ITCorporation

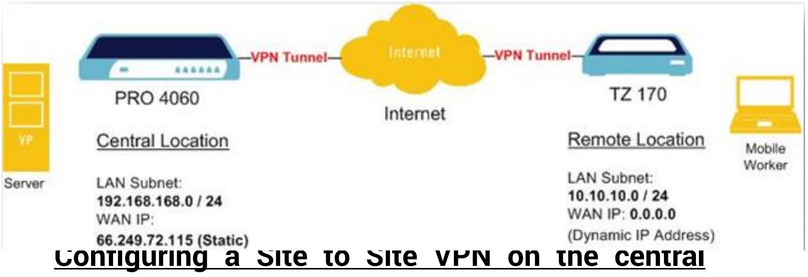
SONICWALL®

• SecureFirst •

Configuring Aggressive Mode Site to Site VPN when a Site has Dynamic WAN Public IP address

KNOWLEDGE DATABASE

Configuring Aggressive Mode Site to Site VPN when a Site has Dynamic WAN Public IP address



Configuring a Site to Site VPN on the central location (Static WAN IP address)

Central location network configuration:

1. LAN Subnet: **192.168.168.0**
2. Subnet Mask: **255.255.255.0**
3. WAN IP: **66.249.72.115**
4. Local IKE ID SonicWall Identifier: **Chicago** (This could be any string except it has to match the remote location VPN's Peer IKE ID SonicWall Identifier)

NOTE: The IP Address can be dynamic but it must always be Public.

This solution explains the configuration of a Site to Site VPN on SonicWall appliances when a site has dynamic WAN IP address.
The VPN policy is setup using **Aggressive Mode.**
Network Setup:

Step 1: Creating **Address Object** for **remote Site:**

- Login to the central location SonicWall appliance
- Navigate to ***Manage | Policies | Objects | AddressObjects*** page.
- Click on **Add** button, enter the following settings.

Name – **newyork vpn**,
Zone – **VPN**,
Type – **Network**,
Network – **10.10.10.0**,
Netmask – **255.255.255.0**

- Click **OK** when finished.

Step 2: Configurating a VPN Policy:

a. Click on ***Manage | Connectivity | VPN | Base Settings***
b. Check the box "***Enable VPN***" under Global VPN Settings.
c. Click on the "***Add***" button under VPN Policies section. The VPN Policy window pops up.

Click the **General** tab

a. Select the Authentication method as **"IKE Using Preshared Secret"**
b. Name: **New York Aggressive Mode VPN**
c. IPsec Primary Gateway Name or Address: **0.0.0.0**

Note: Since the WAN IP address changes frequently, it is recommended to use the 0.0.0.0 IP address as the Primary Gateway.

d. IPsec Secondary Gateway Name or Address: **0.0.0.0**
e. Shared Secret: **SonicWall** (The Shared Secret would be the same at both SonicWall's. You can choose any Secret Key, but it should be entered sam on both sites)
f. Local IKE ID: SonicWall Identifier - **Chicago** (This could be any string except it has to match the remote location VPN's **Peer IKE ID SonicWall Identifier**)

g. Peer IKE ID: SonicWall Identifier - **newyork** (This could be any string except it has to match the remote location VPN's **Local IKE ID SonicWall Identifier**)

Click the **Network** tab

Ø Local Networks

Select **Choose local network from list,** and select the Address Object – **X0 Subnet** (LAN subnet)

Ø Destination Networks

Select **Choose destination network from list,** and select the Address Object – **newyork vpn**

Click the **Proposals** tab

IKE (Phase 1) Proposal

Exchange: **Aggressive Mode**
DH Group: **Group 2**
Encryption: **3DES**
Authentication: **SHA1**
Life Time (seconds): **28800**

IPsec (Phase 2) Proposal

Protocol: **ESP**
Encryption: **3DES**
Authentication: **SHA1**

Enable Perfect Forward Secrecy(not checked)

DH Group: **Group 2**
Life Time (seconds): **28800**

Click the **Advanced** tab

Ensure that the **VPN Policy bound to: Zone WAN**

- Click **OK** when finished

Configuring a Site to Site VPN on the remote location (Dynamic WAN IP address)

Note: The Dynamic WAN IP Address must be Public.

Network Configuration:

1. LAN Subnet: **10.10.10.0**
2. Subnet Mask: **255.255.255.0**
3. WAN IP: DHCP (As this is a Dynamic IP Address)
4. Local IKE ID SonicWall Identifier: **newyork** (This has to match the central location VPN's **Peer IKE ID SonicWall Identifier**)

Step 1: Creating **Address Object** for **remote site:**

- Login to the Remote location SonicWall appliance
- Navigate to ***Manage | Policies | Objects | AddressObjects*** page.
- Click on **Add** button, enter the following settings.

Name – **Chicago vpn**
Zone – **VPN**
Type – **Network**
Network – **192.168.168.0**
Netmask – **255.255.255.0**

- Click **OK** when finished

Step 2: Configuration VPN Policy:

a. Click on ***Manage | Connectivity | VPN | Base Settings***.
b. Check the box "***Enable VPN***" under Global VPN Settings.

c. Click on the "***Add***" button under the VPN Policies section. The VPN Policy window pops up.

Click the **General** tab

a. Select the Authentication method as "**IKE Using Preshared Secret**"
b. Name: **Chicago Aggressive Mode VPN**
c. IPsec Primary Gateway Name or Address: **66.249.72.115 (Gateway of the main site, which is static IP)**
d. IPsec Secondary Gateway Name or Address: **0.0.0.0**
e. Shared Secret: **SonicWall**
f. Local IKE ID: SonicWall Identifier - **newyork** (This has to match the central location VPN's **Peer IKE ID SonicWall Identifier**)
g. Peer IKE ID: SonicWall Identifier – **Chicago** (This has to match the central location VPN's **Local IKE ID SonicWall Identifier**)

Click the **Network** tab

Ø <u>Local Networks</u>

Select **Choose local network from list,** and select the Address Object – **LAN Primary Subnet**

Ø <u>Destination Networks</u>

Select **Choose destination network from list**, and select the Address Object – **Chicago vpn**

Click the **Proposals** tab

IKE (Phase 1) Proposal

Exchange: **Aggressive Mode**
DH Group: **Group 2**
Encryption: **3DES**
Authentication: **SHA1**
Life Time (seconds): **28800**

IPsec (Phase 2) Proposal

Protocol: **ESP**
Encryption: **3DES**
Authentication: **SHA1**

Enable Perfect Forward Secrecy (not checked)

DH Group: **Group 2**
Life Time (seconds): **28800**

Click the **Advanced** tab

Enable Keep Alive box should be checked
VPN Policy bound to: **Zone WAN**

- Click **OK** when finished

How to Test:
From the remote location try to ping an IP address on the central location.

Note: Before receiving successful replies, you might see couple of "Request Timed Out" messages while the VPN tunnel is still establishing.