ITCorporation

SONICWALL®

SecureFirst

VPN: Configuring Site to Site VPN using the Quick Configuration on SonicOS Enhanced

KNOWLEDGE DATABASE

VPN: Configuring Site to Site VPN using the Quick Configuration on SonicOS Enhanced

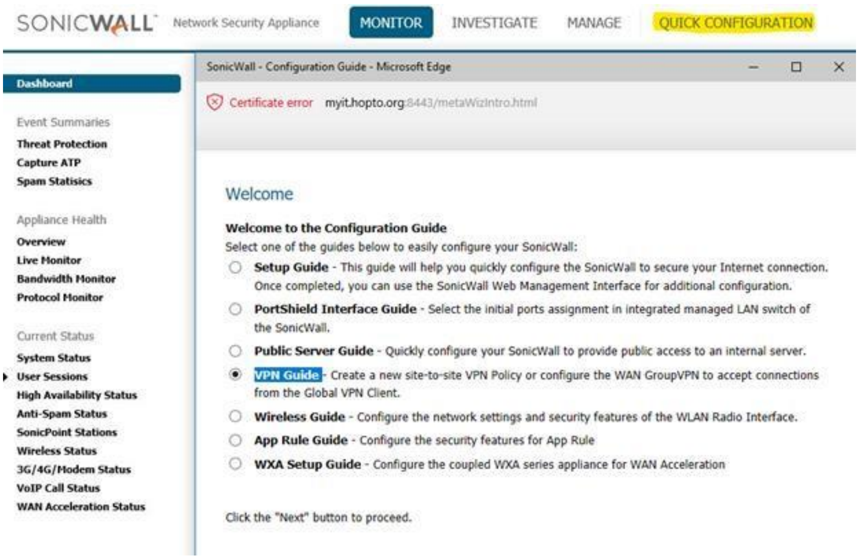
The VPN Policy Quick Configuration walks you step-by-step through the configuration of Site to Site VPN on the SonicWall. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicWall Management Interface for optional advanced configuration options.

Procedure:

Using the VPN Quick Configuration to Configure Site to Site VPN using Preshared Secret

Step 1. Click **Quick Configuration** on the top Navigation menu

Step 2. In the **Welcome to the SonicWall Configuration Guide** select **VPN Guide** and click **Next.**



Welcome

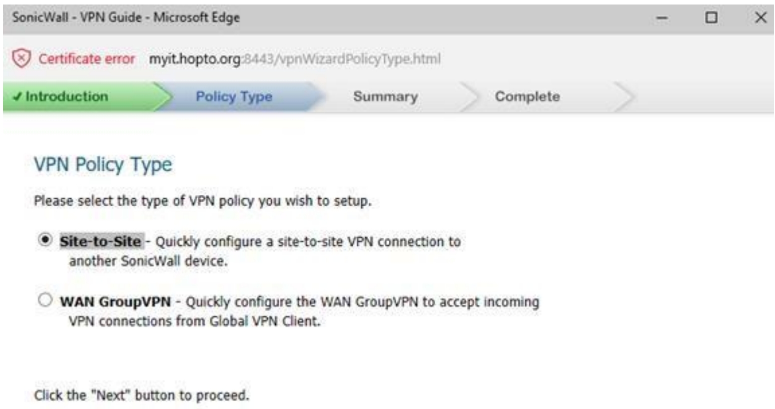
Welcome to the Configuration Guide

Select one of the guides below to easily configure your SonicWall:

- ○ **Setup Guide** - This guide will help you quickly configure the SonicWall to secure your Internet connection. Once completed, you can use the SonicWall Web Management Interface for additional configuration.
- ○ **PortShield Interface Guide** - Select the initial ports assignment in integrated managed LAN switch of the SonicWall.
- ○ **Public Server Guide** - Quickly configure your SonicWall to provide public access to an internal server.
- ● **VPN Guide** - Create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept connections from the Global VPN Client.
- ○ **Wireless Guide** - Configure the network settings and security features of the WLAN Radio Interface.
- ○ **App Rule Guide** - Configure the security features for App Rule
- ○ **WXA Setup Guide** - Configure the coupled WXA series appliance for WAN Acceleration

Click the "Next" button to proceed.

Step 3. In the **VPN Policy Type** page, select **Site-to-Site** and click **Next.**


SonicWall - VPN Guide - Microsoft Edge
Certificate error
myit.hopto.org:8443/vpnWizardPolicyType.html
✓ Introduction
Policy Type
Summary
Complete

VPN Policy Type

Please select the type of VPN policy you wish to setup.

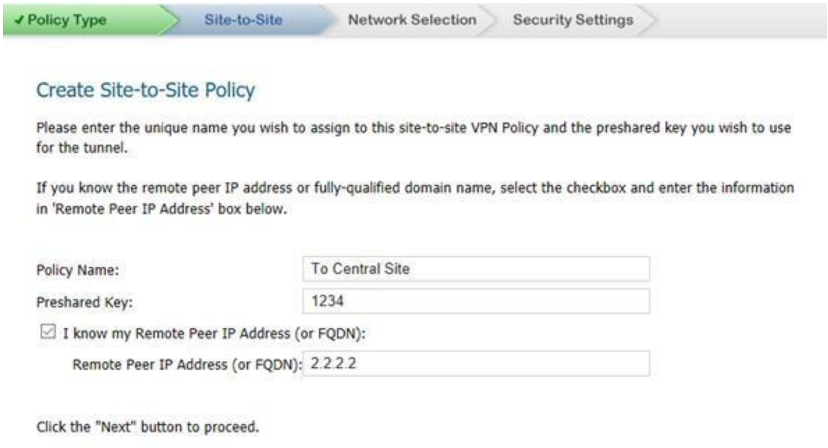
- ● **Site-to-Site** - Quickly configure a site-to-site VPN connection to another SonicWall device.
- ○ **WAN GroupVPN** - Quickly configure the WAN GroupVPN to accept incoming VPN connections from Global VPN Client.

Click the "Next" button to proceed.

Step 4. In the **Create Site-to-Site Policy** page, enter the following information:

- **Policy Name:** Enter a name you can use to refer to the policy. For example, Boston Office.
- **Preshared Key:** Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWall generated Preshared Key.
- **I know my Remote Peer IP Address (or FQDN):** If you check this option, this SonicWall can initiate the contact with the named remote peer. If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.
- **Remote Peer IP Address (or FQDN):** If you checked the option above, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, boston.yourcompany.com).

Step 5. Click **Next.**



Create Site-to-Site Policy

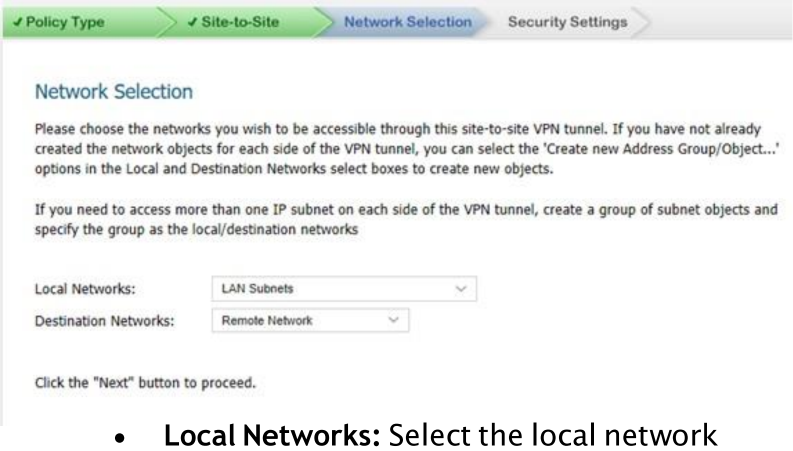
Please enter the unique name you wish to assign to this site-to-site VPN Policy and the preshared key you wish to use for the tunnel.

If you know the remote peer IP address or fully-qualified domain name, select the checkbox and enter the information in 'Remote Peer IP Address' box below.

Policy Name: To Central Site
Preshared Key: 1234
☑ I know my Remote Peer IP Address (or FQDN):
Remote Peer IP Address (or FQDN): 2.2.2.2

Click the "Next" button to proceed.

Step 6. In the **Network Selection** page, select the local and destination resources this VPN will be connecting:



Network Selection

Please choose the networks you wish to be accessible through this site-to-site VPN tunnel. If you have not already created the network objects for each side of the VPN tunnel, you can select the 'Create new Address Group/Object...' options in the Local and Destination Networks select boxes to create new objects.

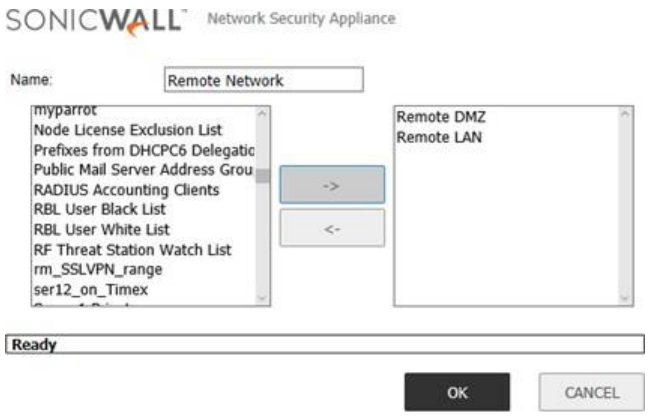
If you need to access more than one IP subnet on each side of the VPN tunnel, create a group of subnet objects and specify the group as the local/destination networks

Local Networks: LAN Subnets
Destination Networks: Remote Network

Click the "Next" button to proceed.

- **Local Networks:** Select the local network resources protected by this SonicWall that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses. If the object or group you want has not been created yet, select **Create Object** or **Create Group.** Create the new object or group in the dialog box that pops up. Then select the new object or group. For this example, select **LAN Subnets.**
- **Destination Networks**: Select the network resources on the destination end of the VPN Tunnel. If the object or group does not exist, select Create new Address Object or Create new Address Group. When creating an Address Object, make sure the Zone is VPN. If the remote network has multiple network segments and you wish to include this in the VPN, create multiple Address Objects and create a group to add them to.

Step 7. Click **Next.**



Name: Remote Network

myparrot
Node License Exclusion List
Prefixes from DHCPC6 Delegatic
Public Mail Server Address Grou
RADIUS Accounting Clients
RBL User Black List
RBL User White List
RF Threat Station Watch List
rm_SSLVPN_range
ser12_on_Timex

Remote DMZ
Remote LAN

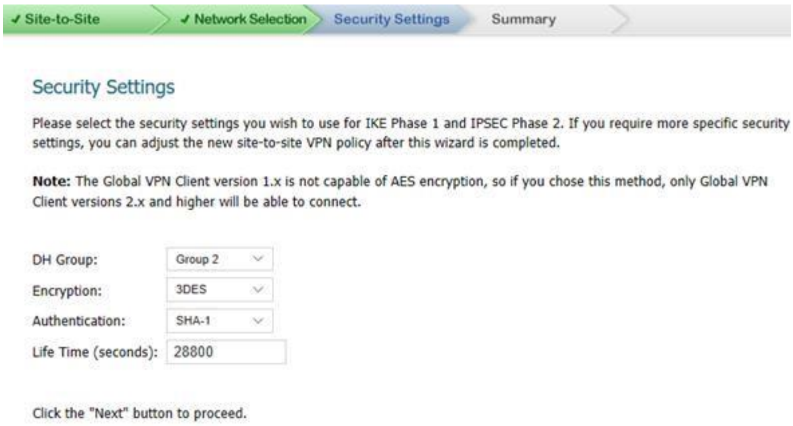
Ready

Step 8. In the IKE Security Settings page, select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the default settings.

- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel.
- **Authentication:** This is the hashing method used to authenticate the key, once it is

exchanged during IKE negotiation. You can choose MD5 or SHA-1.

- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).



Security Settings

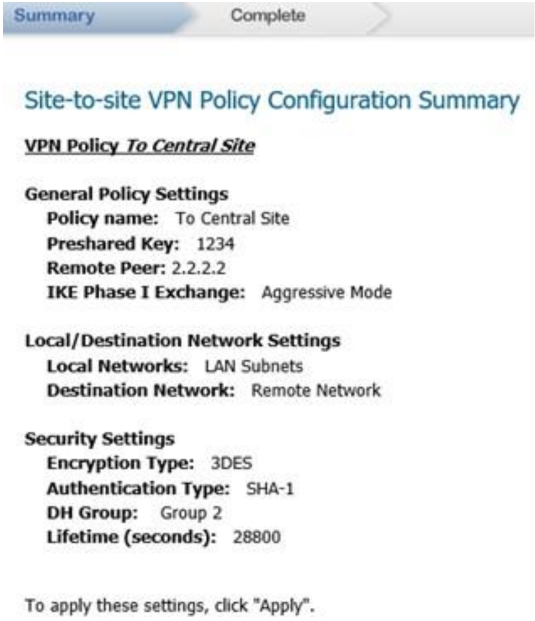
Please select the security settings you wish to use for IKE Phase 1 and IPSEC Phase 2. If you require more specific security settings, you can adjust the new site-to-site VPN policy after this wizard is completed.

Note: The Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only Global VPN Client versions 2.x and higher will be able to connect.

DH Group: Group 2
Encryption: 3DES
Authentication: SHA-1
Life Time (seconds): 28800

Click the "Next" button to proceed.

Step 9. The Configuration Summary page details the settings that will be pushed to the security appliance when you apply the configuration.
Step 10. Click **Apply** to create the VPN.



Site-to-site VPN Policy Configuration Summary

VPN Policy *To Central Site*

General Policy Settings
Policy name: To Central Site
Preshared Key: 1234
Remote Peer: 2.2.2.2
IKE Phase I Exchange: Aggressive Mode

Local/Destination Network Settings
Local Networks: LAN Subnets
Destination Network: Remote Network

Security Settings
Encryption Type: 3DES
Authentication Type: SHA-1
DH Group: Group 2
Lifetime (seconds): 28800

To apply these settings, click "Apply".

How to Test:

To verify that your VPN tunnel is working properly, it is necessary to ping the IP address of a computer on the remote network. By pinging the remote network, you send data packets to the remote network and the remote network replies that it has received the data packets. Your administrator supplies the remote IP address that you can use for testing. The following steps explain how to ping a remote IP address.

1. Locate the Windows Start button in the lower left hand corner of the desktop operating system. Click Start, then Run, and then type Command in the Open filepath box. A DOS window opens to the C:> prompt.
2. Type ping, then the IP address of the host computer. Press Enter to begin the data communication.
3. A successful ping communication returns data packet information to you. An unsuccessful ping returns a message of Request Timed Out.