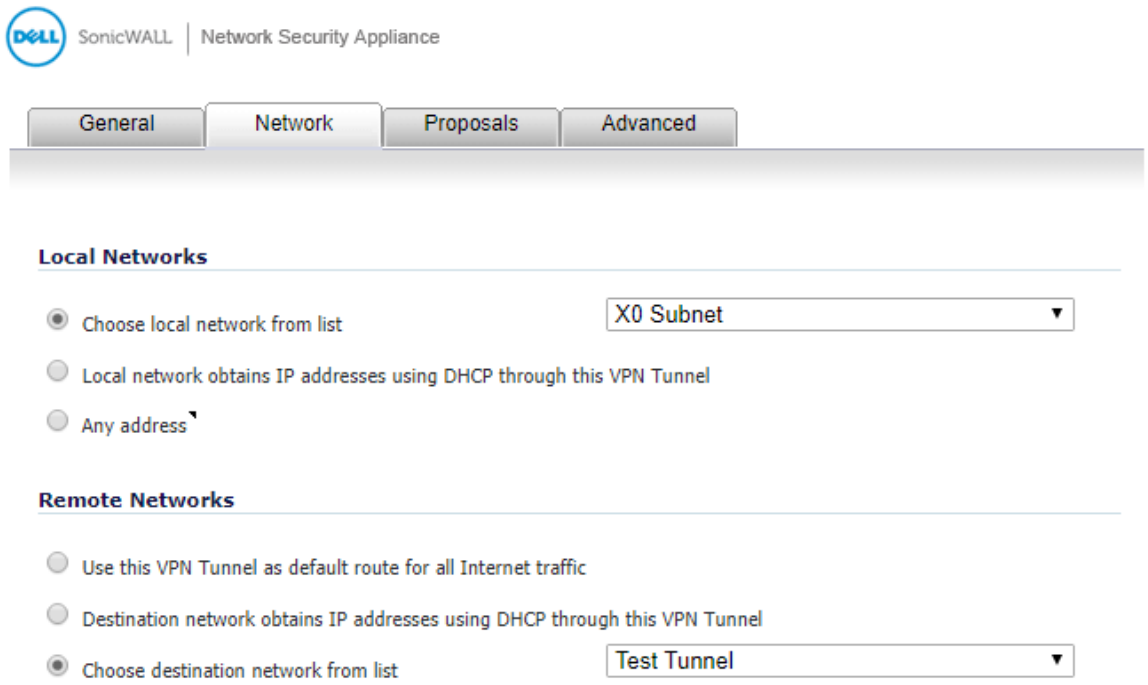
NOTE: The *Network* and *Netmask* must match the local subnet on the Accelerated router. Settings depicted in the screenshot above assume the router is still configured per its defaults.

Step 2: Configure a VPN policy on the SonicWall

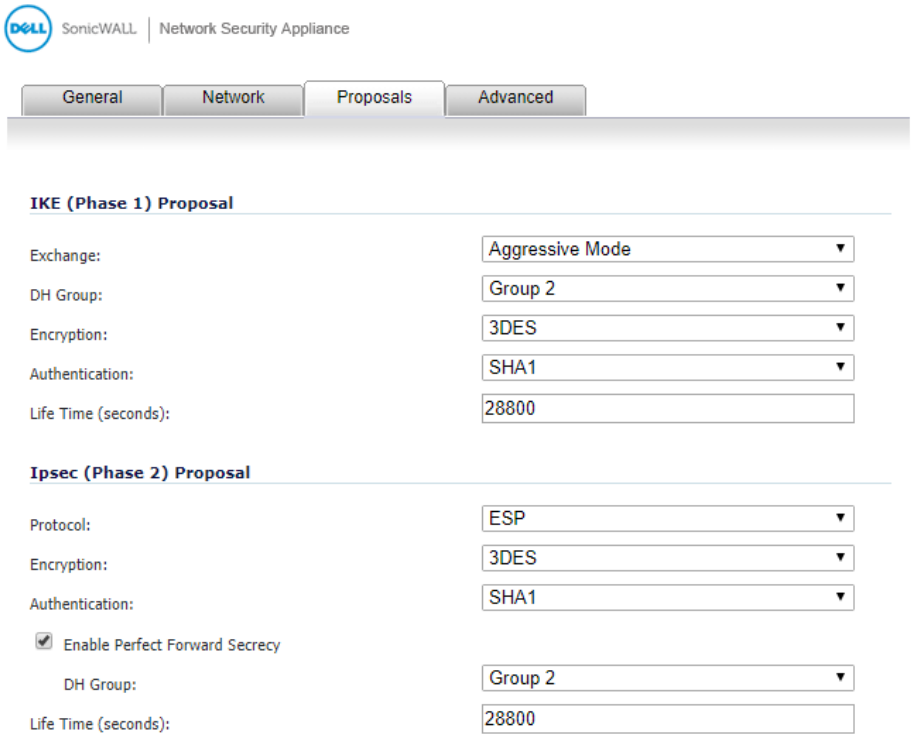


1. Navigate to *VPN > Settings* page. Click *Add* button. The VPN Policy window is displayed.
2. Click the *General* tab.
3. Select *IKE using Preshared Secret* from the *Authentication Method* menu.
4. Enter a name for the policy in the *Name* field.
5. Enter the WAN IP address of the Accelerated connection in the *IPsec Primary Gateway Name or Address* field.
6. Enter a *Shared Secret* password to be used to setup the Security Association the Shared Secret and Confirm Shared Secret fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

NOTE: The shared secret must match the Pre-shared key entered into the Accelerated configuration.

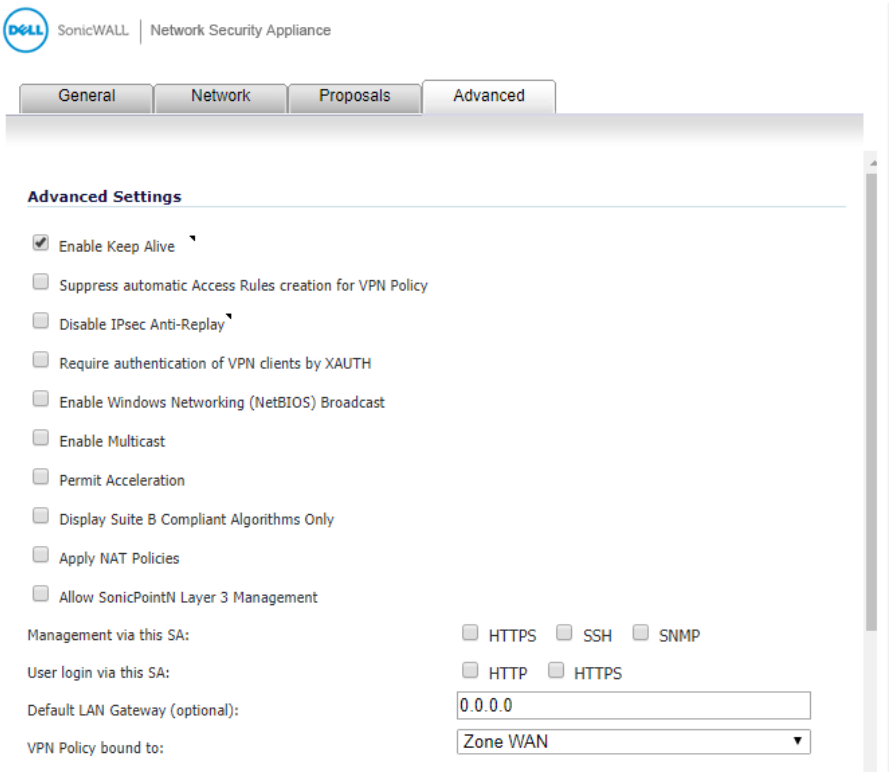


7. Click the ***Network*** tab.
8. Under ***Local Networks***, select ***Choose local network from list*** and specify the "X0 Subnet."
9. Under ***Remote Networks***, select ***Choose destination network from list*** and specify the Address Object created in Step 1 above.



10. Click the ***Proposals*** tab.

11. Under ***IKE (Phase 1) Proposal***, change the ***Exchange*** field to "Aggressive Mode."
12. Leave the default settings for ***Encryption*** and ***Authentication*** ("3DES" and "SHA1," respectively) for both ***Phase 1*** and ***Phase 2 Proposals***.
13. ***Life Time*** may be left at its default value as well.
14. Under ***Ipsec (Phase 2) Proposal***, leave "ESP" as the selected ***Protocol***
15. Check ***Enable Perfect Forward Secrecy***, leaving Group 2 selected in the corresponding field.



16. Click the ***Advanced*** tab.
17. Select ***Enable Keep Alive***.
18. Finalize these settings by clicking the ***OK*** button.