

SONICWALL[®]

• SecureFirst •

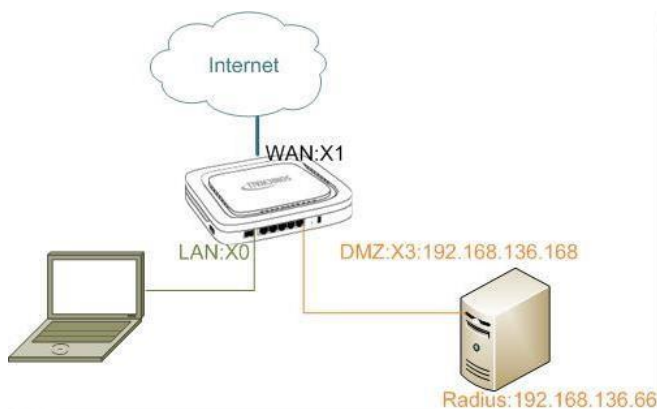
How to configure an IPv6 IPSec
VPN in SonicOS Enhanced

KNOWLEDGE
DATABASE

How to configure an IPv6 IPSec VPN in SonicOS Enhanced

IPv6 IPSec VPN provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to-network VPN connections.

Network Setup:



RESOLUTION:

Deployment Steps:

Step 1: Creating Address Objects for VPN subnets.

Step 2: Configuring a VPN policy on Site A SonicWall.

Step 3: Configuring a VPN policy on Site B SonicWall

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 SonicWall Management Interface

2. Navigate to **Network | Address Objects**, click on **ADD** button.

Address Object on Site A SonicWALL	Address Object on Site B SonicWALL
Name: <input type="text" value="Tempe Office(Site B)"/>	Name: <input type="text" value="Seattle Office(Site A)"/>
Zone Assignment: <input type="text" value="VPN"/>	Zone Assignment: <input type="text" value="VPN"/>
Type: <input type="text" value="Network"/>	Type: <input type="text" value="Network"/>
Network: <input type="text" value="2014:5600::"/>	Network: <input type="text" value="2014:3600::"/>
Netmask/Prefix Length: <input type="text" value="64"/>	Netmask/Prefix Length: <input type="text" value="64"/>
Ready	Ready
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	<input type="button" value="OK"/> <input type="button" value="Cancel"/>

2. 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 SonicWall

1. Navigate to **VPN | Settings** page and select the IPv6 option in the View IP Version radio button at the top right. Click **Add** button. The VPN Policy window is displayed.

General	Network	Proposals	Advanced
Security Policy			
Authentication Method:	<input type="text" value="IKE using Preshared Secret"/>		
Name:	<input type="text" value="Tempe Office (Site B)"/>		
IPsec Primary Gateway Name or Address:	<input type="text" value="2001:5600::1"/>		
IPsec Secondary Gateway Name or Address:	<input type="text"/>		
IKE Authentication			
Shared Secret:	<input type="text" value="*****"/>	<input type="text"/>	
Confirm Shared Secret:	<input type="text" value="*****"/>	<input checked="" type="checkbox"/> Mask Shared Secret	
Local IKE ID:	<input type="text" value="IPv6 Address"/>	<input type="text"/>	
Peer IKE ID:	<input type="text" value="IPv6 Address"/>	<input type="text"/>	

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 IPv6 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.

Note: 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_IPv6_ADDR) is used for negotiations.

3. Click the **Network** tab

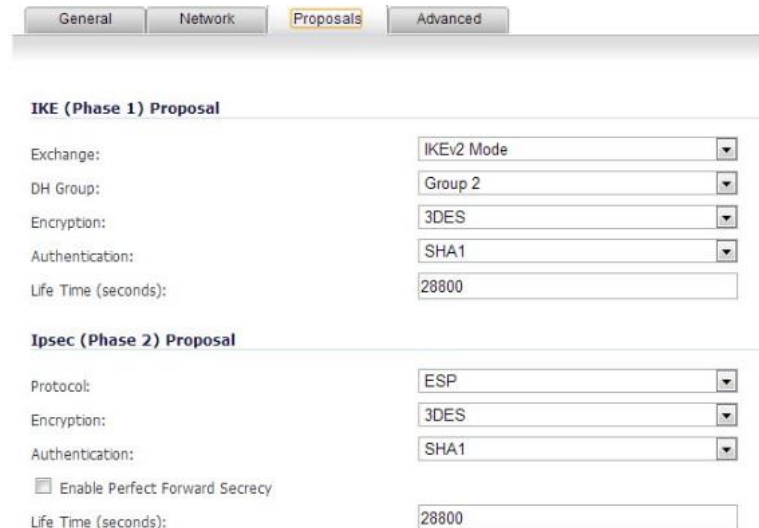


- Under **Local Networks**, select a local network from **Choose local network from list:** and select the address object **X0 IPv6 Primary Static Address Subnet** (LAN Primary Subnet)

Note: DHCP over VPN is not supported, thus the DHCP options for protected network are not available

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

4. Click the **Proposals** tab



- Under **IKE (Phase 1) Proposal**, select **IKEv2 Mode** from the Exchange menu. 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.

Note: 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.

See also: <http://en.wikipedia.org/wiki/IPsec>

5. Click the **Advanced** tab

General Network Proposals **Advanced**

Advanced Settings

Enable Keep Alive

Suppress automatic Access Rules creation for VPN Policy

Disable IPsec Anti-Replay

Apply NAT Policies

Management via this SA: HTTPS SNMP

User login via this SA: HTTP HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Zone WAN

Using Primary IP Address

Specify the local gateway IP address

IKEv2 Settings

Do not send trigger packet during IKE SA negotiation

Accept Hash & URL Certificate Type

Send Hash & URL Certificate Type

once both sides become available again without having to wait for the proposed Life Time to expire.

- To manage the local SonicWall through the VPN tunnel, select **HTTPS** 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.

- 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 SonicWall

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

3. Click the **General** tab.

Security Policy

Authentication Method: IKE using Preshared Secret

Name: Seattle Office (Site A)

IPsec Primary Gateway Name or Address: 2001:3600::1

IPsec Secondary Gateway Name or Address: ::

IKE Authentication

Shared Secret:

Confirm Shared Secret: Mask Shared Secret

Local IKE ID: IPv6 Address

Peer IKE ID: IPv6 Address

Select **IKE using Preshared Secret** from the **Authentication Method** menu.

- Enter a name for the policy in the **Name** field.
- Enter the **WAN IPv6 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.

Note: 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_IPv6_ADDR) is used for negotiations.

3. Click the **Network** tab.