



NetVanta 2000 Series Technical Note

Configuring a Site to Site VPN Policy using Main Mode (Static IP address on both sites) in SonicOS Enhanced

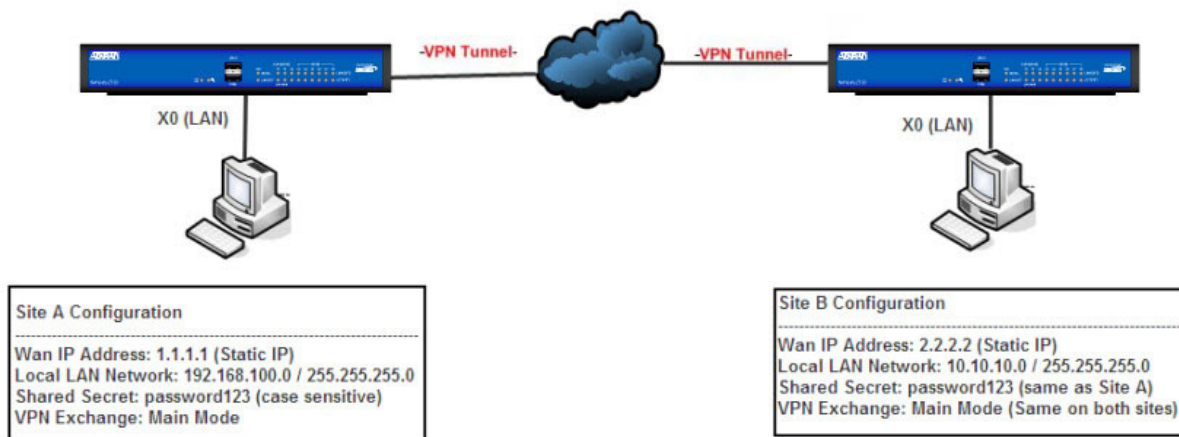


This document is applicable to NetVanta 2600 series, 2700 series, and 2800 series units.

Overview / Scenario:

When configuring a Site-to-Site VPN tunnel in SonicOS Enhanced firmware using Main Mode both the NetVanta 2000 Series appliances (Site A and Site B) must have a routable Static WAN IP address.

Network Setup:



Deployment Steps:

- Step 1: Creating Address Objects for VPN subnets.
- Step 2: Configuring a VPN policy on Site A ADTRAN.
- Step 3: Configuring a VPN policy on Site B ADTRAN

Step 4: How to test this scenario.

Procedure:

To manually configure a VPN Policy using IKE with Preshared Secret, follow the steps below:

Step 1: Creating Address Objects for VPN subnets:

1. Login to the NetVanta 2000 Series Management Interface

The image displays two side-by-side screenshots of the NetVanta management interface, separated by a vertical line. Each screenshot shows the configuration for an address object on a specific site's ADTRAN.

Left Screenshot: Address Object on Site A ADTRAN

- Name: Tempe Office (Site B)
- Zone Assignment: VPN
- Type: Network
- Network: 10.10.10.0
- Netmask: 255.255.255.0
- Status: Ready
- Buttons: Add, Close

Right Screenshot: Address Object on Site B ADTRAN

- Name: Seattle Office (Site A)
- Zone Assignment: VPN
- Type: Network
- Network: 192.168.100.0
- Netmask: 255.255.255.0
- Status: Ready
- Buttons: Add, Close

2. Navigate to **Network > Address Objects**, scroll down to the bottom of the page and click on the **ADD** button.

3. Configure the Address Objects as mentioned in the figure above, click **Add** and click **Close** when finished.

Step 2: Configuring a VPN policy on Site A ADTRAN

1. Navigate to **VPN > Settings** page and Click the **Add** button. The VPN Policy window is displayed.

The screenshot shows the VPN Policy configuration window with the following fields and options:

- General** | Network | Proposals | Advanced
- Security Policy**
 - Authentication Method: IKE using Preshared Secret
 - Name: Tempe Office (Site B)
 - IPsec Primary Gateway Name or Address: 2.2.2.2
 - IPsec Secondary Gateway Name or Address: 0.0.0.0
- IKE Authentication**
 - Shared Secret: [Masked]
 - Confirm Shared Secret: [Masked] Mask Shared Secret
 - Local IKE ID: IP Address []
 - Peer IKE ID: IP Address []
- Ready
- OK | Cancel | Help

2. Click the **General** tab

- Select **IKE using Preshared Secret** from the **Authentication Method** menu.
- Enter a name for the policy in the Name field.
- Enter the **WAN IP address** of the remote connection in the **IPsec Primary Gateway Name or Address** field (Enter Site B's WAN IP address).
- If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.



Secondary gateways are not supported with IKEv2.

- 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.

- Optionally, you may specify a **Local IKE ID** (optional) and **Peer IKE ID** (optional) for this Policy. By default, the IP Address (ID_IPv4_ADDR) is used for Main Mode negotiations, and the NetVanta 2000 Series Identifier (ID_USER_FQDN) is used for Aggressive Mode.

3. Click the **Network** tab

The screenshot shows a configuration window with four tabs: General, Network, Proposals, and Advanced. The Network tab is active. Under the heading "Local Networks", there are three radio button options: "Choose local network from list" (selected), "Local network obtains IP addresses using DHCP through this VPN Tunnel", and "Any address". A dropdown menu next to the selected option shows "X0 Subnet". Under the heading "Destination Networks", there are three radio button options: "Use this VPN Tunnel as default route for all Internet traffic", "Destination network obtains IP addresses using DHCP through this VPN Tunnel", and "Choose destination network from list" (selected). A dropdown menu next to the selected option shows "Tempe Office (Site B)". At the bottom, there is a "Ready" status bar and three buttons: "OK", "Cancel", and "Help".

- Under **Local Networks**, select a local network from **Choose local network from list:** and select the address object **X0 Subnet** (LAN Primary Subnet)

NOTE *DHCP over VPN is not supported with IKEv2.*

- Under **Destination Networks**, select **Choose destination network from list:** and select the address object **Tempe Office** (Site B network)

4. Click the **Proposals** tab

The screenshot shows a configuration window with four tabs: General, Network, Proposals, and Advanced. The 'Proposals' tab is selected. Below the tabs, there are two main sections: 'IKE (Phase 1) Proposal' and 'IPsec (Phase 2) Proposal'. Each section contains several configuration fields with dropdown menus and text boxes. At the bottom of the window, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

Section	Field	Value
IKE (Phase 1) Proposal	Exchange:	Main Mode
	DH Group:	Group 2
	Encryption:	3DES
	Authentication:	SHA1
	Life Time (seconds):	28800
IPsec (Phase 2) Proposal	Protocol:	ESP
	Encryption:	3DES
	Authentication:	SHA1
	<input type="checkbox"/> Enable Perfect Forward Secrecy	
	DH Group:	Group 2
	Life Time (seconds):	28800

- Under **IKE (Phase 1) Proposal**, select **Main Mode** from the Exchange menu. Aggressive Mode is generally used when WAN addressing is dynamically assigned. IKEv2 causes all the negotiation to happen via IKE v2 protocols, rather than using IKE Phase 1 and Phase 2. If you use IKE v2, both ends of the VPN tunnel must use IKE v2.

- Under **IKE (Phase 1) Proposal**, the default values for DH Group, Encryption, Authentication, and Life Time are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. You can also choose AES-128, AES-192, or AES-256 from the Authentication menu instead of 3DES for enhanced authentication security.



The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Under **IPsec (Phase 2) Proposal**, the default values for Protocol, Encryption, Authentication, Enable Perfect Forward Secrecy, DH Group, and Lifetime are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

5. Click the **Advanced** tab

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

- To manage the local NetVanta 2000 Series appliance through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**. Select **HTTP, HTTPS, or both** in the **User login via this SA** to allow users to login using the SA.

- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to Use this VPN Tunnel as default route for all Internet traffic, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

- Select an interface or zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

- Click **OK** to apply the settings.

Step 3: Configuring a VPN policy on Site B ADTRAN

1. Login to the Site B ADTRAN appliance and navigate to **VPN > Settings** page and Click the **Add** button. The VPN Policy window is displayed.

2. Click the **General** tab.

The screenshot shows the 'General' tab of the VPN Policy configuration window. The 'Security Policy' section includes the following fields:

- Authentication Method: IKE using Preshared Secret (dropdown menu)
- Name: Seattle Office (Site A) (text field)
- IPsec Primary Gateway Name or Address: 1.1.1.1 (text field)
- IPsec Secondary Gateway Name or Address: 0.0.0.0 (text field)

The 'IKE Authentication' section includes the following fields:

- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted] Mask Shared Secret
- Local IKE ID: IP Address (dropdown menu) [Redacted]
- Peer IKE ID: IP Address (dropdown menu) [Redacted]

At the bottom, there is a 'Ready' status bar and three buttons: OK, Cancel, and Help.

- Select **IKE using Preshared Secret** from the **Authentication Method** menu.
- Enter a name for the policy in the **Name** field.
- Enter the **WAN IP address** of the remote connection in the **IPsec Primary Gateway Name or Address** field (Enter Site A's WAN IP address).
- If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.



Secondary gateways are not supported with IKEv2.

- 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.

- Optionally, you may specify a **Local IKE ID** (optional) and **Peer IKE ID** (optional) for this Policy. By default, the IP Address (ID_IPv4_ADDR) is used for Main Mode negotiations, and the NetVanta 2000 Series Identifier (ID_USER_FQDN) is used for Aggressive Mode.

3. Click the **Network** tab.

The screenshot shows a configuration window with four tabs: General, Network, Proposals, and Advanced. The 'Network' tab is active. Below the tabs, there are two sections: 'Local Networks' and 'Destination Networks'. In the 'Local Networks' section, the first radio button 'Choose local network from list' is selected, and a dropdown menu shows 'X0 Subnet'. The other two radio buttons are unselected. In the 'Destination Networks' section, the third radio button 'Choose destination network from list' is selected, and a dropdown menu shows 'Seattle Office (Site A)'. At the bottom of the window, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

- Under **Local Networks**, select a local network from **Choose local network from list:** and select the address object **X0 Subnet** (LAN Primary Subnet)

NOTE *DHCP over VPN is not supported with IKEv2.*

- Under **Destination Networks**, select **Choose destination network from list:** and select the address object **Seattle Office** (Site A network)

4. Click the **Proposals** tab:

NOTE *Settings must be same as Site A.*

5. Click the **Advanced** tab

Advanced Settings

Enable Keep Alive

Suppress automatic Access Rules creation for VPN Policy

Require authentication of VPN clients by XAUTH

User group for XAUTH users: --Select a user group--

Enable Windows Networking (NetBIOS) Broadcast

Enable Multicast

Apply NAT Policies

Translated Local Network: --Select Translated Local Network--

Translated Remote Network: --Select Translated Remote Network--

Management via this SA: HTTP HTTPS SSH

User login via this SA: HTTP HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

Ready

OK Cancel Help

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

- To manage the local NetVanta 2000 Series appliance through the VPN tunnel, select **HTTP, HTTPS**, or both from Management via this SA. Select **HTTP, HTTPS, or both** in the **User login via this SA** to allow users to login using the SA.

- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to Use this VPN Tunnel as default route for all Internet traffic, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

- Select an interface or zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

- Click **OK** to apply the settings.

How to Test this Scenario:

Try to ping an IP address from Site A to Site B or Vice Versa.



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