NetVanta 2000 Series FAQ

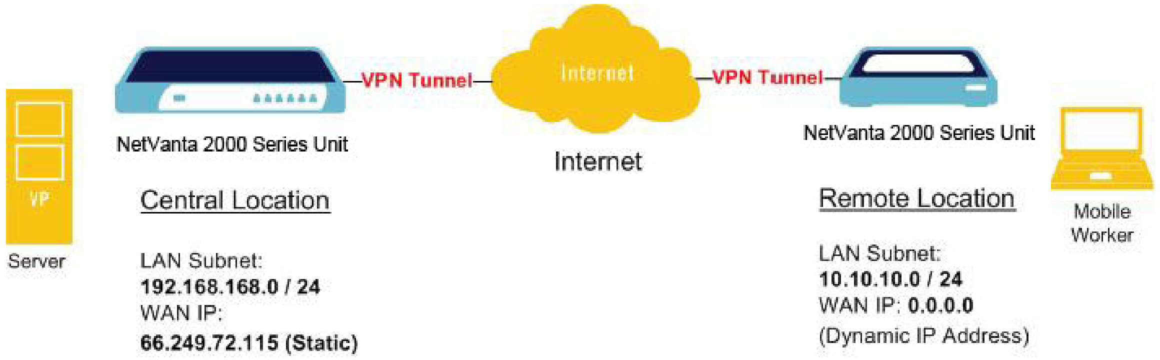
Configuring Site to Site VPN when a Site has Dynamic WAN IP address in Enhanced OS (Aggressive Mode)

> NOTE *This document is applicable to NetVanta 2600 series, 2700 series, and 2800 series units.*

This solution explains the configuration of a Site to Site VPN on NetVanta 2000 Series apliance when a site has dynamic WAN IP address. The VPN policy is setup using Aggressive Mode.

Procedure:

Network Setup:



Configuring a Site to Site VPN on the Central Location (Static WAN IP address)

Device used on Central Site: Running Enhanced OS 4.0.0.2e firmware.

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 ADTRANl Identifier: **chicago** (This could be any string except it has to match the Remote Location VPN's Peer IKE ID ADTRANl Identifier)

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

- Login to the Central Location NetVanta 2000 Series appliance

- Navigate to **Network > Address Objects** page.

- Scroll down to the bottom of the page and 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 **VPN > 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: **ADTRAN** (The Shared Secret would be the same at both ADTRAN’s)

f. Local IKE ID: ADTRAN Identifier **- chicago** (This could be any string except it has to match the Remote Location VPN's **Peer IKE ID ADTRANl Identifier**)

g. Peer IKE ID: ADTRAN Identifier - **newyork** (This could be any string except it has to match the Remote Location VPN's **Local IKE ID ADTRANl 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)

Device used on Remote location: Appliance running Enhanced OS 3.2.3.0 firmware

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 ADTRAN Identifier: **newyork** (This has to match the Central Location VPN's **Peer IKE ID ADTRAN1 Identifier**)

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

- Login to the Central Location firewall

- Navigate to **Network > Address Objects** page.

- Scroll down to the bottom of the page and 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 **VPN > 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**

d. IPsec Secondary Gateway Name or Address: **0.0.0.0**

e. Shared Secret: **ADTRAN**

f. Local IKE ID: ADTRAN Identifier **-** **newyork** (This has to match the Central Location VPN's **Peer IKE ID ADTRANl Identifier**)

g. Peer IKE ID: ADTRAN Identifier – chicago (This has to match the Central Location VPN's **Local IKE ID ADTRANl Identifier**)

Click the **Network** tab

Ø Local Networks

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

Ø Destination Networks

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.*