SONICWALL®

SonicOS 8

IPSec VPN

Administration Guide



Contents

About SonicOS **5**
Working with SonicOS 5
SonicOS Workflow 6
How to Use the SonicOS Administration Guides 7
Guide Conventions 9

IPSec VPN Overview **10**
About Virtual Private Networks 10
VPN Types 11
- IPsec VPN 12
- DHCP over VPN 12
- L2TP with IPsec 12
- SSL VPN 13

VPN Security 14
- About IKEv1 15
- About IKEv2 15
- Mobility and Multi-homing Protocol for IKEv2 (MOBIKE) 16
- About IPsec (Phase 2) Proposal 16
- About Suite B Cryptography 17

VPN Base Settings and Displays 17
- Policies 18
- Active Tunnels 19
- Down Tunnels 20
- Settings 21

IPv6 VPN Configuration 21

Site to Site VPNs **23**
Planning Site to Site Configurations 23
General VPN Configuration 24
- Configuring Settings on the General Tab 25
- Configuring Settings on the Network Tab 26
- Configuring Settings on the Proposals Tab 27
- Configuring Settings on the Advanced Tab 28

Managing GroupVPN Policies 29
- Configuring IKE Using a Preshared Secret Key 30
- Configuring IKE Using 3rd Party Certificates 35
- Downloading a GroupVPN Client Policy 41

Two-Factor Authentication (2-FA) for Global VPN Client 43
Creating Site to Site VPN Policies 44
Configuring with a Preshared Secret Key 45
Configuring with a Manual Key 54
Configuring with a Third-Party Certificate 58
Configuring the Remote SonicWall Network Security Appliance 67

VPN Auto Provisioning 70
About VPN Auto Provisioning 70
Defining VPN Auto Provisioning 70
Benefits of VPN Auto Provisioning 71
How VPN Auto Provisioning Works 71
Configuring a VPN AP Server 75
Starting the VPN AP Server Configuration 75
Configuring VPN AP Server Settings on General 76
Configuring VPN AP Server Settings on Network 78
Configuring Advanced Settings on Proposals 80
Configuring Advanced Settings on Advanced 81
Configuring a VPN AP Client 82

Rules and Settings 86
Adding a Tunnel Interface 86
Creating a Static Route for the Tunnel Interface 92
Route Entries for Different Network Segments 93
Redundant Static Routes for a Network 93

Advanced 94
Configuring Advanced VPN Settings 94
Configuring IKEv2 Settings 96
Using OCSP with SonicWall Network Security Appliances 97
OpenCA OCSP Responder 98
Loading Certificates to Use with OCSP 98
Using OCSP with VPN Policies 100

DHCP over VPN 101
DHCP Relay Mode 101
Configuring the Central Gateway for DHCP Over VPN 102
Configuring DHCP over VPN Remote Gateway 103
Current DHCP over VPN Leases 105

L2TP Servers and VPN Client Access 107
Configuring the L2TP Server 107
Viewing Currently Active L2TP Sessions 109
Configuring Microsoft Windows L2TP VPN Client Access 110

Configuring macOS L2TP VPN Client Access 113
Configuring iOS L2TP VPN Client Access 116

AWS VPN 120
Overview 120
Creating a New VPN Connection 120
Reviewing the VPN Connection 121
Configuration on the Firewall 121
Configuration on Amazon Web Services 122
Route Propagation 122
AWS Regions 123
Deleting VPN Connections 123

SonicWall Support 124
About This Document 125

1

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describe how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators with the management interface, API (Application Program Interface), and Command Line Interface (CLI) for firewall configuration. You can configure and manage your firewall by setting objects to secure and protect the network services, manage traffic, and provide the desired level of network service.explaining how to configure various types of IPSec VPN Policies, site to site policies, VPN Auto Provisioning, and so on.

Topics:

- Working with SonicOS
- SonicOS Workflow
- How to Use the SonicOS Administration Guides
- Guide Conventions

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and outside threats to your network. SonicOS functions in conjunction with SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices such as access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

The following table details the SonicWall firewall series and the specific performance, security, and feature sets they provide within the enterprise.

Firewall Type	Comments
TZ Series	The entry level TZ Series, also known as desktop firewalls, delivers revamped features such as 5G readiness, better connectivity options, improved threat protection, SSL and decryption performance that addresses HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support. It provides advanced networking and security features, like the multi-engine Capture Advanced Threat Protection (ATP) cloud-based sandbox service with patent-pending Real-Time Deep Memory Inspection (RTDMI™).
NSa Series	NSa firewalls provide your mid-sized network with enhanced security. These firewalls are designed specifically for businesses with more than 250 workstations. The NSa provides cloud-based and on-box capabilities such as TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSv Series	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

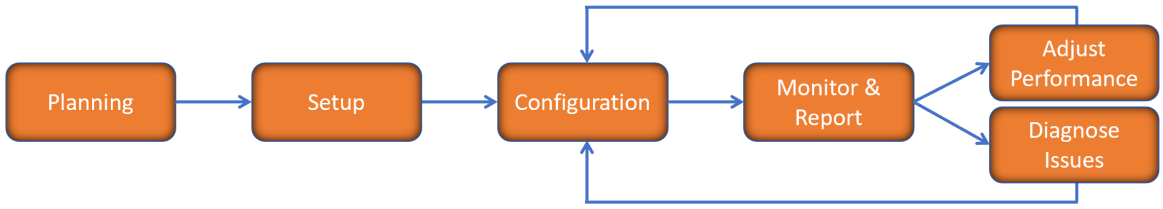
In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls.

For more information, refer to:

- SonicOS API Reference Guide
- SonicOS CLI Reference Guide

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

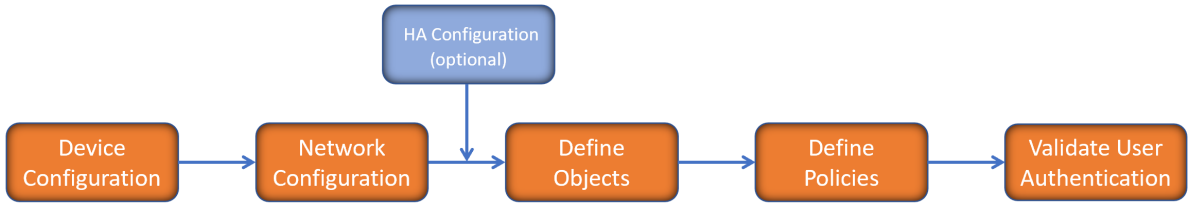


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. For more information, refer to the specific Administration Guide for a SonicOS feature.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

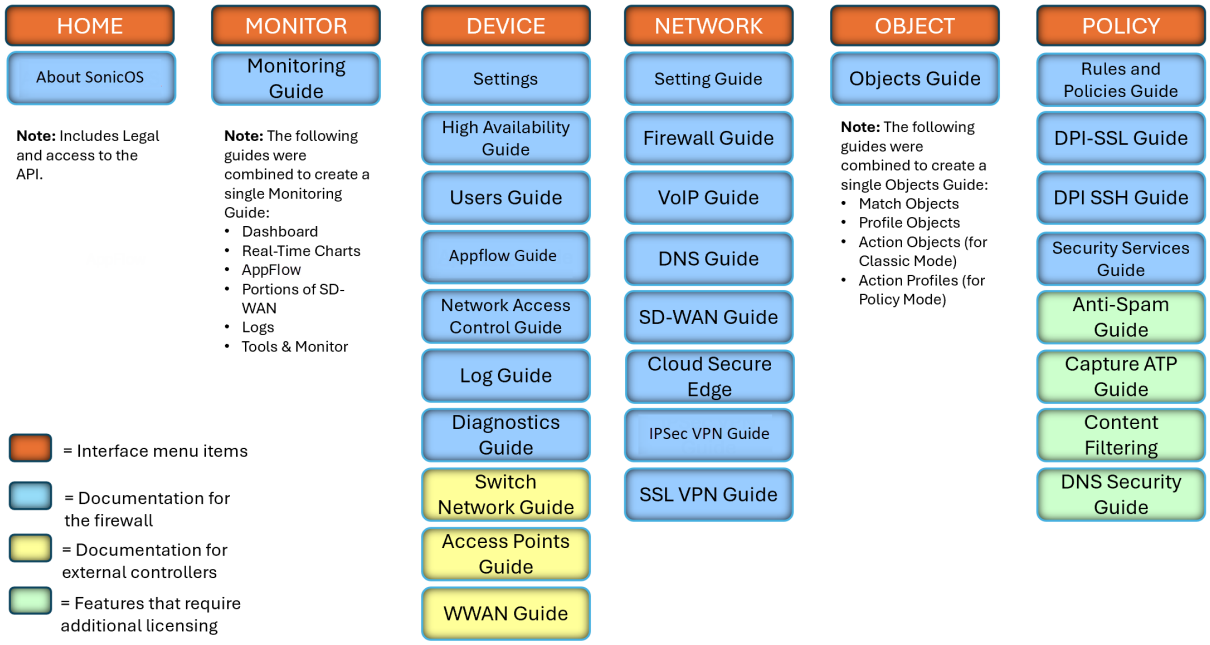


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 8 Monitor Guide and the SonicOS 8 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicOS management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the Technical Documentation Portal.

Guide Conventions

These text conventions are used in this guide:

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function | Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, **NETWORK | System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page.
`Code`	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=***<your serial number>*, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

2

IPSec VPN Overview

The VPN options provide the features for configuring and displaying your VPN policies. You can configure various types of IPsec VPN policies, such as site-to-site policies, including GroupVPN, and route-based Tunnel Interface policies. For specific details on the setting for these kinds of policies, go to the following sections:

- Site to Site VPNs
- VPN Auto Provisioning
- Tunnel Interface Route-based VPN

This section provides information on VPN types, discusses some of the security options you can select, and describes the interface for the **NETWORK | IPSec VPN > Rules and Settings** page. Subsequent sections describe how to configure site to site and route-based VPN, advanced settings, DHCP over VPN and L2TP servers.

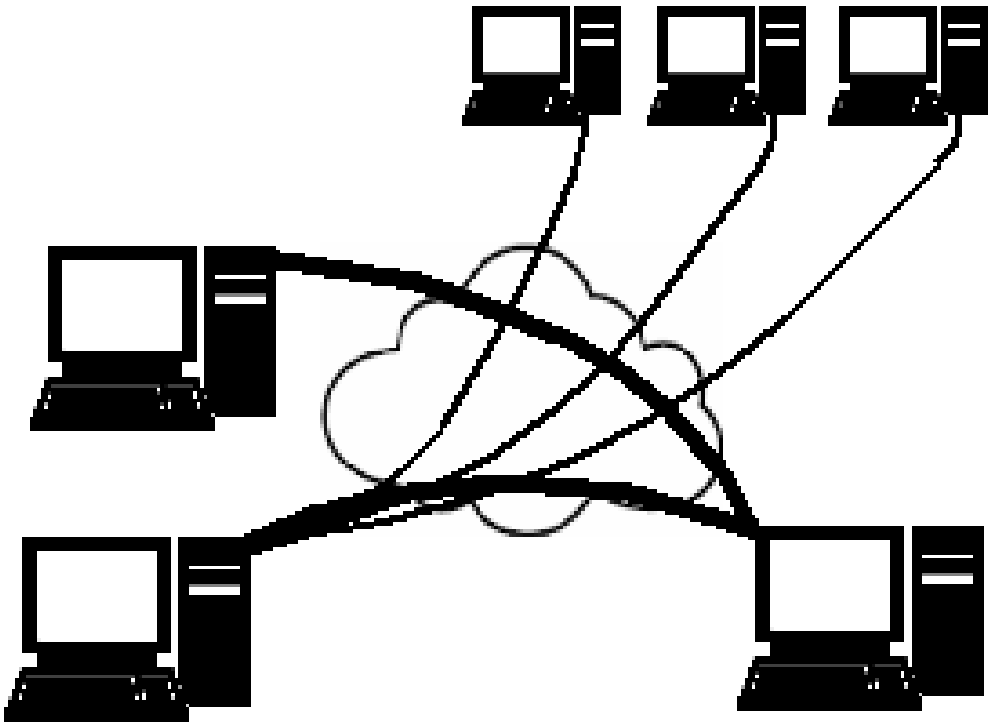
Topics:

- About Virtual Private Networks
- VPN Types
- VPN Security
- VPN Base Settings and Displays
- IPv6 VPN Configuration
- VPN Auto-Added Access Rule Control

About Virtual Private Networks

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It also offers security to protect the data from viewing or tampering en route.

A VPN is created by establishing a secure tunnel through the Internet. This tunnel is a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. It is flexible in that you can change it at any time to add more nodes, change the nodes, or remove them altogether. VPN is less costly, because it uses the existing Internet infrastructure.



VPNs can support either remote access—connecting a user's computer to a corporate network—or site to site, which is connecting two networks. A VPN can also be used to interconnect two similar networks over a dissimilar middle network: for example, two IPv6 networks connecting over an IPv4 network.

VPN systems might be classified by:

- Protocols used to tunnel the traffic
- Tunnel's termination point location, for example, on the customer edge or network provider edge
- Type of topology of connections, such as site to site or network to network
- Levels of security provided
- OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- Number of simultaneous connections

VPN Types

Several types of VPN protocols can be configured for use:

- IPsec VPN
- DHCP over VPN
- L2TP with IPsec
- SSL VPN

IPsec VPN

SonicOS supports the creation and management of IPsec VPNs. These VPNs are primarily configured at **NETWORK | IPSec VPN > Rules and Settings** and **NETWORK | IPSec VPN > Advanced**.

IPsec (Internet Protocol Security) is a standards-based security protocol that was initially developed for IPv6, but it is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals of authentication, integrity, and confidentiality. IPsec uses encryption and encapsulates an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

An advantage of using IPsec is that security arrangements can be handled without requiring changes to individual user computers. It provides two types of security service:

- Authentication Header (AH), which essentially allows authentication of the sender of data
- Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data

You can use IPsec to develop policy-based VPN (site to site) or route-based VPN tunnels or Layer 2 Tunneling Protocol (L2TP).

DHCP over VPN

SonicOS allows you to configure a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, you want to have all VPN networks on one logical IP subnet and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.

The firewall at the remote and central sites are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The firewall at the remote site passes DHCP broadcast packets through its VPN tunnel. The firewall at the central site relays DHCP packets from the client on the remote network to the DHCP server on the central site.

L2TP with IPsec

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself, and because of that lack of confidentiality in the L2TP protocol, it is often implemented along with IPsec. The general process for setting up an L2TP/IPsec VPN is:

1. Negotiate an IPsec security association (SA), typically through Internet key exchange (IKE). This is carried out over UDP port 500, and commonly uses either a shared password (also called pre-shared keys), public keys, or X.509 certificates on both ends, although other keying methods exist.

2. Establish Encapsulating Security Payload (ESP) communication in transport mode. The IP protocol number for ESP is 50 (compare TCP's 6 and UDP's 17). At this point, a secure channel has been established, but no tunneling is taking place.
3. Negotiate and establish L2TP tunnel between the SA endpoints. The actual negotiation of parameters takes place over the SA's secure channel, within the IPsec encryption. L2TP uses UDP port 1701.

When the process is complete, L2TP packets between the endpoints are encapsulated by IPsec. Because the L2TP packet itself is wrapped and hidden within the IPsec packet, no information about the internal private network can be garnered from the encrypted packet. Also, UDP port 1701 does not need to be opened on firewalls between the endpoints, because the inner packets are not acted upon until after IPsec data has been decrypted and stripped, which only takes place at the endpoints.

SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional IPsec VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It can be used to give remote users access to Web applications, client/server applications, and internal network connections.

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of computers, accessing resources from many locations. The two major types of SSL VPNs are:

- SSL Portal VPN
- SSL Tunnel VPN

The SSL Portal VPN allows single SSL connection to a Web site so the end user can securely access multiple network services. The site is called a portal because it is one door (a single page) that leads to many other resources. The remote user accesses the SSL VPN gateway using any modern Web browser, identifies himself or herself to the gateway using an authentication method supported by the gateway and is then presented with a Web page that acts as the portal to the other services.

The SSL tunnel VPN allows a Web browser to securely access multiple network services, including applications and protocols that are not Web-based, through a tunnel that is running under SSL. SSL tunnel VPNs require that the Web browser be able to handle active content, which allows them to provide functionality that is not accessible to SSL portal VPNs. Examples of active content include Java, JavaScript, Active X, or Flash applications or plug-ins.

SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. It also uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SRA/SMA appliance uses SSL to secure the VPN tunnel. One advantage of SSL VPN is that SSL is built into most web browsers. No special VPN client software or hardware is required.

NOTE: SonicWall makes Secure Mobile Access (SMA) appliances you can use in concert with or independently of a SonicWall network security appliance running SonicOS. For information on SonicWall SMA appliances, refer to https://www.sonicwall.com/products/remote-access/remote-access-appliances .

VPN Security

IPsec VPN traffic is secured in two stages:

1. **Authentication**: The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
2. **Encryption**: The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN), the exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS supports two versions of IKE:

IKE version 1 (IKEv1)	Uses a two phase process to secure the VPN tunnel. First, the two nodes authenticate each other and then they negotiate the methods of encryption.
	You can find more information about IKEv1 in the three specifications that initially define IKE: RFC 2407, RFC 2408, and RFC 2409. They are available on the web at: • http://www.faqs.org/rfcs/rfc2407.html – The Internet IP Security Domain of Interpretation for ISAKMP • http://www.faqs.org/rfcs/rfc2408.html – RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP) • http://www.faqs.org/rfcs/rfc2409.html – RFC 2409 - The Internet Key Exchange (IKE)
IKE version 2 (IKEv2)	Is the default type for new VPN policies because of improved security, simplified architecture, and enhanced support for remote users. A VPN tunnel is initiated with a pair of message exchanges. The first pair of messages negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange. The second pair of messages authenticates the previous messages, exchange identities and certificates, and establish the first CHILD_SA (security association). Parts of these messages are encrypted and integrity protected with keys established through the first exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
	You can find more information about IKEv2 in the specification, RFC 4306, available on the Web at: http://www.ietf.org/rfc/rfc4306.txt.

IMPORTANT: IKEv2 is not compatible with IKEv1. When using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels.

DHCP over VPN is not supported in IKEv2.

For more VPN security information, see:

- About IKEv1
- About IKEv2
- Mobility and Multi-homing Protocol for IKEv2 (MOBIKE)
- About IPsec (Phase 2) Proposal
- About Suite B Cryptography

About IKEv1

In IKEv1, two modes are used to exchange authentication information:

- **Main Mode**: The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:
  1. The initiator sends a list of cryptographic algorithms the initiator supports.
  2. The responder replies with a list of supported cryptographic algorithms.
  3. The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
  4. The responder replies with the public key for the same cryptographic algorithm.
  5. The initiator sends identity information (usually a certificate).
  6. The responder replies with identity information.
- **Aggressive Mode**: To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:
  1. The initiator proposes a cryptographic algorithm to use and sends its public key.
  2. The responder replies with a public key and identity proof.
  3. The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

About IKEv2

IKE version 2 (IKEv2) is a newer protocol for negotiating and establishing security associations. Secondary gateways are supported with IKEv2. IKEv2 is the default proposal type for new VPN policies.

IKEv2 is not compatible with IKEv1. When using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels. DHCP over VPN is not supported in IKEv2.

IKEv2 has the following advantages over IKEv1:

- More secure
- More reliable
- Simpler
- Faster
- Extensible
- Fewer message exchanges to establish connections
- EAP Authentication support
- MOBIKE support
- Built-in NAT traversal
- Keep Alive is enabled as default

IKEv2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKEv2 greatly reduces the number of message exchanges needed to establish a Security Association over IKEv1 Main Mode, while being more secure and flexible than IKEv1 Aggressive Mode. This reduces the delays during re-keying. As VPNs grow to include more and more tunnels between multiple nodes or gateways, IKEv2 reduces the number of Security Associations required per tunnel, thus reducing required bandwidth and housekeeping overhead.

Security Associations (SAs) in IKEv2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Mobility and Multi-homing Protocol for IKEv2 (MOBIKE)

The Mobility and Multi-homing Protocol (MOBIKE) for IKEv2 provides the ability for maintaining a VPN session, when a user moves from one IP address to another, without the need for reestablishing IKE security associations with the gateway. For example, a user could establish a VPN tunnel while using a fixed Ethernet connection in the office. MOBIKE allows the user to disconnect the laptop and move to the office's wireless LAN without interrupting the VPN session.

MOBIKE operation is transparent and does not require any extra configuration by you or consideration by users.

About IPsec (Phase 2) Proposal

The IPsec (Phase 2) proposal occurs with both IKEv1 and IKEv2. In this phase, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encapsulating Security Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authenticated and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following **Encryption** methods for traffic through the VPN:

• DES	• AES-128	• AESGCM16-128	• AESGMAC-128
• 3DES	• AES-192	• AESGCM16-192	• AESGMAC-192
• None	• AES-256	• AESGCM16-256	• AESGMAC-256

SonicOS supports the following **Authentication** methods:

• MD5	• SHA1	• AES-XCBC	• None
	• SHA256		
	• SHA384		
	• SHA512		

About Suite B Cryptography

SonicOS supports Suite B cryptography, which is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. It serves as an interoperable cryptographic base for both classified and unclassified information. Suite B cryptography is approved by National Institute of Standards and Technology (NIST) for use by the U.S. Government.

Most of the Suite B components are adopted from the FIPS standard:

- Advanced Encryption Standard (AES) with key sizes of 128 to 256 bits (provides adequate protection for classified information up to the SECRET level).
- Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures (provides adequate protection for classified information up to the SECRET level).
- Elliptic Curve Diffie-Hellman (ECDH) key agreement (provides adequate protection for classified information up to the SECRET level).
- Secure Hash Algorithm 2 (SHA256, SHA384, SHA512) message digest (provides adequate protection for classified information up to the TOP SECRET level).

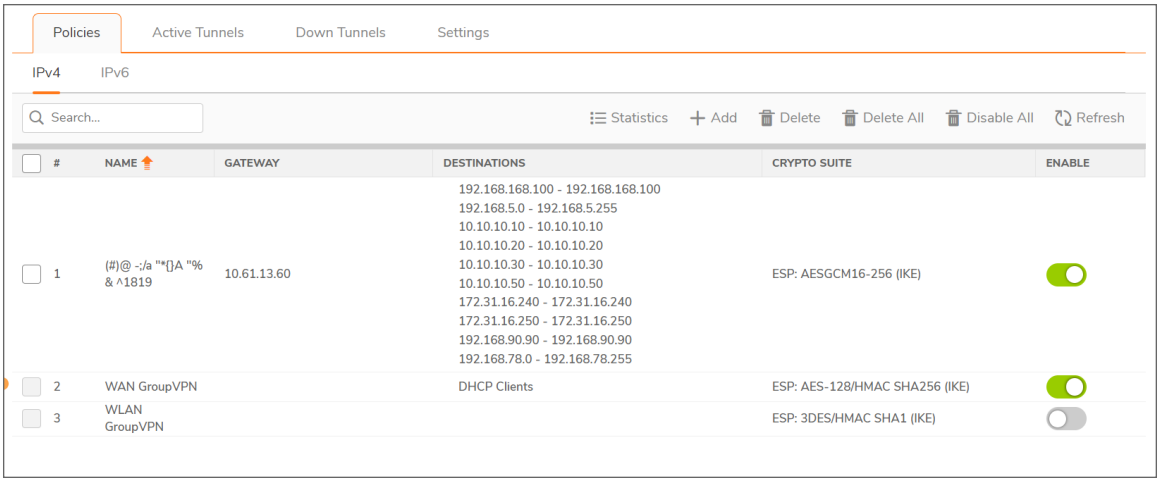
VPN Base Settings and Displays

The VPN pages offer a series of tables and settings, depending on the options selected.

For details on the **NETWORK | IPSec VPN > Rules and Settings** page, refer to the following:

- Policies
- Active Tunnels
- Settings

IPSEC VPN > RULES AND SETTINGS PAGE

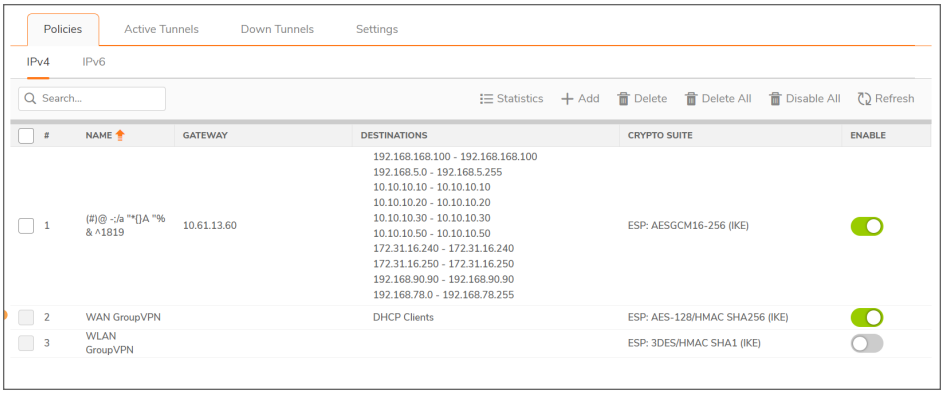


View IP Version	Sets IP version view. Options are IPv4 or IPv6.

NOTE: SonicWall VPN supports both IPv4 and IPv6 (Internet Protocol version 4 and Internet Protocol version 6). You can toggle between the versions by selecting the one you want in the upper left side of the window. The default view is for IPv4.

Policies

All defined VPN policies are displayed in the **NETWORK | IPSec VPN > Rules and Settings** on the **Policies** tab.



Each entry displays the following information:

- **Name** – The default name or user-defined VPN policy name.
- **Gateway** – The IP address of the remote firewall. If the wildcard IP address, `0.0.0.0`, is used, it is displayed as the IP address.
- **Destinations** – The IP addresses of the destination networks.

- **Crypto Suite** – The type of encryption used for the VPN policy.
- **Enable** – Shows whether the policy is enabled. A checked box enables the VPN Policy. Clearing the box disables it.
- **Configure** – Options for managing the individual VPN policies:
    - **Edit** icon allows you to edit the VPN policy.
    - **Delete** icon deletes the policy on that line. The predefined GroupVPN policies cannot be deleted, so the Delete icons are dimmed.
    - **Download** icon exports the VPN policy configuration as a file for local installation by SonicWall Global VPN Clients.

The following buttons are shown in the **Policies** table:

Search	Standard search engine to help locate specific VPN policies.
Statistics	Statics of the Site to Site policies and Group VPN Policies.
+Add	Accesses the **VPN Policy** window to configure site to site VPN policies.
Delete	Deletes the selected (checked box before the VPN policy name in the **Name** column first) You cannot delete the GroupVPN policies.
Delete All	Deletes all VPN policies in the **VPN Policies** table except the default GroupVPN policies.
Disable All	Disables all VPN Policies in the **VPN Policies** table except the default GroupVPN policies.
Refresh	Refreshes the page.

ⓘ **NOTE:** You can refresh the active tunnels by using the **Refresh** option at the top of the **Policies** and **Active Tunnels** tables.

Some statistics about the VPN policies are also summarized below the table, for both site to site and GroupVPN policies:

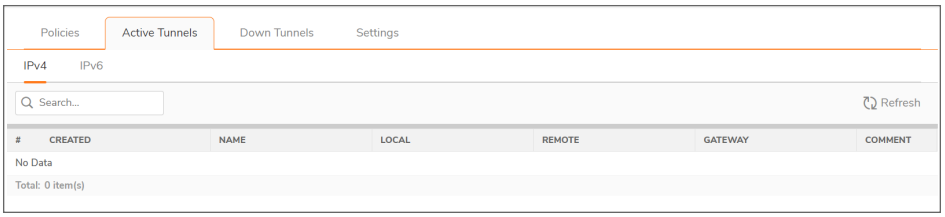
- Number of policies defined
- Number of policies enabled
- Maximum number of policies allowed

You can define up to four GroupVPN policies, one for each zone. These GroupVPN policies are listed by default in the **VPN Policies** table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on **the** Edit icon in the **Configure** column for the GroupVPN displays the **Security Policy** window for configuring the GroupVPN policy.

ⓘ **NOTE:** A VPN Policy cannot have two different WAN interfaces if the VPN Gateway IP is the same.

Active Tunnels

A list of currently active VPN tunnels is displayed in this section.



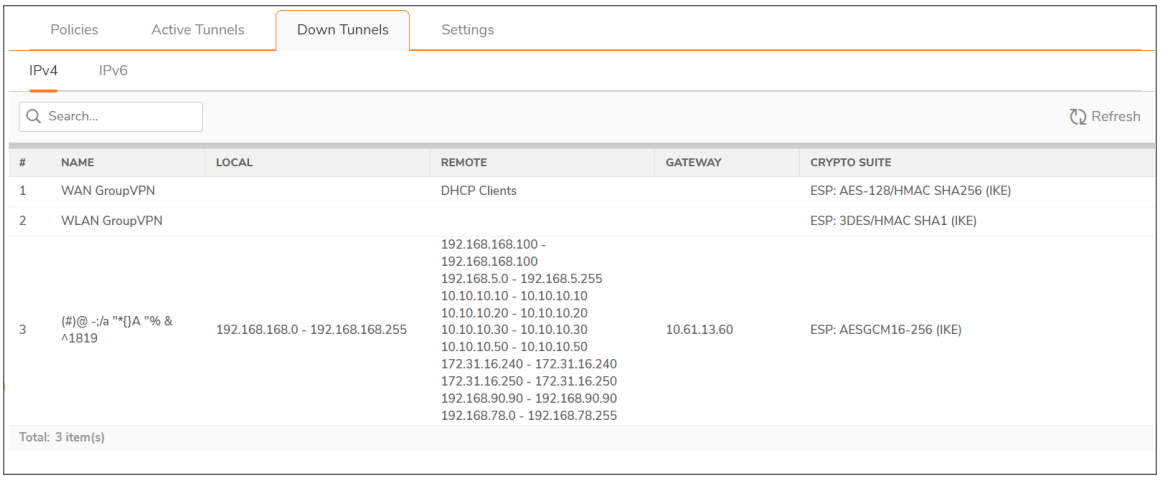
The Currently Active VPN Tunnels table displays this information for each tunnel:

Search	Standard search engine to help locate specific active tunnels.
Created	Date and time the tunnel was created
Name	Name of the VPN Policy
Local	Local LAN IP address of the tunnel
Remote	Remote destination network IP address
Gateway	Peer gateway IP address
Comment	More information about the tunnel
Left-arrow icon	When the mouse hovers over the Left-arrow icon, the respective VPN policy is displayed in the middle of the **VPN Policies** table

You can refresh the active tunnels by using the **Refresh** option at the top of the **Policies** and **Active Tunnels** tables.

Down Tunnels

A list of currently not active VPN tunnels is displayed in this section.



The Down Tunnels table displays this information for each tunnel:

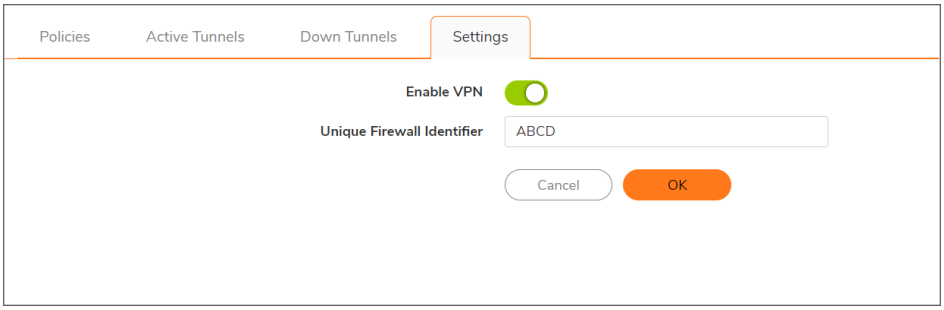
Search	Standard search engine to help locate specific down tunnels.

Name	Name of the VPN Policy
Local	Local LAN IP address of the tunnel
Remote	Remote destination network IP address
Gateway	Peer gateway IP address
Crypto Suite	The cryptographic algorithms

You can refresh the active tunnels by using the **Refresh** option at the top of the **Policies** and **Active Tunnels** tables.

Settings

The **Settings** tab of the **NETWORK | IPSec VPN > Rules and Settings** page displays the following information:



Enable VPN	Select to enable VPN policies through the SonicWall® security policies.
Unique Firewall Identifier	Identifies this SonicWall appliance when configuring VPN tunnels. The default value is the serial number of the appliance. You can change the identifier to something meaningful to you. The Unique Firewall Identifier displays in TOTP authenticator apps when users enroll for two-factor authentication with GVC.

IPv6 VPN Configuration

Site to Site VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs on the **IPv6** tab on the **NETWORK | IPSec VPN > Rules and Settings** page.

There are certain VPN features that are currently not supported for IPv6, including:

- IKEv1 is not supported.
- GroupVPN is not supported.
- Tunnel Interface route-based VPN is not supported.

- DHCP Over VPN is not supported.
- L2TP Server is not supported.

When configuring an IPv6 VPN policy:

- On the **General** screen:
  - The **Gateways** must be configured using IPv6 addresses. FQDN is not supported.
  - Under I**KE Authentication**, IPV6 addresses can be used for the local and peer IKE IDs.
- On the **Network** screen:
  - IPV6 address objects (or address groups that contain only IPv6 address objects) must be selected for the **Local Network** and **Remote Network**.
  - **DHCP Over VPN** is not supported, thus the DHCP options for protected network are not available.
  - The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed, but you can select an ***all zero*** IPv6 Network address object for the same functionality and behavior.
- On the **Proposals** screen, only **IKEv2 mode** is supported.
- On the **Advanced** screen, several options are disabled for IPv6 VPN policies:
  - **Suppress automatic Access Rules creation for VPN Policy** is disabled.
  - **Enable Windows Networking (NetBIOS) Broadcast** is disabled.
  - **Enable Multicast** is disabled.
  - **Apply NAT Policies** is disabled.

ⓘ **NOTE:** Because an interface might have multiple IPv6 address, sometimes the local address of the tunnel might vary periodically. If the user needs a consistent IP address, configure the **VPN policy bound to** option as an interface instead of a zone, and specify the address manually. The address must be one of the IPv6 addresses for that interface.

3

Site to Site VPNs

SonicWall VPN is based on the industry-standard IPsec VPN implementation. It provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners through the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dial-up Internet access can securely and easily access your network resources with the SonicWall Global VPN Client (GVC) and GroupVPN on your firewall. Remote office networks can securely connect to your network using site to site VPN connections that enable network-to-network VPN connections.

The maximum number of policies you can add depends on which SonicWall model you have. The larger models allow more connections.

NOTE: Remote users must be explicitly granted access to network resources. Depending on how you define access, you can affect the ability of remote clients using GVC to connect to GroupVPN, but you can also affect remote users using NetExtender and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the allow list on the VPN Access window. To access this window, select the **DEVICE | Users > Local Users & Groups > Local Users > Add User > VPN Access**.

This section describes site to site policies, including GroupVPN. Other sections describe auto provisioning and Tunnel Interface policies for route-based VPN. For specific details on the setting for these kinds of policies, go to the following sections:

- VPN Auto Provisioning
- Tunnel Interface Route-based VPN

Topics:

- Planning Site to Site Configurations
- General VPN Configuration
- Managing GroupVPN Policies
- Creating Site to Site VPN Policies

Planning Site to Site Configurations

You have many options when configuring site to site VPN and can include the following options:

Branch Office (Gateway to Gateway)	A SonicWall firewall is configured to connect to another SonicWall firewall through a VPN tunnel. Or, a SonicWall firewall is configured to connect through IPsec to another manufacturer's firewall.
Hub and Spoke Design	All SonicWall VPN gateways are configured to connect to a central hub, such as a corporate firewall. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWall network security appliance.
Mesh Design	All sites connect to all other sites. All sites must have static IP addresses.

SonicWall has video clips and knowledge base articles that can help you with some of those decisions.

ⓘ **VIDEO:** Informational videos with site to site VPN configuration examples are available online. For example, see *How to Create a Site to Site VPN in Main Mode using Preshared Secret* or *How to Create Aggressive Mode Site to Site VPN using Preshared Secret*.
Additional videos are available at: Video-Tutorials.

ⓘ **TIP:** See the knowledge base articles for information about Site to Site VPNs:
VPN: Types of Site to Site VPN Scenarios and Configurations (SW12884)
Troubleshooting articles of Site to Site VPN (SW7570)

When designing your VPN configurations, be sure to document all pertinent IP addressing information. You might want to create a network diagram to use as a reference. A few other things to note:

- The firewall must have a routable WAN IP address whether it is dynamic or static.
- In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

General VPN Configuration

This section reviews the general process for site to site configurations. Specific scenarios might be different and some are described in subsequent sections. Note that configuring IPsec VPNs for IPv4 and IPv6 are very similar; however, certain VPN features are currently not supported in IPv6. See IPv6 VPN Configuration for information.

To configure a VPN:

1. Navigate to the **NETWORK | IPSec VPN > Rules and Settings** page.
2. Make the appropriate version selection either IPv4 or IPv6.
3. Click **+Add**.
4. Complete the **General**, **Network**, **Proposals**, and **Advanced** tabs on the **VPN Policy** dialog. The following sections provide additional information for each of those tabs.

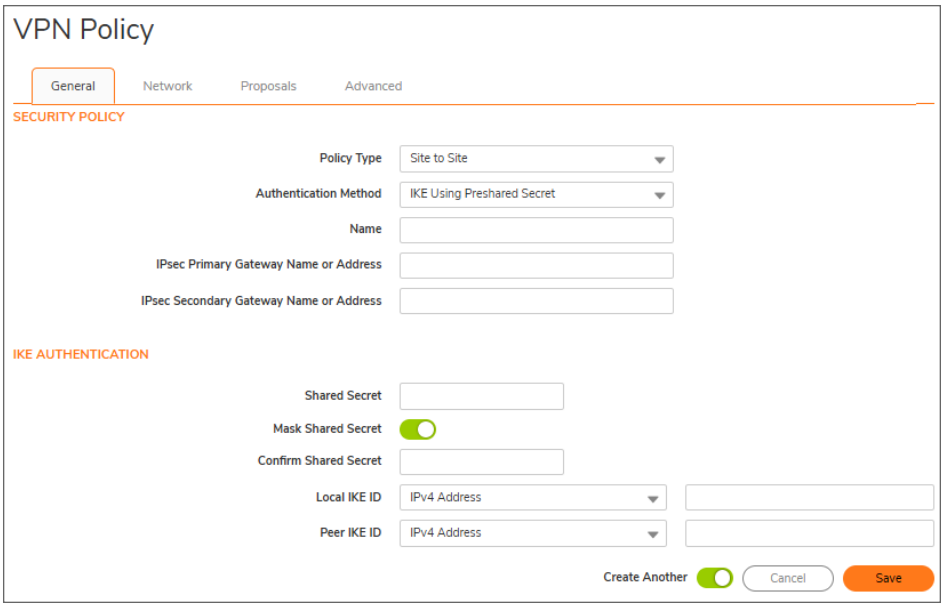
Topics:

- Configuring Settings on the General Tab
- Configuring Settings on the Network Tab
- Configuring Settings on the Proposals Tab
- Configuring Settings on the Advanced Tab

Configuring Settings on the General Tab

On the **General** tab, begin defining the site to site VPN policy. There are some slight differences between IPv4 and IPv6 networks, which are noted.

IPV4 +ADD VPN POLICY: GENERAL



1. If configuring an IPv4 VPN, select **Policy Type** from the drop-down menu.

   ⓘ | **NOTE:** The **Policy Type** field is not available for IPv6.

2. Select the authentication method from the **Authentication Method** drop-down menu. The remaining fields in the **General** tab change depending on which option you select. The following options are available.

IPv4	IPv6
Manual Key	Manual Key
IKE using Preshared Secret (default)	IKE using Preshared Secret (default)
IKE using 3rd Party Certificates	IKE using 3rd Party Certificates

IPv4	IPv6
SonicWall Auto Provisioning Client	
SonicWallAuto Provisioning Server	

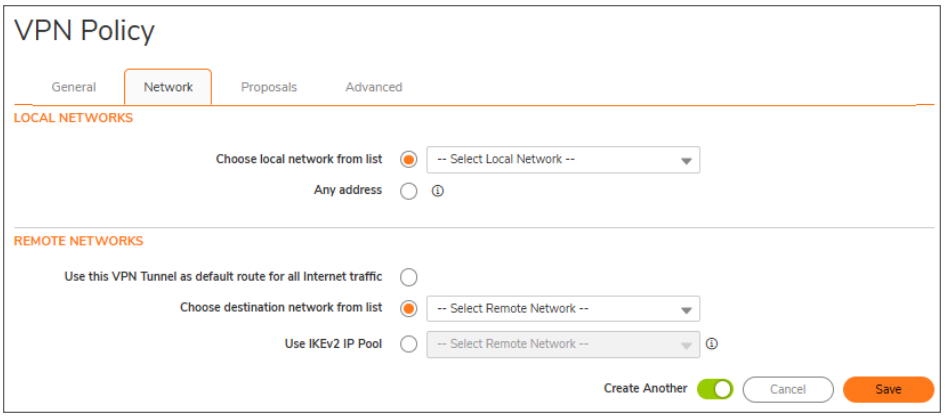
3. Type in a Name for the policy.
4. For **IPsec Primary Gateway Name or Address**, type in the gateway name or address.
5. For **IPsec Secondary Gateway Name or Address**, type in the gateway name or address.
6. Under **IKE Authentication**, provide the required authentication information.

   ⓘ **NOTE:** When configuring IKE authentication, IPv6 addresses can be used for the local and peer IKE IDs.

Configuring Settings on the Network Tab

On the **Network** tab, define the networks that comprise the site to site VPN policy.

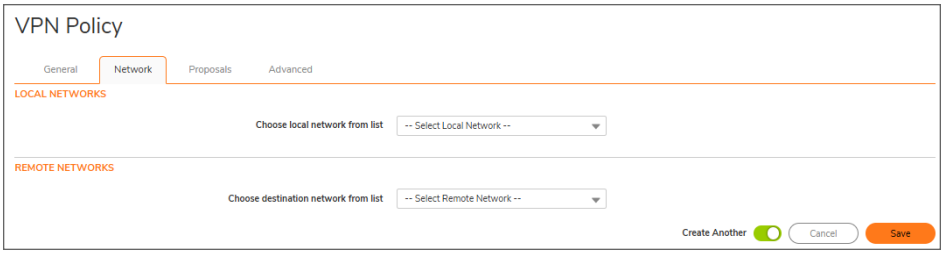
IPV4 +ADD VPN POLICY: NETWORK



On the **Network** tab of the VPN policy, select the local and remote networks from the **Local Network** and **Remote Network** options.

For IPv6, the drop-down menus are the only option provided and only address objects that can be used by IPv6 are listed. Because DHCP is not supported, those options are not available. Also the **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed. An all-zero IPv6 Network address object could be selected for the same functionality and behavior.

IPV6 +ADD VPN POLICY: NETWORK



For IPv4, additional options are provided. Under **Local Networks**, you can **Choose local network from list** or choose **Any address**. If **Any address** is selected, auto-added rules are created between Trusted Zones and the VPN zone.

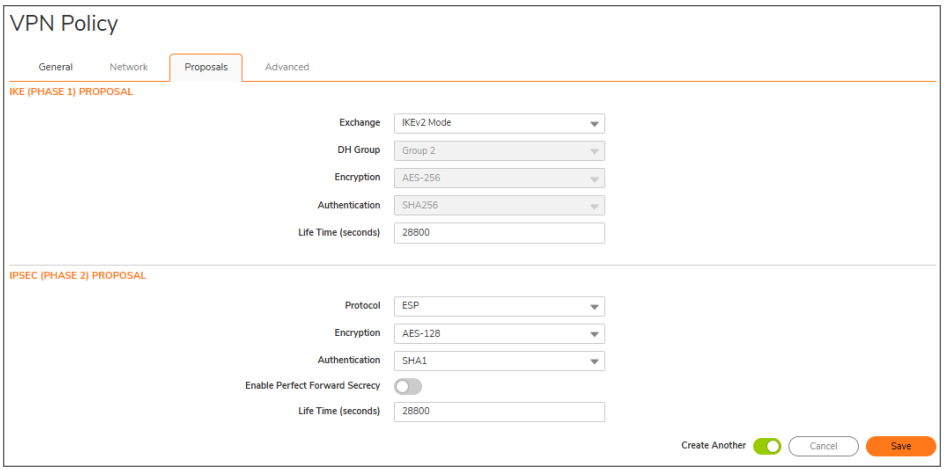
For IPv4 under **Remote Networks**, you can chose one of the following:

- **Use this VPN tunnel as default route for all Internet traffic**.
- **Choose destination network from list**. If none are listed you can create a new address object or address group.
- **Use IKEv2 IP Pool**. Select this to support IKEv2 Config Payload.

Configuring Settings on the Proposals Tab

On the **Proposals** tab, define the security parameters for your VPN policy. The page is the same for IPv4 and IPv6, but the options are different depending on what you selected. IPv4 offers both IKEv1 and IKEv2 options in the **Exchange** field, whereas IPv6 only has IKEv2.

IPV4 +ADD VPN POLICY: PROPOSALS



In the **IKE (PHASE 1) Proposal** section, select the **Exchange**, **DH Group**, **Encryption**, **Authentication**, and **Life Time in seconds** from the drop down.

In the **IPSEC (PHASE 2) Proposal** section, select the **Protocol**, **Encryption**, **Authentication**, and **Life Time in seconds** from the drop down. If you select the **Enable Perfect Forward Secrecy** option, select the **DH Group** from the drop down.

Click **Save** to save your options.

Configuring Settings on the Advanced Tab

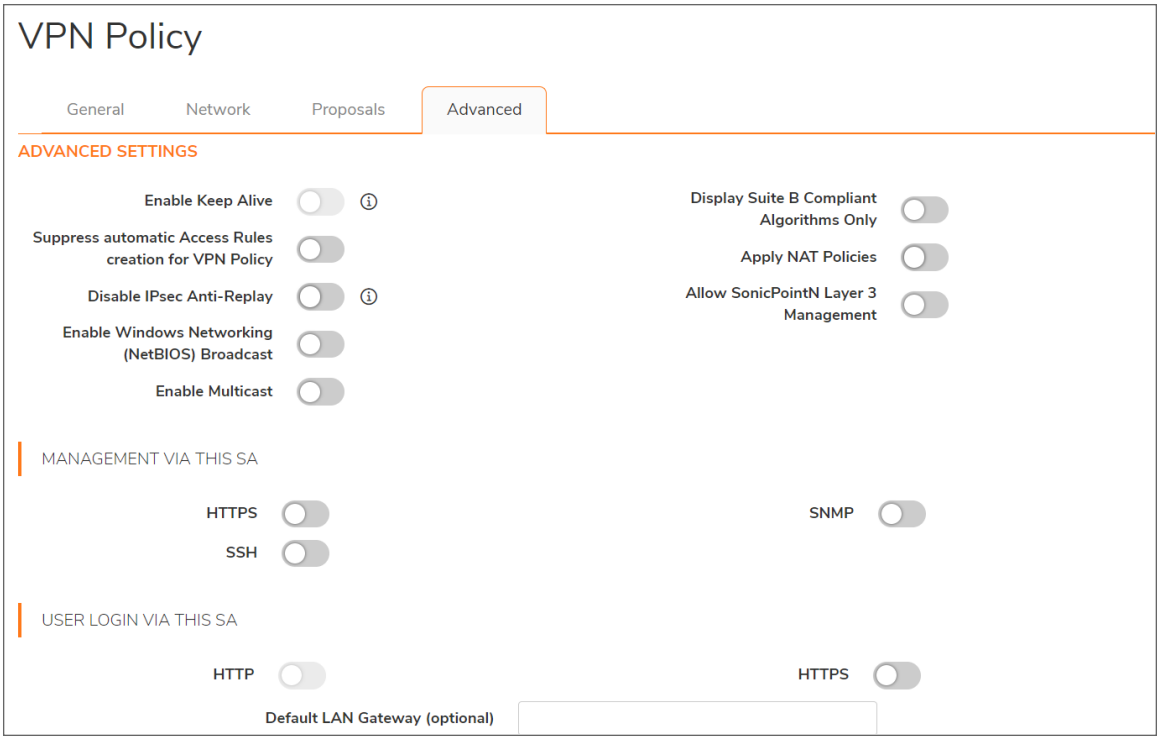
The **Advanced** tabs for IPv4 and IPv6 are similar, but some options are available only for one version or the other, as shown in Advanced Settings: Option Availability. Options also change depending on the authentication method selected.

ADVANCED SETTINGS: OPTION AVAILABILITY

Option	IP Version	
	IPv4	**IPv6**
Enable Keep Alive	Supported	Supported
Suppress automatic Access Rules creation for VPN Policy	Supported	–
Disable IPsec Anti-Replay	Supported	Supported
Enable Windows Networking (NetBIOS) Broadcast	Supported	–
Enable Multicast	Supported	–
Display Suite B Compliant Algorithms Only	Supported	Supported
Apply NAT Policies	Supported	–
Using Primary IP Address	–	Supported
Specify the local gateway IP address	–	Supported
Preempt Secondary Gateway	Supported	Supported
Primary Gateway Detection Interval (seconds)	Supported	Supported
Do not send trigger packet during IKE SA negotiation	Supported	Supported
Accept Hash & URL Certificate Type	Supported	Supported
Send Hash & URL Certificate Type	Supported	Supported

Because an interface might have multiple IPv6 addresses, sometimes the local address of the tunnel might vary periodically. If a user needs a consistent IP address, select either the Using Primary IP Address or Specify the local gateway IP address option, or configure the VPN policy to be bound to an interface instead of a Zone. With Specify the local gateway IP address, specify the address manually. The address must be one of the IPv6 addresses for that interface.

IPV6+ADD VPN POLICY: ADVANCED



Managing GroupVPN Policies

The GroupVPN feature provides automatic VPN policy provisioning for Global VPN Clients (GVC). The GroupVPN feature on the SonicWall network security appliance and GVC streamlines VPN deployment and management. Using the Client Policy Provisioning technology, you define the VPN policies for GVC users. This policy information downloads automatically from the firewall (VPN Gateway) to GVC, saving remote users the burden of provisioning VPN connections.

GroupVPN policies facilitate the set up and deployment of multiple Global VPN Clients by the firewall administrator. **GroupVPN** is only available for GVC and you should use XAUTH/RADIUS or third-party certificates in conjunction with it for added security. For more information on how to create GroupVPN policies for any zones, navigate to **OBJECT | Match Objects > Zones | +Add Zone**.

SonicOS provides default GroupVPN policies for the WAN zone and the WLAN zone, as these are generally the less trusted zones. These default GroupVPN policies are listed in the **VPN Policies** table on the **NETWORK | IPSec VPN > Rules and Settings** page and can be customized:

- WAN GroupVPN
- WLAN GroupVPN

NOTE: GroupVPN policies are not automatically created in SonicOS with factory default settings. However, these policies remain unchanged on appliances that are upgraded from an earlier version of SonicOS. For information about Group VPN and Global VPN Client, refer to Types of Group VPN.

NOTE: Two-factor authentication (2-FA) is supported for GVC connections using Group VPN. To enable 2FA, configure the one-time password method on the user group referenced by the Group VPN policy's XAUTH settings. GVC version 5.0 or later is required for 2-FA support. For more information, refer to Two-Factor Authentication (2-FA) for Global VPN Client.

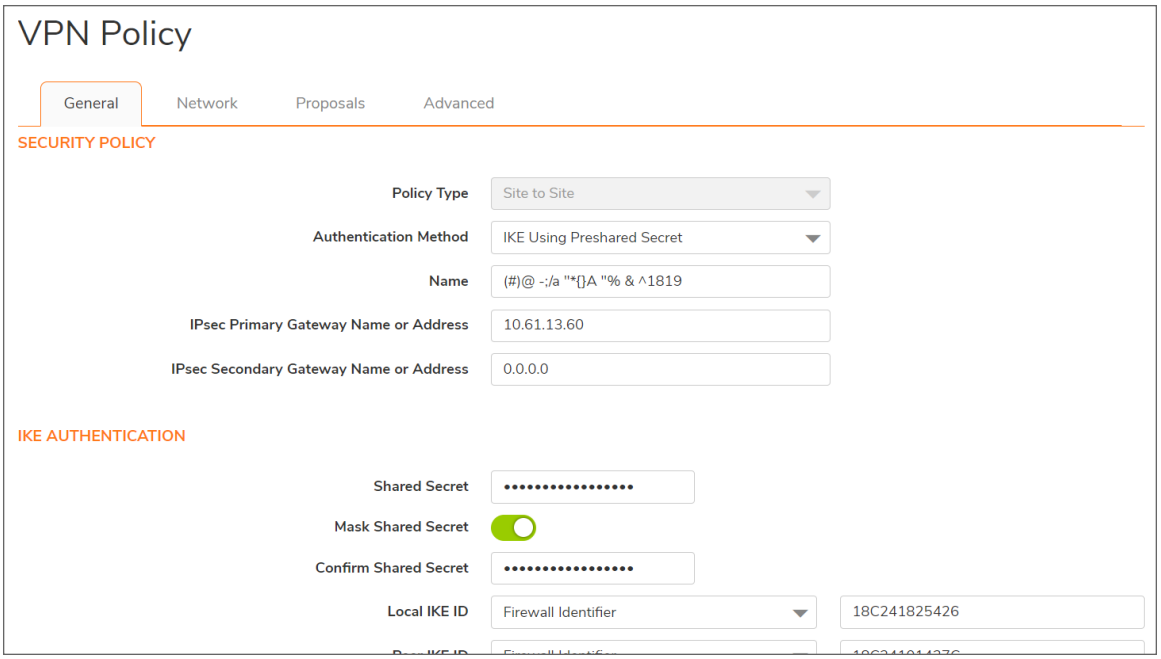
Topics:

- Configuring IKE Using a Preshared Secret Key
- Configuring IKE Using 3rd Party Certificates
- Downloading a GroupVPN Client Policy

Configuring IKE Using a Preshared Secret Key

To configure the WAN GroupVPN using a preshared secret key:

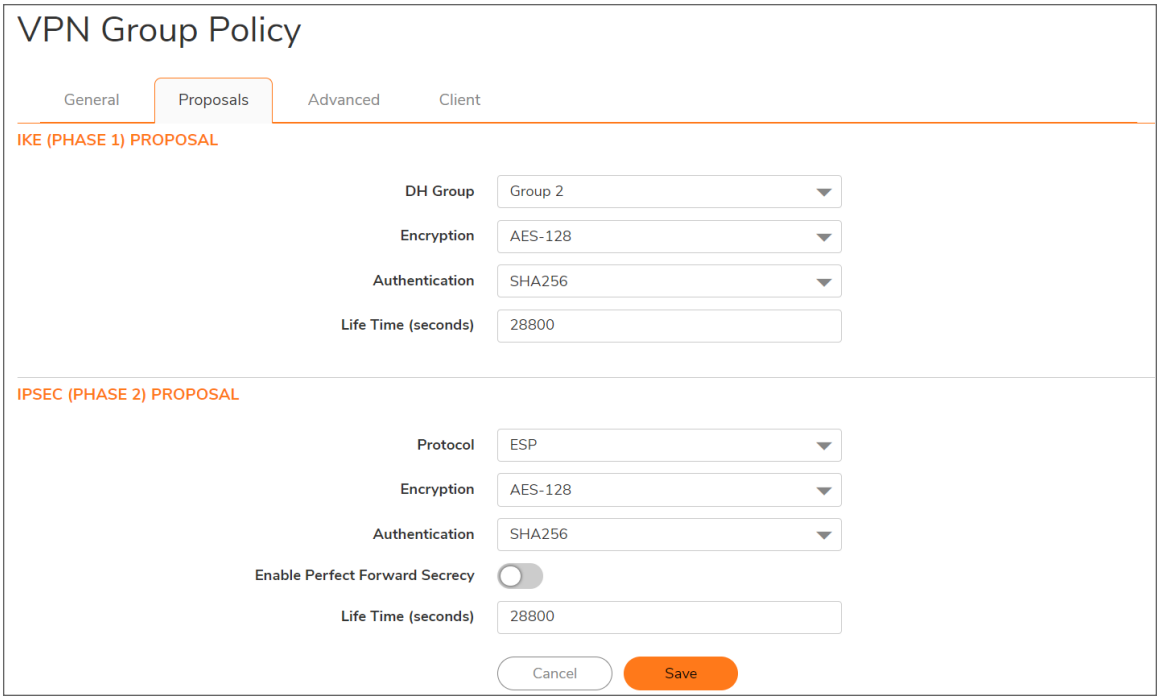
1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click the **Edit** icon for the WAN GroupVPN policy.



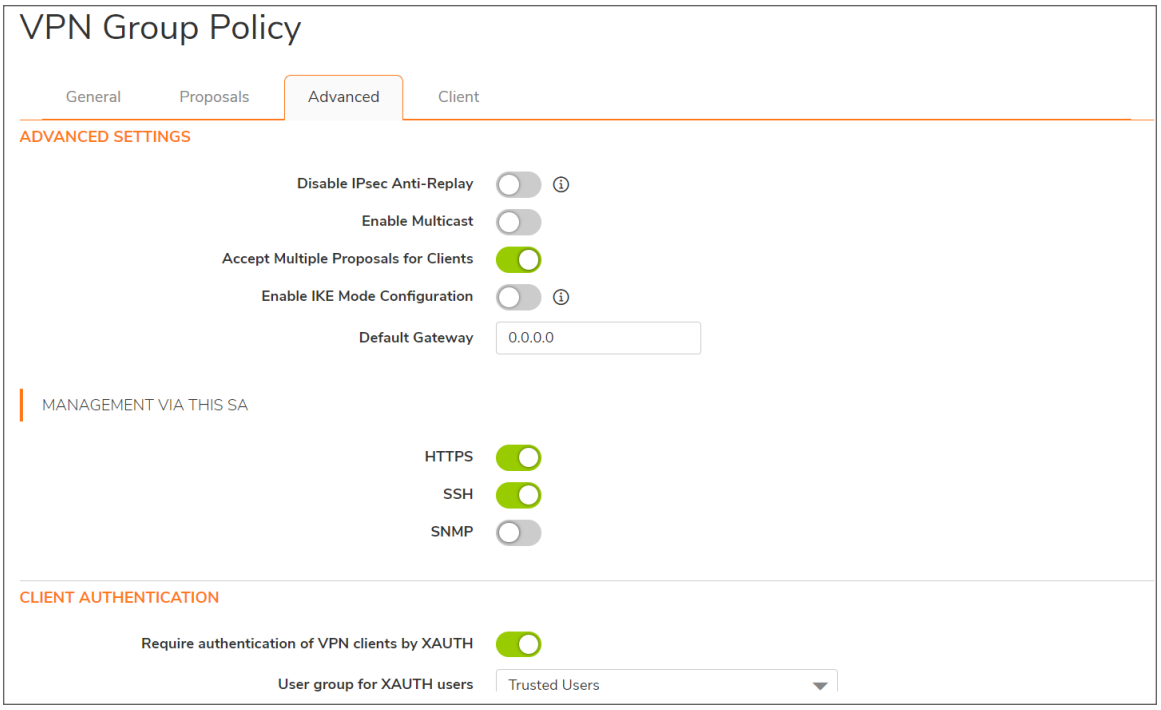
On the **General** tab, edit the **Security Policy** details. The **IKE using Preshared Secret** is the default setting for **Authentication Method**. A shared secret code is automatically generated by the firewall and written in the **Shared Secret** field. You can generate your own shared secret. A self-defined shared secret code must be a minimum of four characters.

ⓘ | **NOTE:** You cannot change the name of any GroupVPN policy.

3. Continue the configuration process.
4. In the **IKE (Phase 1) Proposal** section, select the following settings:
    - Select **Group 2** (default) from the **DH Group** drop-down menu.
    - In the **Encryption** drop-down menu, select **DES**, **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.
    - From the **Authentication** drop-down menu, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, or **SHA512**.
    - In the **Life Time (seconds)** field, enter a value. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.



5. In the **IPsec (Phase 2) Proposal** section, select the following settings:
    - From the **Protocol** drop-down menu, select **ESP** (default).
    - In the **Encryption** drop-down menu, select **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.
    - In the **Authentication** drop-down menu, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBC**, or **None**.
    - Check **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security.
    - Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
6. Click **Advanced**.

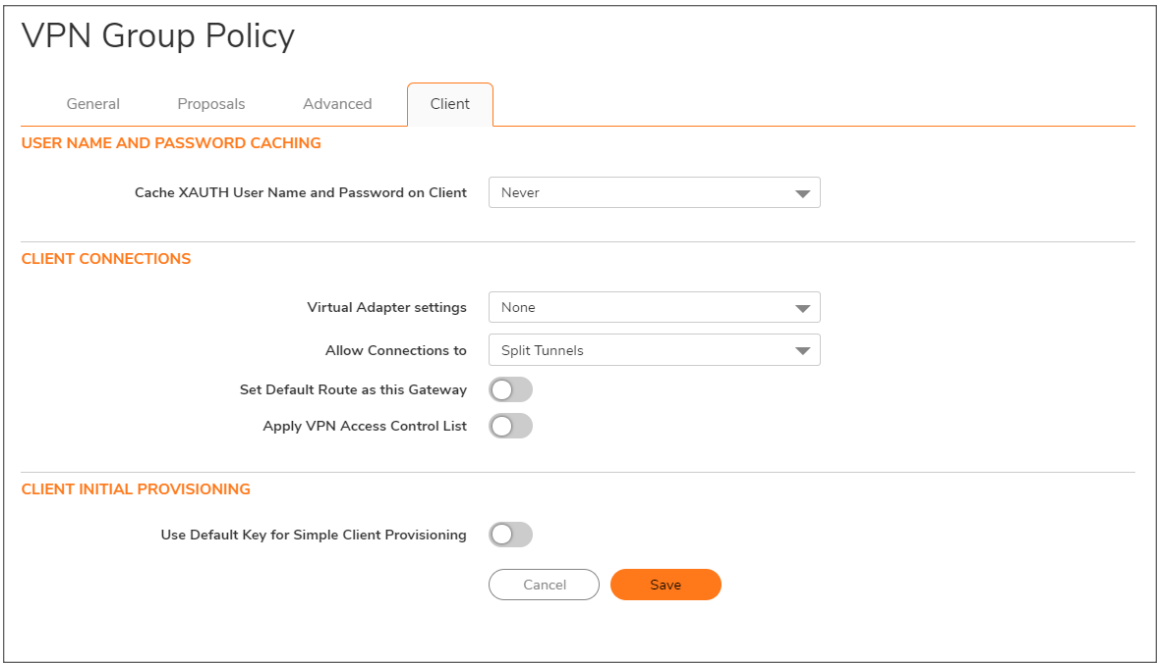


7. Select any of the following optional settings you want to apply to your GroupVPN policy:

Advanced Settings	
Disable IPsec Anti-Replay	Stops packets with duplicate sequence numbers from being dropped.
Enable Multicast	Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
Accept Multiple Proposals for Clients	Allows multiple proposals for clients, such as the IKE (Phase 1) Proposal or the IKE (Phase 2) Proposal, to be accepted.
Enable IKE Mode Configuration	Allows SonicOS to assign internal IP address, DNS Server, or WINS Server to third-party clients, like iOS devices or Avaya IP phones.
Management via this SA:	If using the VPN policy to manage the firewall, select the management method, either **HTTP**, **SSH**, or **HTTPS**. **NOTE:** SSH is valid for IPv4 only.
Default Gateway	Allows you to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the firewall and compared to static routes configured in the firewall. As packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received through an IPsec tunnel, the firewall looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
Client Authentication	

Advanced Settings	
Require Authentication of VPN Clients via XAUTH	Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone from User Group for XAUTH users** from the **User group for XAUTH** users menu. ⓘ **NOTE:** If the selected user group has a one-time password method configured (OTP via Mail or TOTP), users will get a prompt for two-factor authentication after entering their username and password.
Allow Unauthenticated VPN Client Access	Allows you to enable unauthenticated VPN client access. If you clear **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new address object or Create new address group** to create a new one.

8. Click **Client**.



9. Select any of the following settings you want to apply to your GroupVPN policy.

USER NAME AND PASSWORD CACHING

Cache XAUTH User Name and Password on Client	Allows the Global VPN Client to cache the user name and password: • If **Never** is selected, the Global VPN Client is not allowed to cache the username and password. The user is prompted for a username and password when the connection is enabled and also every time there is an IKE Phase 1 rekey. This is the default. • If **Single Session** is selected, the Global VPN Client user is prompted for username and password each time the connection is enabled and is valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey. • If **Always** is selected Global VPN Client user prompted for username and password only once when the connection is enabled. When prompted, the user is given the option of caching the username and password.

CLIENT CONNECTIONS

Virtual Adapter Settings	The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing is a requirement, obtain the MAC address of the Virtual Adapter and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of SonicWall GVC. Select one of the following: Choose **None** if a Virtual Adapter is not used by this GroupVPN connection. This is the default. Choose **DHCP Lease** if the Virtual Adapter obtains its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page. Choose DHCP Lease or Manual Configuration when the GVC connects to the firewall, the policy from the firewall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the firewall so it can proxy ARP for the manually assigned IP address. By design, the Virtual Adapter currently has no limitations on IP address assignments. Only duplicate static addresses are not permitted.

Allow Connections to	Client network traffic that matches the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select one of the following: • **This Gateway Only** allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked. • **All Secured Gateways** allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, Internet traffic is also sent through the VPN tunnel. • If this option is selected along without **Set Default Route as this Gateway**, the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled. • **Split Tunnels** allows the VPN user to have both local Internet connectivity and VPN connectivity. This is the default.
Set Default Route as this Gateway	Select this checkbox if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting. By default, this option is not enabled.
Apply VPN Access Control List	Select this checkbox to apply the VPN access control list. When this option is enabled, specified users can access only those networks configured for them. This option is not enabled by default.
CLIENT INITIAL PROVISIONING	
Use Default Key for Simple Client Provisioning	Uses Aggressive mode for the initial exchange with the gateway, and VPN clients uses a default Preshared Key for authentication. This option is not enabled by default.

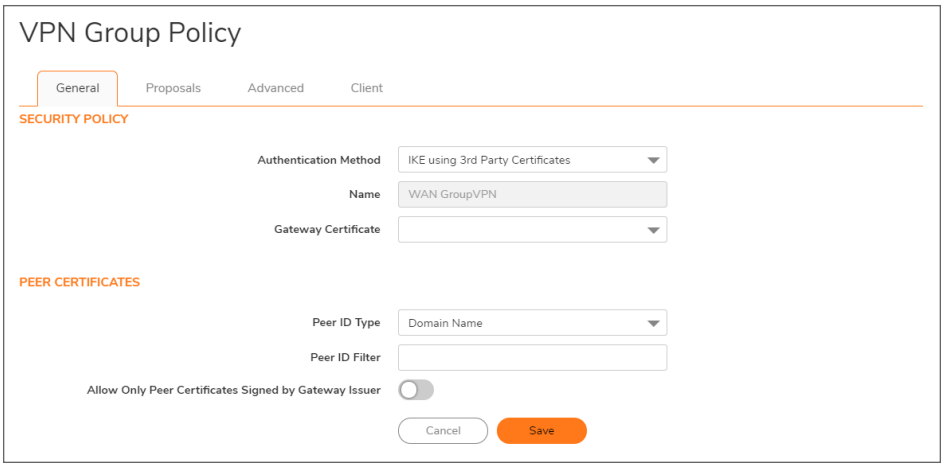
10. Click **Save**.
11. Click **ACCEPT** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

Configuring IKE Using 3rd Party Certificates

Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the firewall.

To configure GroupVPN with IKE using 3rd Party Certificates:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click the **Edit** icon for the **WAN GroupVPN** policy.



3. In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** drop-down menu.

   ⓘ | **NOTE:** The VPN policy name is GroupVPN by default and cannot be changed.

4. Select a certificate for the firewall from the **Gateway Certificate** drop-down menu.

   If you did not download your third-party certificates before starting this procedure, the **Gateway Certificates** field shows - **No verified third-party certs**.

5. In the **Peer Certificates** section, select one of the following from the **Peer ID Type** drop-down menu:

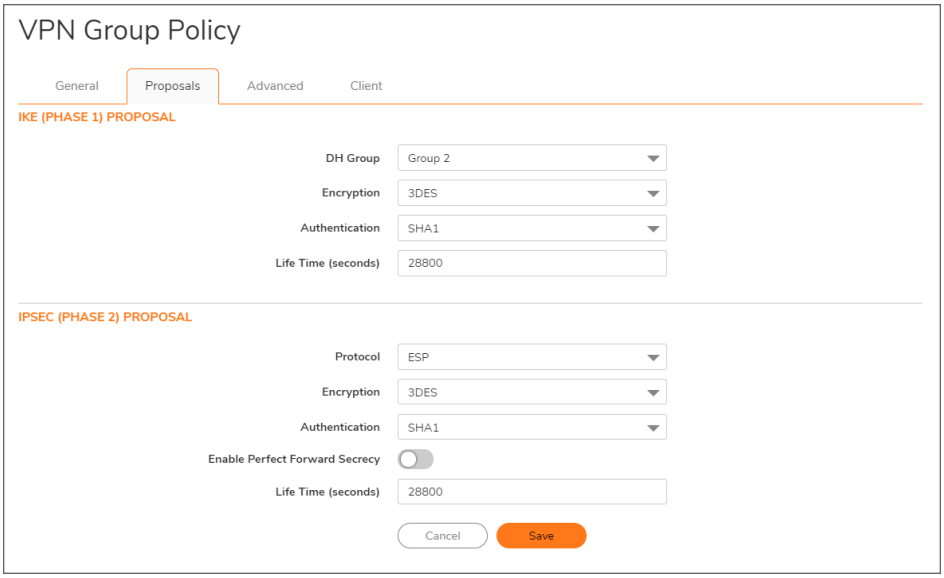
Distinguished Name	Based on the certificate's Subject Distinguished Name field, which is contained on all certificates by default and is set by the issuing Certificate Authority. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: `/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub.` Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, for example, c=us.
E-mail ID	**E-mail ID** and **Domain ID** are based on the certificate's Subject Alternative Name field, which is not contained on all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter does not work.
Domain ID	

6. Enter the Peer ID filter in the Peer ID Filter field.

   The **Email ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and ? (for a single character). For example, when **Email ID** is selected, the string

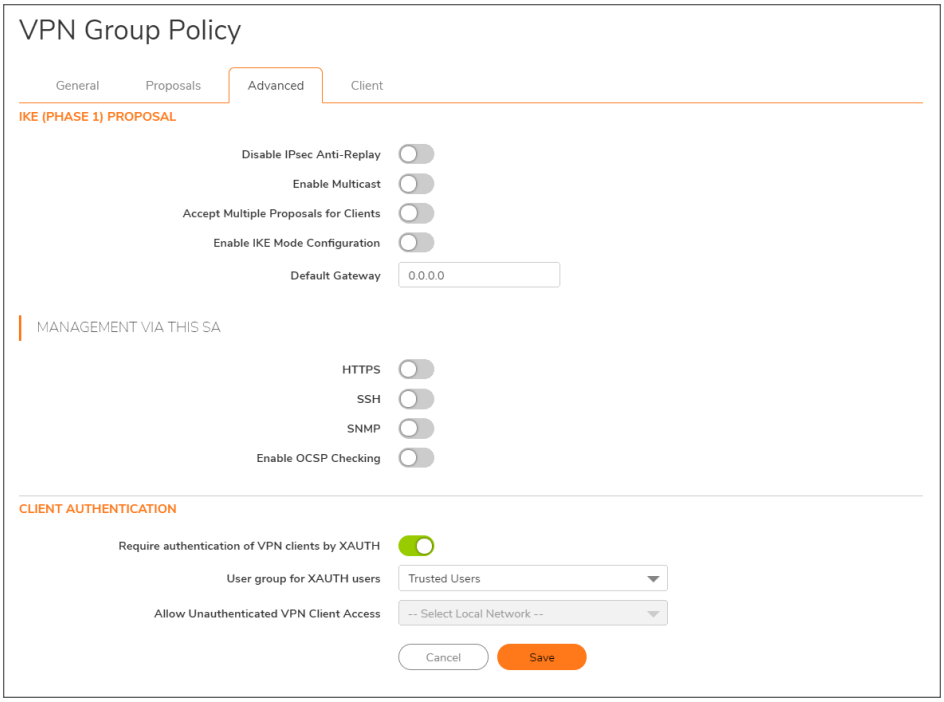
`*@SonicWall.com` allows anyone with an email address that ended in `@SonicWall.com` to have access; when **Domain Name** is selected, the string `*sv.us.SonicWall.com` allows anyone with a domain name that ended in `sv.us.SonicWall.com` to have access.

7. Select **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.
8. Click **Proposals**.



9. In the **IKE (Phase 1)** section, select the following settings:
    a. For **DH Group**, select **Group 1**, **Group 2 (default)**, **Group 5**, or **Group 14**.
    b. **For Encryption, select DES, 3DES (default), AES-128, AES-192, or AES-256.**
    c. For **Authentication**, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**,**SHA512**, **AES-XCBC**, or **None**.
    d. In the **Life Time (seconds)** field, enter a value. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.
10. In the **IPsec (Phase 2)** section, select the following settings:
    a. For **Protocol**, select **ESP** (default).
    b. For **Encryption**, select **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.
    c. For **Authentication**, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**,**SHA512**, **AES-XCBC**, or **None**
    d. Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security.
    e. Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

11. Click **Advanced**.

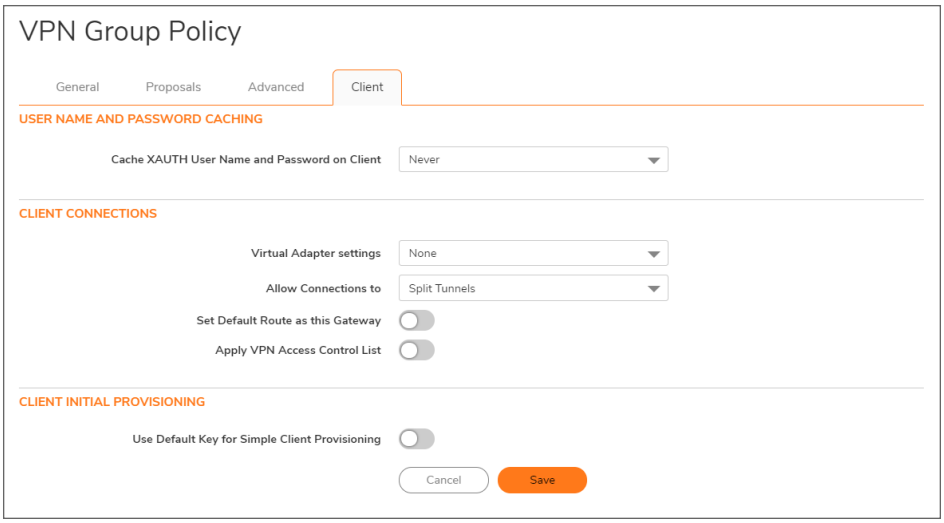


12. Select any of the following optional settings that you want to apply to your GroupVPN Policy:

Disable IPsec Anti-Replay	Anti-Replay is a form of partial sequence integrity and it detects arrival of duplicated I datagrams (within a constrained window).
Enable Multicast	Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
Accept Multiple Proposal fro Clients	Allows multiple proposals for clients, such as the IKE (Phase 1) Proposal or the IKE (Phase 2) Proposal, to be accepted.
Enable IKE Mode Configuration	Allows SonicOS to assign internal IP address, DNS Server or WINS Server to Third-Party Clients like iOS devices or Avaya IP Phones.
Management via this SA	If using the VPN policy to manage the firewall, select one or more management methods, **HTTP**, **SSH**, or **HTTPS**. ⓘ | **NOTE:** SSH is valid for IPv4 only.

Default Gateway	Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** checkbox. Default LAN Gateway allows you to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the firewall and compared to static routes configured in the firewall. Because packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received through an IPsec tunnel, the firewall looks up a route for the LAN. If no route is found, the firewall checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
Enable OCSP Checking and OCSP Responder URL	Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status.
Require Authentication of VPN Clients via XAUTH	Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
User group for XAUTH users	Allows you to select a defined user group for authentication.
Allow Unauthenticated VPN Client Access	Allows you to specify network segments for unauthenticated Global VPN Client access.

13. Click **Client**.



14. Select any of the following boxes that you want to apply to Global VPN Client provisioning:

Cache XAUTH User Name and Password	Allows the Global VPN Client to cache the user name and password: • Choose **Never** to prohibit the Global VPN Client from caching the username and password. The user is prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey. • Choose **Single Session** to prompt the user for username and password each time the connection is enabled, which is valid until the connection is disabled. This username and password is used through IKE phase 1 rekey. • Choose **Always** to prompt the user for username and password only once when the connection is enabled. When prompted, the user is given the option of caching the username and password.
Virtual Adapter Settings	The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing is a requirement, obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of **SonicWall** GVC. • Choose **None** to not use the Virtual Adapter by this GroupVPN connection. • Choose **DHCP Lease** to have the Virtual Adapter obtain its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page. • Choose **DHCP Lease or Manual Configuration** and when the GVC connects to the firewall, the policy from the firewall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the firewall so that it can proxy ARP for the manually assigned IP address. By design, IP address assignments currently has no limitations on for the Virtual Adapter. Only duplicate static addresses are not permitted.

Allow Connections to	Client network traffic that matches the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select one of the following options: • **This Gateway Only** allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked. • **All Secured Gateways** allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, Internet traffic is also sent through the VPN tunnel. If this option is selected along without **Set Default Route as this Gateway**, the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled. ⓘ **NOTE:** Only one of the multiple gateways can have Set Default Route as this Gateway enabled. • **Split Tunnels** allows the VPN user to have both local Internet connectivity and VPN connectivity. This is the default.
Set Default Route as this Gateway	Enable this checkbox if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
Apply VPN Access Control List	Enable this option to control client connections with an access control list.
Use Default Key for Simple Client Provisioning	Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

15. Click **Ok**.
16. Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

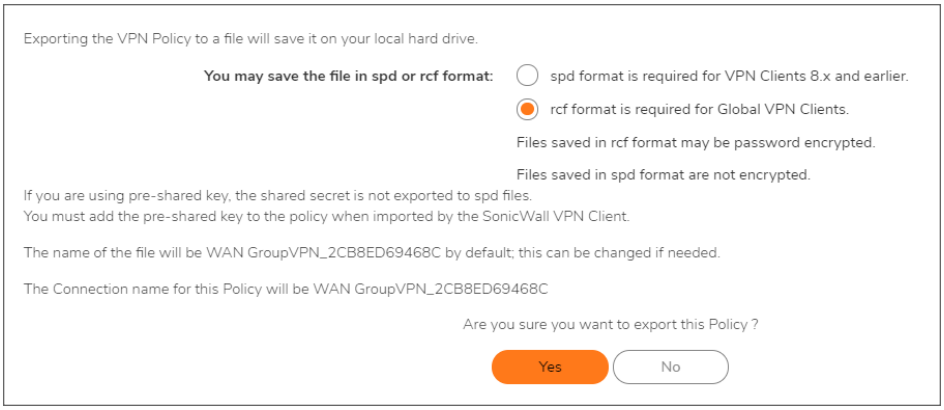
Downloading a GroupVPN Client Policy

You can provide a file to your end users that contains configuration settings for their Global VPN clients. Simply download the GroupVPN client policy from the firewall.

ⓘ **IMPORTANT:** The GroupVPN SA (Secure Association) must be enabled on the firewall to download a configuration file.

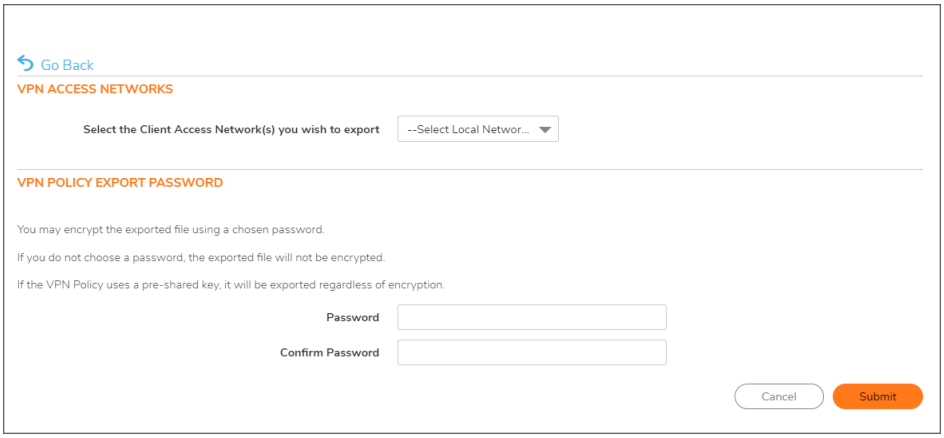
To download the Global VPN Client configuration settings:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Be sure the policy you want to export is enabled.
3. Click the **Download** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table.



rcf format is required for SonicWall Global VPN Clients is the default. Files saved in the rcf format can be password encrypted. The firewall provides a default file name for the configuration file, which you can change.

4. Click **Yes**.



5. In the drop-down menu for **Select the client Access Network(s) you wish to export**, select **VPN Access Network**.
6. Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.
7. Click **Submit**. If you did not enter a password, a message appears confirming your choice.
8. Click **Ok**. You can change the configuration file before saving.
9. Save the file.
10. Click **Close**.

The file can be saved or sent electronically to remote users to configure their Global VPN Clients.

Two-Factor Authentication (2-FA) for Global VPN Client

SonicOS supports two-factor authentication (2-FA) for IPSec Group VPN connections using the SonicWall Global VPN Client (GVC). This feature adds a second layer of authentication—either a Time-Based One-Time Password (TOTP) or a One-Time Password (OTP) delivered via email—to the standard username and password credentials, mitigating the risk of unauthorized access through compromised credentials.

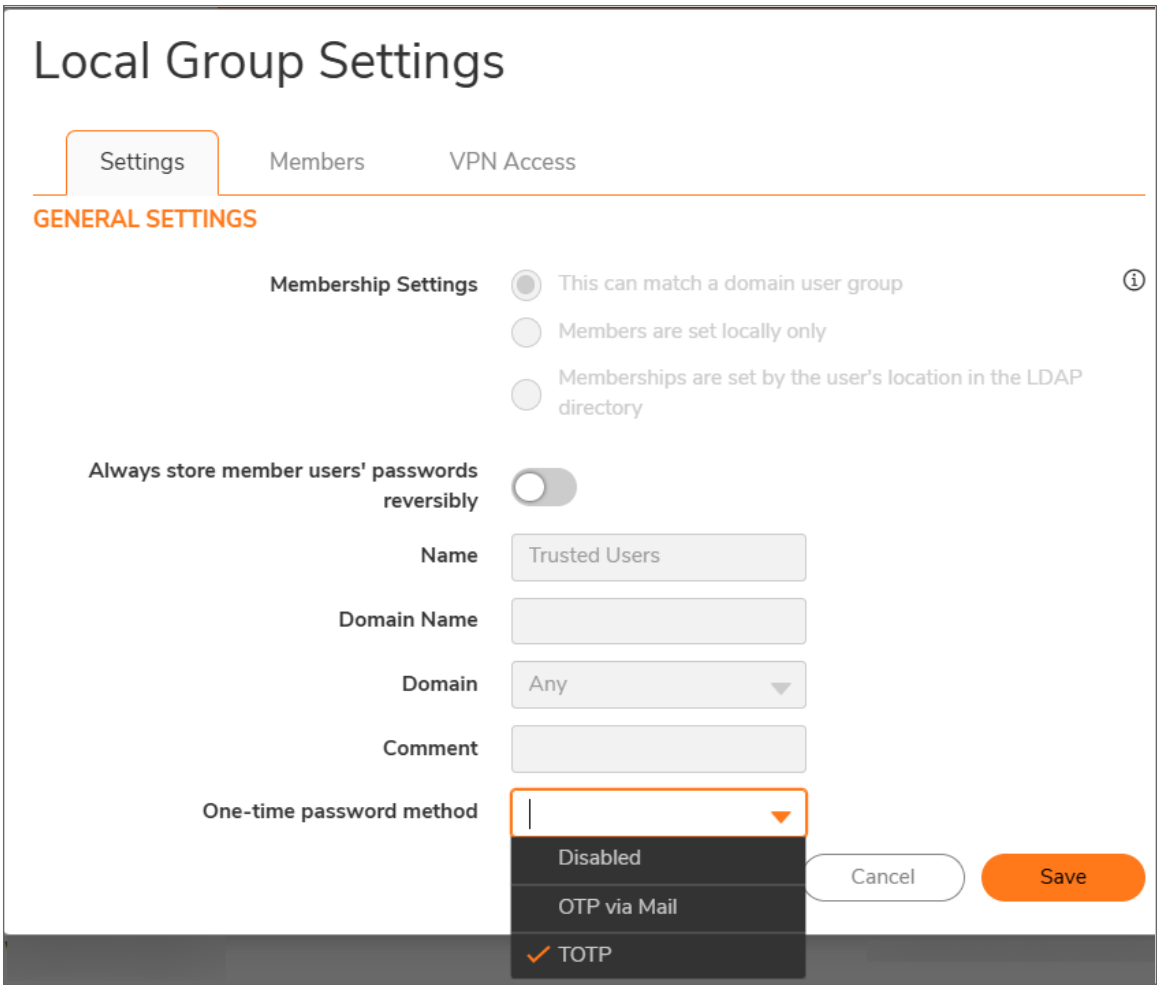
ⓘ | **NOTE:** The minimum required GVC version is 5.0 or later.

The 2-FA for GVC is configured by enabling the one-time password method on the user group referenced by the Group VPN policy.

ⓘ | **NOTE:** Two-factor authentication for GVC uses the same configuration workflows and settings used for SSL VPN two-factor authentication.The 2FA token is bound to the user account. If a user is configured for both SSL VPN and GVC access, the same **TOTP** enrollment or **OTP** method applies to both connection types.

To configure 2FA for GV:

1. Navigate to **DEVICE | Users > Local Users & Groups**.
2. Click **Local Groups** and select the user group referenced by the Group VPN policy (for example, Trusted Users).
3. Click **Edit**.
4. On the **Local Group Settings**, under **One-time password method** drop-down, select one of the following:
    a. **OTP via Mail** — Sends a one-time code to the user's configured email address at each login.
    b. **TOTP** — Requires users to enroll a TOTP authenticator app and provide a time-based code at each login.



5. Click **Save**.

Creating Site to Site VPN Policies

A site to site VPN allows offices in multiple locations to establish secure connections with each other over a public network. It extends the company's network, making computer resources from one location available to employees at other locations.

You can create or modify existing site to site VPN policies. To add a policy, click **+Add** in the **VPN Policies** table; to modify an existing policy click the **Edit** icon for that policy. The following options can be set up when configuring a site to site VPN:

- Configuring with a Preshared Secret Key
- Configuring with a Manual Key
- Configuring with a Third-Party Certificate

- **SonicWall Auto Provisioning Client** or **SonicWall Auto Provisioning Server**. For information about these options, see *VPN Auto Provisioning*.

This section also contains information on how to configure the remote SonicWall firewall and how to configure a static route to act as a failover in case the VPN tunnel failure.

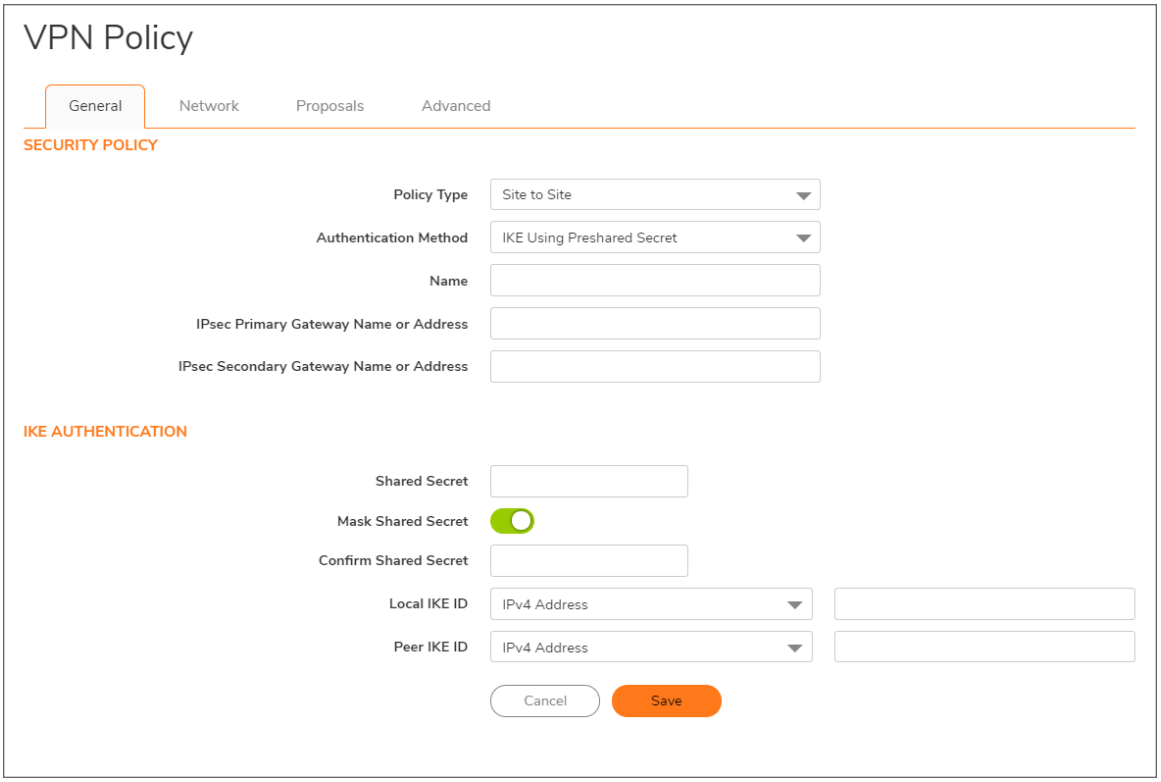
- Configuring the Remote Network Security Appliance
- Configuring VPN Failover to a Static Route

NOTE: Informational videos with site to site VPN configuration examples are available online. For example, see How to Create a Site to Site VPN in Main Mode using Preshared Secret or How to Create Aggressive Mode Site to Site VPN using Preshared Secret.
Additional videos are available at: Video Tutorials.

Configuring with a Preshared Secret Key

To configure a VPN Policy using Internet Key Exchange (IKE) with a preshared secret key:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click **+Add** to create a new policy or click the **Edit** icon if you are updating an existing policy.



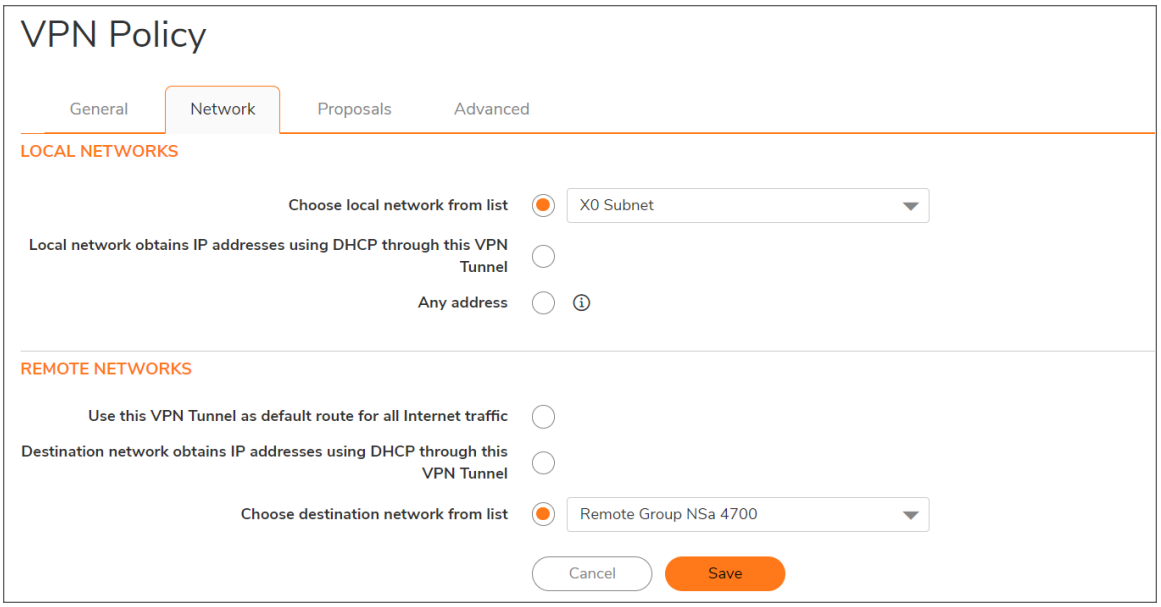
3. From **Policy Type** on the **General** screen, select **Site to Site**.
4. From **Authentication Method**, select **IKE using Preshared Secret**.

5. Enter a name for the policy in the **Name** field.
6. Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.
7. If the Remote VPN device supports more than one endpoint, enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field (optional).
8. In the **IKE Authentication** section, in the **Shared Secret** and **Confirm Shared Secret** fields, enter a Shared Secret password. This is used to set up the SA (Security Association). The Shared Secret password must be at least four characters long, and should include both numbers and letters.
9. To see the shared secret key in both fields, clear the check box for **Mask Shared Secret**. By default, **Mask Shared Secret** is selected, which causes the shared secret key to be displayed as black circles.
10. Optionally, specify a **Local IKE ID** and **Peer IKE ID** for this Policy.

    You can select from the following IDs from the drop-down menu:

    - **IPv4 Address**
    - **Domain Name**
    - **E-mail Address**
    - **Firewall Identifier**
    - **Key Identifier**

    By default, the **IP Address** (`ID_IPv4_ADDR`) is used for Main Mode negotiations, and the firewall Identifier (`ID_USER_FQDN`) is used for Aggressive Mode.
11. Enter the address, name, or ID in the **Local IKE ID** and **Peer IKE ID** fields.
12. Click **Network**.



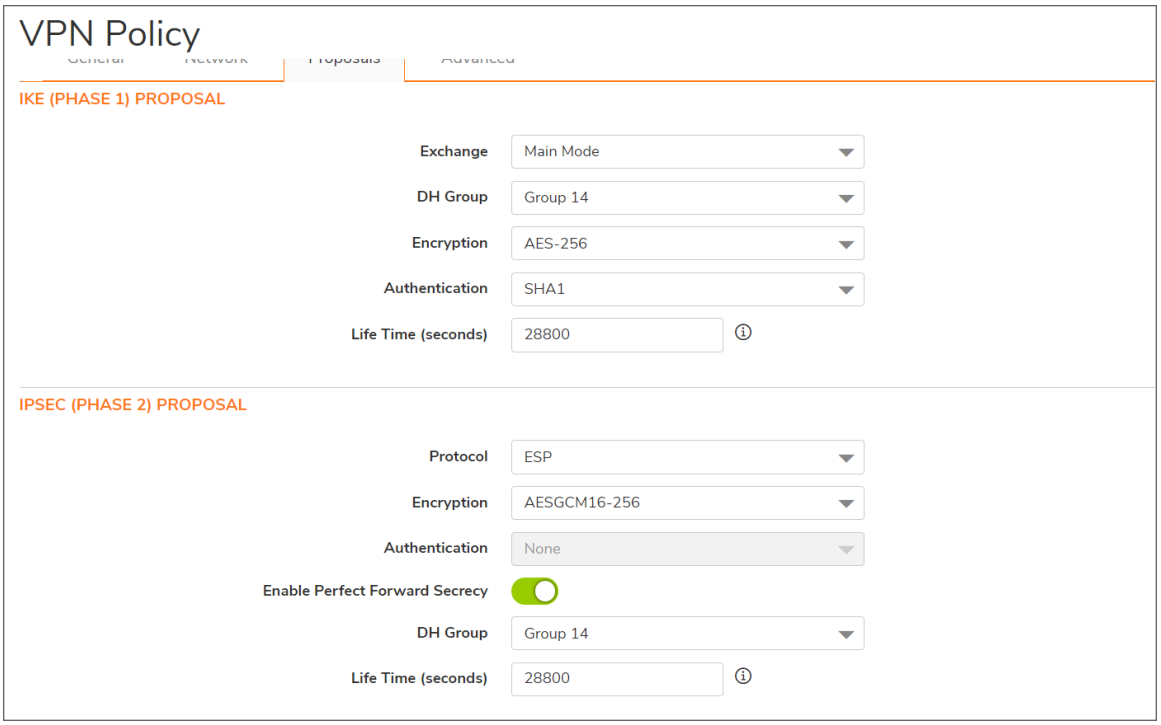
13. Under **Local Networks**, select one of the following:

Choose local network from list	Select a local network from the drop-down menu if a specific network can access the VPN tunnel.
Local Network obtain IP addresses using DHCP through this VPN Tunnel	Select this option for local networks to obtain IP addresses using DHCP through this VPN tunnel.
Any address	Use this option if traffic can originate from any local network or if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone. ⓘ | **NOTE:** DHCP over VPN is not supported with IKEv2.

14. Under **Remote Networks**, select one of the following:

Use this VPN Tunnel as default route for all Internet traffic	Select this option if traffic from any local user cannot leave the firewall unless it is encrypted. ⓘ | **NOTE:** You can only configure one SA to use this setting.
Destination network obtains IP addresses using DHCP through this VPN Tunnel	Select this option if the remote network requests IP addresses from a DHCP Server in the local network. ⓘ | **NOTE:** This option is only available if **Main Mode** or **Aggressive Mode** is selected on the **Proposals** tab.
Choose Destination network from list	Select a remote network from the drop-down menu.

15. Click **Proposals**.



16. Under **IKE (Phase 1) Proposal**, choose one of the following options from the **Exchange** drop-down menu:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phase 1. ⓘ **NOTE:** If you select **IKE v2 Mode**, both ends of the VPN tunnel must use IKE v2. When selected, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and cannot be defined.

17. Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

ⓘ **NOTE:** If **IKEv2 Mode** is selected for the **Exchange** field, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and no selection can be made for those options.

ⓘ **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

a. For the **DH Group**, when in **Main Mode** or **Aggressive Mode**, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1
384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

b. For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **3DES**, **DES**, **AES-128** (default), **AES-192**, or **AES-256** from the drop-down menu.

c. For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **SHA-1** (default), **MD5**, **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.

d. For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

1. Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

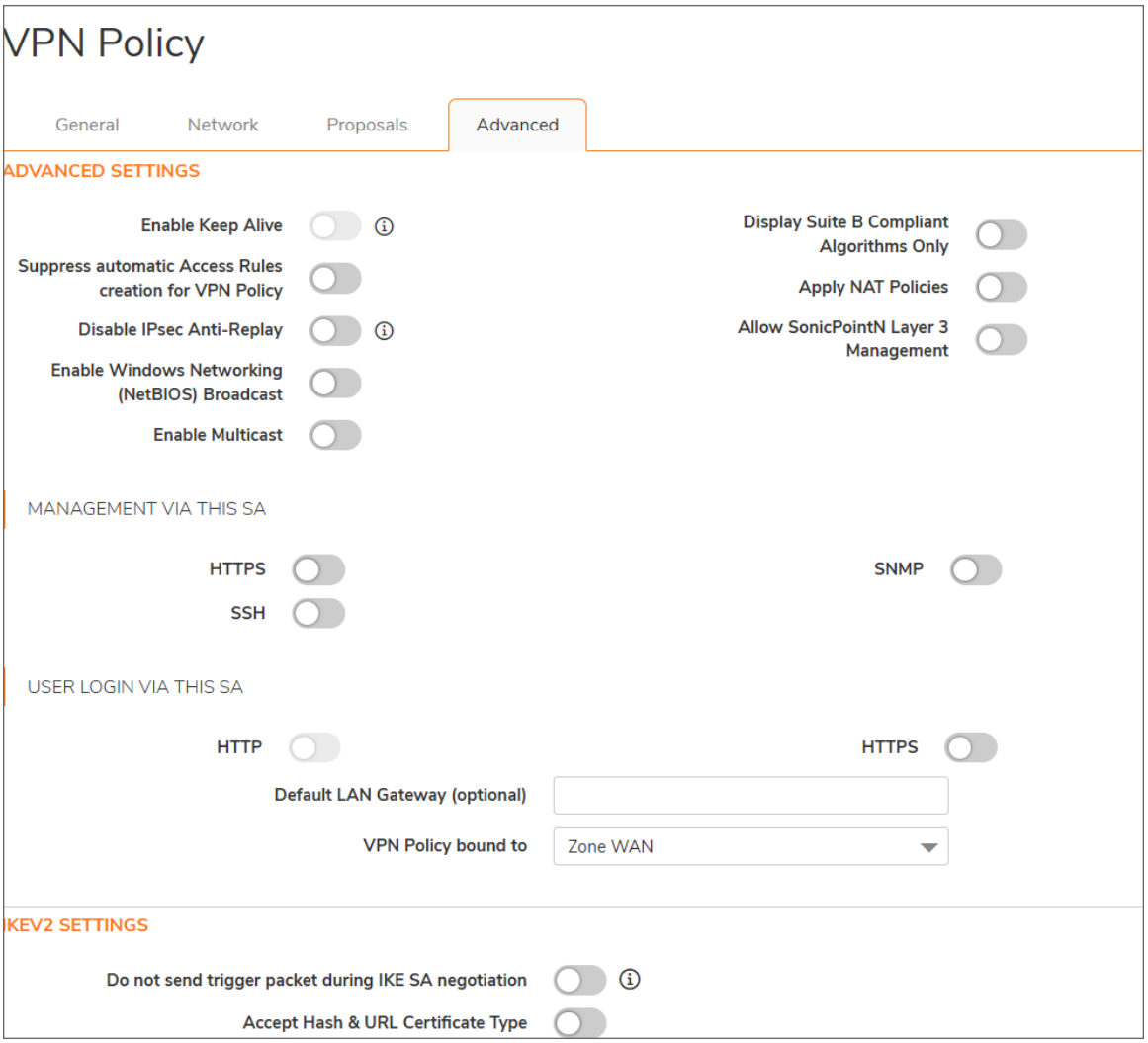
   ⓘ | **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

   - If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	DES
AESGCM16-192	3DES
AESGCM16-256	AES-128
AESGMAC-128	AES-192
AESGMAC-192	AES-256
AESGMAC-256	None

   - If you selected **AH** in the **Protocol** field, the **Encryption** field is dimmed and you cannot select any options.

18. Click **Advanced**.



19. Select any of the optional settings you want to apply to your VPN policy. The options change depending on options you selected in the **Proposals** screen.

Options	Main Mode or Aggressive Mode (See figure Advanced Settings for Main and Aggressive Modes below)	IKEv2 Mode (See figure Advanced Settings for IKEv2 Mode below)
Advanced Settings		
Enable Keep Alive	Select to use heartbeat messages between peers on this VPN tunnel if one end of the tunnel fails, using a keep-alive heartbeat allows automatic renegotiation of the tunnel after both sides are available again without having to wait for the proposed Life Time to expire. ⓘ **NOTE:** The Keep Alive option is disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address 0.0.0.0.	Cannot be selected for IKEv2 mode.
Suppress automatic Access Rules creation for VPN Policy	When not selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control for more information.	When not selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control for more information.
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).
Require authentication of VPN clients by XAUTH	Requires that all inbound traffic on this VPN policy is from a user authenticated by XAUTH/RADIUS. Unauthenticated traffic is not allowed on the VPN tunnel.	Not available in IKEv2 Mode.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.

Options	Main Mode or Aggressive Mode (See figure Advanced Settings for Main and Aggressive Modes below)	IKEv2 Mode (See figure Advanced Settings for IKEv2 Mode below)
Advanced Settings		
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
WXA Group	Select **None** (default) or **Group One**.	Select **None** (default) or **Group One**.
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
Management via this SA	Select any of HTTPS, SSH, or SNMP for this option to manage the local SonicWall firewall through the VPN tunnel.	Select any of HTTPS, SSH, or SNMP for this option to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select HTTP, HTTPS, or both to allow users to login using the SA. HTTP user login is not allowed with remote authentication.	Select HTTP, HTTPS, or both to allow users to login using the SA. HTTP user login is not allowed with remote authentication.

Options	Main Mode or Aggressive Mode (See figure Advanced Settings for Main and Aggressive Modes below)	IKEv2 Mode (See figure Advanced Settings for IKEv2 Mode below)
Advanced Settings		
Default LAN Gateway (optional)	f you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected Use this VPN Tunnel as a default route for all Internet traffic (on the Network screen, under Remote Networks) enter the router address.	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected Use this VPN Tunnel as a default route for all Internet traffic (on the Network screen, under Remote Networks) enter the router address
VPN Policy bound to	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. Important: Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. Important: Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.
Preempt Secondary Gateway	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the Primary Gateway Detection Interval (seconds) option. The default time is 28800 seconds, or 8 hours.	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the Primary Gateway Detection Interval (seconds) option. The default time is 28800 seconds, or 8 hours.
IKEv2 Settings		
Do not send trigger packet during IKE SA negotiation	Not available in Main or Aggressive modes.	Is not selected (default). Should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.

Options	Main Mode or Aggressive Mode (See figure Advanced Settings for Main and Aggressive Modes below)	IKEv2 Mode (See figure Advanced Settings for IKEv2 Mode below)
Advanced Settings		
Accept Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

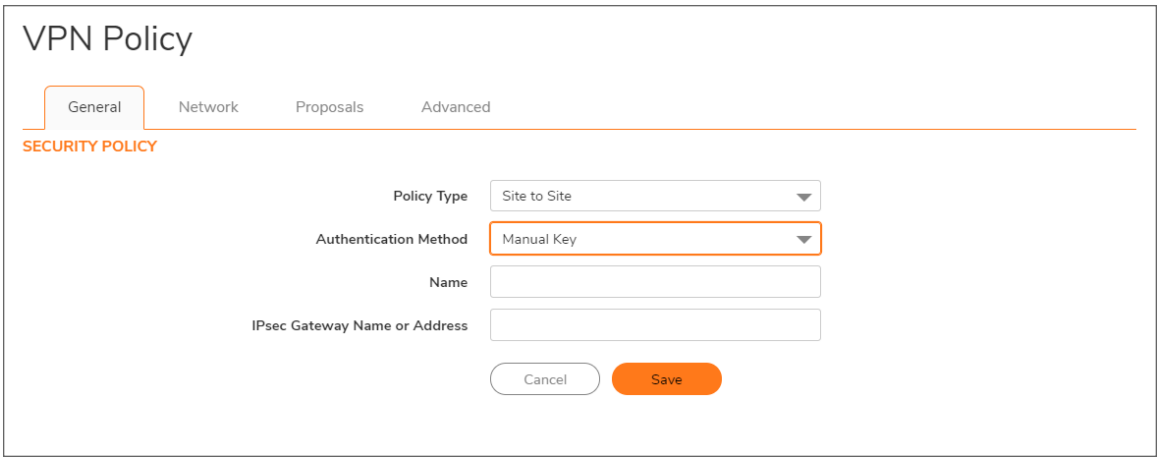
20. Click **OK**.
21. Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

Configuring with a Manual Key

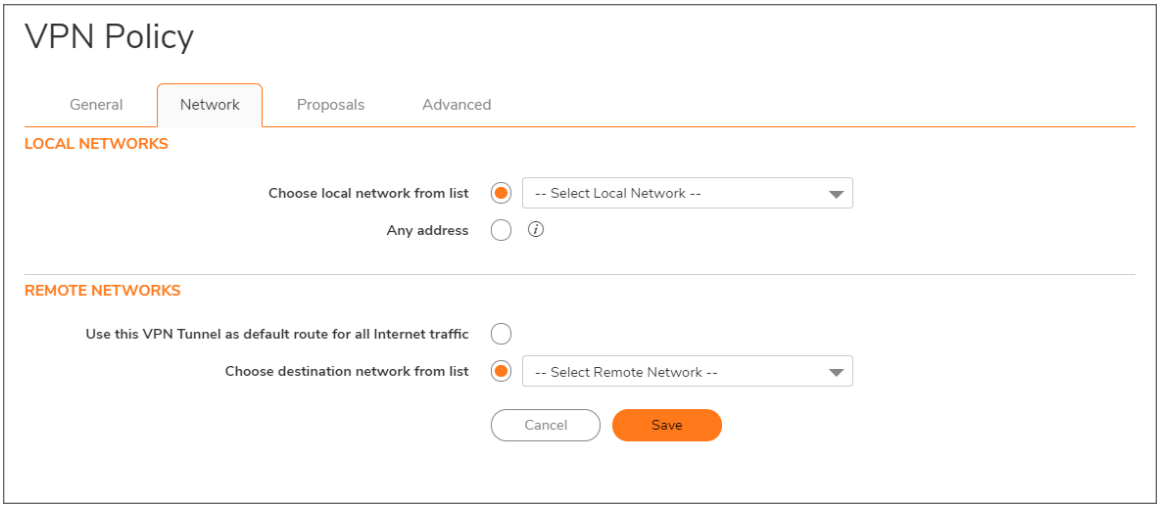
You can manually define encryption keys for establishing an IPsec VPN tunnel. You define manual keys when you need to specify what the encryption or authentication key is (for example, when one of the VPN peers requires a specific key) or when you need to disable encryption and authentication.

To configure a VPN policy using Manual Key:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click **+Add** to create a new policy or click the Edit icon if you are updating an existing policy.
3. In the **Authentication Method** field, select **Manual Key** from drop-down menu. The window shows only the Manual Key options.



4. Enter a name for the policy in the **Name** field.
5. Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.
6. Click **Network**.

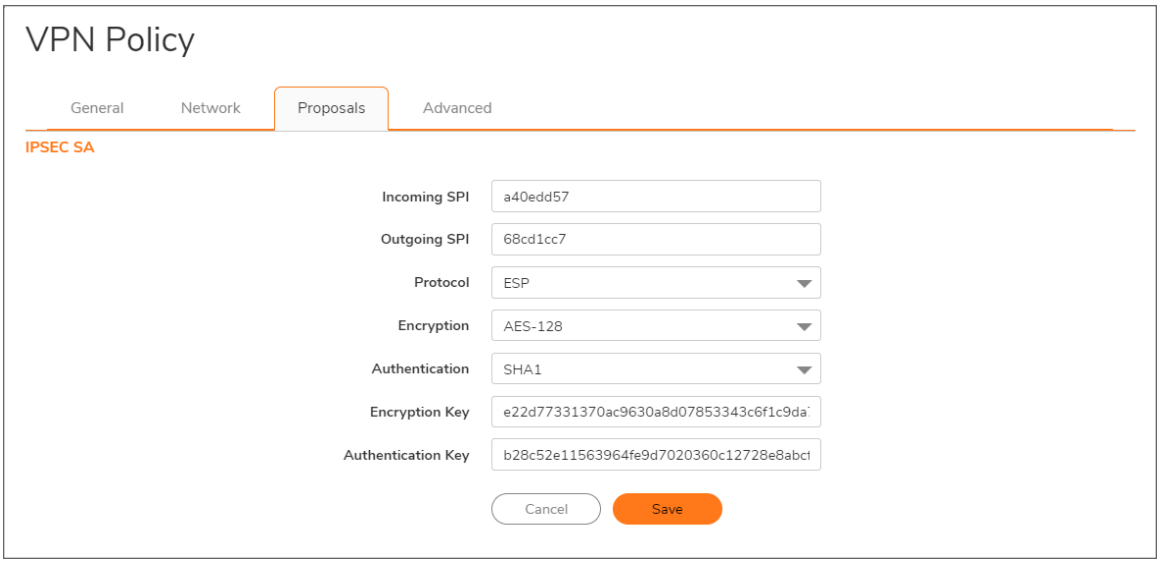


7. Under **Local Networks**, select one of these options:
   - If a specific local network can access the VPN tunnel, select a that local network from the Choose local network from list drop-down menu.
   - If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone.
8. Under **Destination Networks**, select one of these:
   - If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

     ⓘ | **NOTE:** You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list**, and select the address object or group.

9. Click **Proposals**.



10. Define an **Incoming SPI** and an **Outgoing SPI**. A Security Parameter Index (SPI) is hexadecimal and can range from 3 to 8 characters in length.

    ⓘ **IMPORTANT:** Each Security Association (SA) must have unique SPIs; no two SAs can share the same SPIs. However, each SA Incoming SPI can be the same as the Outgoing SPI.

11. The default values for **Protocol**, **Encryption**, and **Authentication** are acceptable for most VPN SA configurations; otherwise, select values from the drop-down menu.

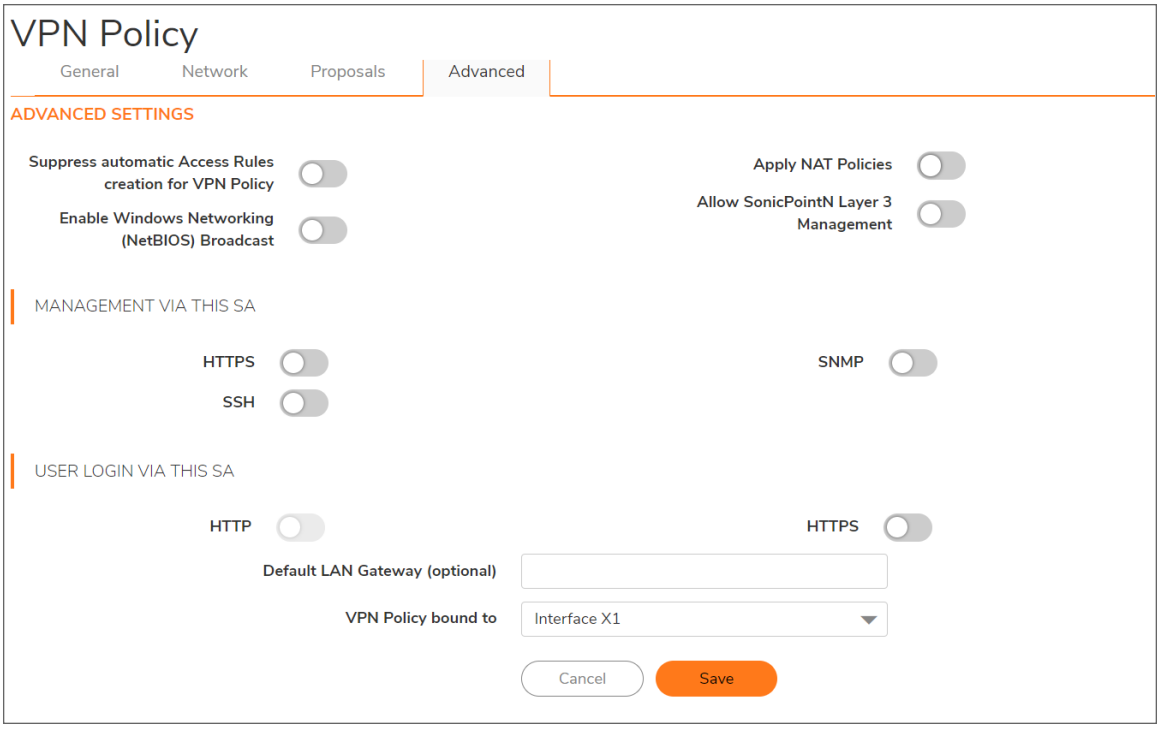
    ⓘ **NOTE:** The values for **Protocol**, **Encryption**, and **Authentication** must match the values on the remote firewall.

    - If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:
        - **DES**
        - **3DES**
        - **AES-128** (default)
        - **AES-192**
        - **AES-256**
        - **None**
    - If you selected **AH** in the **Protocol** field, the **Encryption** field is grayed out, and you cannot select any options.

12. In the **Encryption Key** field, enter a 48-character hexadecimal encryption key or use the default value. This encryption key is used to configure the remote SonicWall encryption key, so write it down to use when configuring the remote firewall.

TIP: Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption or authentication key, an error message is displayed at the bottom of the browser window.

13. In the **Authentication Key** field, enter a 40-character hexadecimal authentication key or use the default value. Write down the key to use while configuring the firewall settings.
14. Click **Advanced**.



15. Select any of the following optional settings you want to apply to your VPN policy.

Option	Definition
Suppress automatic Access Rules creation for VPN Policy	When not selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control for more information.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.

Option	Definition
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both side of a tunnel use either the same or overlapping subnets. ⓘ **TIP:** Informational videos with interface configuration examples are available online. For example, see *How to Configure NAT over VPN in a Site to Site VPN with Overlapping Networks*. Additional videos are available at: https://www.sonicwall.com/support/video-tutorials.
Management via this SA	Select **HTTPS**, **SSH**, **SNMP** or any combination of these three to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to log in using the SA. ⓘ **NOTE:** HTTP user login is not allowed with remote authentication.
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the **Network** screen under **Remote Networks**) enter the router address.
VPN Policy bound to	Select an interface or zone from the drop-down menu. ⓘ **IMPORTANT:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.

16. Click **OK**.
17. Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

Configuring with a Third-Party Certificate

ⓘ **NOTE:** You must have a valid certificate from a third-party certificate authority installed on your SonicWall firewall before you can configure your VPN policy using a third-party IKE certificate.

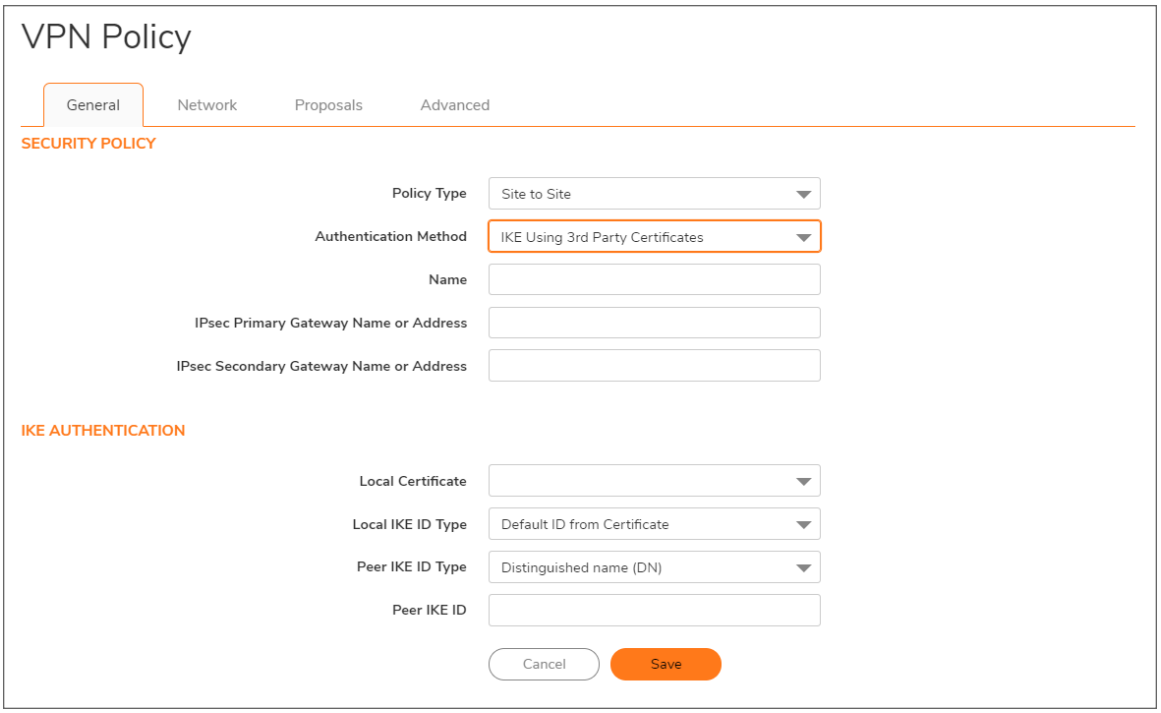
With SonicWall firewalls, you can opt to use third-party certificates for authentication instead of the SonicWall Authentication Service. Using certificates from a third-party provider or using local certificates is a more manual process; therefore, experience with implementing Public Key Infrastructure (PKI) is necessary to understand the key components of digital certificates.

SonicWall supports the following two certificate providers:

- VeriSign
- Entrust

To create a VPN SA using IKE and third-party certificates:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click **+Add** to create a new policy or click the **Edit** icon if you are updating an existing policy.
3. In the **Authentication Method** field, select **IKE using 3rd Party Certificates**. The **VPN Policy** window displays the third-party certificate options in the **IKE Authentication** section.



4. Type a name for the Security Association in the **Name** field.
5. Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWall in the **IPsec Primary Gateway Name or Address** field.
6. If you have a secondary remote SonicWall, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.
7. Under **IKE Authentication**, select a third-party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.
8. For **Local IKE ID Type**, the default is **Default ID from Certificate**. Or, choose one of the following:
    - Distinguished Name (DN)
    - Email ID (UserFQDN)
    - Domain Name (FQDN)
    - IP Address (IPV4)

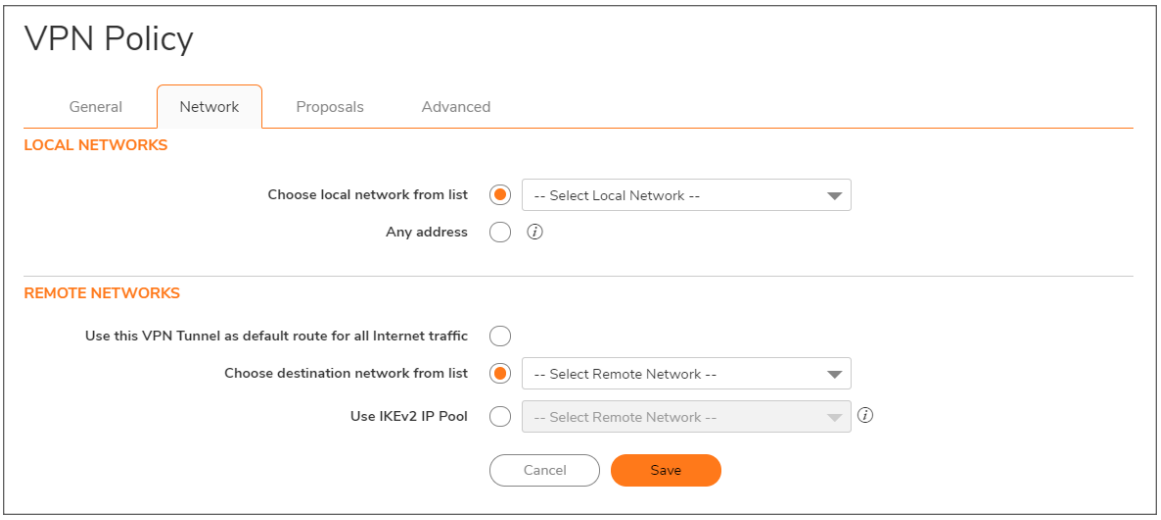
    These alternate selections are the same as those for **Peer IKE ID Type**, described in the next step.

9. From the **Peer IKE ID Type** drop-down menu, select one of the following Peer ID types:

Peer IKE ID Type Option	Definition
Default ID from Certificate	Authentication is taken from the default ID on the certificate.
Distinguished Name (DN)	Authentication is based on the certificate's Subject Distinguished Name field, which is contained in all certificates by default. The entire Distinguished Name field must be entered for site to site VPNs. Wild card characters are not supported. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub**.
Email ID (UserFQDN)	Authentication based on the **Email ID (UserFQDN)** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site to site VPNs, wild card characters cannot be used. The full value of the Email ID must be entered. This is because site to site VPNs are expected to connect to a single peer, whereas Group VPNs expect to connect to multiple peers.
Domain Name (FQDN)	Authentication based on the **Domain Name (FQDN)** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site to site VPNs, wild card characters cannot be used. The full value of the Domain Name must be entered because site to site VPNs are expected to connect to a single peer, whereas Group VPNs expect to connect to multiple peers.
IP Address (IPV4)	Based on the IPv4 IP address.

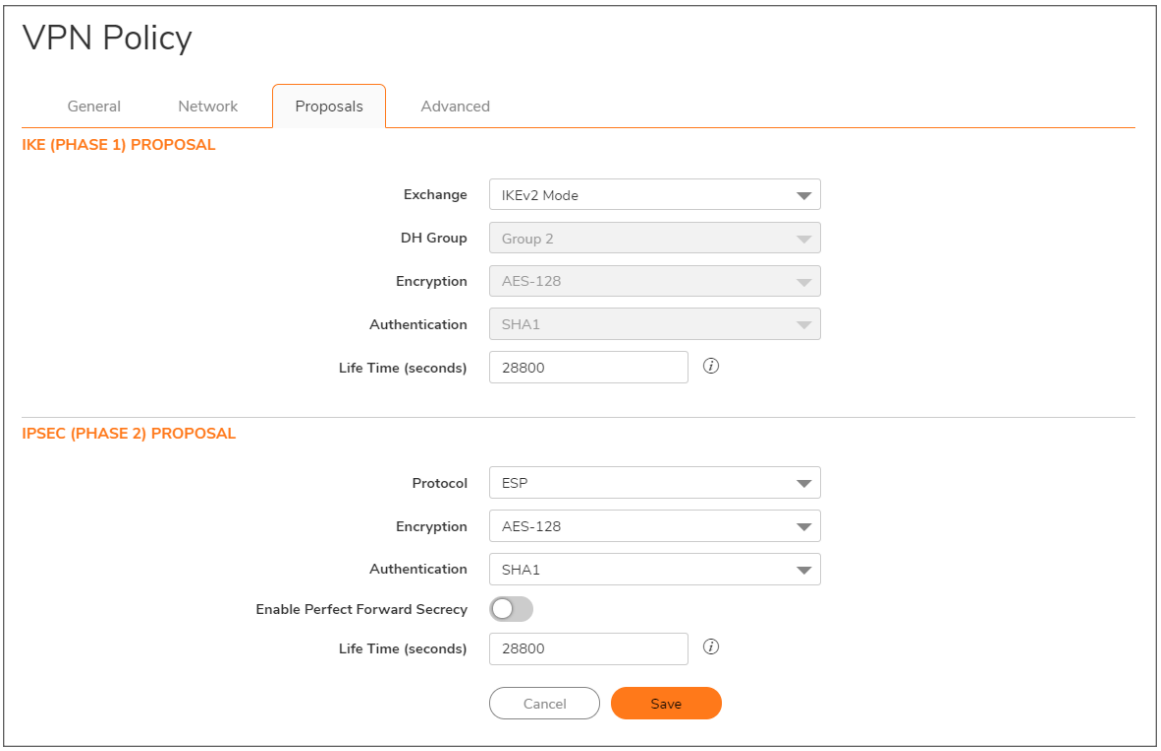
ⓘ **NOTE:** To find the certificate details (Subject Alternative Name, Distinguished Name, and so on), navigate to the **DEVICE | Settings > Certificates** page.

10. Type an ID string in the Peer IKE ID field.
11. Click **Network**.



12. Under **Local Networks**, select one of these options:
    - Select a local network from the **Choose local network from list** drop-down menu if a specific local network can access the VPN tunnel.
    - Select **Any Address** if traffic can originate from any local network. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone.
13. Under **Remote Networks**, select one of these options:
    - Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the firewall unless it is encrypted.

      ⓘ | **NOTE:** You can only configure one SA to use this setting.
    - Alternatively, select **Choose Destination network from list**, and select the address object or group from the drop-down menu.
    - Select **Use IKEv2 IP Pool** if you want to support IKEv2 Config payload, and select the address object or IP Pool Network from the drop-down menu.
14. Click **Proposals**.



15. In the IKE (Phase 1) Proposal section, select the following settings:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phases. ⓘ **NOTE:** If you select **IKE v2 Mode**, both ends of the VPN tunnel must use IKE v2. When selected, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and cannot be defined.

16. Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

ⓘ **NOTE:** If **IKEv2 Mode** is selected for the **Exchange** field, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and no selection can be made for those options.

ⓘ **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

a. For the **DH Group**, when in **Main Mode** or **Aggressive Mode**, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1
384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

b. For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **DES**, **3DES**, **AES-128** (default), **AES-192**, or **AES-256** from the drop-down menu.

c. For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **MD5**, **SHA-1** (default), **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.

17. For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

18. Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

    ⓘ | **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

    a. Select the desired protocol for **Protocol**.

    If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	DES
AESGCM16-192	3DES
AESGCM16-256	AES-128
AESGMAC-128	AES-192
AESGMAC-192	AES-256
AESGMAC-256	None

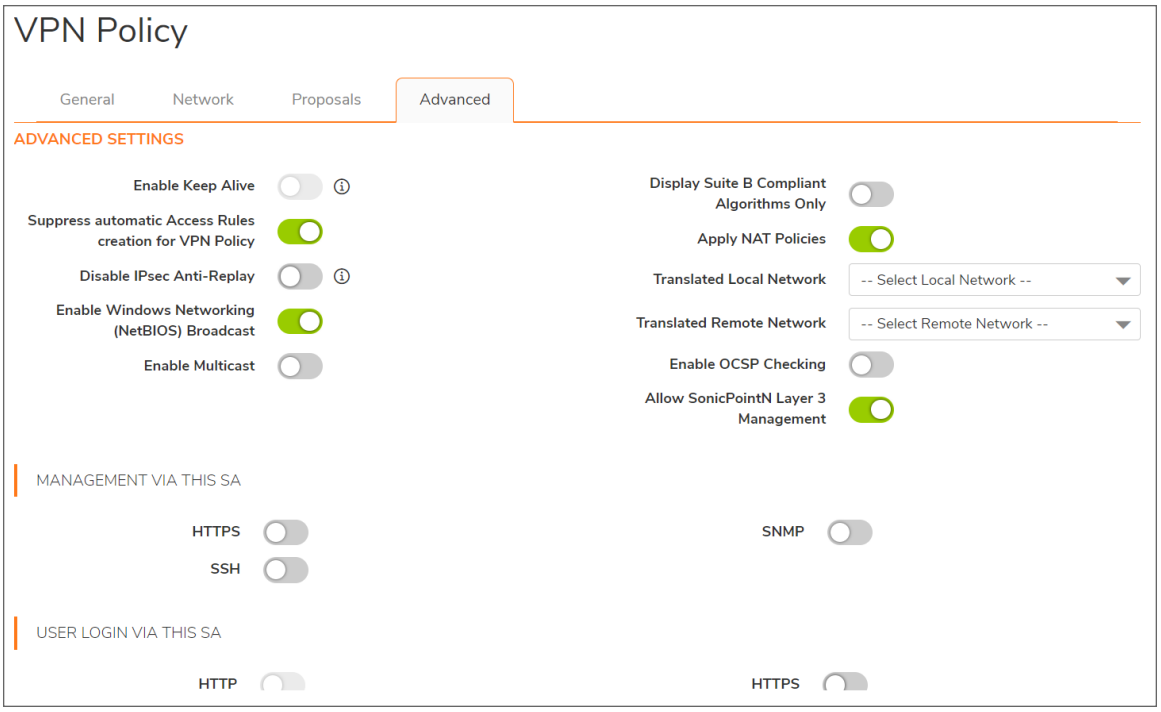
    If you selected **AH** in the **Protocol** field, the **Encryption** field is dimmed and you cannot select any options.

    b. For **Authentication**, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBC**, or **None**.

    c. Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security and select **Group 2** from the **DH Group** menu.

    d. Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

19. Click **Advanced**.



20. Select any configuration options you want to apply to your VPN policy:

ADVANCED SETTINGS

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Enable Keep Alive	Select to use heartbeat messages between peers on this VPN tunnel if one end of the tunnel fails, using a keep-alive heartbeat allows automatic renegotiation of the tunnel after both sides are available again without having to wait for the proposed Life Time to expire. ⓘ **NOTE:** The Keep Alive option is disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address `0.0.0.0`.	Cannot be selected for IKEv2 mode.
Suppress automatic Access Rules creation for VPN Policy	When not selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control for more information.	When not selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control for more information.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).
Require authentication of VPN clients by XAUTH	Requires that all inbound traffic on this VPN policy is from a user authenticated by XAUTH/RADIUS. Unauthenticated traffic is not allowed on the VPN tunnel.	Not available in IKEv2 Mode.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
Enable OCSP Checking	Select if you want to check VPN certificate status and provide the **OCSP Responder URL** in the field provided.	Select if you want to check VPN certificate status and provide the **OCSP Responder URL** in the field provided.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Management via this SA	Select **HTTPS**, **SSH**, **SNMP** or any combination of these three to manage the local SonicWall firewall through the VPN tunnel.	Select **HTTPS**, **SSH**, **SNMP** or any combination of these three to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to log in using the SA. ⓘ **NOTE:** HTTP user login is not allowed with remote authentication.	Select **HTTP**, **HTTPS**, or both to allow users to log in using the SA. ⓘ **NOTE:** HTTP user login is not allowed with remote authentication.
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the Network view of this page, under **Remote Networks**) enter the router address.	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the Network view of this page, under **Remote Networks**) enter the router address.
VPN Policy bound to	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. ⓘ **IMPORTANT:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. ⓘ **IMPORTANT:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.
Preempt Secondary Gateway	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the **Primary Gateway Detection Interval (seconds)** option. The default time is **28800** seconds, or 8 hours.	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the **Primary Gateway Detection Interval (seconds)** option. The default time is **28800** seconds, or 8 hours.
IKEv2 Settings		

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Do not send trigger packet during IKE SA negotiation	Not available in Main or Aggressive modes.	Is not selected (default). Should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.
Accept Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

21. Click **OK**.
22. Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

Configuring the Remote SonicWall Network Security Appliance

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click **+Add**. The **VPN Policy** dialog displays.
3. On the **General** screen, select **Manual Key** from the **Authentication Method** drop-down menu.
4. Enter a name for the appliance in the **Name** field.
5. Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.
6. Click **Network**.
7. Under **Local Networks**, select one of these:

- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone.

8. Under **Remote Networks**, select one of these:
   - If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

     ⓘ | **NOTE:** You can only configure one SA to use this setting.
   - Alternatively, select **Choose Destination network from list**, and select the address object or group.
9. Click **Proposals**.
10. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

    ⓘ | **NOTE:** Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.
11. The default values for **Protocol**, **Encryption**, and **Authentication** are acceptable for most VPN SA configurations.

    ⓘ | **NOTE:** The values for **Protocol**, **Encryption**, and **Authentication** must match the values on the opposite side of the tunnel.
12. Enter a 48-character hexadecimal encryption key in the **Encryption Key** field. Use the same value as used on the firewall on the opposite side of the tunnel.
13. Enter a 40-character hexadecimal authentication key in the **Authentication Key** field. Use the same value as used on the firewall on the opposite side of the tunnel.

    ⓘ | **TIP:** Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.
14. Click **Advanced**.
15. Select any of the following optional settings you want to apply to your VPN policy:
    - The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
    - Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
    - For **WXA Group**, select **None** or **Group One**.
    - Select **Apply NAT Policies** if you want the firewall to translate the Local, Remote or both networks communicating through this VPN tunnel. Two drop-down menus display:
      - To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.

- To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

  NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the remote SonicWall through the VPN tunnel, select **HTTP**, **SSH**, **SNMP**, or any combination of these three 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.

  NOTE: HTTP user login is not allowed with remote authentication.

- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

  IMPORTANT: Two different WAN interfaces cannot be selected from the VPN Policy bound to drop-down menu if the VPN Gateway IP address is the same for both.

16. Click **OK**.
17. Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

TIP: If Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

4

VPN Auto Provisioning

You can configure various types of IPsec VPN policies, such as site-to-site policies, including GroupVPN, and route-based policies. For specific details on the setting for these kinds of policies, go to the following sections:

- Site to Site VPNs
- Tunnel Interface Route-based VPN

Topics in this section include:

- About VPN Auto Provisioning
- Configuring a VPN AP Server
- Configuring a VPN AP Client

About VPN Auto Provisioning

The SonicOS VPN Auto Provisioning feature simplifies the provisioning of site to site VPNs between two SonicWall firewalls. This section provides conceptual information and describes how to configure and use the VPN Auto Provisioning feature.

- Defining VPN Auto Provisioning
- Benefits of VPN Auto Provisioning
- How VPN Auto Provisioning Works

Defining VPN Auto Provisioning

The VPN Auto Provisioning feature simplifies the VPN provisioning of SonicWall firewalls. This is especially useful in large scale VPN deployments. In a classic hub-and-spoke site-to-site VPN configuration, there are many complex configuration tasks needed on the spoke side, such as configuring the Security Association and configuring the Protected Networks. In a large deployment with many remote gateways, or spokes, this can be a challenge. VPN Auto Provisioning provides a simplified configuration process to eliminate many configuration steps on the remote VPN peers.

NOTE: The Hub in a hub-and-spoke site-to-site VPN configuration can be referred to using various names, such as Server, Hub Gateway, Primary Gateway, Central Gateway. In the context of the **VPN Auto Provisioning** feature, the term ***VPN AP Server*** is used for the Hub. Similarly, the term VPN AP Client is used to refer to a Spoke, Client, Remote Gateway, Remote Firewall, or Peer Firewall.

Benefits of VPN Auto Provisioning

The obvious benefit of the VPN Auto Provisioning feature is ease of use. This is accomplished by hiding the complexity of initial configuration from the SonicOS administrator, similar to the provisioning process of the SonicWall Global VPN Client (GVC).

When using SonicWall GVC, a user merely points the GVC at a gateway; security and connection configuration occur automatically. VPN Auto Provisioning provides a similar solution for provisioning site-to-site hub-and-spoke configurations, simplifying large scale deployment to a trivial effort.

An added advantage is that after the initial VPN auto-provisioning, policy changes can be controlled at the central gateway and automatically updated at the spoke end. This solution is especially appealing in Enterprise and Managed Service deployments where central management is a top priority.

How VPN Auto Provisioning Works

There are two steps involved in VPN Auto Provisioning:

- SonicWall Auto Provisioning Server configuration for the central gateway, or VPN AP Server
- SonicWall Auto Provisioning Client configuration for the remote firewall, or VPN AP Client

Both are configured by adding a VPN policy on the **NETWORK | IPSec VPN > Rules and Settings** page.

In Server mode, you configure the Security Association (SA), Protected Networks, and other configuration fields as in a classic site-to-site VPN policy. In Client mode, limited configuration is needed. In most cases the remote firewall administrator simply needs to configure the IP address to connect to the peer server (central gateway), and then the VPN can be established.

NOTE: SonicWall does not recommend configuring a single appliance as both an AP Server and an AP Client at the same time.

VPN Auto Provisioning is simple on the client side while still providing the essential elements of IP security:

Access Control	Network access control is provided by the VPN AP Server. From the VPN AP Client perspective, destination networks are entirely under the control of the VPN AP Server administrator. However, a mechanism is provided to control access to VPN AP Client local networks.
Authentication	Authentication is provided with machine authentication credentials. In Phase 1 of the IPsec proposal, the Internet Key Exchange (IKE) protocol provides machine-level authentication with *preshared keys* or *digital signatures*. You can select one of these authentication methods when configuring the VPN policy.

	For the preshared key authentication method, the administrator enters the VPN Auto Provisioning client ID and the key, or secret. For the digital signatures authentication method, the administrator selects the X.509 certificate which contains the client ID from the firewall's local certificate store. The certificate must have been previously stored on the firewall.
	To increase security, user level credentials through XAUTH are supported. The user credentials are entered when adding the VPN policy. XAUTH extracts them as authorization records by using a key or magic cookie, rather than using a challenge/response mechanism in which a user dynamically enters a username and password. Besides providing additional authentication, the user credentials provide further access control to remote resources and/or a local proxy address used by the VPN AP Client. User credentials allow sharing of a single VPN AP Server policy among multiple VPN AP Client devices by differentiating the subsequent network provisioning.
Data confidentiality and integrity	Data confidentiality and integrity are provided by Encapsulated Security Payload (ESP) crypto suite in Phase 2 of the IPsec proposal.

When policy changes occur at the VPN AP Server that affect a VPN AP Client configuration, the VPN AP Server uses IKE re-key mechanisms to ensure that a new Security Association with the appropriate parameters is established.

About Establishing the IKE Phase 1 Security Association

Because the goal of the VPN AP Client is ease of use, many IKE and IPsec parameters are defaulted or auto-negotiated. The VPN AP Client initiates Security Association establishment, but does not know the configuration of the VPN AP Server at initiation.

To allow IKE Phase 1 to be established, the set of possible choices is restricted; the VPN AP Client proposes multiple transforms (combined security parameters) from which the VPN AP Server can select its configured values. A Phase 1 transform contains the following parameters:

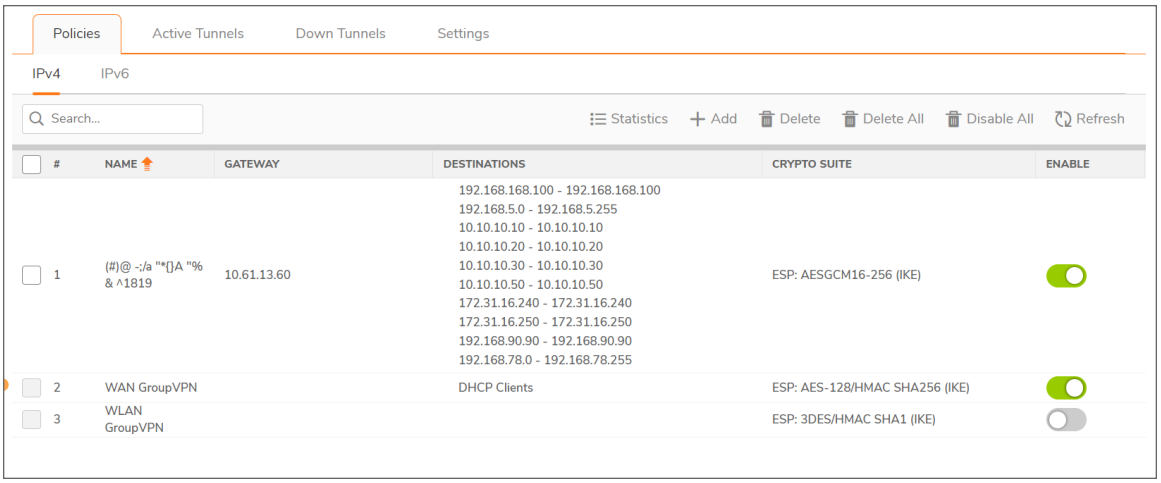
- **Authentication** – One of the following:
  - PRESHRD – Uses the preshared secret.
  - RSA_SIG – Use an X.509 certificate.
  - SW_DEFAULT_PSK – Uses the Default Provisioning Key.
  - XAUTH_INIT_PRESHARED – Uses the preshared secret combined with XAUTH user credentials.
  - XAUTH_INIT_RSA – Uses an X.509 certificate combined with XAUTH user credentials.
  - SW_XAUTH_DEFAULT_PSK – Uses the Default Provisioning Key combined with XAUTH user credentials.

  All the previously mentioned transforms contain the restricted or default values for the Phase 1 proposal settings:
  - Exchange - Aggressive Mode
  - Encryption – AES-256

- Hash – SHA1
- DH Group – Diffie-Hellman Group 5
- Life Time (seconds) – 28800

The VPN AP Server responds by selecting a single transform from those contained in the VPN AP Client proposal. If the VPN AP Server selects a transform which uses an XAUTH Authentication Method, the VPN AP Client awaits an XAUTH challenge following Phase 1 completion. If a non-XAUTH transform is chosen, the provisioning phase begins. The VPN AP Server provisions the VPN AP Client with the appropriate policy values including the Shared Secret, if one was configured on the VPN AP Server, and the VPN AP Client ID that was configured on the VPN AP Server.

After the Phase 1 SA is established and policy provisioning has completed, the Destination Networks appear in the **VPN Policies** section of the **NETWORK | IPSec VPN > Rules and Settings** page.

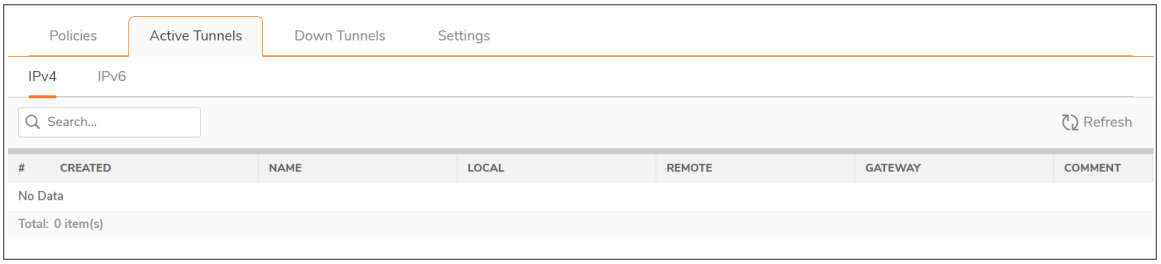


About Establishing IKE Phase 2 using a Provisioned Policy

The values received during the VPN AP provisioning transaction are used to establish any subsequent Phase 2 Security Associations. A separate Phase 2 SA is initiated for each Destination Network. Traffic must be initiated from behind the remote side in order to trigger the Phase 2 SA negotiation. The SA is built based on the address object specified when configuring the VPN AP server policy settings on the **Network** screen (see *Configuring VPN AP Server Settings on Network*).

NOTE: If the same VPN policy on the AP Server is shared with multiple remote AP Clients, each remote network must be specifically listed as a unique address object. The individual address objects can be summarized in an Address Group when added to the **Remote Networks** section during configuration of the VPN AP server policy settings on the **Network** screen. A single address object cannot be used to summarize multiple remote networks as the SA is built based on the specific address object.

Upon success, the resulting tunnel appears in the Active Tunnels list.



A NAT rule is also added to the **POLICY | Rules and Policies > NAT Rules** table.

As Phase 2 parameters are provisioned by the VPN AP Server, there is no chance of a configuration mismatch. If Phase 2 parameters change at the VPN AP Server, all Phase 1 and Phase 2 Security Associations are deleted and renegotiated, ensuring policy synchronization.

Configuring a VPN AP Server

VPN AP Server settings are configured on the server (hub) firewall by adding a VPN policy on the **NETWORK | IPSec VPN > Rules and Settings** page in SonicOS.

Because of the number of settings being described, the configuration is presented in multiple sections:

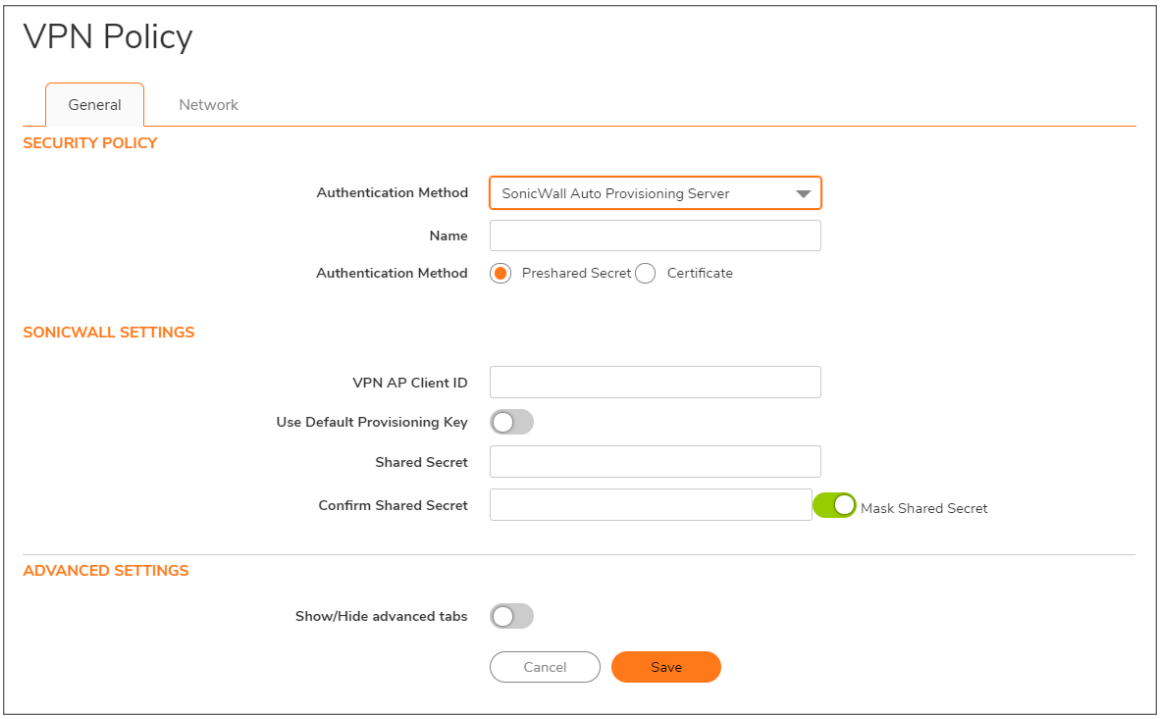
- Starting the VPN AP Server Configuration
- Configuring VPN AP Server Settings on General
- Configuring VPN AP Server Settings on Network
- Configuring Advanced Settings on Proposals
- Configuring Advanced Settings on Advanced

Starting the VPN AP Server Configuration

To begin configuration of VPN AP Server firewall settings using VPN Auto Provisioning:

1. Navigate to the **NETWORK | IPSec VPN > Rules and Settings** page.
2. Select **IPv4** for **View IP Version**.
3. Click **+Add**. The **VPN Policy** dialog displays.
4. In the **Authentication Method** drop-down menu, select **SonicWall Auto Provisioning Server**. The

display changes.



Configuring VPN AP Server Settings on General

To configure VPN AP server settings on the General screen:

1. In the **Name** field, type in a descriptive name for the VPN policy.
2. For **Authentication Method**, select either:
   - **IKE Using Preshared Secret** – Uses the VPN Auto Provisioning client ID and shared secret that you enter next. This option is selected by default. Proceed to Step 3.
   - **Certificate** – Uses the X.509 certificate that you select next (the certificate must have been previously stored on the appliance). Skip to Step 9.

     ⓘ **NOTE:** If VPN AP Server policies are to be shared (as in hub-and-spoke deployments), SonicWall recommends using X.509 certificates to provide true authentication and prevent man-in-the-middle attacks.
3. If you selected **IKE Using Preshared Secret** for the **Authentication Method**, then under **SonicWall Settings**, type the VPN Auto Provisioning client ID into the **VPN AP Client ID** field.This field is automatically populated with the value you entered into the **Name** field, but it can be changed.

   ⓘ **NOTE:** This VPN policy value has to match at both the AP Server and AP Client side. A single AP Server policy can also be used to terminate multiple AP Clients.

4. Check the box for **Use Default Provisioning Key** to allow VPN AP Clients to use the default key known to all SonicWall appliances for the initial Security Association. After the SA is established, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Client for future use.

   If this checkbox is cleared, VPN AP Clients must use the configured Shared Secret. This allows the administrator to modify the configured Shared Secret on the VPN AP Server only and then briefly allow Default Provisioning Key use to update the VPN AP Clients with the new Shared Secret value.

   ⓘ **NOTE:** For best security, SonicWall recommends that the Default Provisioning Key option is only enabled for a short time during which the VPN AP Client can be provisioned with the Shared Secret while under administrative scrutiny.

5. If you want, clear the **Mask Shared Secret** checkbox before typing anything into the **Shared Secret** field. This checkbox is selected by default, which hides typed characters. If this checkbox is reselected, then the values from the **Shared Secret** field are automatically copied to the **Confirm Shared Secret** field.

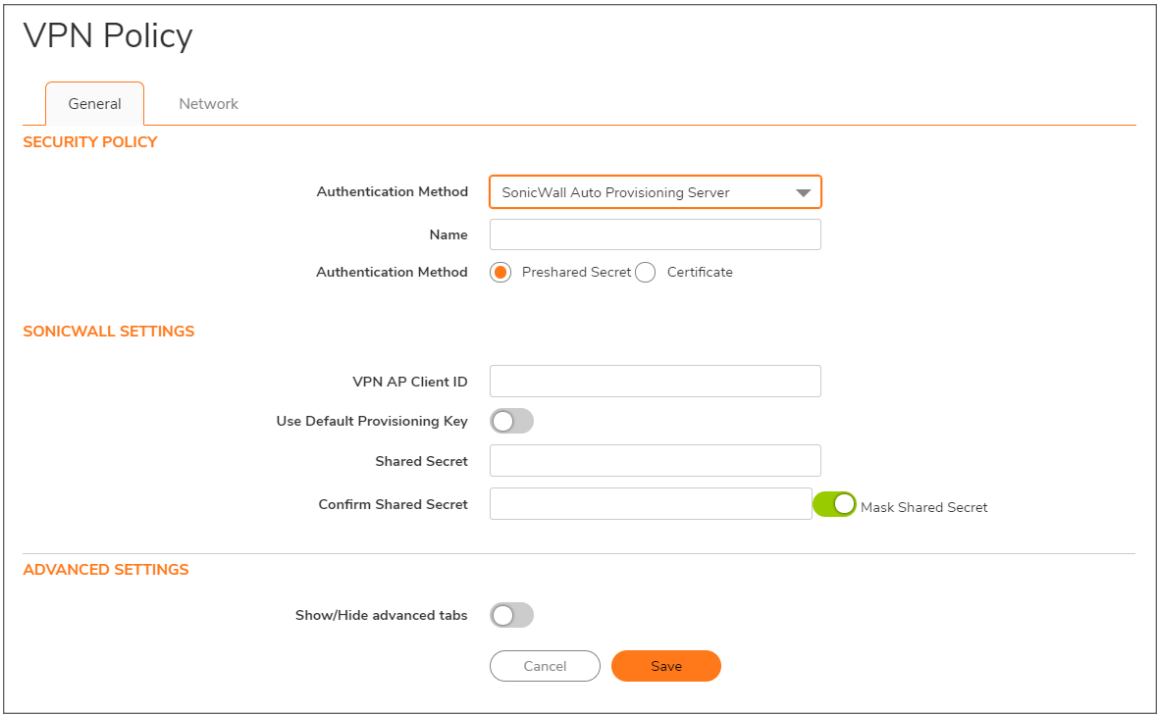
6. In the **Shared Secret** field, type in the shared secret key. A minimum of four characters is required.

   If **Use Default Provisioning Key** is checked, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Clients. If **Use Default Provisioning Key** is cleared, then this shared secret must also be configured on the VPN AP Clients.

7. In the **Confirm Shared Secret** field, type in the shared secret again. It must match the value entered in the **Shared Secret** field.

8. Go to Step 12.

9. If you selected **Certificate** for the **Authentication Method**, then under **SonicWall Settings** select the desired certificate from the **Local Certificate** drop-down menu.



10. Select one of the following from the **VPN AP Client ID Type** drop-down menu:

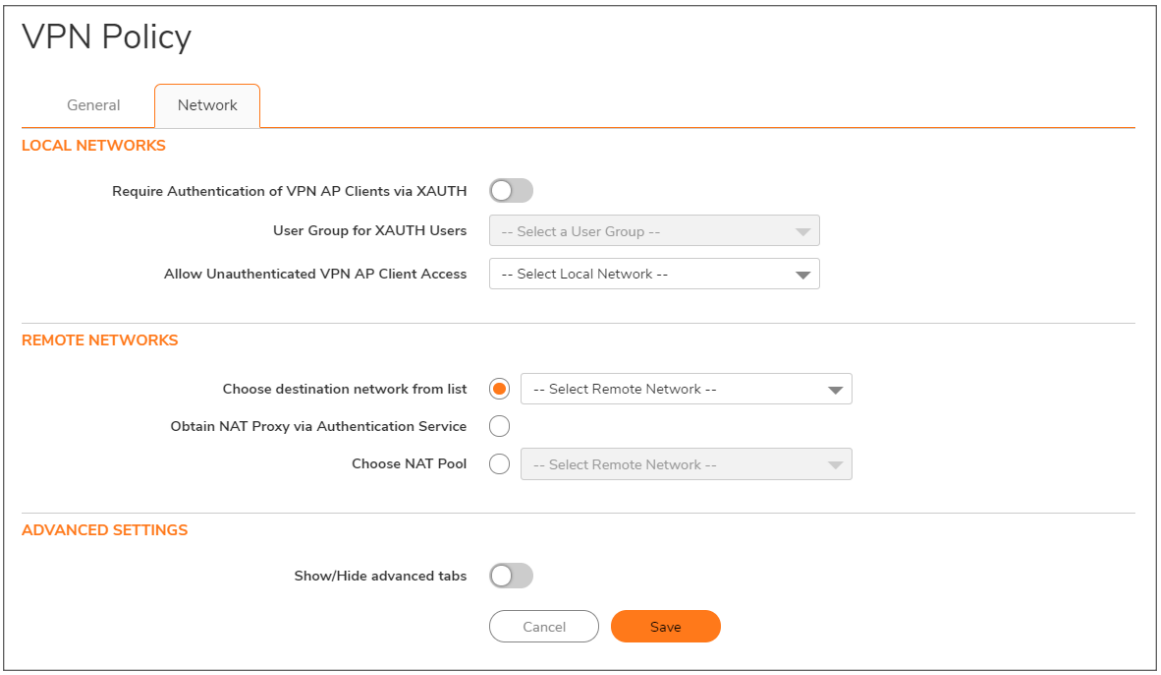
- **Distinguished name (DN)**
- **E-Mail ID (UserFQDN)**
- **Domain name (FQDN)**
- **IP Address (IPV4)**

11. In the **VPN AP Client ID Filter**, type in a matching string or filter to be applied to the Certificate ID presented during IKE negotiation.
12. Continue to *Configuring VPN AP Server Settings on Network*.

Configuring VPN AP Server Settings on Network

To configure VPN AP server settings on the Network screen:

1. Navigate to the **NETWORK | IPSec VPN > Rules and Settings** page.
2. Select **IPv4** for the **IP Version**.
3. Click **+Add**. The **VPN Policy** dialog displays.
4. On the **General** tab, select **SonicWall Auto Provisioning Server** for the **Authentication Method**.
5. Click the **Network** tab.



6. Under **Local Networks**, select **Require Authentication of VPN AP Clients via XAUTH** to force the use of user credentials for added security when establishing the SA.
7. If the XAUTH option is enabled, select the user group for the allowed users from the **User Group for XAUTH Users** drop-down menu. You can select an existing group such as Trusted Users or another

standard group, or select **Create a new user group** to create a custom group.

For each authenticated user, the authentication service returns one or more network addresses which are sent to the VPN AP Client during the provisioning exchange.

If XAUTH is enabled and a user group is selected, the user on the VPN AP Client side must meet the following conditions for authentication to succeed:

- The user must belong to the selected user group.
- The user can pass the authentication method configured in **DEVICE | Users > Settings | User Authentication Method**.
- The user has VPN access privileges.

8. If the XAUTH option is disabled, select a network address object or group from the **Allow Unauthenticated VPN AP Client Access** drop-down menu, or select **Create a new address object/group** to create a custom object or group. The selected object defines the list of addresses and domains that can be accessed through this VPN connection. It is sent to the VPN AP Client during the provisioning exchange and then used as the VPN AP Client's remote proxy ID.
9. Under **Remote Networks**, select one of the following radio buttons and choose from the associated list, if applicable:
   - **Choose destination network from list** – Select a network object from the drop-down menu of remote address objects that are actual routable networks at the VPN AP Client side, or create a custom object.

   ⓘ **NOTE:** VPN Auto Provisioning does not support using a “super network” that includes all the AP Clients’ protected subnets. To allow multiple AP Clients with different protected subnets to connect to the same AP Server, configure an Address Group that includes all of the AP Clients’ protected subnets and use that in the Choose destination network from list field. This Address Group must be kept up to date as new AP Clients are added.

   - **Obtain NAT Proxy via Authentication Service** – Select this option to have the RADIUS server return a Framed-IP Address attribute for the user, which is used by the VPN AP Client to NAT its internal addresses before sending traffic down the IPsec tunnel.
   - **Choose NAT Pool** – Select a network object from the drop-down menu, or create a custom object. The chosen object specifies a pool of addresses to be assigned to the VPN AP Client for use with NAT. The client translates its internal address to an address in the NAT pool before sending traffic down the IPsec tunnel.

     ⓘ **NOTE:** When deploying VPN Auto Provisioning, you should allocate a large enough NAT IP address pool for all the existing and expected VPN AP Clients. Otherwise, additional VPN AP Clients cannot work properly if all the IP addresses in the pool have already been allocated.

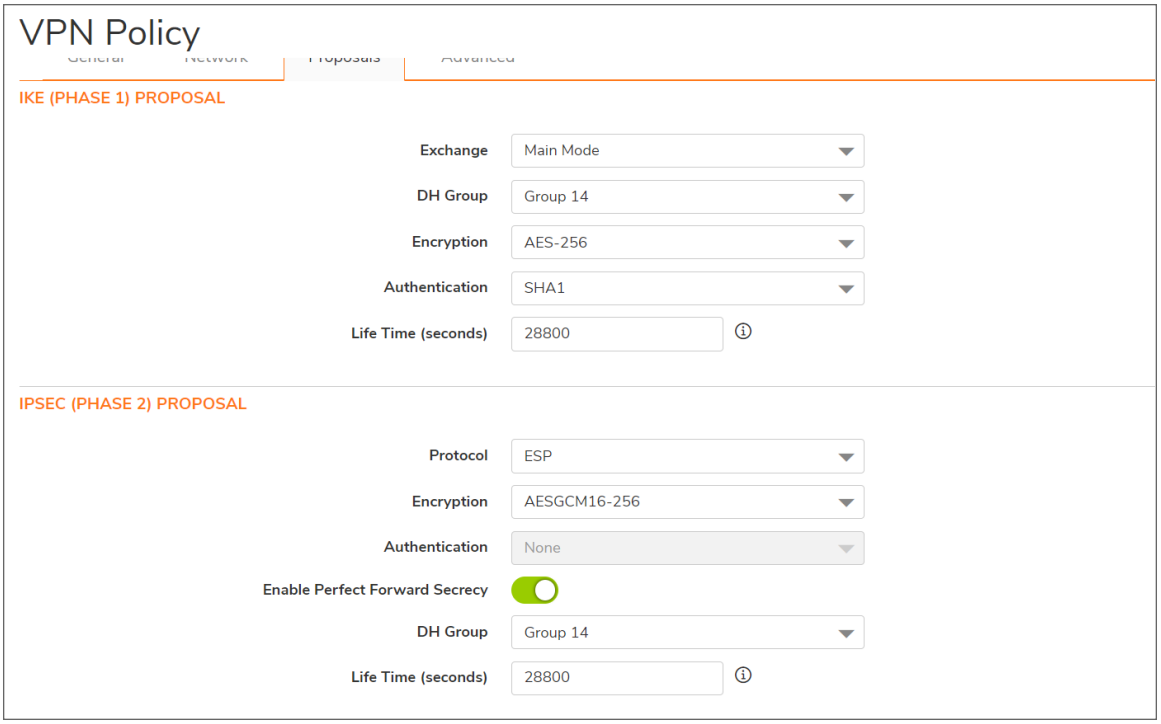
     ⓘ **NOTE:** Configuring a large IP pool does not consume more memory than a small pool, so it is safe and a best practice to allocate a large enough pool to provide redundancy.
10. Continue to *Configuring Advanced Settings on Proposals*.

Configuring Advanced Settings on Proposals

The configured parameters are automatically provisioned to the VPN AP Client prior to Phase 2 establishment, so there is no chance of configuration discrepancies between the VPN AP Server and VPN AP Client.

To configure VPN AP Server settings on the Proposals screen:

1. On the **General** or **Network** tab, click **Proposals**.



2. Under **IKE (Phase 1) Proposal**, enter the phase 1 proposal lifetime in seconds. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

   To simplify auto-provisioning, the other fields in this section are dimmed and preset to:

   - **Exchange: Aggressive Mode**
   - **DH Group: Group 5**
   - **Encryption: AES-256**
   - **Authentication: SHA1**

3. Under **Ipsec (Phase 2) Proposal**, select the desired encryption algorithm from the **Encryption** drop-down menu. The default is **AES-128**.

   The **Protocol** field is dimmed and preset to **ESP** to use the Encapsulated Security Payload (ESP) crypto suite.

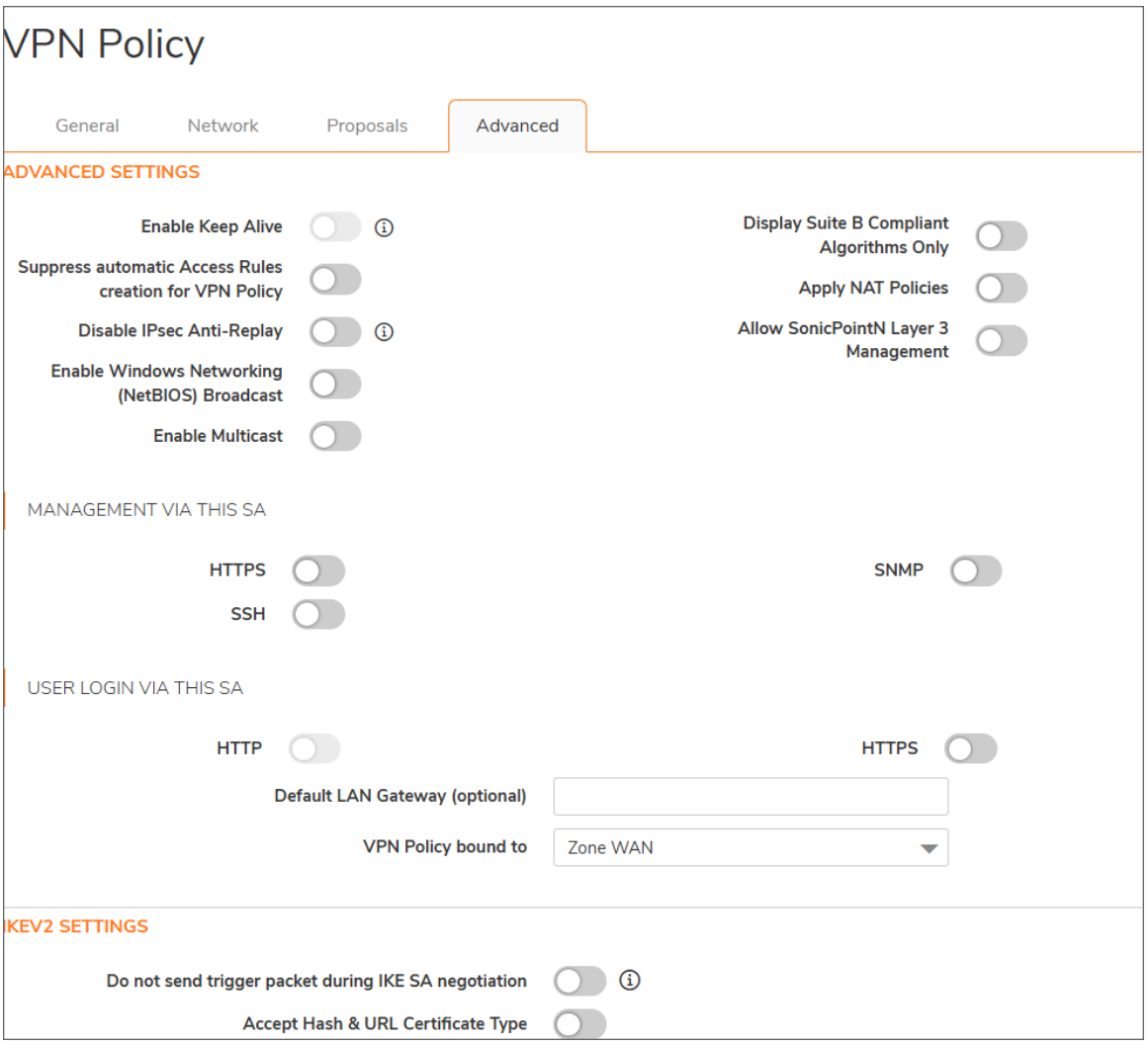
4. Select the desired authentication encryption method from the **Authentication** drop-down menu. The default is **SHA1**.

5. Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. If selected, the **DH Group** drop-down menu is displayed. Select the desired group from the list. The default is Group 2.
6. Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every eight hours.
7. Continue to *Configuring Advanced Settings on Advanced*.

Configuring Advanced Settings on Advanced

To configure VPN AP Server settings on the Advanced screen:

1. Click **Advanced**.



2. Select **Disable IPsec Anti-Replay** to prevent packets with duplicate sequence numbers from being dropped.
3. Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass from the VPN AP Server over any VPN AP Client SA established using this policy.
4. If you are using SonicWall WAN Acceleration, select a value from the **WXA Group** drop-down menu.
5. Optionally select **Display Suite B Compliant Algorithms Only**.
6. For **Management via this SA**, select one or more of the checkboxes to allow remote users to manage the VPN AP Server through the VPN tunnel using **HTTPS**, **SSH**, or **SNMP**.
7. For **User login via this SA**, select one or more of the checkboxes to allow remote users to log in through the VPN tunnel using **HTTP** or **HTTPS**.
8. In the **Default LAN Gateway (optional)** field, optionally enter the default LAN gateway IP address of the VPN AP Server. If a static route cannot be found for certain traffic, the VPN AP Server forwards the traffic out the configured default LAN gateway.

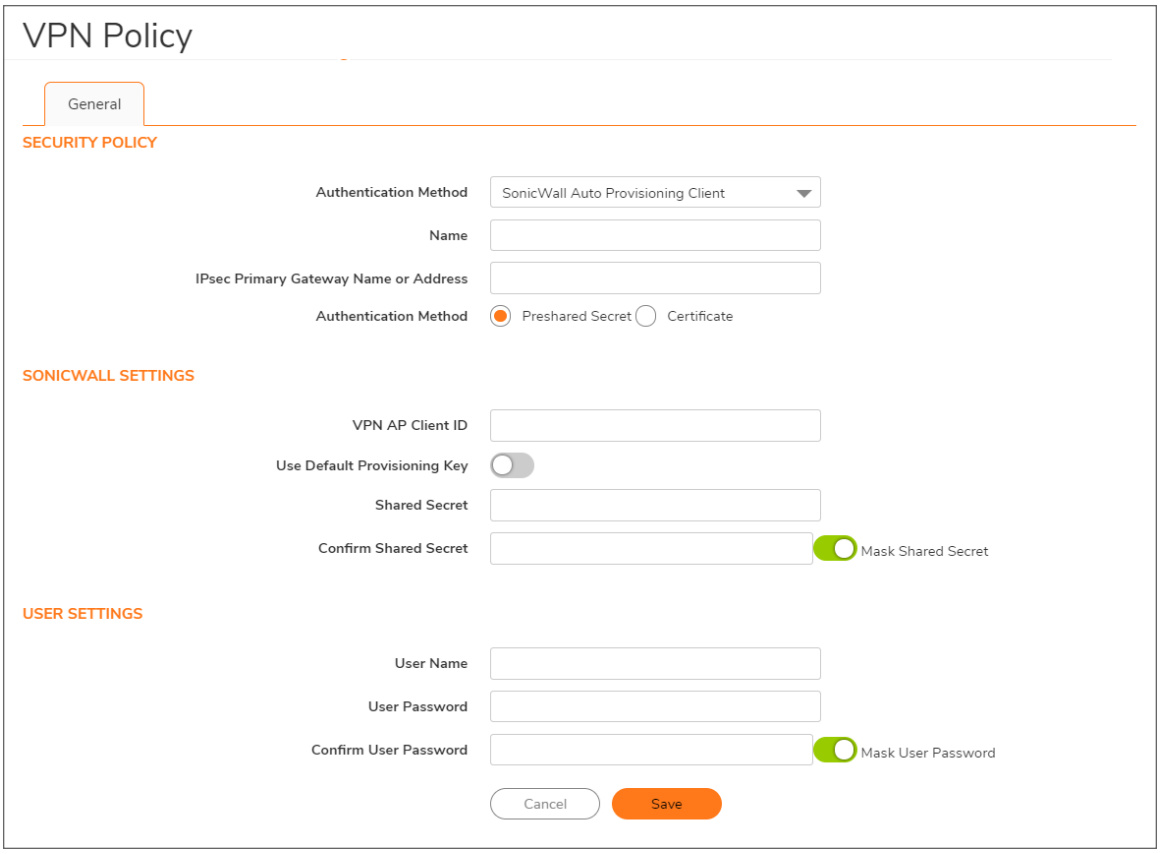
   ⓘ | **NOTE:** This option might not work in some versions of SonicOS.
9. Select an interface or zone in the **VPN Policy bound to** drop-down menu to bind this VPN policy to a specific interface or zone. **Zone WAN** is the default.
10. When finished, click **Save**.

Configuring a VPN AP Client

VPN AP Client settings are configured on the client firewall by adding a VPN policy on the **NETWORK | IPSec VPN > Rules and Settings** page in SonicOS.

To configure remote client firewall settings using VPN Auto Provisioning:

1. Navigate to the **NETWORK | IPSec VPN > Rules and Settings** page.
2. Select **IPv4** for the IP Version.
3. Click **+Add**. The **VPN Policy** dialog displays.
4. In the **Authentication Method** drop-down menu, select **SonicWall Auto Provisioning Client**. The page refreshes with different fields.



5. In the **Name** field, type in a descriptive name for the VPN policy.
6. In the **IPsec Primary Gateway Name or Address** field, enter the Fully Qualified Domain Name (FQDN) or the IPv4 address of the VPN AP Server.
7. For **Authentication Method**, select either:
   - **Preshared Secret** – Uses the VPN Auto Provisioning client ID and shared secret that you enter next. This option is selected by default. Proceed to Step 8.
   - **Certificate** – Uses the X.509 certificate that you select next (the certificate must have been previously stored on the appliance). Skip to Step 14.
8. If you selected **Preshared Secret** for the **Authentication Method**, then under **SonicWall Settings**, type the VPN Auto Provisioning client ID into the **VPN AP Client ID** field.

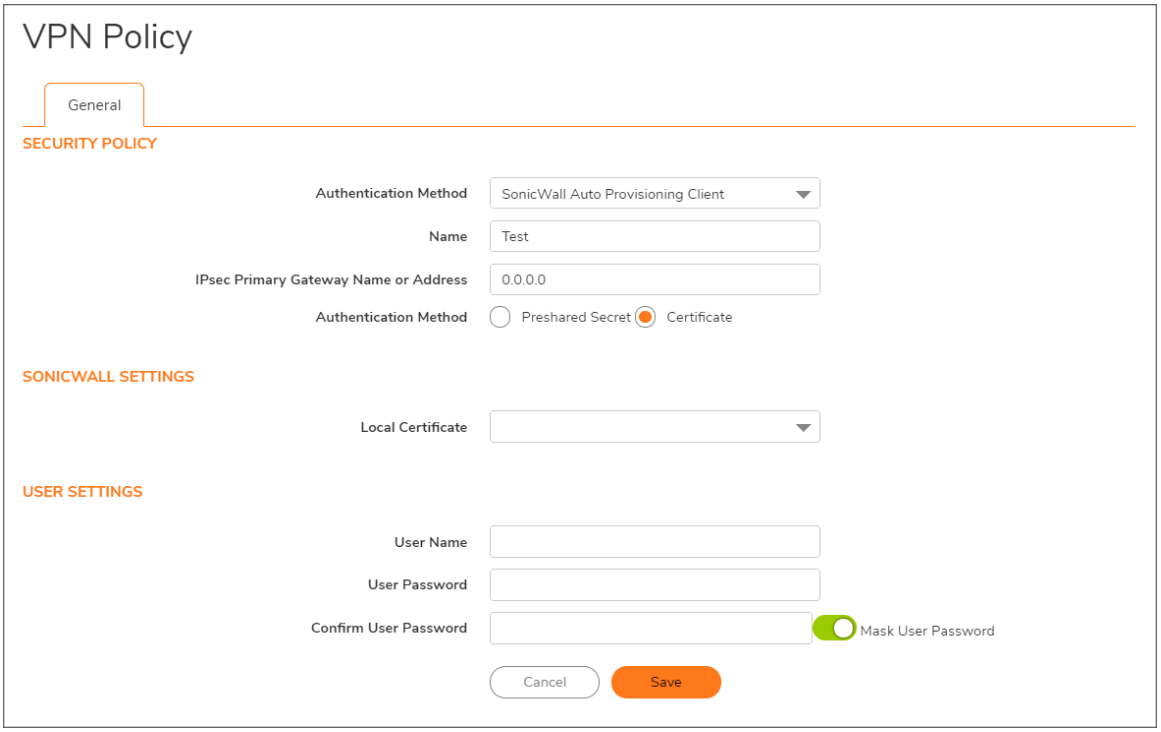
   The client ID is determined by the configuration of the VPN AP Server (the SonicWall firewall configured as the **SonicWall Auto Provisioning Server**).

   ⓘ **NOTE:** This VPN policy value has to match at both the AP Server and AP Client side. A single AP Server policy can also be used to terminate multiple AP Clients.
9. Optionally, select **Use Default Provisioning Key** to use the default key known to all SonicWall appliances for the initial Security Association. After the SA is established, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Client for future use.

NOTE: The VPN AP Server must be configured to accept the Default Provisioning Key. If it is not, SA establishment fails.

If you selected **Use Default Provisioning Key**, skip to Step 13.

10. If you did not select **Use Default Provisioning Key**, then optionally clear the **Mask Shared Secret** checkbox before typing anything into the **Shared Secret** field. This checkbox is selected by default, which hides typed characters. If this checkbox is reselected, then the values from the **Shared Secret** field are automatically copied to the **Confirm Shared Secret** field.
11. In the **Shared Secret** field, type in the shared secret. This must be the same as the shared secret configured on the VPN AP Server, and must be a minimum of four characters.
12. In the **Confirm Shared Secret** field, type in the shared secret again. It must match the value entered in the **Shared Secret** field.
13. Skip to Step 15 for information about entering the user credentials under **User Settings**. User credentials are optional.
14. If you selected **SonicWall Auto Provisioning Client** for the **Authentication Method**, then under **SonicWall Settings** select the desired certificate from the **Local Certificate** drop-down menu.



15. Under **User Settings**, type the user name to be used for the optional user credentials into the **User Name** field. This user name is sent through XAUTH for user-level authentication.
16. Optionally clear the **Mask User Password** checkbox before typing anything into the **User Password** field. This checkbox is selected by default. If selected, the typed characters are represented as dots. Clearing this checkbox displays the values in plain text and automatically copies the value entered in the **User Password** field to the **Confirm User Password** field.
17. In the **User Password** field, type in the user password.

18. In the **Confirm User Password** field, type in the user password again.
19. When ready, click **Save** to add the VPN policy.

5

Rules and Settings

This describes how to configure Tunnel Interface Route-based VPN policies, which provide a route-based VPN solution. Tunnel Interface VPN policies differ from site to site VPN policies, which force the VPN policy configuration to include the network topology configuration. This makes it difficult to configure and maintain the VPN policy with a constantly changing network topology. Refer to Site to Site VPNs for details.

With the route-based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates an *unnumbered Tunnel Interface* between two end points. Static or dynamic routes can then be added to the Tunnel Interface. The route-based VPN approach moves network configuration from the VPN policy configuration to static or dynamic route configuration.

Route-based VPN makes configuring and maintaining the VPN policy easier, and provides flexibility on how traffic is routed. You can define multiple paths for overlapping networks over a clear or redundant VPN.

For auto provisioning of VPN networks, refer to VPN Auto Provisioning for details.

Topics:

- Adding a Tunnel Interface
- Route Entries for Different Network Segments
- Redundant Static Routes for a Network

Adding a Tunnel Interface

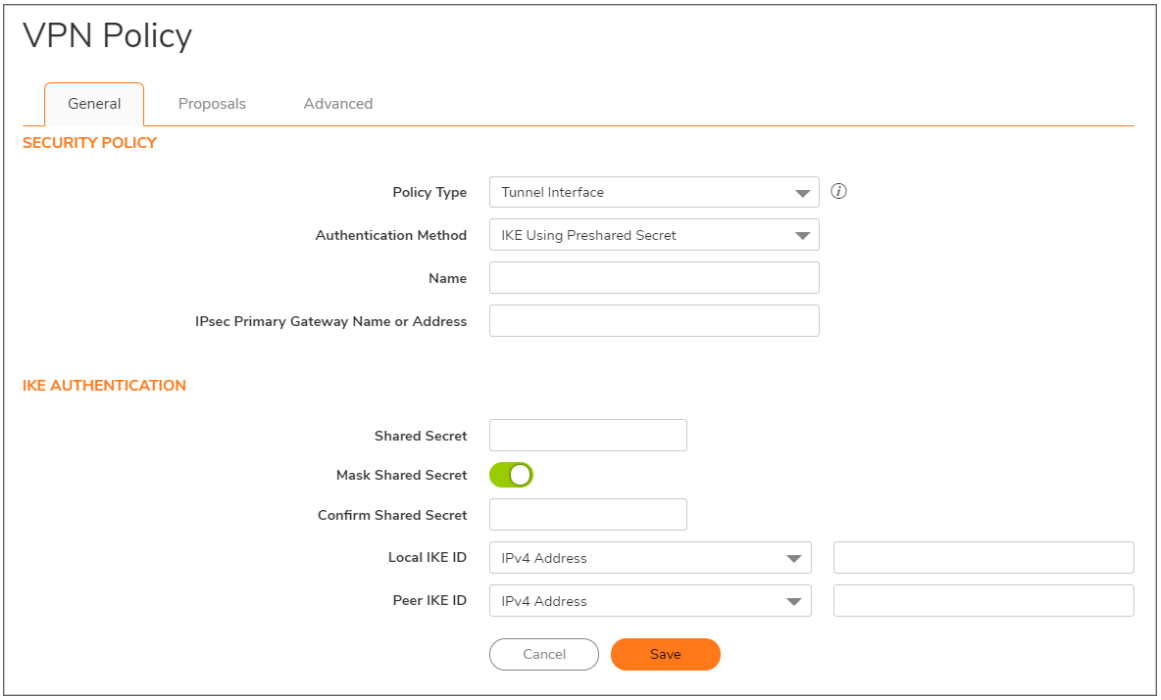
Route-based VPN configuration is a two-step process:

1. Create a Tunnel Interface. The cryptography suites used to secure the traffic between two end-points are defined in the Tunnel Interface.
2. Create a static or dynamic route using Tunnel Interface.

The Tunnel Interface is created when a Policy of type **Tunnel Interface** is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

To add a Tunnel Interface:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Select **IPv4** or **IPv6** as the IP Version option.
3. Click **+Add**.



4. On the **General** screen, select **Tunnel Interface** as the **Policy Type**. The options change.
5. Select one the following for **Authentication Method**:

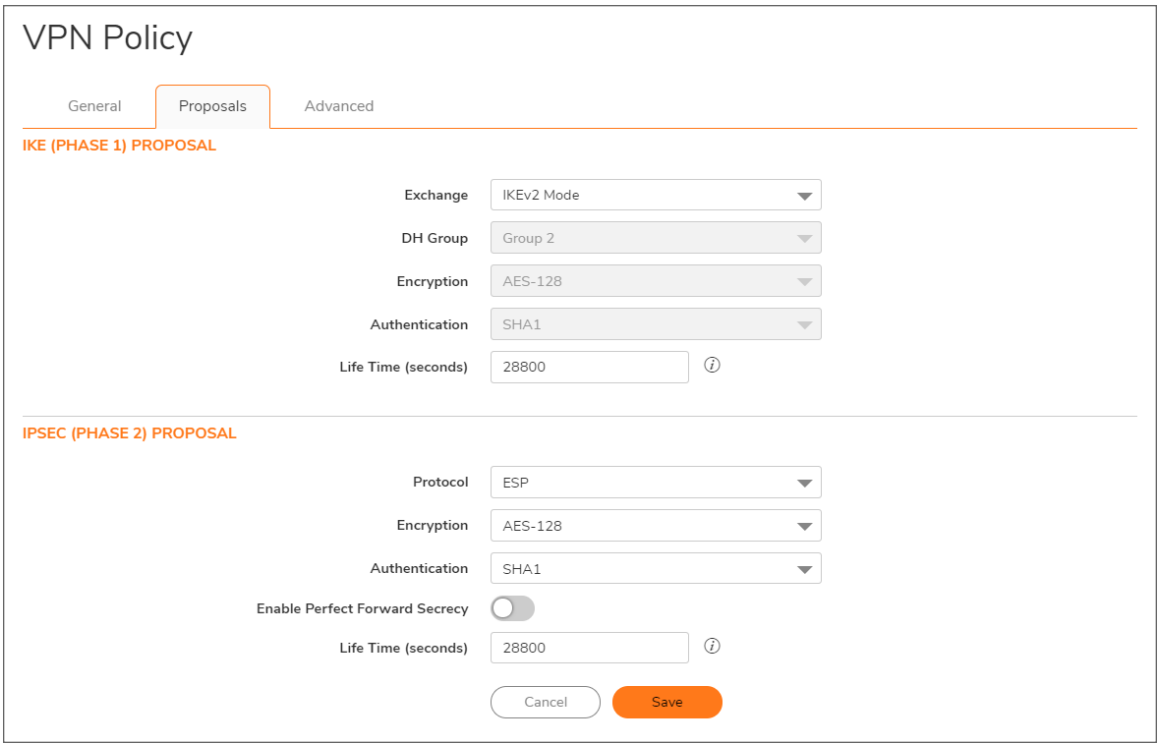
   - **Manual Key**
   - **IKE using Preshared Secret** (default)
   - **IKE using 3rd Party Certificates**
   - **SonicWall Auto Provisioning Client**
   - **SonicWall Auto Provisioning Server**

   The remaining fields in the **General** screen change depending on which option you select.

   For more information about the available selections, see:

   - Configuring with a Manual Key
   - Configuring with a Preshared Secret Key
   - Configuring with a Third-Party Certificate
   - Configuring a VPN AP Client
   - Configuring a VPN AP Server

6. Click **Proposals**.



7. Under **IKE (Phase 1) Proposal**, choose one of the following options from the **Exchange** drop-down menu:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phases. ⓘ **NOTE:** If you select IKE v2 Mode, both ends of the VPN tunnel must use IKE v2. When selected, the DH Group, Encryption, and Authentication fields are disabled and cannot be defined.

8. Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

   ⓘ **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

   a. For the DH Group, when in Main Mode or Aggressive Mode, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1
384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

b. For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **DES**, **3DES**, **AES-128** (default), **AES-192**, or **AES-256** from the drop-down menu.

c. For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **SHA-1** (default), **MD5**, **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.

d. For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every eight hours.

9. Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

   ⓘ | **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

   a. In the **Protocol** field, select **ESP** or **AH**.

   b. In the **Encryption** field, if you selected **ESP** in the **Protocol** field, you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	DES
AESGCM16-192	3DES
AESGCM16-256	AES-128
AESGMAC-128	AES-192
AESGMAC-192	AES-256
AESGMAC-256	None

   ⓘ | **NOTE:** If you selected **AH** in the **Protocol** field, the **Encryption** field is disabled, and you cannot select any options.

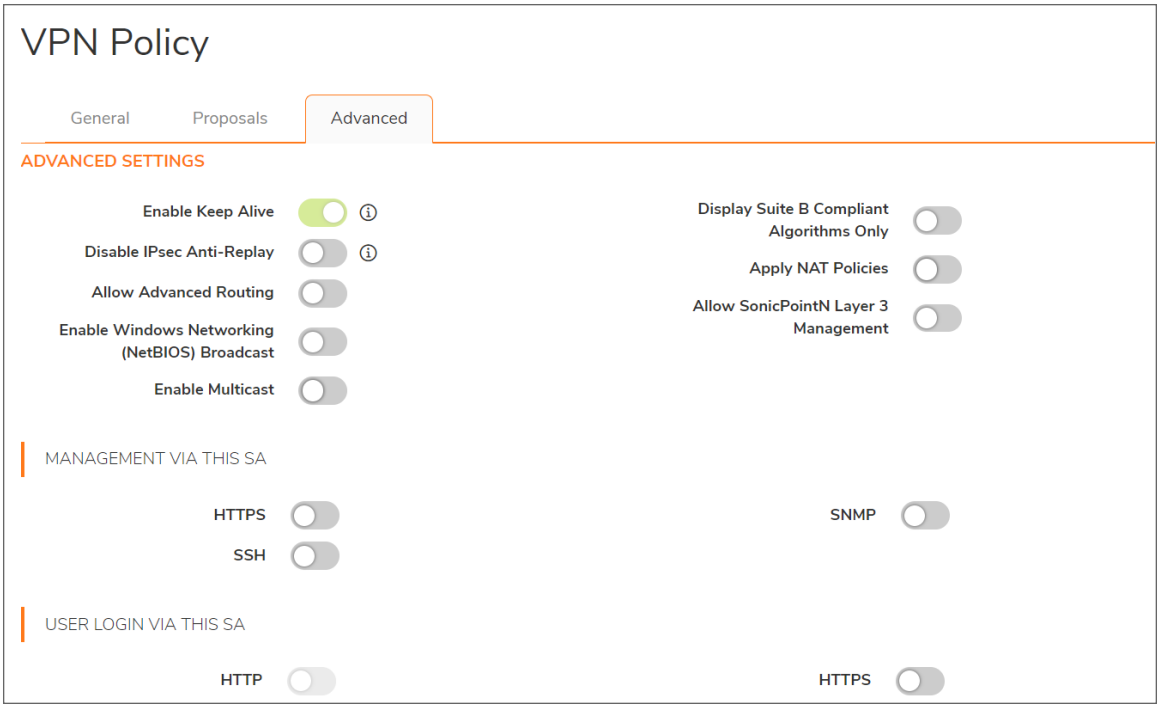
   c. In the **Authentication** field, select the authentication method from the drop-down menu:

   - **MD5**
   - **SHA1 (default)**
   - **SHA256**
   - **SHA384**
   - **SHA512**
   - **AES-XCBC**

d. Select **Enable Perfect Forward Secrecy** if you want added security.

e. Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

10. Click **Advanced**.



11. The following advanced options can be configured; by default, none are selected:

ADVANCED SETTINGS

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Enable Keep Alive	Cannot be selected for a route-based interface.	Cannot be selected for a route-based interface.
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window)	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window)
Allow Advanced Routing	Adds this Tunnel Interface to the list of interfaces in the Routing Protocols table on the **NETWORK | System > Dynamic Routing** page.	Adds this Tunnel Interface to the list of interfaces in the Routing Protocols table on the **NETWORK | System > Dynamic Routing** page.
	NOTE: This option must be selected if the Tunnel Interface is to be used for advanced routing (RIP, OSPF). Making this an optional setting avoids adding all Tunnel Interfaces to the **Routing Protocols** table, which helps streamline the routing configuration.	

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Enable Transport Mode	This option is used to protect packets that are already encapsulated by another tunneling protocol such as Generic Routing Encapsulation (GRE). It encrypts only the payload and ESP trailer, so the IP header of the original packet is not encrypted.	Not available for IKEv2 Mode.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
Management via this SA	Select any of **HTTPS**, **SSH**, or **SNMP** for this option to manage the local SonicWall firewall through the VPN tunnel.	Select any of **HTTPS**, **SSH**, or **SNMP** for this option to manage the local SonicWall firewall through the VPN tunnel.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to login using the SA. ⓘ **NOTE:** HTTP user login is not allowed with remote authentication.	Select **HTTP**, **HTTPS**, or both to allow users to login using the SA. ⓘ **NOTE:** HTTP user login is not allowed with remote authentication.
VPN Policy bound to	Select an interface from the drop-down menu. ⓘ **IMPORTANT:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface from the drop-down menu. ⓘ **IMPORTANT:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.

IKEV2 SETTINGS

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Do not send trigger packet during IKE SA negotiation	Not available	Is not selected (default). It should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.
Accept Hash & URL Certificate Type	Not available	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

12. Click **Save**.
13. Click **Accept** on the **NETWORK | IPSec VPN > Rules and Settings** page to update the VPN Policies.

Creating a Static Route for the Tunnel Interface

After you have successfully added a Tunnel Interface, you can then create a Static Route to go with it.

To create a Static Route for a Tunnel Interface:

1. Navigate to **NETWORK | IPSec VPN > Rules and Settings**.
2. Click **+Add** to display the VPN Policy dialog.
3. Select the **Tunnel Interface** from the **Policy Type** drop-down menu that lists all available tunnel interfaces.

   NOTE: If the **Auto-add Access Rule** option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using the tunnel interface.
4. Configure the rest of the settings as necessary.
5. Click **Save**.

Route Entries for Different Network Segments

After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

Redundant Static Routes for a Network

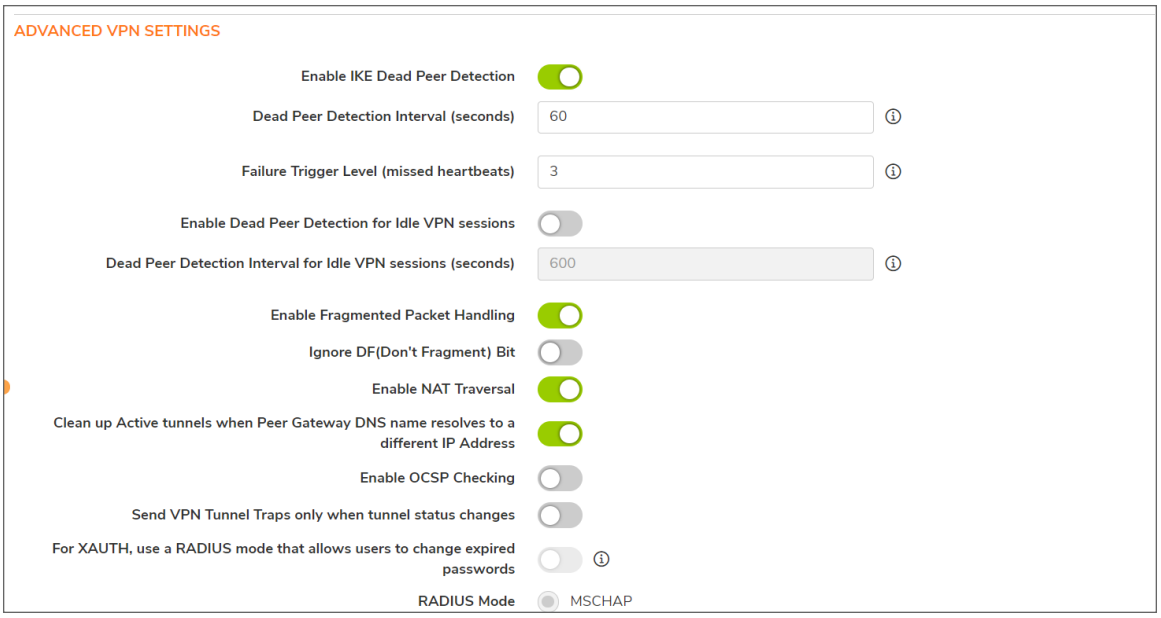
After more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination. If no redundant routes are available, you can add a static route to a drop tunnel interface to prevent VPN traffic from being sent out the default route.

6

Advanced

The **NETWORK | IPSec VPN > Advanced** page has two sections:

- Advanced VPN Settings
- IKEv2 Settings



Topics:

- Configuring Advanced VPN Settings
- Configuring IKEv2 Settings

Configuring Advanced VPN Settings

Advanced VPN Settings globally affect all VPN policies. This section also provides solutions for Online Certificate Status Protocol (OCSP). OCSP allows you to check VPN certificate status without Certificate

Revocation Lists (CRLs). This allows timely updates regarding the status of the certificates used on your firewall.

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the firewall.
    - **Dead Peer Detection Interval** - Enter the number of seconds between “heartbeats.” The default value is 60 seconds.
    - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the firewall. The firewall uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
    - **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the firewall after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message `Fragmented IPsec packet dropped`, select this feature. Do not select it until the VPN tunnel is established and in operation.
    - **Ignore DF (Don't Fragment) Bit** - Select this checkbox to ignore the DF bit in the packet header. Some applications can explicitly set the ‘Don’t Fragment’ option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the firewall to ignore the option and fragment the packet regardless.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.

  ⓘ **NOTE:** Enabling "KeepAlive" incorrectly on both ends of a tunnel can cause negotiation conflicts and tunnel instability. Follow these guidelines when configuring KeepAlive:
  Enable KeepAlive on only one peer in a site-to-site VPN tunnel. Enabling it on both sides simultaneously can result in conflict and unpredictable tunnel behavior.
  When one peer has a dynamic IP address, enable KeepAlive on that dynamic peer.
  For Static-to-static tunnels, enable KeepAlive on the peer that is responsible for initiating tunnel re-establishment, typically the hub.
- **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See *Using OCSP with SonicWall Network Security Appliances*.
- **Send VPN Tunnel Traps only when tunnel status changes** - Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.
    - **Use RADIUS in** - The primary reason for choosing this option is so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time. When using RADUIS to authenticate VPN client users, select whether RADIUS is used in one of these modes:

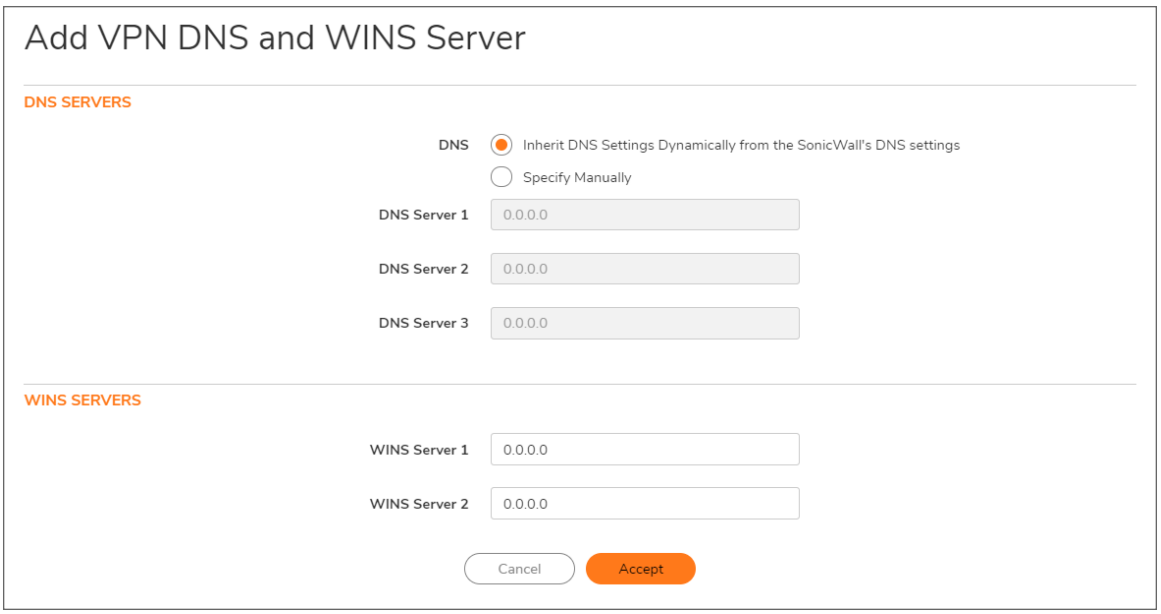
- **MSCHAP**
- **MSCHAPv2** mode for XAUTH (allows users to change expired passwords)

Also, if this is set and LDAP is selected as the **Authentication method for login** on the **DEVICE | Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for VPN client users are done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

ⓘ | **NOTE:** Password updates can only be done by LDAP when using either:

- Active Directory with TLS and binding to it using an administrative account
- Novell eDirectory.

- **DNS and WINS Server Settings for VPN Client** – To configure DNS and WINS server settings for Client, such as a third-party VPN Client through GroupVPN, or a Mobile IKEv2 Client, click **Configure**. The **Add VPN DNS And WINS Server** dialog displays.



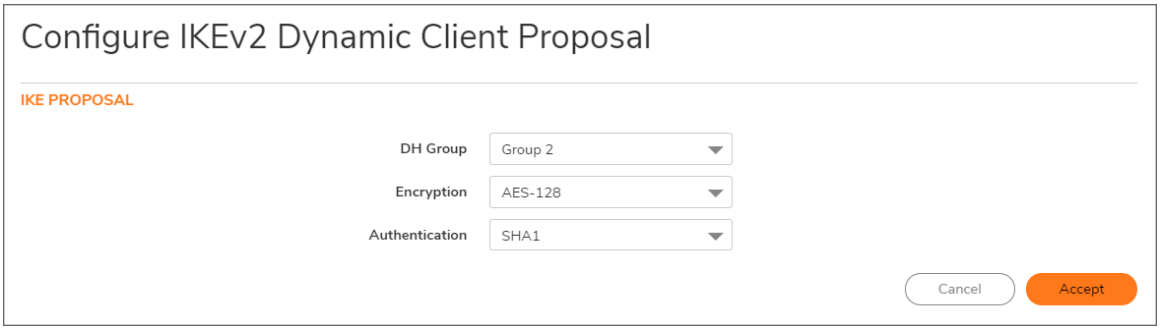
- **DNS Servers** – Select whether to specify the DNS servers dynamically or manually:
  - **Inherit DNS Settings Dynamically from the SonicWall's DNS settings** – The SonicWall appliance obtains the DNS server IP addresses automatically.
  - **Specify Manually** – Enter up to three DNS server IP addresses in the **DNS Server 1/3** fields.
- **WINS Servers** – Enter up to two WINS server IP address in the **WINS Server 1/2** fields.

Configuring IKEv2 Settings

IKEv2 Settings affect IKE notifications and allow you to configure dynamic client support.

- **Send IKEv2 Cookie Notify** – Sends cookies to IKEv2 peers as an authentication tool.
- **Send IKEv2 Invalid SPI Notify** – Sends an invalid Security Parameter Index (SPI) notification to IKEv2 peers when an active IKE security association (SA) exists. This option is selected by default.
- **IKEv2 Dynamic Client Proposal** – SonicOS provides IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings.

  Clicking **Configure** launches the **Configure IKEv2 Dynamic Client Proposal** dialog.



  SonicOS supports these **IKE Proposal** settings:

  - **DH Group**: **Group 1**, **Group 2** (default), **Group 5**, **Group 14**, and the following five Diffie-Hellman groups that are included in Suite B cryptography:
    - **256-bit Random ECP Group**
    - **384-bit Random ECP Group**
    - **521-bit Random ECP Group**
    - **192-bit Random ECP Group**
    - **224-bit Random ECP Group**
  - **Encryption** – **DES**, **3DES** (default), **AES-128**, **AES-192**, **AES-256**
  - **Authentication**– MD5, SHA1 (default), SHA256, SHA384, or SHA512

  If a VPN Policy with IKEv2 exchange mode and a `0.0.0.0` IPSec gateway is defined, however, you cannot configure these IKE Proposal settings on an individual policy basis.

  ⓘ | **NOTE:** The VPN policy on the remote gateway must also be configured with the same settings.

Using OCSP with SonicWall Network Security Appliances

OCSP is designed to augment or replace CRL in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

The main disadvantage of Certificate Revocation Lists is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by

every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions might or might not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client cannot accept the response from the OSCP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at http://www.openca.org. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to Use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the firewall.

1. On the **DEVICE | Settings > Certificates** page, click **Import**. This brings up the **Import Certificate** page.
2. Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

The firewall OCSP settings can be configured on a policy level or globally.

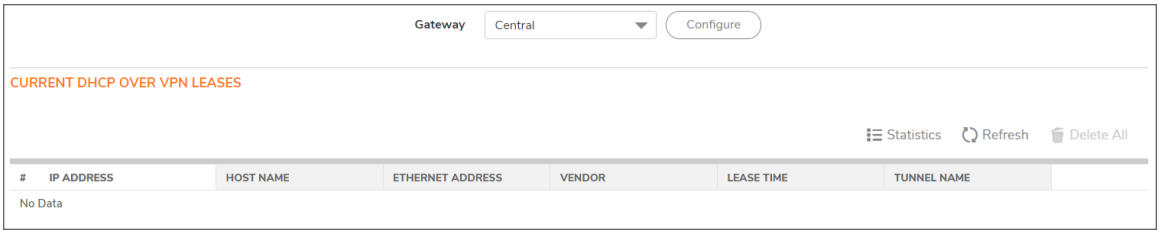
To configure OCSP checking for individual VPN policies, use the Advanced tab of the VPN Policy configuration page:

1. Select **Enable OCSP Checking**.
2. Specify the **OCSP Responder URL** of the OCSP server, for example http://192.168.168.220:2560 where `192.168.168.220` is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.

7

DHCP over VPN

The **NETWORK | IPSec VPN > DHCP over VPN** page allows you to configure a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



Topics:

- DHCP Relay Mode
- Configuring the Central Gateway for DHCP Over VPN
- Configuring DHCP over VPN Remote Gateway
- Current DHCP over VPN Leases

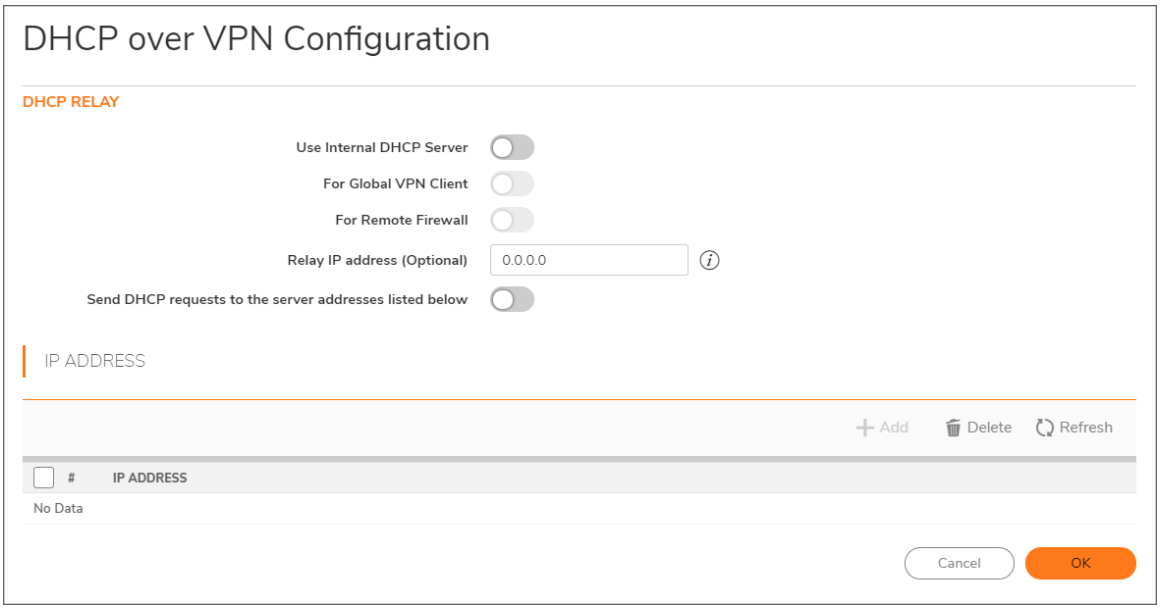
DHCP Relay Mode

The firewall at the remote and central sites are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The firewall at the remote site (**Remote**) passes DHCP broadcast packets through its VPN tunnel. The firewall at the central site (**Central**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

Configuring the Central Gateway for DHCP Over VPN

To configure DHCP over VPN for the Central Gateway:

1. Select **NETWORK | IPSec VPN > DHCP over VPN**.
2. Select **Central** from the **Gateway** drop-down menu.
3. Click **Configure**.



4. Select one of the following:
   - If you want to use the DHCP Server for global VPN clients or for a remote firewall or for both, select the **Use Internal DHCP Server** option.
     - To use the DHCP Server for global VPN clients, select the **For Global VPN Clients** option.
     - To use the DHCP Server for a remote firewall, select the **For Remote Firewall** option.
   - If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
     1. Click **+Add**.
     2. Type the IP addresses of DHCP servers in the **IP Address** field.
     3. Click **OK**. The firewall now directs DHCP requests to the specified servers.
5. Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

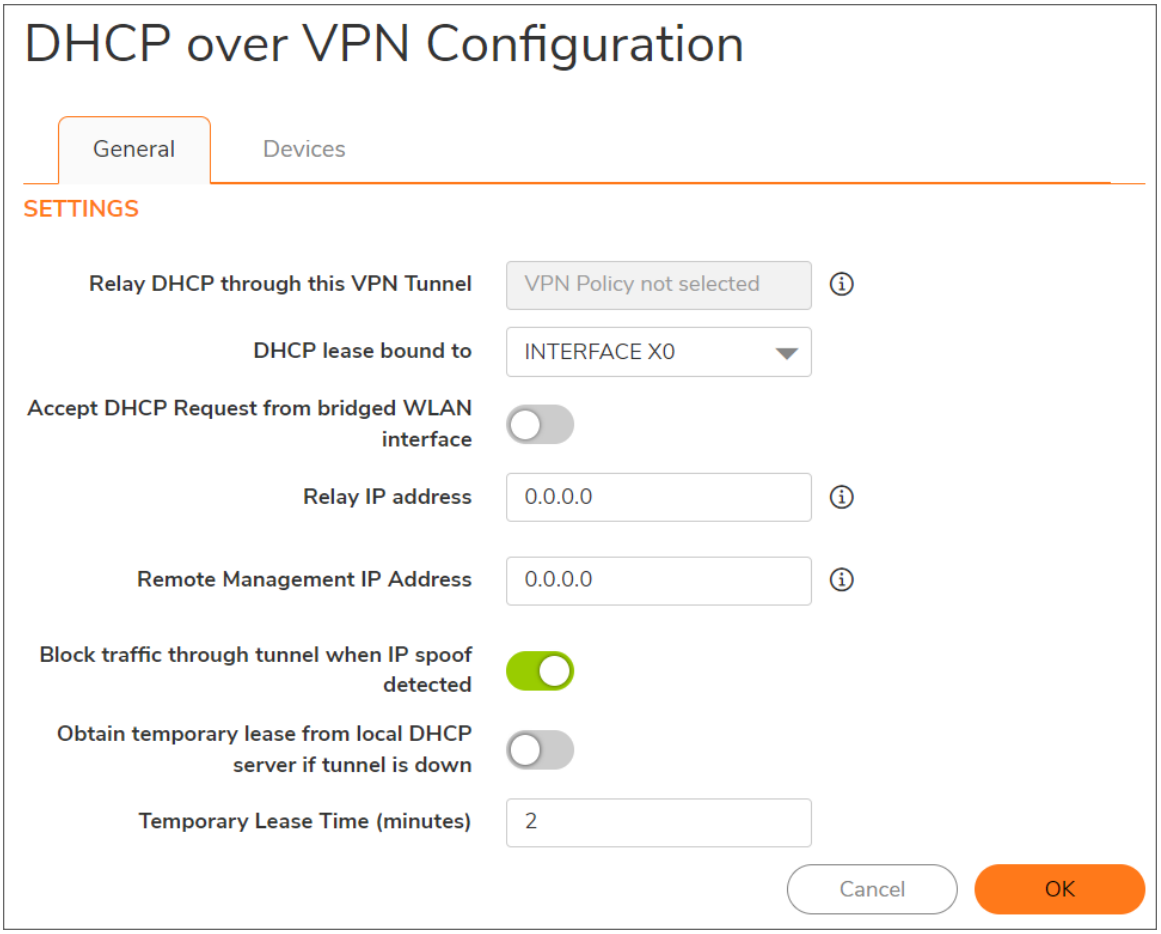
When set, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of this SonicWall's LAN IP address. This address is only used when no Relay IP Address has been set on the Remote Gateway, and must be reserved in the DHCP scope on the DHCP server.

6. Click **OK**.

Configuring DHCP over VPN Remote Gateway

To configure DHCP over VPN Remote Gateway:

1. Select **Remote** from the **Gateway** drop-down menu.
2. Click **Configure**.

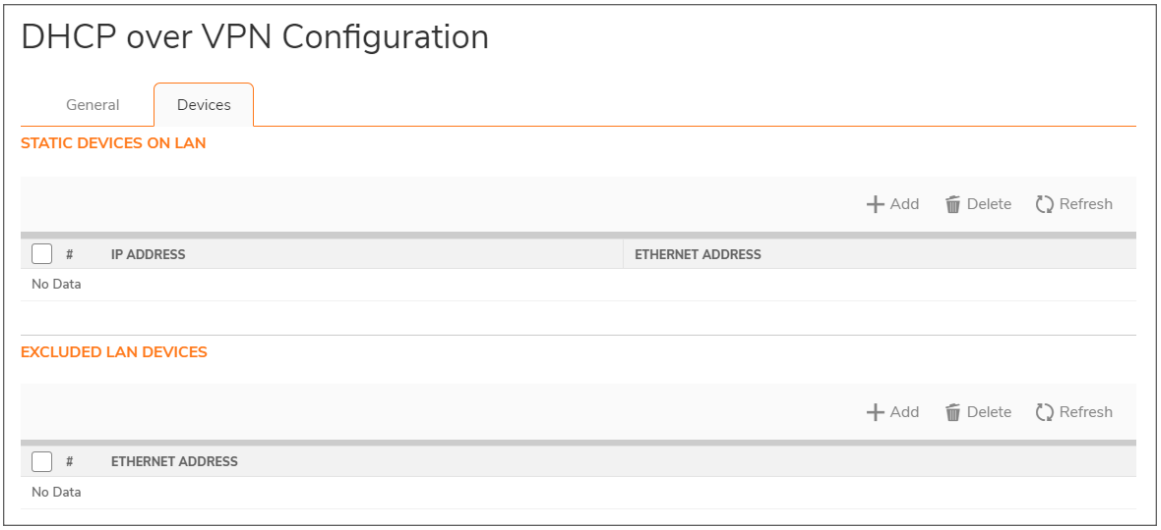


3. On the **General** screen, the VPN policy name is automatically displayed in the **Relay DHCP through this VPN Tunnel** field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.

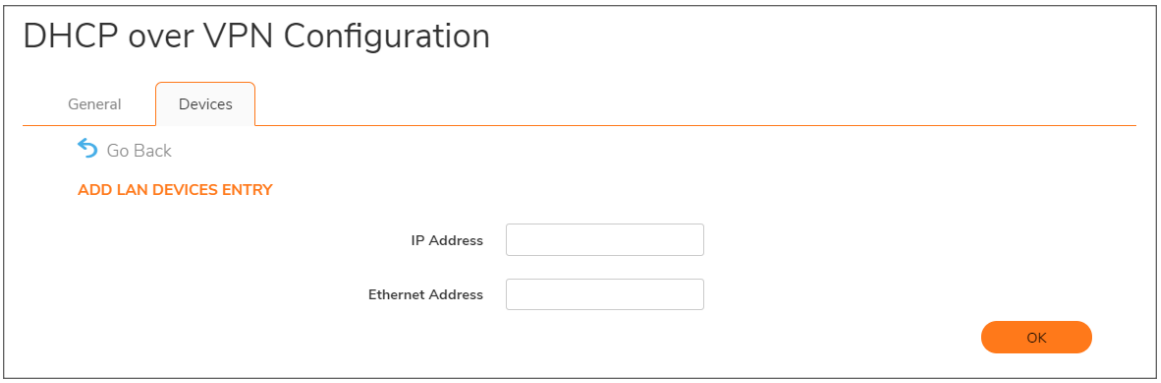
NOTE: Only VPN policies using IKE can be used as VPN tunnels for DHCP. The VPN tunnel must use IKE and the local network must be set appropriately. The local network obtains IP addresses using DHCP through this VPN Tunnel.

4. Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.
5. If you enter an IP address in the **Relay IP Address** field, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of the Central Gateway's address and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this firewall remotely through the VPN tunnel from behind the Central Gateway.

   NOTE: The Relay IP address and **Remote Management IP Address** fields cannot be zero if management through the tunnel is required.
6. If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the firewall from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.
7. If you enable **Block traffic through tunnel when IP spoof detected**, the firewall blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the firewall to respond to IP spoofs.
8. If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. After the tunnel is again active, the local DHCP server stops issuing leases. Enable Obtain temporary lease from local DHCP server if tunnel is down. By enabling this checkbox, you have a failover option in case the tunnel ceases to function.
9. If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is 2 minutes.
10. To configure devices on your LAN, click **Devices**.



11. To configure **Static Devices on the LAN**, click **+Add** to display the **Add LAN Devices Entry** dialog.



12. Type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.

    An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses.

13. Click **OK**.
14. To exclude devices on your **LAN**, click **+Add** to display the **Add Excluded LAN Entry** dialog.
15. Enter the MAC address of the device in the **Ethernet Address** field.
16. Click **OK**.
17. Click **OK** to exit the **DHCP over VPN Configuration** dialog.

NOTE: You must configure the local DHCP server on the remote firewall to assign IP leases to these computers.

NOTE: If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.

TIP: If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, that is, two LANs.

NOTE: Wireless clients are assigned an IP address in this subnet. The IP address and a DHCP server are automatically created and assign DHCP addresses.

Current DHCP over VPN Leases

The **Current DHCP over VPN Leases** table shows the details on the current bindings: **IP Address**, **Host Name**, **Ethernet Address, Lease Time**, and **Tunnel Name**. The last column in the table, **Configure**, enables you to configure or delete a table entry (binding) to:

- Edit a binding, click **Edit**.
- Delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Delete** icon. The operation takes a few seconds to complete. When completed, a message confirming the update is displayed at the bottom of the Web browser window.
- Delete all VPN leases, click **Delete All**.

8

L2TP Servers and VPN Client Access

The SonicWall network security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows or Google Android clients. In situations where running the Global VPN Client (GVC) is not possible, you can use the SonicWall L2TP Server to provide secure access to resources behind the firewall.

You can use Layer 2 Tunneling Protocol (L2TP) to create a VPN over public networks. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.

Topics:

- Configuring the L2TP Server
- Viewing Currently Active L2TP Sessions
- Configuring Microsoft Windows L2TP VPN Client Access
- Configuring macOS L2TP VPN Client Access
- Configuring iOS L2TP VPN Client Access

ⓘ **NOTE:** For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server on SonicOS** located on the SonicWall support site: https://www.sonicwall.com/support.

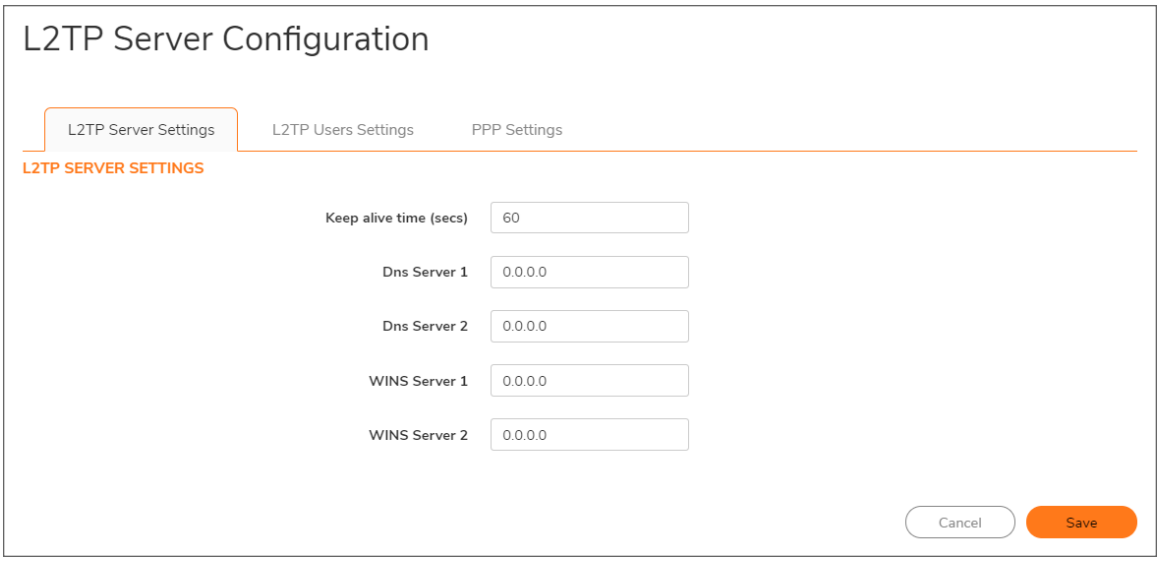
Configuring the L2TP Server

The **NETWORK | IPSec VPN > L2TP Server** page provides the settings for configuring the SonicWall network security appliance as a L2TP Server.

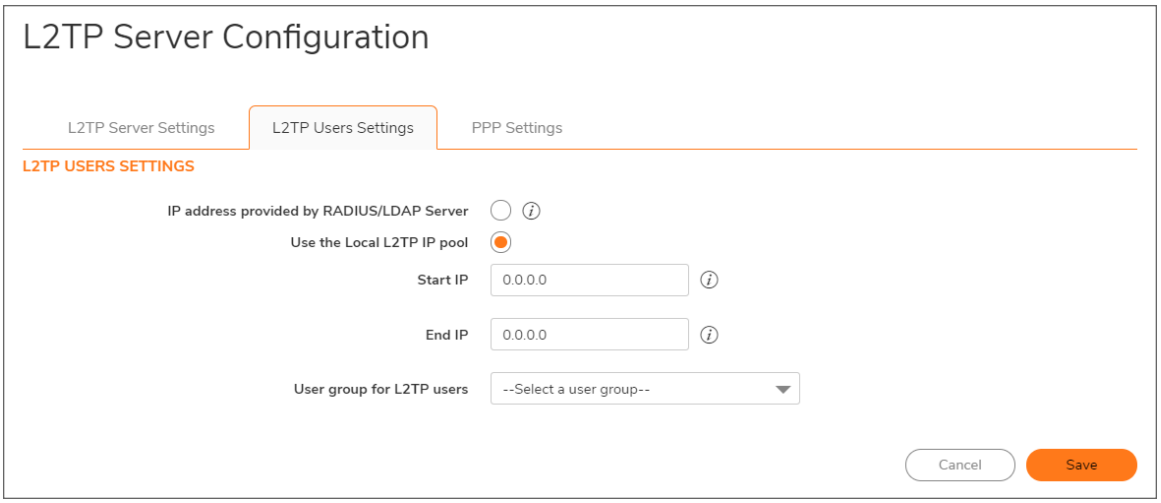
To configure the L2TP Server:

1. Navigate to the **NETWORK | IPSec VPN > L2TP Server** page.
2. Select **Enable L2TP Server**. **Configure** becomes available.

3. Click **Configure** to display the **L2TP Server Configuration** dialog.



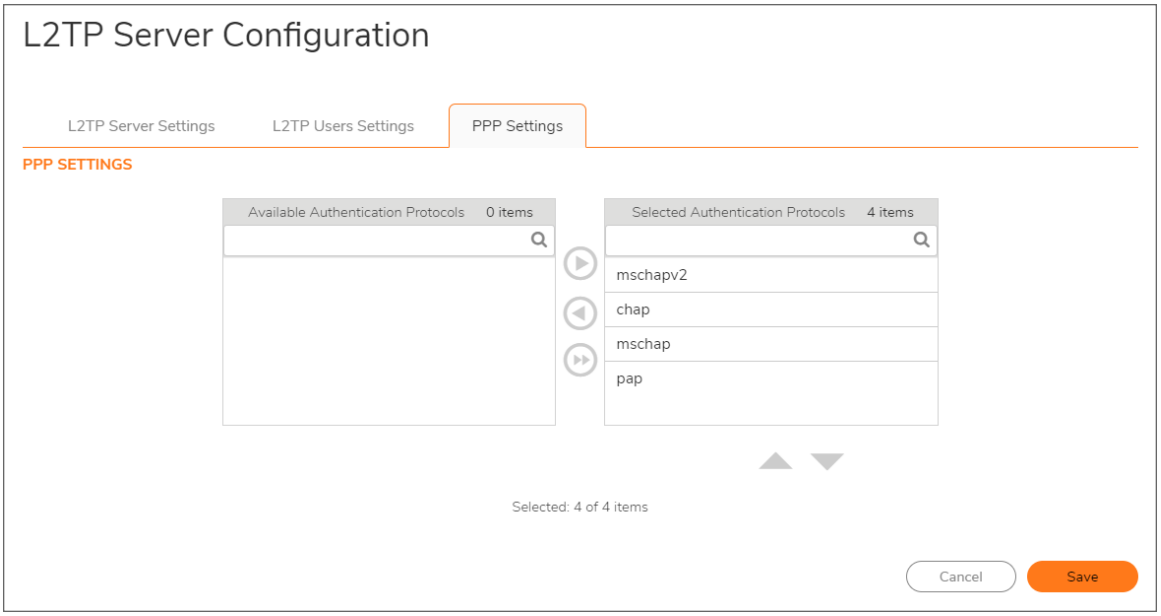
4. On the **L2TP Server** screen, enter a value, in seconds, in the **Keep alive time (secs)** field. This specifies how often special packets are sent to keep the connection open. The default is **60** seconds.
5. Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.
6. Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.
7. Click **L2TP User Settings**.



8. Select one of the following radio buttons for IP address settings:

IP address provided by RADIUS/LDAP Server	By default, this option is not selected. Choose it if a RADIUS/LDAP server provides IP addressing information to the L2TP clients. The **Start IP** and **End IP** fields are no longer active. ⓘ **NOTE:** To use this option RADIUS or LDAP authentication must be selected on the **DEVICE | Users > Settings** page. If this option is selected, an informational message to this effect is displayed. click **OK**.
Use the Local L2TP IP Pool	This is the default IP address setting. Choose it if the L2TP Server provides IP addresses. Enter the range of private IP addresses on the LAN in the **Start IP** and **End IP** fields.

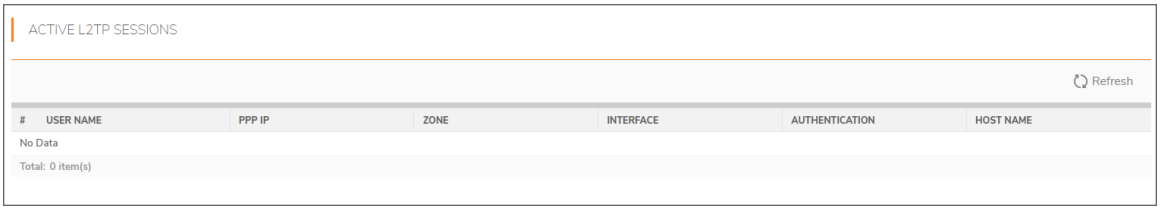
9. If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.
10. Click **PPP Settings**.



11. Select an authentication protocol and click **+Add** to add it. You can also remove authentication protocols or rearrange the order of authentication.
12. Click **OK**.

Viewing Currently Active L2TP Sessions

The **Active L2TP Sessions** section displays the currently active L2TP sessions.



The following information is displayed:

User Name	The user name assigned in the local user database or the RADIUS user database.
PPP IP	The source IP address of the connection.
Zone	The zone used by the L2TP client.
Interface	The interface used to access the L2TP Server, whether it is a VPN client or another firewall.
Authentication	Type of authentication used by the L2TP client.
Host Name	The name of the L2TP client connecting to the L2TP Server.

Configuring Microsoft Windows L2TP VPN Client Access

This provides an example for configuring L2TP client access to the WAN GroupVPN SA using the built-in L2TP Server and Microsoft's L2TP VPN Client.

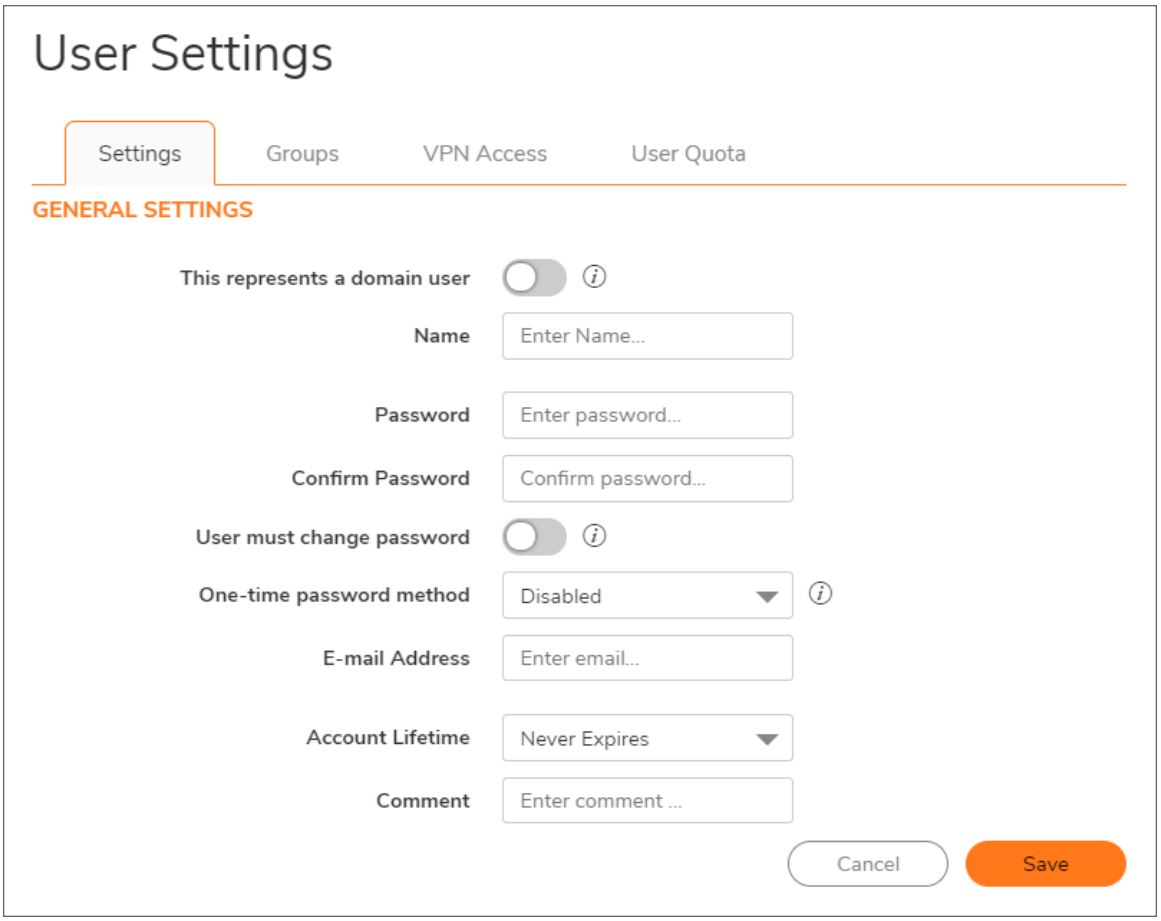
NOTE: SonicOS supports only X.509 certificates for L2TP clients; PKCS #7 encoded X.509 certificates are not supported in SonicOS for L2TP connections.

To enable Microsoft L2TP VPN Client access to the WAN GroupVPN SA:

1. Navigate to the **NETWORK | VPN > Rules and Settings** page.
2. For the **WAN GroupVPN** policy, click the **Edit** icon in the **Configure** column.
3. On the **General** screen, select **IKE using Preshared Secret** for the Authentication Method.
4. Enter a shared secret passphrase in the **Shared Secret** field to complete the client policy configuration.
5. Click **Save**.
6. Navigate to the **NETWORK | IPSec VPN > L2TP Server** page.
7. In the **L2TP Server** section, select **Enable L2TP Server**.
8. Click **Configure**.
9. Provide the following L2TP Server Settings:
    - **Keep alive time (secs)**: 60
    - **DNS Server 1**: 199.2.252.10 (or use your ISP's DNS)

- **DNS Server 2**: 4.2.2.2 (or use your ISP's DNS)
- **DNS Server 3**: 0.0.0.0 (or use your ISP's DNS)
- **WINS Server 1**: 0.0.0.0 (or use your WINS IP)
- **WINS Server 2**: 0.0.0.0 (or use your WINS IP)

10. Click **L2TP Users Settings**.
11. Set the following options:
    - **IP address provided by RADIUS/LDAP Server** if a RADIUS/LDAP Server provides IP addressing information to the L2TP clients. If the L2TP Server provides IP addresses, select **Use the Local L2TP IP pool**.
    - **Use the Local L2TP IP pool**: Enabled (selected; the default)
    - **Start IP**: 10.20.0.1 (use your own IP)
    - **End IP**: 10.20.0.20 (use your own IP)
12. Select **Trusted Users** from the **User group for L2TP users** drop-down menu.
13. Click **Save**.
14. Navigate to the **DEVICE | Users > Local Users & Groups** page.
15. Click **Local Users**.
16. Click **+Add User** to display the **User Settings** dialog.



17. Specify a user name and password in the **Name**, **Password**, and **Confirm Password** fields.
18. Click **Save**.

> **NOTE:** By editing the VPN > LAN access rule or another VPN access rule (under **POLICY | Rules and Policies > Access Rules**), you can restrict network access for L2TP clients. To locate a rule to edit, select the **All Types** view on the **Access Rules** table and look at the **Source** column for **L2TP IP Pool**.

   a. On your Microsoft Windows computer, complete the following L2TP VPN Client configuration to enable secure access:
   b. Navigate to the **Start > Control Panel > Network and Sharing Center**.
   c. Open the **New Connection Wizard**.
   d. Choose **Connect to a workplace**.
   e. Click **Next**.
   f. Choose **Virtual Private Network Connection**. Click **Next**.
   g. Enter a name for your VPN connection. Click **Next**.

h. Enter the Public (WAN) IP address of the firewall. Alternatively, you can use a domain name that points to the firewall.

i. Click **Next**, and then click **Finish**.

j. In the Connection window, click **Properties**.

k. Click **Security**.

l. Click on **IPSec Settings**.

m. Enable **Use preshared key for authentication**.

n. Enter your preshared secret key and click **OK**.

o. Click **Networking**.

p. Change **Type of VPN** from **Automatic to L2TP IPSec VPN**.

q. Click **OK**.

r. Enter your XAUTH username and password.

s. Click **Connect**.

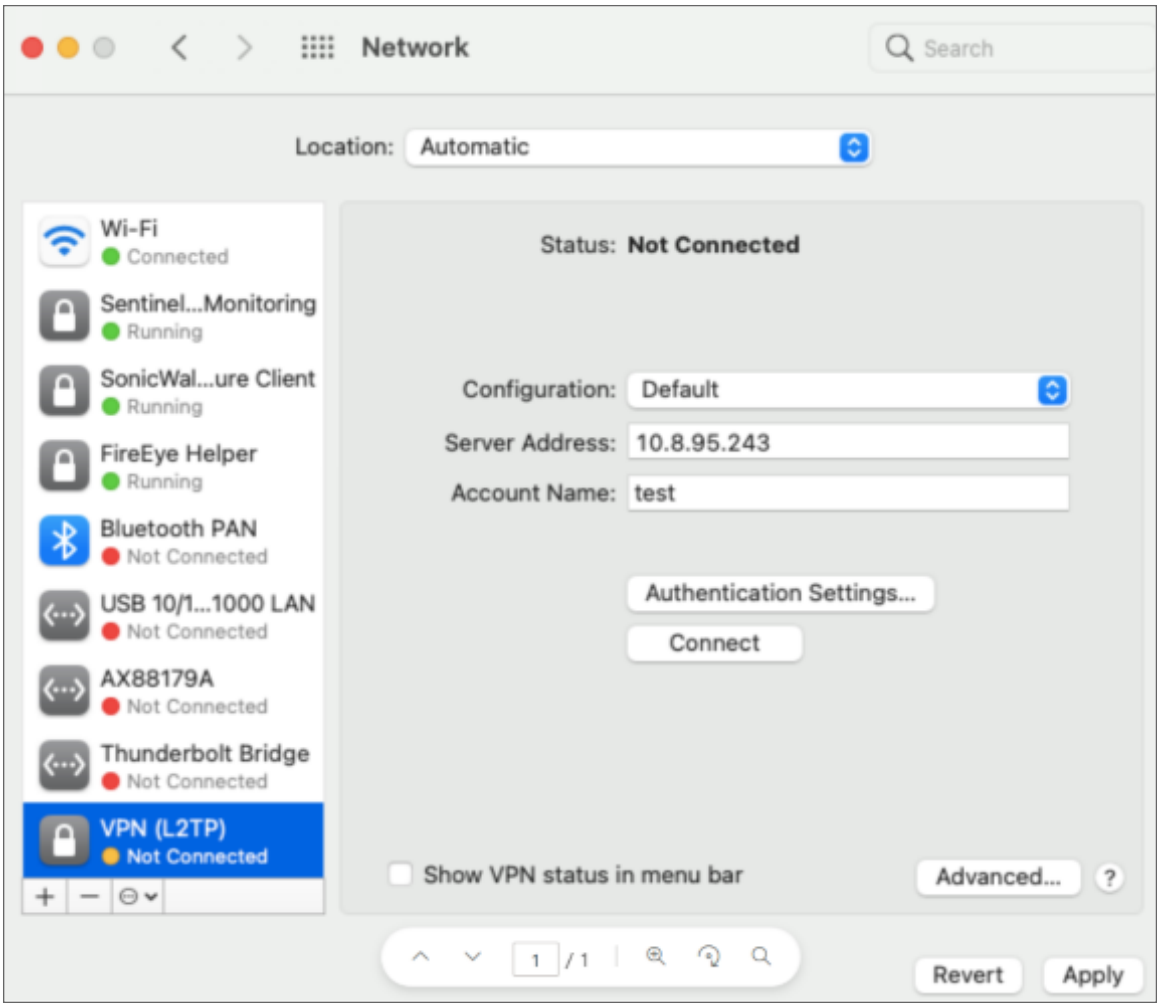
19. Verify your Microsoft Windows L2TP VPN device is connected by navigating to the **NETWORK | IPSec VPN > Rules and Settings** page. The VPN client is displayed in the **Currently Active VPN Tunnels** section.

Configuring macOS L2TP VPN Client Access

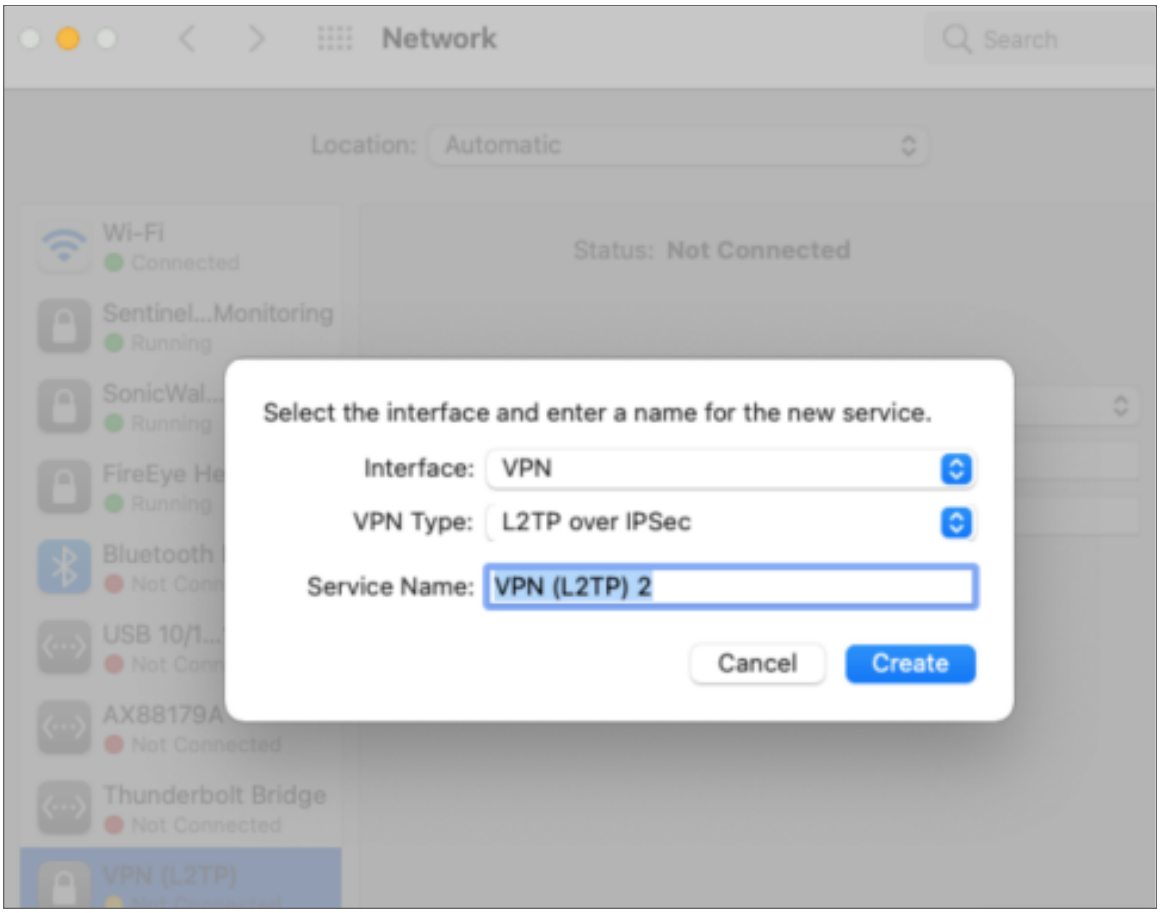
This provides an example for configuring L2TP client access on macOS.

To configure L2TP clients on macOS:

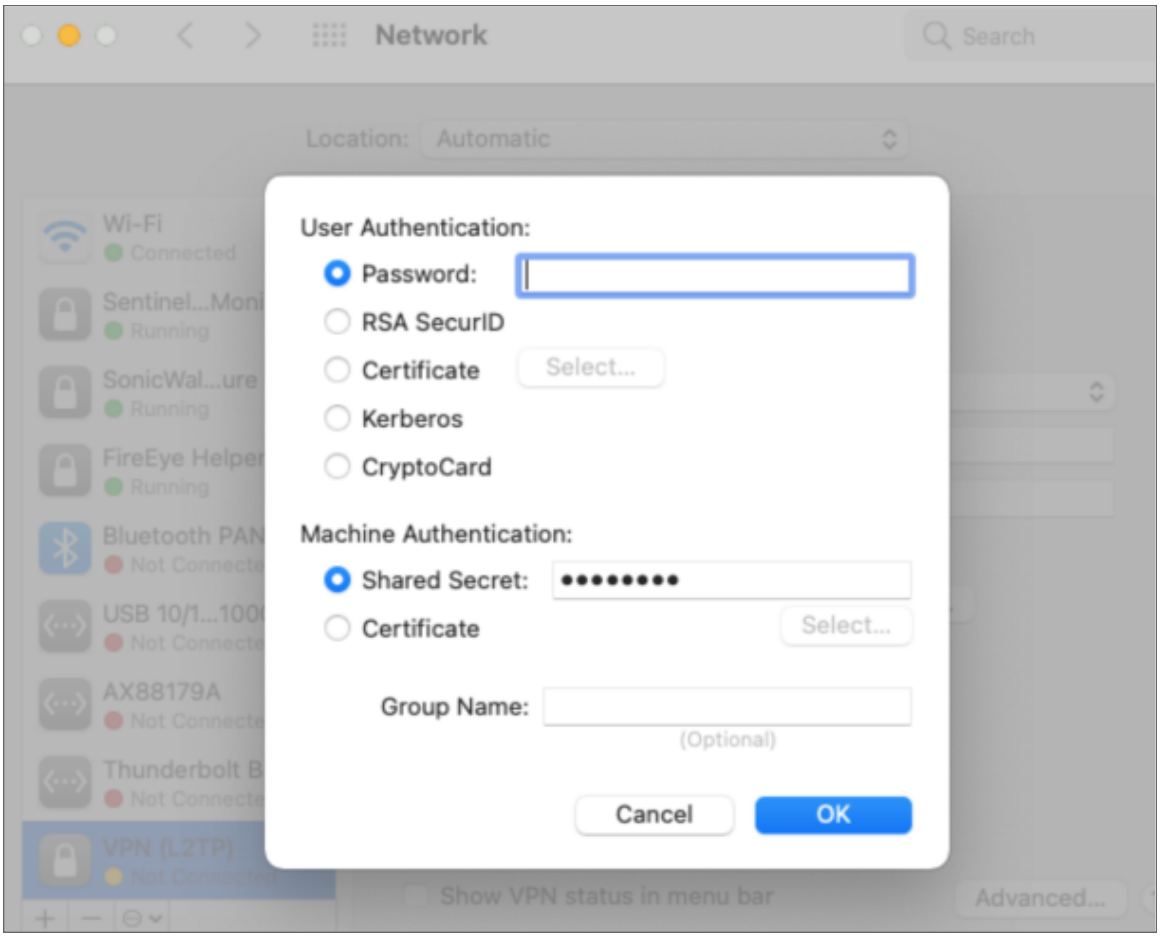
1. Click on **System Preferences** icon.
2. On the **System Preferences** window, click on **Network** icon. The **Network** page is displayed.



3. Click on the + icon to create L2TP VPN Connection.



4. Select the VPN option for the **Interface** field.
5. Select L2TP over IPSec for the **VPN Type** option.
6. Add the name in the Service Name field.
7. Click **Create**.
8. Specify the User Authentication details in the next window. Select **Password** from the **User Authentication** options and specify your account password that was created on SonicWall.



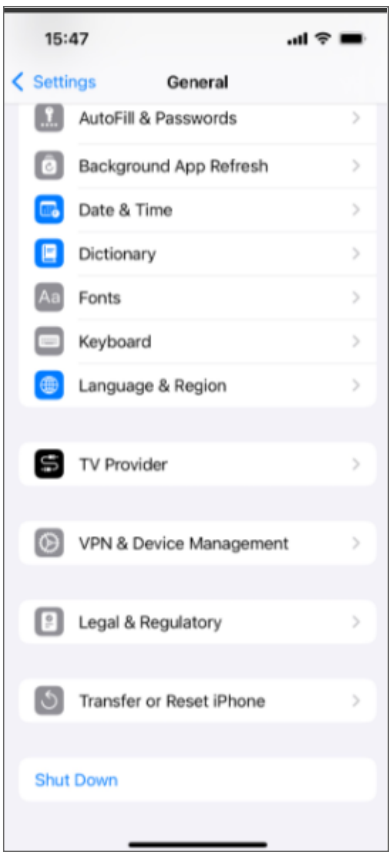
9. Select **Shared Secret** from the **Machine Authentication** options.
10. Click **OK**.

Configuring iOS L2TP VPN Client Access

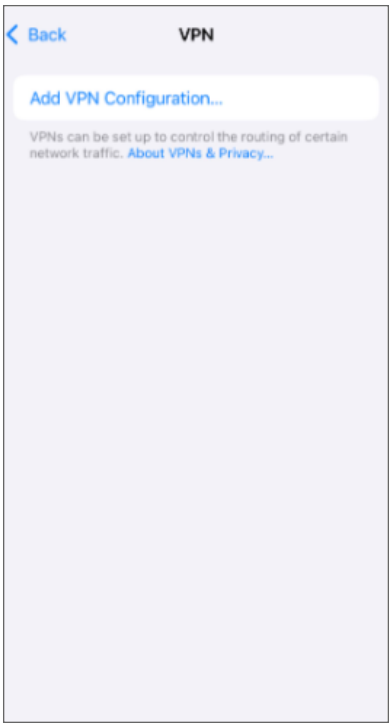
This provides an example for configuring L2TP client access on iOS.

To configure L2TP clients on iOS:

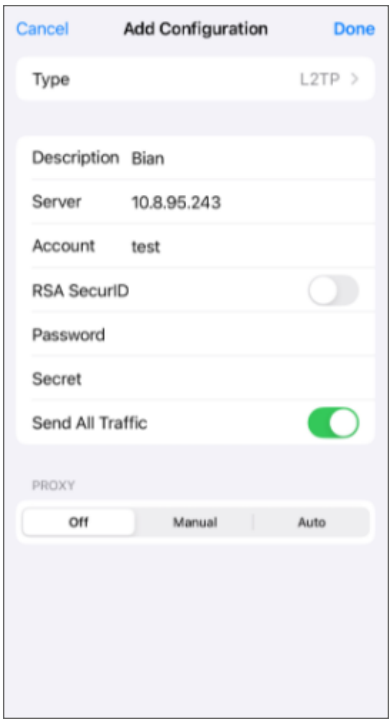
1. Navigate to **Settings > General.**



2. On the **General** page, click on **VPN Device Management**. The VPN screen is displayed.



3. On the **VPN** screen, click on **Add VPN Configuration** option. The **Add Configuration** page is displayed.



4. Specify the details of **Server**, **Account**, **Password**, and **Secret** for mapping. The **Secret** to be specified here is the **Shared Secret** on the **VPN Group Policy** page of the firewall.

5. Click **Done**.

9

AWS VPN

The AWS VPN page makes it easy to create VPN connection from the SonicWall firewall to Virtual Private Clouds (VPCs) on Amazon Web Services (AWS). For more information about Amazon Virtual Private Cloud, refer to https://aws.amazon.com/vpc/.

IMPORTANT: Before setting up AWS VPN, be sure to configure the firewall with the AWS credentials that it needs to use. Navigate to **NETWORK | System > AWS Configuration** to do this. In addition, click **Test Configuration** to validate the settings before proceeding.

Topics:

- Overview
- Creating a New VPN Connection
- Reviewing the VPN Connection
- Route Propagation
- AWS Regions
- Deleting VPN Connections

Overview

To get to AWS VPN, navigate to **NETWORK | IPSec VPN > AWS VPN**. The **AWS VPN** page is dominated by a table showing the VPCs in the AWS regions of interest. Each row in the table can be expanded to show the subnets, organized by route table, for the VPC. Other columns in the table show status information, and the buttons can be used to create and delete VPN connections to the corresponding VPC.

The table on the firewall's AWS VPN page reflects the VPC information that is available on the AWS Console under the **VPC Dashboard**.

Creating a New VPN Connection

Creating a new VPN Connection from the firewall is relatively simple. To start the process, simply click **CREATE VPN CONNECTION** on the appropriate row for the Amazon VPC that you wish to connect to the firewall.

The **New VPN Connection** window appears. Provide the public IP address of the firewall as seen from AWS. Code running on AWS attempts to detect the address and prepopulate the text input field. Verify that the address is reachable from outside the local network. If the firewall is behind a router or some other proxy, NAT rules should be put in place to ensure VPN traffic initiated from the AWS side can route back to the firewall.

ⓘ **NOTE:** In some circumstances, you might be asked whether to enable Route Propagation. Refer to *Route Propagation* for more information.

The IP address you entered is used as the Customer Gateway. Click **OK** to close the dialog and initiate a series of processes that configure both the firewall and AWS in order to establish a VPN Connection between them.

Messages appear in the table row for the VPC that is the subject of the new VPN Connection, keeping you informed of the progress at the different stages.

If an error occurs at any stage, a message appears with details of the problem and all the changes that have been made are reversed. This should allow you to correct any issues and try again.

Reviewing the VPN Connection

After creating a new VPN connection between the firewall and a VPC on AWS, you can view details of how the process changed their respective configurations.

On the firewall, navigate to **NETWORK | IPSec VPN > AWS VPN**. Find the row in the VPC table corresponding to the AWS VPC in question and click Information.

ⓘ **NOTE:** Because the VPN connection has only just been created, the status is reported as still **pending**. Use Refresh on the AWS VPN page to reload the data in the table and on the associated VPN Connection Details window.

The following sections describe the configuration on the firewall and on AWS.

- Configuration on the Firewall
- Configuration on Amazon Web Services

Configuration on the Firewall

As part of the process to create a new VPN connection, an Address Object representing the VPC is added and can be viewed in SonicOS on the **Address Objects** page. Navigate to **OBJECT | Match Objects > Addresses**. The convention used to name the object combines the AWS IDs of the VPN connection and the VPC itself. The Address Object is a network type, with the network being that of the remote VPC.

Two VPN policies are also created, showing that AWS uses two VPNs per VPN connection to provide redundancy for a failover mechanism. Navigate to **NETWORK | IPSec VPN > Rules and Settings**. The VPN policy names used on the firewall are based on the AWS ID for the connection along with a suffix to differentiate between the two policies.

Matching the two VPN policies, two tunnel interfaces are created. Navigate to **NETWORK | System > Interfaces**. They also use a naming convention based on the ID of the VPN Connection.

Similarly, two route policies are created, both using the Address Object representing the VPC as their destination. Navigate to **NETWORK | System > Dynamic Routing**. Each one uses a different tunnel interface.

Configuration on Amazon Web Services

The process of creating a VPN Connection from the AWS VPN page in the firewall GUI also makes changes to the configuration on AWS. Using the AWS Console, under the VPC Dashboard, view VPN connections. Using the VPC ID as a filter, find the VPN connection that was created.

The customer gateway, the endpoint at the firewall, and the IP address specified when first creating the VPN connection can also be viewed on the AWS Console. Navigate to the Customer Gateways page, under the **VPC Dashboard**.

Route Propagation

Additional steps need to be taken to ensure connections can be made to and from resources on subnets within a particular VPC. You must also propagate the connections to the route table that is used for the subnet of interest. Three ways can be used to enable propagation to the route tables in a VPC.

- When Creating the VPN Connection

  If the firewall detects that route propagation is disabled for one or more route tables within a VPC, the popup dialog includes a checkbox allowing you to specify that Route Propagation should be enabled for all route tables within that VPC. However, this is not a a consistent approach; it does allows propagation for some route tables and not others.

- Using checkboxes for each route table

  After a VPN connection has been established, expanding a row in the VPC table on the AWS VPN page reveals all of the subnets in that VPC, organized by route table. Each route table row includes a checkbox that can be used to enable or disable propagation for that particular route table and the subnets it governs.

- On the AWS Console

  The subnets for each VPC can be viewed on the subnets page under the VPC Dashboard on the AWS Console. Selecting a subnet identifies the governing route table and provides a hyperlink so that you can jump to the relevant page.

  Otherwise, you can navigate to the Route Table page and use the filter to narrow the search by VPC or subnet.

To enable or disable route propagation to a specific route table:

1. Select the route table in question.
2. Click the **Route Propagation** tab.
3. Click **Edit**.
4. Check or uncheck the **Propagate** box as appropriate.
5. Click **Save** to commit your changes.

AWS Regions

Resources on Amazon Web Services are distributed across a number of AWS regions. A customer can have VPCs in any or all regions. The AWS VPN page includes a drop-down control allowing you to select one or more regions of interest. The VPCs from all selected regions are displayed in the table and new VPN connections can be made to any of those VPCs.

The region selection control is initialized with the default region as specified on the AWS configuration and is used to send firewall logs to AWS CloudWatch Logs on the AWS Logs page. Regardless of the initial selection, you can choose which regions from which to show the associated VPCs in the table.

Deleting VPN Connections

The AWS VPN page includes a facility for removing unwanted VPN Connections.

For VPCs that have a corresponding VPN Connection, the button in the related table row in the VPC table changes from a **Create VPN Connection** function to **Delete VPN Connection.** After clicking the button, the system asks for confirmation and then initiates a process that deletes as many configuration settings as it safe to do without affecting other VPN connections from this or other firewalls. It removes the associated VPN and route policies, and the tunnel interfaces on the firewall. On AWS, it removes the Customer Gateway, but only if it is not being used elsewhere (perhaps on other VPN Connections from the same firewall but to other VPCs). It does not delete the VPN gateway or change the route propagation settings.

10

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University
    - For Technical Certifications
    - For Training and Assets

About This Document

SonicOS IPSec VPN Administration Guide
Updated - July 2026
Software Version - 8
232-006187-00 Rev C

Copyright © 2026 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035