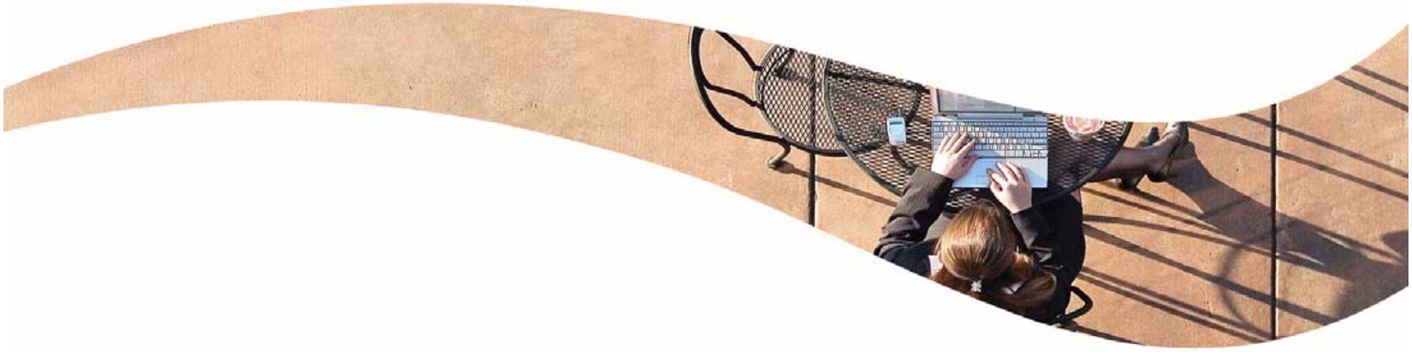


SonicOS Enhanced 3.2
IKE Version 2 Support

Document Scope

This document describes the changes to SonicOS Enhanced 3.2 to include support of the new IKEv2 standard for creating IPsec VPN tunnels. The document gives a brief overview of IPsec VPNs, describes the new features added to SonicOS Enhanced 3.2, and details the procedures for configuring VPNs.

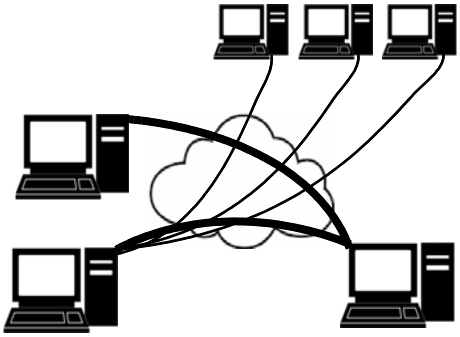
This document contains the following sections:

IKE VPN Overview

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 provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.

A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the internet. Because this tunnel is not a physical connection, it is more flexible--you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing internet infrastructure.



VPN Terms

- *AH* - Authentication Header protocol - an Internet protocol offering data integrity and data origin authentication with optional anti-replay protection.
- *Certificate* - an ISO standard defined in recommendation X.509 for binding public/private cryptographic keys to an identity. Certificates may be exchanged by IKE peers to provide authentication during IKE_SA establishment.
- *CHILD_SA* - Security Association for ESP or AH set up via the IKE_SA.
- *Crypto Suite* - complete set of algorithms used to protect an SA.

- *DOS* - Denial of Service - an attack wherein resources are consumed by spurious messages received at an excessive rate. DOS is especially effective if the attacker can induce the victim to perform actions which further consume resources, for instance, computationally intensive tasks or large memory allocations.
- *ESP* - Encapsulating Security Payload protocol - an Internet protocol offering data integrity, confidentiality, and origin authentication with optional anti-replay protection.
- *IKE* - Internet Key Exchange protocol- IKE is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations (SAs).
- *IKEv2* - Internet Key Exchange protocol version 2 - Version 2 of the IKE specification combines ISAKMP (RFC 2408), IKE (RFC 2409), the Internet DOI (RFC 2407), NAT Traversal, Legacy authentication, and remote address acquisition. IKEv2 does not interoperate with version 1, but has a shared header format allowing both versions to unambiguously run over the same UDP port.
- *IKE_SA* - IKE Security Association - the Security Association that provides security services for the IKE protocol itself.
- *Pre-Shared Key* - Cryptographic keying material pre-configured at each end of an IKE Security Association that is used to authenticate the IKE peers and in the generation of keying materials.
- *Security Association* - a simplex “connection” that affords security services to the traffic carried by it. Security Associations are created in pairs to provide bi-directional communication.

VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN**: IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

  IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

  SonicOS supports the creation and management of IPsec VPNs.
- **SSL VPN**: Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SSL VPN 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 SSL-VPN devices that you can use in concert with or independently of a SonicWALL UTM appliance running SonicOS. For information on SonicWALL SSL-VPN devices, see the SonicWALL Website: <http://www.sonicwall.com/products/ssl-vpn2000.html>

VPN Security

IPsec VPN traffic is secured in two stages:

- **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.
- **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 Enhanced supports two versions of IKE, version 1 and version 2.

IKE v1

IKE v1 uses a two phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel.
- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys.

IKE Phase 1

In IKE v1, there are two modes of exchanging authentication information: Main Mode and Aggressive Mode.

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-Helman 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 algorithms 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.

IKE Phase 2

In IKE phase 2, 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 rekeying is needed.

The two types of security for individual packets are:

- **Encryption Secured 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 authentic 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
- 3DES
- AES-128
- AES-192
- AES-256

Note You can find more information about IKE v1 in the three specifications that define initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the web at:
<http://rfc.net/rfc2407.html>
<http://rfc.net/rfc2408.html>
<http://rfc.net/rfc2409.html>

IKEv2

IKE version 2 is a new protocol for negotiating and establishing SAs. IKE v2 features improved security, a simplified architecture, and enhanced support for remote users. In addition, IKE v2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKE V2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode. This reduces the delays during rekeying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKE v2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

IKE v2 is not compatible with IKE v1. If using IKE v2, all nodes in the VPN must use IKE v2 to establish the tunnels.

SAs in IKE v2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Note There is no restriction on nesting IKE v1 tunnels within an IKE v2 tunnel and visa-versa. For example, if you are connecting to a wireless device using WiFiSec, which uses an IKE v1 tunnel, you can then connect over the internet to a corporate network using a site-to-site VPN tunnel established with IKE v2.

Initialization and Authentication in IKE v2

IKE v2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- Initialize communication: The first pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.

1. Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.
2. Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.

- Authenticate: The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.

3. Initiator identity proof, such as a shared secret or a certificate, and a request to establish a child SA.
4. Responder sends the matching identity proof and completes negotiation of a child SA.

Negotiating SAs in IKE v2

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKE v1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

1. Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.
2. Responder sends the accepted child SA offer and, if encryption information was included, a public key.

Note You can find more information about IKE v2 in the specification, RFC 4306, available on the web at: <http://rfc.net/rfc4306.html>

IKE VPN Features Added in SonicOS Enhanced 3.2

The following features have been added to enable IKEv2 support:

- Selection of IKEv2 Exchange Mode
- Disabling Trigger Packets
- Selecting Cookie Notify Protection
- Prevention of Certificate Authentication Mode with IKEv2
- Prevention of Secondary Gateway Selection
- Prevention of XAUTH
- Minor Modifications Common to both IKEv1 and IKEv2

The following features have been added to enhance configuration and management of VPNs using either IKEv1 or IKEv2:

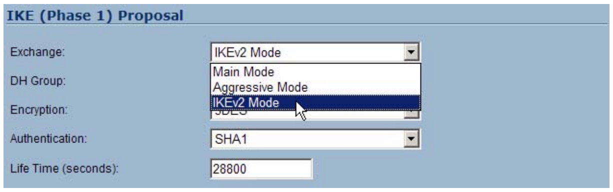
- Addition of an IKE Authentication section to the General tab
- Changing the IPSec Keying Mode label to Authentication Method
- Hiding the entered Shared Secret value and addition of a Confirmed Shared Secret text entry field.
- Hiding the OCSP Responder URL text entry section if OCSP is not enabled
- Hiding the Ignore DF (Don't Fragment) Bit checkbox if fragmented packet handling is not enabled

Selection of IKEv2 Exchange Mode

A new selection is added to the **VPN Policy** > **Proposals** > **Exchange** drop list to allow selection of *IKEv2 Mode*. Selection of the option sets a new exchange type which is ultimately submitted to the SonicWALL device. This selection also causes several changes in the appearance of GUI: fields and options are hidden or displayed to allow selection of certain IKEv2 options or to prevent selection of features not supported in this IKEv2 release.

Usage

Navigate to the **VPN** > **Settings** page and either edit an existing policy or add a new policy. **Note**: IKEv2 is not supported in any of the *GroupVPN* policies. In the popup window, select the **Proposals** tab and click on the **Exchange** drop list. Select *IKEv2 Mode* to enable the IKEv2 exchange for the policy.



IKE (Phase 1) Proposal

Exchange: IKEv2 Mode

DH Group:

Encryption:

Authentication: SHA1

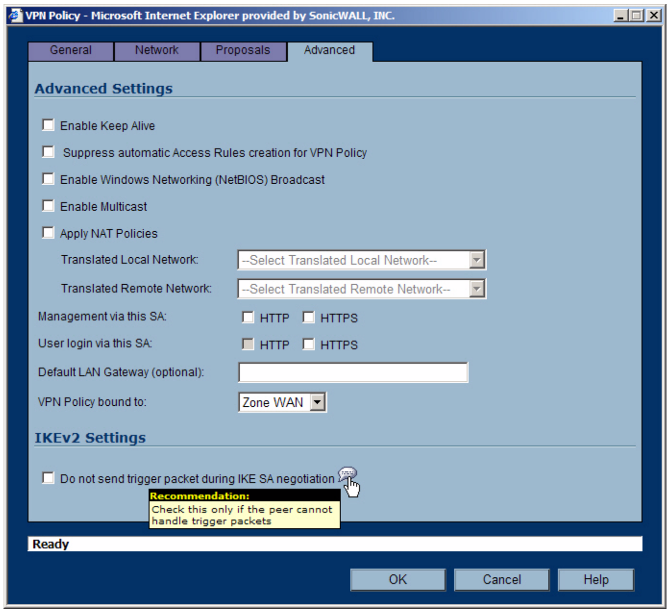
Life Time (seconds): 28800

Disabling Trigger Packets

The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers. An *IKEv2 Settings* section is added to the **Advanced** tab when *IKEv2 Mode* has been selected. This section contains a checkbox which prevents inclusion of *Trigger Packet* payloads when selected. This checkbox is cleared by default and should only be selected when required for interoperability.

Usage

On the **VPN Policy** popup window’s **Advanced** tab, click in the *Do not send trigger packet during IKE SA negotiation* checkbox to disable this option.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

Advanced Settings

☐ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

☐ Apply NAT Policies

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

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

Management via this SA: ☐ HTTP ☐ HTTPS

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

IKEv2 Settings

☐ Do not send trigger packet during IKE SA negotiation

Recommendation:
Check this only if the peer cannot handle trigger packets

Ready

Selecting Cookie Notify Protection

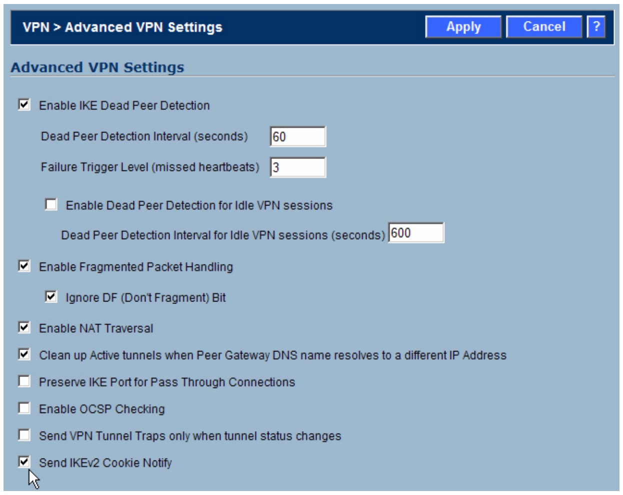
One of the vulnerabilities in IKEv1 is a DOS attack wherein the attacker initiates IKE negotiation from multiple spoofed source IP addresses. The IKE responder must generate Diffie-Hellman values to produce the response. The generation of these values is computationally intensive. In addition, the IKE responder maintains some state attributes for the in-process session including retransmission timers and will attempt retransmission some arbitrary number of times before freeing the resources.

IKEv2 includes a mechanism to combat this type of attack which is referred to as a COOKIE Notify. The IKEv2 responder will send a Notify message of type COOKIE that the Initiator must include when re-initiating the IKE session. The responder can do this in a completely stateless fashion through careful selection of the COOKIE generation algorithm. Even without the stateless generation, Diffie-Hellman generation is avoided unless the Peer proves, via inclusion of the COOKIE, that it can receive messages at the IP address from which IKE was initiated. No retransmissions will be attempted in either case which further conserves resources.

The initial SonicOS 3.2 ENH release of IKEv2 allows Cookie Notify protection to be set on a global basis from the **VPN** > **Advanced** page. An Administrator who believes that the SonicWALL is under attack can enable this protection. Since this protection does add to the total round-trips required to establish an IKEv2 SA, it is disabled by default. However, an Administrator may choose to enable this protection at all times, trading a slight performance hit for increased security.

Usage

To enable IKEv2 Cookie Notify protection, navigate to the **VPN** > **Settings** page. A checkbox entitled *Send IKEv2 Cookie Notify* has been added at the bottom of the page. Clicking in this checkbox will enable Cookie Notify protection on a global basis for all IKEv2 VPN policies.



Advanced VPN Settings

☑ Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds) 60

Failure Trigger Level (missed heartbeats) 3

□ Enable Dead Peer Detection for Idle VPN sessions

Dead Peer Detection Interval for Idle VPN sessions (seconds) 600

☑ Enable Fragmented Packet Handling

☑ Ignore DF (Don't Fragment) Bit

☑ Enable NAT Traversal

☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

□ Preserve IKE Port for Pass Through Connections

□ Enable OCSP Checking

□ Send VPN Tunnel Traps only when tunnel status changes

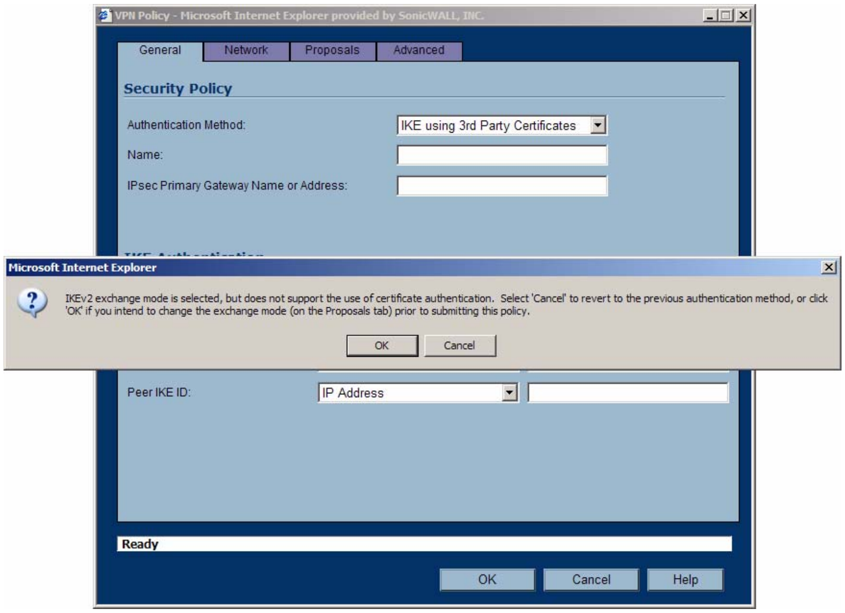
☑ Send IKEv2 Cookie Notify

Prevention of Certificate Authentication Mode with IKEv2

The IKEv2 specification includes Authentication with Digital Signatures just as IKEv1 does, but the initial SonicOS 3.2 ENH IKEv2 feature does not support this authentication method. This method is selected from the **VPN Policy** popup window via a drop list on the **General** tab. An option for *IKE using 3rd Party Certificates* can be selected. If the **Exchange** method selected on the **Proposals** tab is *IKEv2 Mode*, a warning popup will be displayed indicating *Certificates are not supported*. An option to continue or to cancel is provided. If the operation is cancelled, the authentication method will revert to the previously selected method. An Administrator may choose to continue if the exchange mode will be subsequently changed to Main or Aggressive Mode. Similarly, if the authentication method has been set to Certificates and the **Exchange** option on the **Proposals** tab is changed from Main or Aggressive mode to IKEv2 mode, the same warning popup will appear. Canceling the operation will revert to the previously selected mode, but an Administrator has the option to select *IKEv2 Mode* and subsequently change the authentication method. If both *IKEv2 Mode* and *IKE using 3rd Party Certificates* are selected and the VPN Policy is submitted, a popup will appear and the submission will be disallowed.

Usage

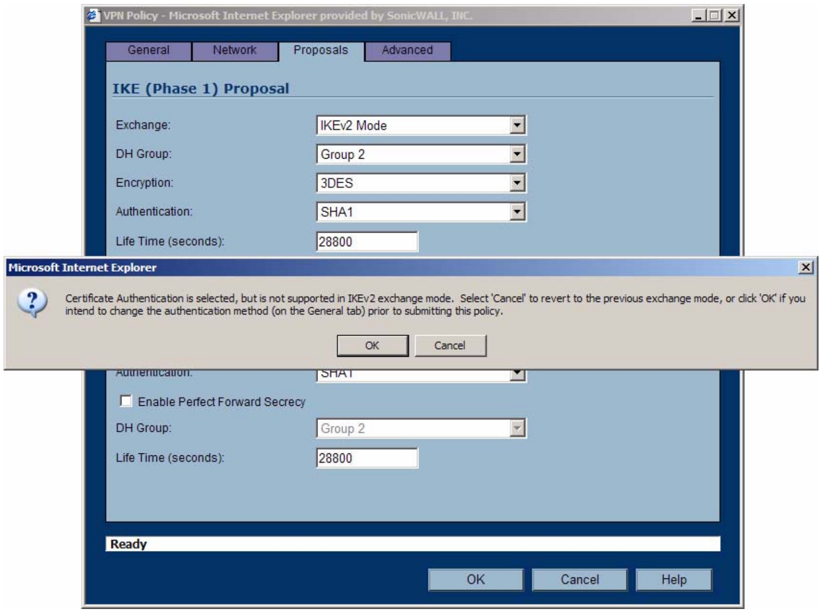
On the **VPN** > **Settings** page, select a VPN policy that is configured for IKEv2. Or, select the **Add** button to create a new policy, select the **Proposals** tab, and select the *IKEv2 Mode* **Exchange** option. On the **General** tab, select the *IKE using 3rd Party Certificates* **Authentication Method**. Since the *IKEv2 Mode* exchange mode has been selected, a popup window will warn *IKEv2 exchange mode is selected, but does not support the use of certificate authentication…*


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Security Policy
Authentication Method:
IKE using 3rd Party Certificates
Name:
IPsec Primary Gateway Name or Address:
Microsoft Internet Explorer
OK
Cancel
Peer IKE ID:
IP Address
Ready
OK
Cancel
Help

IKEv2 exchange mode is selected, but does not support the use of certificate authentication. Select 'Cancel' to revert to the previous authentication method, or click 'OK' if you intend to change the exchange mode (on the Proposals tab) prior to submitting this policy.

Hit the **Cancel** button to revert to the previously selected authentication method. Hit **OK** to choose *IKE using 3rd Party Certificates*. To use Certificates, the IKE exchange mode must be changed to either Main or Aggressive on the **Proposals** tab.

Hit **OK** and then select the **Proposals** tab. Change the **Exchange** option to either *Main Mode* or *Aggressive Mode*. Then select *IKEv2 Mode*. A warning popup will appear stating *Certificate Authentication is selected, but is not supported in IKEv2 exchanged mode…*


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

IKE (Phase 1) Proposal

Exchange: IKEv2 Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Microsoft Internet Explorer

Certificate Authentication is selected, but is not supported in IKEv2 exchange mode. Select 'Cancel' to revert to the previous exchange mode, or click 'OK' if you intend to change the authentication method (on the General tab) prior to submitting this policy.

Authentication: SHA1

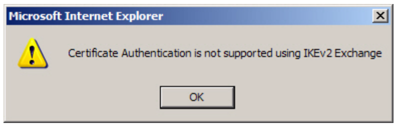
☐ Enable Perfect Forward Secrecy

DH Group: Group 2

Life Time (seconds): 28800

Ready

Hit the **Cancel** button to revert to the previously selected exchange mode. Hit **OK** to switch to IKEv2 mode.



Microsoft Internet Explorer

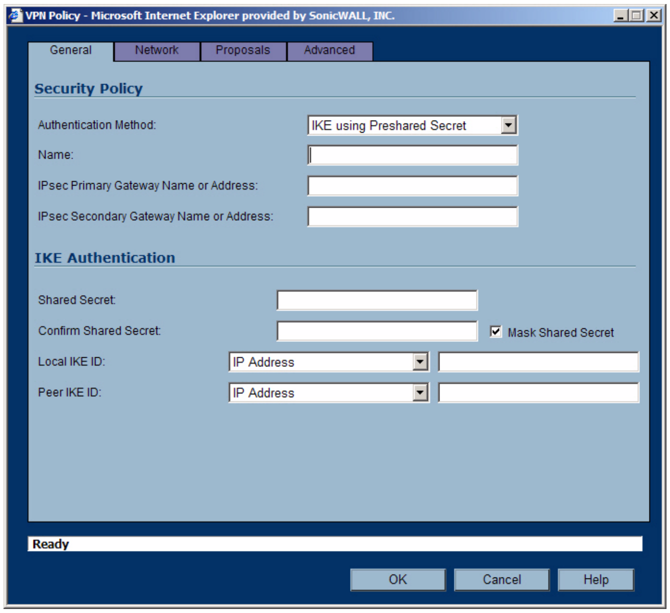
Certificate Authentication is not supported using IKEv2 Exchange

Prevention of Secondary Gateway Selection

When using IKEv1 in a VPN policy, a Secondary Gateway may be entered. If the IKE Peer cannot be reached at the configured Gateway domain name or IP address, the Secondary Gateway configuration will be used to attempt the IKE negotiation. This option is not supported with IKEv2 in SonicOS 3.2 ENH. When the IKEv2 exchange mode is selected, the **IPsec Secondary Gateway Name or Address** text box on the **General** tab will not be displayed.

Usage

If the **Proposals > Exchange** is *Main Mode* or *Aggressive Mode* and the **General > Authentication Method** is *IKE using Preshared Secret* or *IKE using 3rd Party Certificates*, the **IPsec Secondary Gateway Name or Address** text field is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Security Policy

Authentication Method: IKE using Preshared Secret

Name:

IPsec Primary Gateway Name or Address:

IPsec Secondary Gateway Name or Address:

IKE Authentication

Shared Secret:

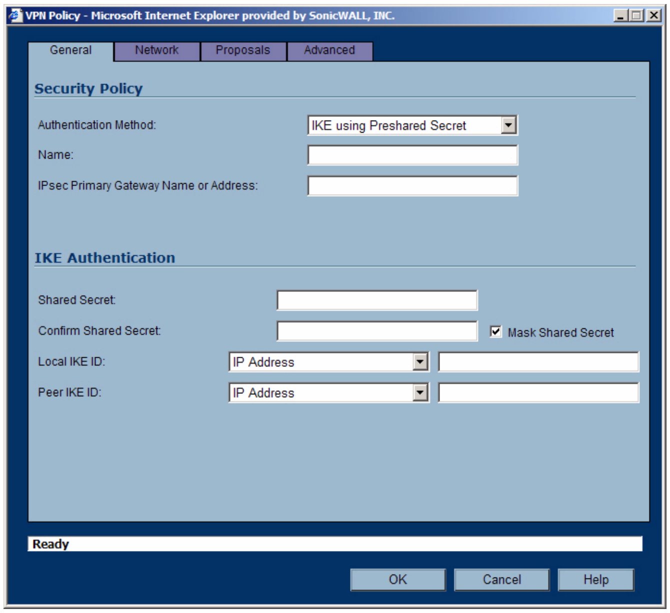
Confirm Shared Secret: ☑ Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

Ready

If the **Proposals > Exchange** is *IKEv2 Mode* and the **General > Authentication Method** is *IKE using Preshared Secret* or *IKE using 3rd Party Certificates*, the **IPsec Secondary Gateway Name or Address** text field is hidden.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Security Policy

Authentication Method: IKE using Preshared Secret

Name:

IPsec Primary Gateway Name or Address:

IKE Authentication

Shared Secret:

Confirm Shared Secret: ☑ Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

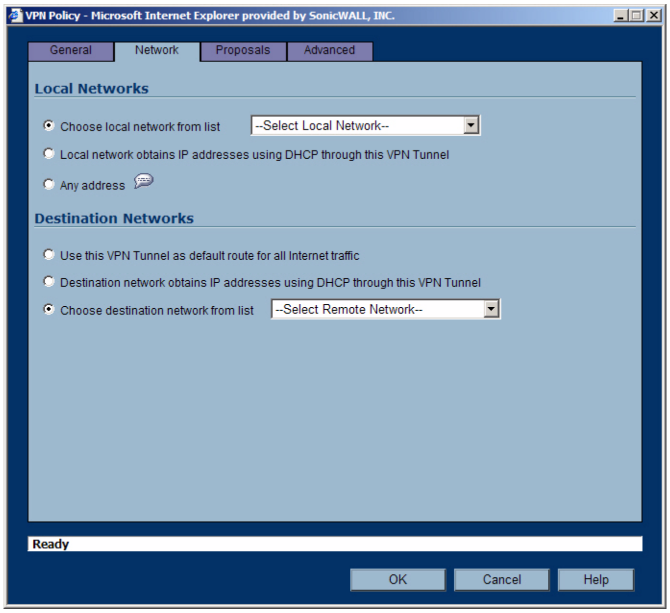
Ready

Prevention of XAUTH

When IKEv1 is used in Main Mode or Aggressive Mode, IP address assignment of protected networks via DHCP is supported. Two radio buttons appear on the **Network** tab to allow selection of this capability for either Local or Remote networks. This capability is not supported in IKEv2 mode so the radio buttons are not displayed.

Usage

If the **Proposals > Exchange** is *Main Mode* or *Aggressive Mode* and the **General > Authentication Method** is *IKE using Preshared Secret* or *IKE using 3rd Party Certificates*, the **DHCP** radio buttons appear in both the **Local Networks** and the **Destination Networks** sections.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Local Networks

● Choose local network from list --Select Local Network--

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

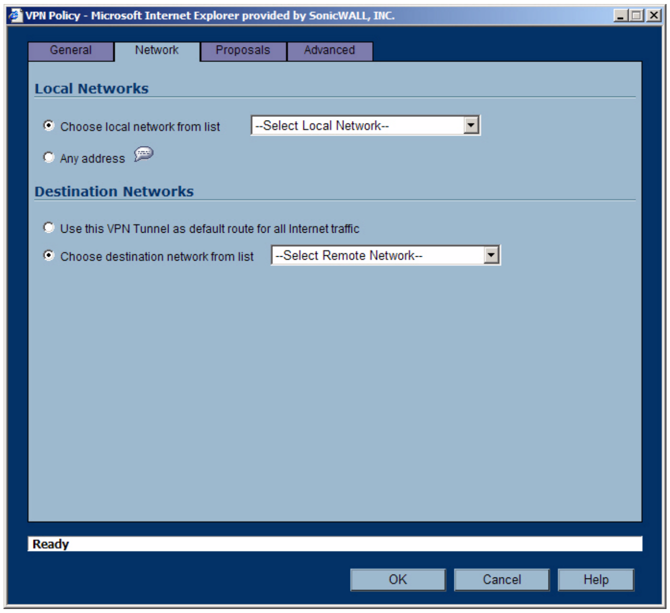
Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list --Select Remote Network--

If the **Proposals > Exchange** is *IKEv2 Mode* and the **General > Authentication Method** is *IKE using Preshared Secret* or *IKE using 3rd Party Certificates*, the **DHCP** radio buttons are hidden in both the **Local Networks** and the **Destination Networks** sections.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Local Networks

● Choose local network from list --Select Local Network--

○ Any address

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

● Choose destination network from list --Select Remote Network--

Ready

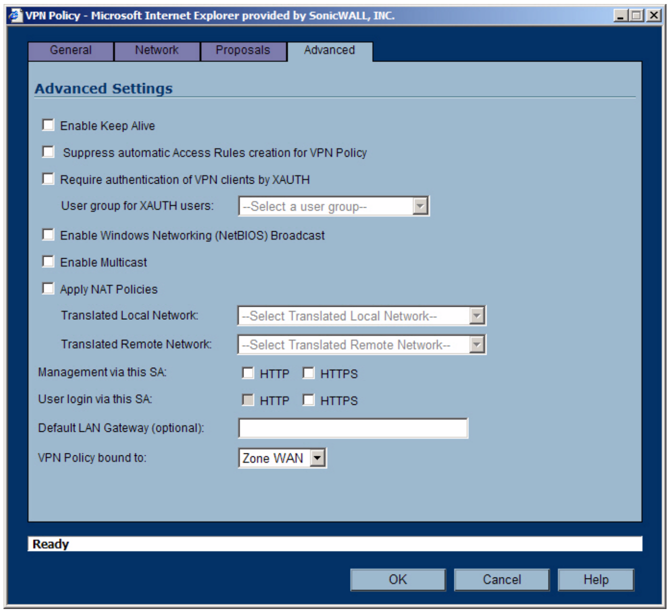
Minor Modifications Common to both IKEv1 and IKEv2

VPN Policies using IKEv1 may be used to terminate connections for third party VPN Client software. SonicOS ENH firmware allows GroupVPN policies to require XAUTH both for User authentication and for User access control to protected resources. Via User and User Group configuration, different Users can receive varied VPN Access lists via a combination of XAUTH and the GVC Client Connection Provisioning protocol. This capability is not provided to third party VPN Clients. Instead, multiple non-GroupVPN policies can be configured with different Local Networks to provide groups of Users access to different sets of resources. These policies may still require XAUTH authentication, so an option is provided on the **Advanced** tab to enable XAUTH and select a required User Group.

This capability is not supported in SonicOS 3.2 ENH for IKEv2 policies. Although XAUTH is widely implemented, it was never standardized as an IETF protocol. Support of user level authentication is provided in IKEv2 via a new standard mechanism called the Extensible Authentication Protocol (EAP). IKEv2 includes a specific EAP payload to provide this capability but this feature is not supported in SonicOS 3.2 ENH. Therefore, when the IKEv2 exchange mode is selected, the XAUTH option is hidden on the **Advanced** tab.

Usage

If the **Proposals > Exchange** is *Main Mode* or *Aggressive Mode* and the **General > Authentication Method** is *IKE using Preshared Secret* or *IKE using 3rd Party Certificates*, the **Require authentication of VPN client by XAUTH** checkbox and the **User group for XAUTH users** drop list both appear on the **Advanced** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Require authentication of VPN clients by XAUTH

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

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

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

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

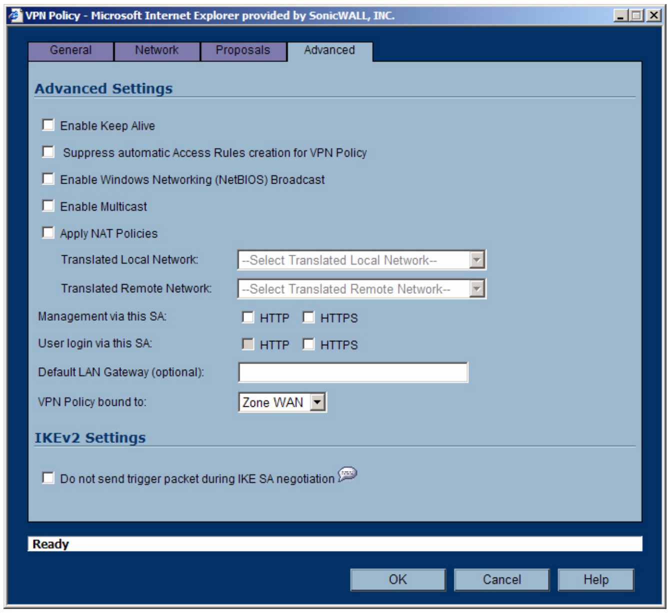
Management via this SA: □ HTTP □ HTTPS

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

If the **Proposals > Exchange** is *IKEv2 Mode* and the **General > Authentication Method** is *IKE using Preshared Secret* or *IKE using 3rd Party Certificates*, the **Require authentication of VPN client by XAUTH** checkbox and the **User group for XAUTH users** drop list are both hidden on the **Advanced** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

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

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

Management via this SA: □ HTTP □ HTTPS

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

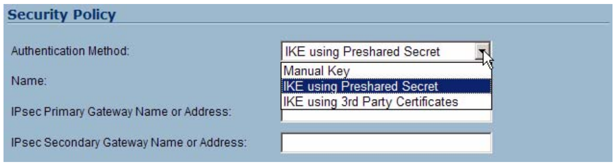
VPN Policy bound to: Zone WAN

IKEv2 Settings

□ Do not send trigger packet during IKE SA negotiation

Changing the IPSec Keying Mode label to Authentication Method

In SonicOS Enhanced 3.2, the **Authentication Method** prompt refers to the list of types of key exchange available. In earlier versions of SonicOS, it was referred to as **IPsec Keying Mode**.


Security Policy

Authentication Method: IKE using Preshared Secret

Name:

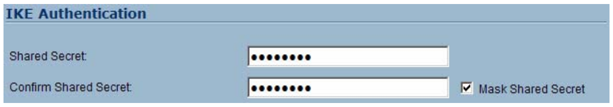
IPsec Primary Gateway Name or Address:

IPsec Secondary Gateway Name or Address:

Hiding the entered Shared Secret value and addition of a Confirmed Shared Secret text entry field.

The **Shared Secret** text entry field on the **General** tab now conceals the entered value.

A **Confirm Shared Secret** text entry field has been added. If the values entered in the two fields do not match, the Administrator is warned via a popup. Submission of the VPN policy will be blocked, requiring entry of matching values.

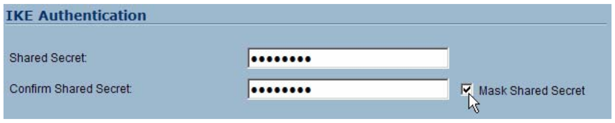

IKE Authentication

Shared Secret: ••••••••

Confirm Shared Secret: •••••••• ☑ Mask Shared Secret

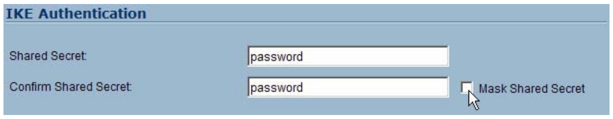
Masked Shared Secret

By default, the **Shared Secret** and new **Confirm Shared Secret** fields are masked to prevent casual observation of the values entered. A **Masked Shared Secret** checkbox is added to toggle masking. The checkbox is set by default. Clearing the checkbox displays the plaintext values.


IKE Authentication

Shared Secret: ••••••••

Confirm Shared Secret: •••••••• ☑ Mask Shared Secret

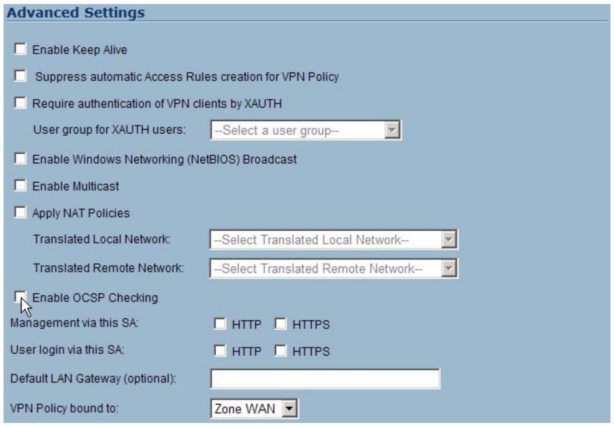

IKE Authentication

Shared Secret: password

Confirm Shared Secret: password □ Mask Shared Secret

Hiding the OCSP Responder URL text entry section if OCSP is not enabled

Select *IKE using 3rd Party Certificates* as the **Authentication Method** on the **General** tab. On the **Advanced** tab, the **Enable OCSP Checking** checkbox will appear.



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Require authentication of VPN clients by XAUTH

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

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

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

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

□ Enable OCSP Checking

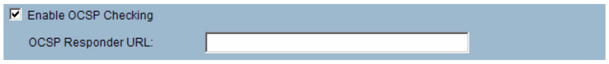
Management via this SA: □ HTTP □ HTTPS

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

Click the **Enable OCSP Checking** checkbox. The **OCSP Responder URL** section appears below the checkbox.

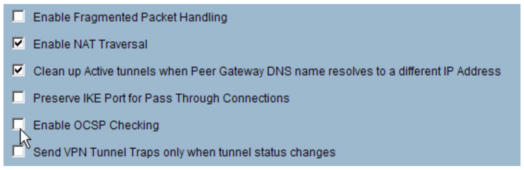


☑ Enable OCSP Checking

OCSP Responder URL:

Advanced Page OCSP and DF

On the **VPN > Advanced** page, the **Enable OCSP Checking** checkbox also appears to allow selecting OCSP as a global requirement. The URL section is similarly hidden unless the checkbox is selected. The **Ignore DF (Don't Fragment) Bit** checkbox is also hidden when the **Enable Fragmented Packet Handling** checkbox is cleared.



□ Enable Fragmented Packet Handling

☑ Enable NAT Traversal

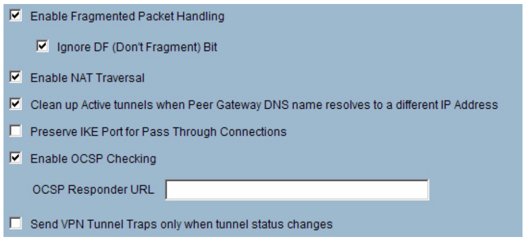
☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

□ Preserve IKE Port for Pass Through Connections

□ Enable OCSP Checking

□ Send VPN Tunnel Traps only when tunnel status changes

When the checkboxes are selected, the dependent fields are displayed.



☑ Enable Fragmented Packet Handling

☑ Ignore DF (Don't Fragment) Bit

☑ Enable NAT Traversal

☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

□ Preserve IKE Port for Pass Through Connections

☑ Enable OCSP Checking

OCSP Responder URL

□ Send VPN Tunnel Traps only when tunnel status changes

Configuring VPNs in SonicOS Enhanced

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

Note

Note For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator's Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator's Guide**.

SonicWALL's GroupVPN provides automatic VPN policy provisioning for SonicWALL Global VPN Clients. The GroupVPN feature on the SonicWALL security appliance and the SonicWALL Global VPN Client (part of the Global security Client) dramatically streamline VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the SonicWALL security appliance (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy for SonicWALL Global Security Clients using the **VPN Policy Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each Zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your SonicWALL model.

Planning Your VPN

Before creating or activating a VPN tunnel, gather the following information. You can print these pages and to use as a planning checklist:

GroupVPN Policy Planning Checklist

On the SonicWALL security appliance:

- **Authentication Method**:
  - □ **IKE using Preshared Secret**
  - □ **IKE using 3rd Party Certificates**.

- **Shared Secret** if using preshared secret.

  ____

- **Gateway Certificate** if using 3rd part certificates. This is a certificate file you have uploaded to your Sonicwall security appliance and plan to distribute to your VPN Clients.

  ____

- **Peer ID Type** if using 3rd party certificates: Choose

  □ **Distinguished name**

  □ **E-Mail ID**

  □ **Domain name**.

- **Peer ID Filter** if using 3rd party certificates.

  ____

- **IKE (Phase 1) Proposal**:
  - **DH Group**:

    □ **Group 1**

    □ **Group 2**

    □ G**roup 5**
  - **Encryption**:

    □ **DES**

    □ **3DES**

    □ **AES-128**

    □ **AES-256**
  - **Authentication**:

    □ **MD5**

    □ **SHA1**
  - **Life Time** (seconds): ______________________________(default 28800)
- **Ipsec (Phase 2) Proposal**
  - **Protocol**: (**ESP** only)
  - **Encryption**:

    □ **DES**

    □ **3DES**

    □ **AES-128**

    □ **AES-192**

    □ **AES-256**
  - **Authentication**:

    □ **MD5**

    □ **SHA1**
  - □ **Enable Perfect Forward Secrecy**
  - **DH Group** (if perfect forward secrecy is enabled

    - □ **Group 1**
    - □ **Group 2**
    - □ **Group 5**
  - **Life Time** (seconds): ____ (default 28800)
- □ **Enable Windows Networking (NetBIOS) Broadcast**
- □ **Enable Multicast**
- **Management via this SA**:

  □ **HTTP**

  □ **HTTPS**
- **Default Gateway**: ____
- □ **Enable OCSP Checking**
  - **OCSP Responder URL**: _____________________________________
- □ **Require Authentication of VPN Clients via XAUTH**
- **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

  ____
- **Allow Unauthenticated VPN Client Access** (the network or subnet you will allow to have access to this VPN without authentication if XAUTH is not selected):

  ____
- **Cache XAUTH User Name and Password on Client** (will the client be able to store the user name and password:

  □ **Never**

  □ **Single Session**

  □ **Always**
- **Virtual Adapter settings**:

  □ **None**

  □ **DHCP Lease**

  □ **DHCP Lease or Manual Configuration**
- **Allow Connections to**:

  □ **This Gateway Only**

  □ **All Secured Gateways**

  □ **Split Tunnels**
- □ **Set Default Route as this Gateway**
- □ **Require Global Security Client for this Connection**
- □ **Use Default Key for Simple Client Provisioning**
  (this allows easier client setup, but is less secure)

On the client

- IP address or Web address of VPN Gateway

- VPN Client:
  - □ GVC or GSC
  - □ GSC only (Require Global Security Client checked on security appliance)
- Shared secret, if selected on security appliance:

  ____
- Certificate, if selected on security appliance:

  ____
- User’s user name and password if XAUTH is required on the security appliance.

Site-to-Site VPN Planning Checklist

On the Initiator

Typically, the request for an IKE VPN SA is made from the remote site.

- **Authentication Method**:
  - □ **Manual Key**
  - □ **IKE using Preshared Secret**
  - □ **IKE using 3rd Party Certificates** (not used with IKEv2)
- **Name** of this VPN: ______________________________________
- **IPsec Primary Gateway Name or Address**: ____________________
- **IPsec Secondary Gateway Name or Address**: __________________
  (not used with manual key, not used with IKEv2)
- **IKE Authentication for** IKE using Preshared Secret:
  - **Shared Secret**: ______________________________________
  - **Local IKE ID**:
    - □ **IP Address** ______________________________________
    - □ **Domain Name** ___________________________________
    - □ **Email Address** ___________________________________
    - □ **SonicWALL Identifier** _____________________________
  - **Peer IKE ID**:
    - □ **IP Address** ______________________________________
    - □ **Domain Name** ___________________________________
    - □ **Email Address** ___________________________________
    - □ **SonicWALL Identifier** _____________________________
- **IKE Authentication for** IKE using 3rd Party Certificate (not used with IKEv2):
  - **Local Certificate**: ___________________________________
  - **Peer IKE ID Type**:
    - □ **Distinguished name**
    - □ **E-Mail ID**
    - □ **Domain name**

   - **Peer IKE ID**: ____
- **Local Networks**

  □ **Choose local network from list** (select an address object):

  ____

  □ **Local network obtains IP addresses using DHCP through this VPN Tunnel** (not used with IKEv2)

  □ **Any address**
- **Destination Networks**

  □ **Use this VPN Tunnel as default route for all Internet traffic**

  □ **Destination network obtains IP addresses using DHCP through this VPN Tunnel**

  □ **Choose destination network from list** (select an address object):

  ____
- **IKE (Phase 1) Proposal**:
  - **Exchange**:

    □ **Main Mode**

    □ **Aggressive Mode**

    □ **IKEv2 Mode**
  - **DH Group**:

    □ **Group 1**

    □ **Group 2**

    □ **Group 5**
  - **Encryption**:

    □ **DES**

    □ **3DES**

    □ **AES-128**

    □ **AES-192**

    □ **AES-256**
  - **Authentication**:

    □ **MD5**

    □ **SHA1**
  - **Life Time** (seconds): ____(default 28800)
- **Ipsec (Phase 2) Proposal**
  - **Protocol**:

    □ **ESP**

    □ **AH**
  - **Encryption**:

    □ **DES**

    □ **3DES**

  - □ **AES-128**
  - □ **AES-192**
  - □ **AES-256**
  - **Authentication**:
    - □ **MD5**
    - □ **SHA1**
  - □ **Enable Perfect Forward Secrecy**
  - **DH Group** (if perfect forward secrecy is enabled
    - □ **Group 1**
    - □ **Group 2**
    - □ **Group 5**
  - **Life Time** (seconds): ______________________________________(default 28800)
- □ **Enable Keep Alive**
- □ **Suppress automatic Access Rules creation for VPN Policy**
- □ **Require authentication of VPN clients by XAUTH** (not with IKEv2)
  - **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

    ____
- □ **Enable Windows Networking (NetBIOS) Broadcast**
- □ **Enable Multicast**
- □ **Apply NAT Policies**
  - **Translated Local Network**: _________________________________
  - **Translated Remote Network**: ________________________________
- □ **Enable OCSP Checking** (IKE with 3rd Party Certificate only)
  - **OCSP Responder URL**: (IKE with 3rd Party Certificate only)

    ____
- **Management via this SA**:

  □ **HTTP**

  □ **HTTPS**
- **User login via this SA**:

  □ **HTTP**

  □ **HTTPS**
- □ **Default LAN Gateway (optional**):
- **VPN Policy bound to**:

  □ **Interface X0,** □ **Interface X1,** □ **Interface X2,** □ **Interface X3,** □ **Interface X4**

  □ **Interface X5,** □ **Interface X6,** □ **Interface X7,** □ **Interface X8,** □ **Interface X9**

  □ **Zone WAN**
- □ Do **not send trigger packet during IKE SA negotiation** (IKEv2 only)

On the Responder

The settings on the responder must be the same as on the initiator except:

- **Name** of this VPN: ____________________
- **IPsec Primary Gateway Name or Address**: not required on the responder
- **IPsec Secondary Gateway Name or Address**: not required on the responder
- **IKE Authentication for** IKE using Preshared Secret:
  - **Local IKE ID**: (must match Peer IKE ID on initiator)
    - □ **IP Address** ____________________
    - □ **Domain Name** ____________________
    - □ **Email Address** ____________________
    - □ **SonicWALL Identifier** ____________________
  - **Peer IKE ID**: (must match Local IKE ID on initiator)
    - □ **IP Address** ____________________
    - □ **Domain Name** ____________________
    - □ **Email Address** ____________________
    - □ **SonicWALL Identifier** ____________________
- **IKE Authentication for** IKE using 3rd Party Certificate (not used with IKEv2):
  - **Local Certificate**: ____________________
  - **Peer IKE ID Type**:
    - □ **Distinguished name**
    - □ **E-Mail ID**
    - □ **Domain name**
  - **Peer IKE ID**: ____________________
- **Local Networks** (must match Destination Networks on initiator)

  □ **Choose local network from list** (select an address object):

  ____

  □ **Local network obtains IP addresses using DHCP through this VPN Tunnel** (not used with IKEv2)

  □ **Any address**
- **Destination Networks** (must match Local Networks on initiator)

  □ **Use this VPN Tunnel as default route for all Internet traffic**

  □ **Destination network obtains IP addresses using DHCP through this VPN Tunnel**

  □ **Choose destination network from list** (select an address object):

  ____
- □ **Apply NAT Policies**
  - **Translated Local Network**: (must match Translated Remote Network on initiator)

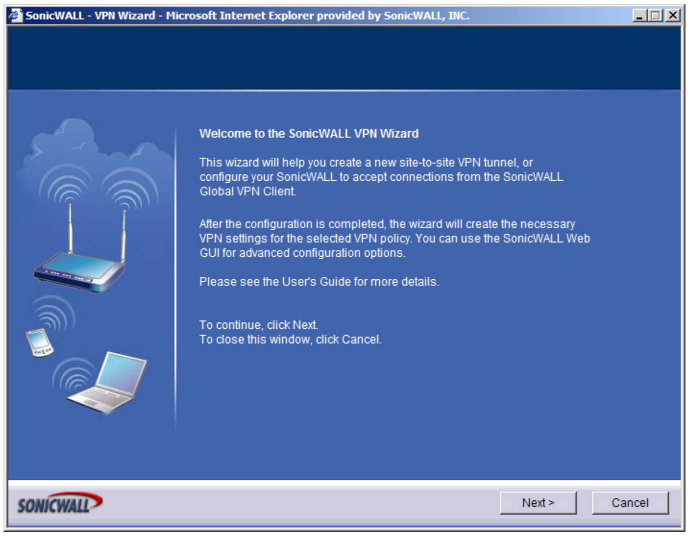
    ____
  - **Translated Remote Network** (must match Translated Local Network on initiator)

    ____

VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the SonicWALL security appliance. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the SonicWALL Management Interface for optional advanced configuration options.

Note For step-by-step instructions on using the VPN Policy Wizard, see Chapter 50 Configuring VPNs with the VPN Policy Wizard.



SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL VPN Wizard

This wizard will help you create a new site-to-site VPN tunnel, or configure your SonicWALL to accept connections from the SonicWALL Global VPN Client.

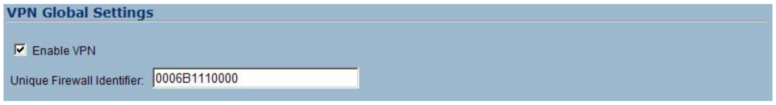
After the configuration is completed, the wizard will create the necessary VPN settings for the selected VPN policy. You can use the SonicWALL Web GUI for advanced configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

VPN Global Settings

The **Global VPN Settings** section of the **VPN** > **Settings** page displays the following information:



VPN Global Settings

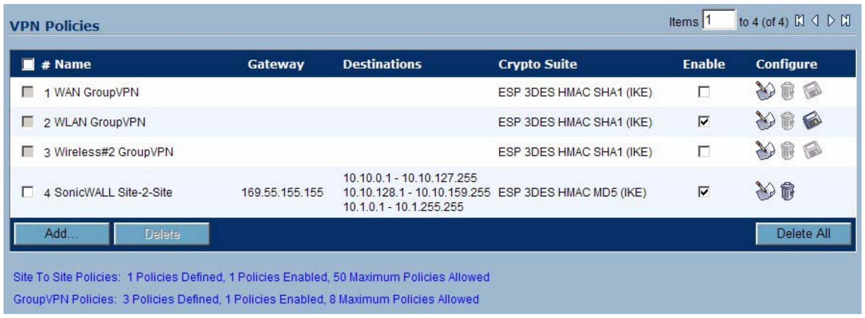
☑ Enable VPN

Unique Firewall Identifier: 0006B1110000

- **Enable VPN** must be selected to allow VPN policies through the SonicWALL security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:



VPN Policies

Items 1 to 4 (of 4)

□ # Name	Gateway	Destinations	Crypto Suite	Enable	Configure
□ 1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
□ 2 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☑	
□ 3 Wireless#2 GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
□ 4 SonicWALL Site-2-Site	169.55.155.155	10.10.0.1 - 10.10.127.255 10.10.128.1 - 10.10.159.255 10.1.0.1 - 10.1.255.255	ESP 3DES HMAC MD5 (IKE)	☑	

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed

GroupVPN Policies: 3 Policies Defined, 1 Policies Enabled, 8 Maximum Policies Allowed

- **Name**: Displays the default name or user-defined VPN policy name.
- **Gateway**: Displays the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations**: Displays the IP addresses of the destination networks.
- **Crypto Suite**: Displays the type of encryption used for the VPN policy.
- **Enable**: Selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure**: Clicking the Edit icon allows you to edit the VPN policy. Clicking the Trashcan allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the Trashcan icons are dimmed. GroupVPN policies also have a Disk icon for exporting the VPN policy configuration as a file for local installation by SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 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 **VPN Policy** window for configuring the GroupVPN policy.

Below the VPN Policies table are the following buttons:

- **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. You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

Navigating and Sorting the VPN Policies Entries

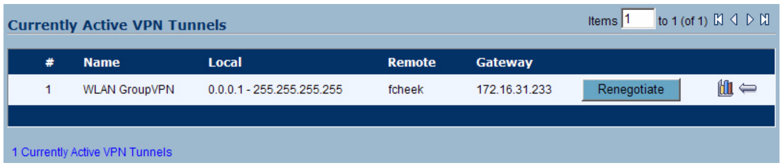
The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System** > **Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.



Currently Active VPN Tunnels

Items 1 to 1 (of 1)

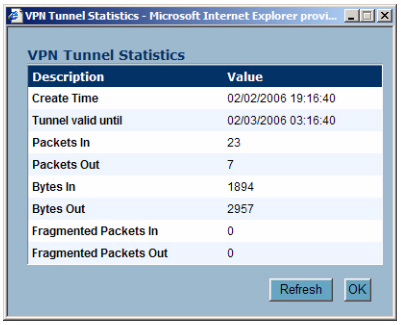
#	Name	Local	Remote	Gateway		
1	WLAN GroupVPN	0.0.0.1 - 255.255.255.255	fcheek	172.16.31.233	Renegotiate	

1 Currently Active VPN Tunnels

Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

Viewing VPN Tunnel Statistics

In the Currently Active VPN Tunnels table, click on the Statistics icon in the row for a tunnel to view the statistics on that tunnel. The VPN Tunnel Statistics icon displays:



VPN Tunnel Statistics - Microsoft Internet Explorer provi...

VPN Tunnel Statistics

Description	Value
Create Time	02/02/2006 19:16:40
Tunnel valid until	02/03/2006 03:16:40
Packets In	23
Packets Out	7
Bytes In	1894
Bytes Out	2957
Fragmented Packets In	0
Fragmented Packets Out	0

- **Create Time**: The date and time the tunnel came into existence.
- **Tunnel valid until**: The time when the tunnel expires and is force to renegotiate.
- **Packets In**: The number of packets received from this tunnel.
- **Packets Out**: The number of packets sent out from this tunnel.
- **Bytes In**: The number of bytes received from this tunnel.
- **Bytes Out**: The number of bytes sent out from this tunnel.
- **Fragmented Packets In**: The number of fragmented packets received from this tunnel.
- **Fragmented Packets Out**: The number of fragmented packets sent out from this tunnel.

Configuring GroupVPN Policies

SonicWALL **GroupVPN** facilitates the set up and deployment of multiple SonicWALL Global VPN Clients by the SonicWALL security appliance administrator. **GroupVPN** is only available for SonicWALL Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

Reference For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator's Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator's Guide**.

The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

SonicWALL supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPsec Keying Mode.

Tip You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNs with the SonicWALL VPN Policy Wizard.

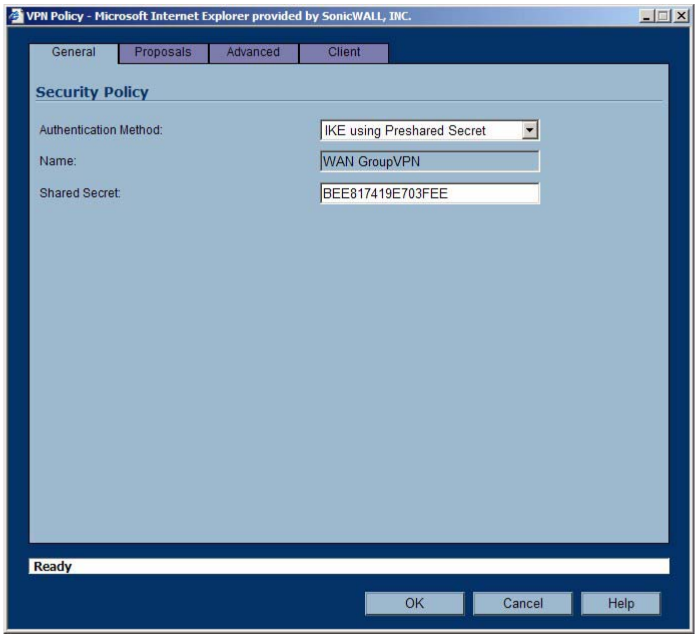
The following instructions explain configuring GroupVPN using the SonicWALL Management Interface.

Note See the **GroupVPN Setup in SonicOS Enhanced** technote on the SonicWALL documentation Web site http://www.sonicwall.com for more GroupVPN configuration information.

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN, follow these steps:

1. Click the Edit icon for the **WAN GroupVPN** entry. The **VPN Policy** window is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

Security Policy

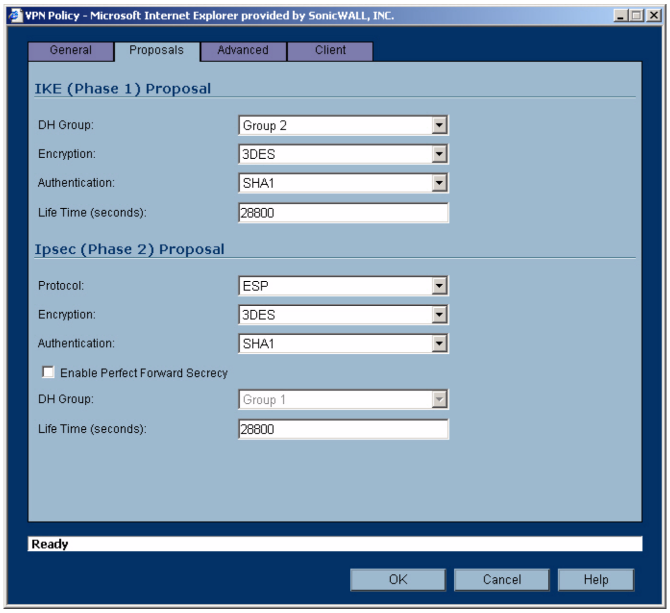
Authentication Method: IKE using Preshared Secret

Name: WAN GroupVPN

Shared Secret: BEE817419E703FEE

2. In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A Shared Secret is automatically generated by the SonicWALL security appliance in the **Shared Secret** field, or you can generate your own shared secret. **Shared Secrets** must be minimum of four characters. You cannot change the name of any GroupVPN policy.

3. Click the **Proposals** tab to continue the configuration process.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

IKE (Phase 1) Proposal

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

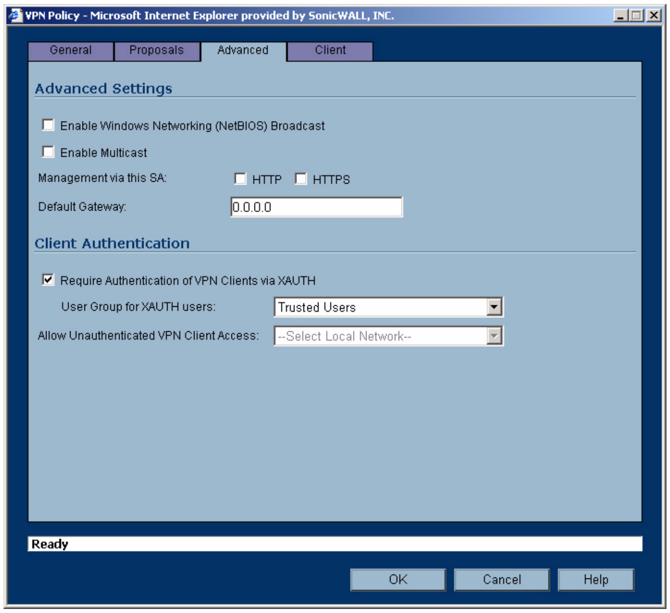
DH Group: Group 1

Life Time (seconds): 28800

Ready

4. In the **IKE (Phase 1) Proposal** section, use the following settings:
   - Select the DH Group from the **DH Group** menu.
   - Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
   - Select the desired authentication method from the **Authentication** menu.
   - 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.
5. In the **IPsec (Phase 2) Proposal** section, select the following settings:
   - Select the desired protocol from the **Protocol** menu
   - Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu
   - Select the desired authentication method from the **Authentication** menu
   - Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
   - 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 the **Advanced** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

Advanced Settings

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

Management via this SA: □ HTTP □ HTTPS

Default Gateway: 0.0.0.0

Client Authentication

☑ Require Authentication of VPN Clients via XAUTH

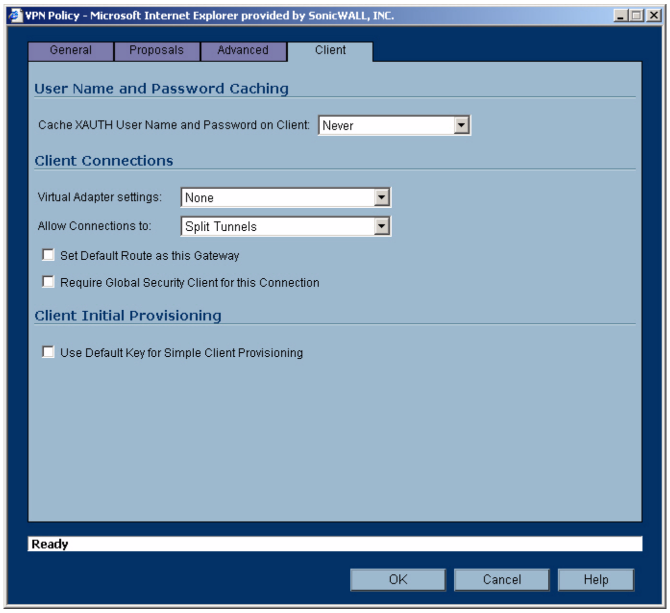
User Group for XAUTH users: Trusted Users

Allow Unauthenticated VPN Client Access: --Select Local Network--

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

- **Enable Windows Networking (NetBIOS) broadcast** - allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Management via this SA**: - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - allows the network administrator to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL security appliance. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWALL 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.
- **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. he **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users**.
- **Allow Unauthenticated VPN Client Access** - allows you to enable unauthenticated VPN client access. If you uncheck **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 addess object** or **Create new address group** to create a new one.

8. Click the **Client** tab, select any of the following settings you want to apply to your GroupVPN policy.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Virtual Adapter settings: None

Allow Connections to: Split Tunnels

□ Set Default Route as this Gateway

□ Require Global Security Client for this Connection

Client Initial Provisioning

□ Use Default Key for Simple Client Provisioning

– **Cache XAUTH User Name and Password on Client** - allows the Global VPN Client to cache the user name and password.

  - **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
  - **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
  - **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be 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 was a requirement, it's necessary to 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 GVC version 3.0 or later.

  - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
  - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
  - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL 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 SonicWALL so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
  - **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 along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is 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**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then 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.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting.
- **Require Global Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Global Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

Note For more information on the SonicWALL Global Security Client, see the SonicWALL Global Security Client Administrator’s Guide.

- **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.

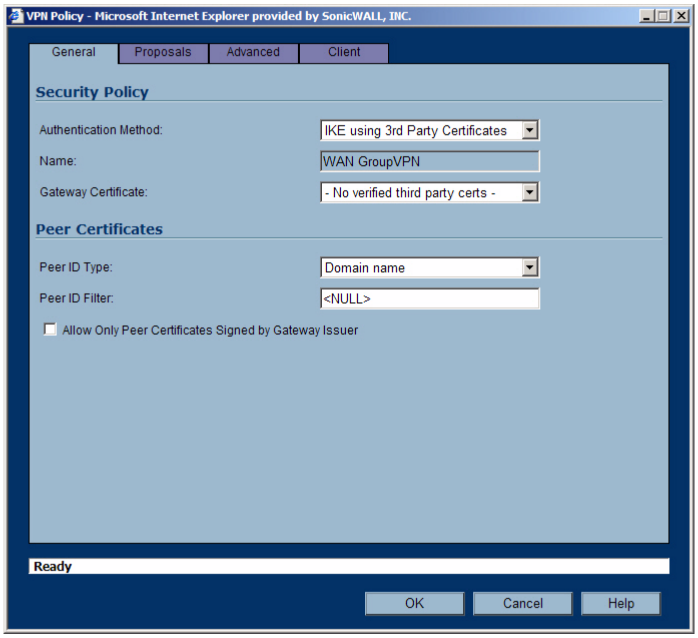
9. Click **OK**.

Configuring GroupVPN with IKE using 3rd Party Certificates

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:

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

1. In the **VPN** > **Settings** page click the edit icon under **Configure**. The **VPN Policy** window is displayed.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

Security Policy

Authentication Method: IKE using 3rd Party Certificates

Name: WAN GroupVPN

Gateway Certificate: - No verified third party certs -

Peer Certificates

Peer ID Type: Domain name

Peer ID Filter: <NULL>

☐ Allow Only Peer Certificates Signed by Gateway Issuer

Ready

2. In the **Security Policy** section, select **IKE using 3rd Party Certificate**s from the **Authentication Method** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.
3. Select a certificate for the SonicWALL from the **Gateway Certificate** menu.
4. Select one of the following Peer ID types from the **Peer ID Type** menu:
   - **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail 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, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when Domain Name is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.
   - **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). 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, i.e. c=us.

5. Enter the Peer ID filter in the **Peer ID Filter** field.
6. Check **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.
7. Click on the **Proposals** tab.
8. In the **IKE (Phase 1) Proposal** section, select the following settings:
   - Select the DH Group from the **DH Group** menu.
   - Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
   - Select the desired authentication method from the **Authentication** menu.
   - 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.
9. In the **IPsec (Phase 2) Proposal** section, select the following settings:
   - Select the desired protocol from the **Protocol** menu
   - Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu
   - Select the desired authentication method from the **Authentication** menu
   - Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
   - 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 on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:
    - **Enable Windows Networking (NetBIOS) broadcast** - allows access to remote network resources by browsing the Windows Network Neighborhood.
    - **Enable Multicast** - enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
    - **Management via this SA** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
    - **Default Gateway** - used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL 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. See the “Using OCSP with SonicWALL Security Appliances” section in **Chapter 44, Configuring VPN Policies** of the *SonicOS Enhanced 3.2 Administrator’s Guide*.
    - **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.

  - **All Unauthenticated VPN Client Access** - allows you to specify network segments for unauthenticated Global VPN Client access.

11. Click on the **Client** tab and 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. Select from:
      - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
      - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
      - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be 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 was a requirement, it's necessary to 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 GVC version 3.0 or later.
      - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
      - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
      - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL 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 SonicWALL so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
    - **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
      - **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 along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is 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**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then 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.

- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
- **Require Global Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Global Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

Note For more information on the SonicWALL Global Security Client and Distributed Security Client, see the SonicWALL Global Security Client Administrator's Guide.

- **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.

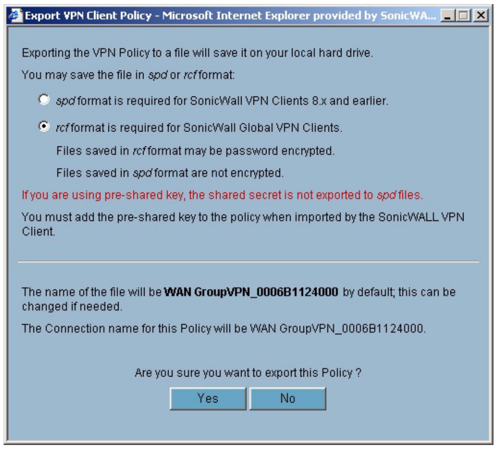
12. Click **OK**.

Exporting a VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:

Warning **The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.**

1. Click the **Disk** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Polic**y window appears.


Export VPN Client Policy - Microsoft Internet Explorer provided by SonicWA...
Yes
No

Exporting the VPN Policy to a file will save it on your local hard drive.

You may save the file in *spd* or *rcf* format:

○ *spd* format is required for SonicWall VPN Clients 8.x and earlier.

● *rcf* format is required for SonicWall Global VPN Clients.

Files saved in *rcf* format may be password encrypted.

Files saved in *spd* format are not encrypted.

If you are using pre-shared key, the shared secret is not exported to *spd* files.

You must add the pre-shared key to the policy when imported by the SonicWALL VPN Client.

The name of the file will be **WAN GroupVPN_0006B1124000** by default; this can be changed if needed.

The Connection name for this Policy will be WAN GroupVPN_0006B1124000.

Are you sure you want to export this Policy ?

2. **rcf format is required for SonicWALL Global VPN Clients** is selected by default. Files saved in the rcf format can be password encrypted. The SonicWALL provides a default file name for the configuration file, which you can change.
3. Click **Yes**. The **VPN Policy Export** window appears.
4. Type a password in the **Passwor**d 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.
5. Click **Submit**. If you did not enter a password, a message appears confirming your choice.
6. Click **OK**. You can change the configuration file before saving.
7. Save the file.

8. Click **Close**.

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

Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP Addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The SonicWALL 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.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWALL is configured to connect to another SonicWALL via a VPN tunnel. Or, a SonicWALL is configured to connect via IPsec to another manufacturer’s firewall.
- **Hub and Spoke Design** - All SonicWALL VPN gateways are configured to connect to a central SonicWALL (hub), such as a corporate SonicWALL. 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.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

Creating Site-to-Site VPN Policies

Tip You can easily create site-to-site VPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNs with the SonicWALL VPN Policy Wizard.

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- IKE using Preshared Key
- Manual Key
- IKE using 3rd Party Certificates

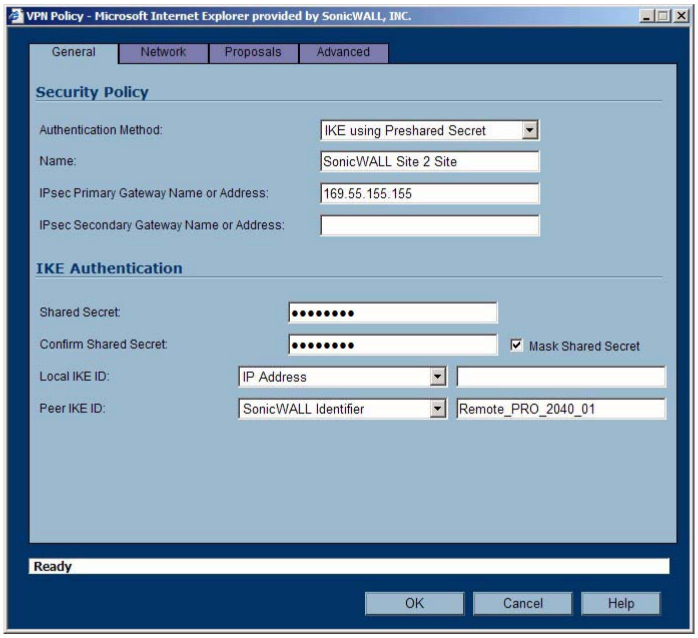
Tip Use the VPN Planning Sheet for Site-to-Site VPN Policies to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.

Reference For configuring VPN policies between SonicWALL security appliances running SonicOS Enhanced and SonicWALL security appliances running SonicWALL Firmware version 6.5 (or higher), see the technote: Creating IKE IPsec VPN Tunnels between SonicWALL Firmware 6.5 and SonicOS Enhanced, available at the SonicWALL documentation Web site http://www.sonicwall.com/services/documentation.html.

Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE), follow the steps below:

1. Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Security Policy

Authentication Method: IKE using Preshared Secret

Name: SonicWALL Site 2 Site

IPsec Primary Gateway Name or Address: 169.55.155.155

IPsec Secondary Gateway Name or Address:

IKE Authentication

Shared Secret: ••••••••

Confirm Shared Secret: •••••••• ☑ Mask Shared Secret

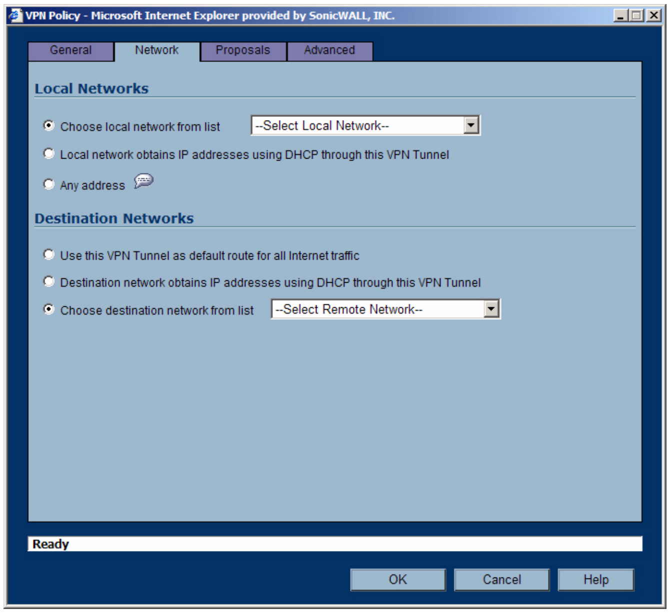
Local IKE ID: IP Address

Peer IKE ID: SonicWALL Identifier Remote_PRO_2040_01

2. In the **General** tab, select **IKE using Preshared Secret** from the **Authentication Method** menu.
3. Enter a name for the policy in the **Name** field.
4. Enter the host name or IP address of the remote connection in the IPsec **Primary Gateway Name or Address** field.
5. If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.
6. Enter a Shared Secret password to be used to setup the Security Association the **Shared Secret** and **Confirm Shared Secret** fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

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

7. Click the **Network** tab.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

Local Networks

● Choose local network from list --Select Local Network--

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

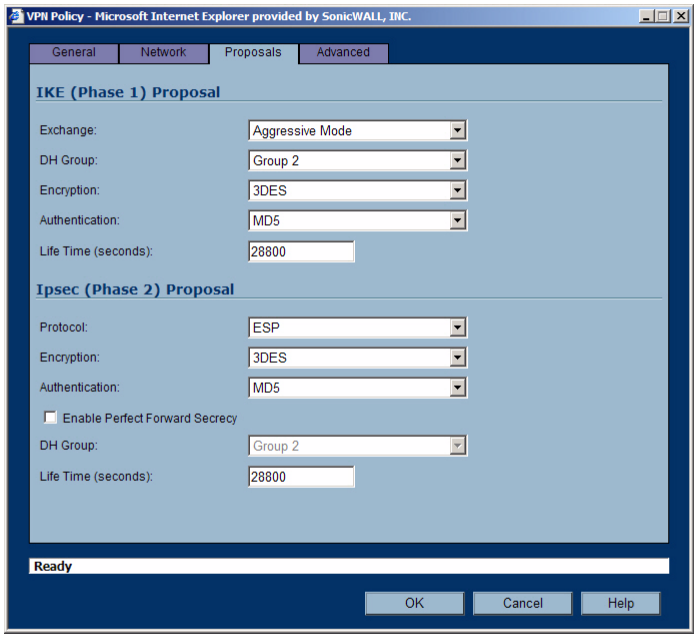
● Choose destination network from list --Select Remote Network--

Ready

8. Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. 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.

9. Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

10. Click **Proposals**.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

IKE (Phase 1) Proposal

Exchange:	Aggressive Mode
DH Group:	Group 2
Encryption:	3DES
Authentication:	MD5
Life Time (seconds):	28800

Ipsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	3DES
Authentication:	MD5
☐ Enable Perfect Forward Secrecy	
DH Group:	Group 2
Life Time (seconds):	28800

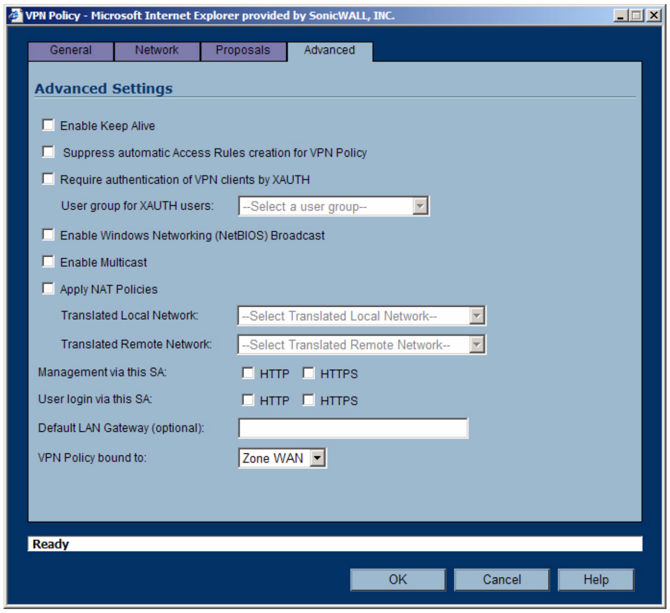
11. Under **IKE (Phase 1) Proposal**, select either **Main Mode**, **Aggressive Mode**, or **IKEv2** from the **Exchange** menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned. **IKEv2** causes all the negotiation to happen via IKE v2 pro0tocols, rather than using IKE Phase 1 and Phase 2. If you use IKE v2, both ends of the VPN tunnel must use IKE v2.

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

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

14. Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

– If you selected **Main Mode** or **Aggressive Mode** in the **Proposals** tab:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Require authentication of VPN clients by XAUTH

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

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

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

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

Management via this SA: □ HTTP □ HTTPS

User login via this SA: □ HTTP □ HTTPS

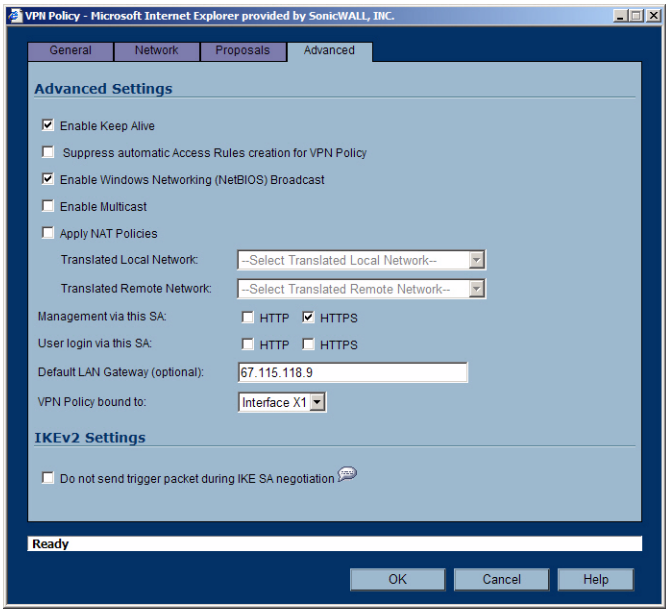
Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- 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.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. 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** menu. 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 local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

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

- If you selected **IKEv2** in the **Proposals** tab:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Advanced Settings

☑ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☑ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

☐ Apply NAT Policies

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

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

Management via this SA: ☐ HTTP ☑ HTTPS

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional): 67.115.118.9

VPN Policy bound to: Interface X1

IKEv2 Settings

☐ Do not send trigger packet during IKE SA negotiation

Ready

  - Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
  - Select **Suppress automatic Access Rules creation for VPN Policy** to turn off the automatic access rules created between the LAN and VPN zones for this VPN policy.
  - Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
  - Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
  - Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. 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** menu. 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 local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
  - Enter the **Default LAN Gateway** if you have more than one gateway and you want this one always to be used first.

- Select an interface or Zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- Under **IKEv2** Settings (visible only if you selected **IKEv2** for **Exchange** on the **Proposals** tab), The **Do not send trigger packet during IKE SA negotiation** checkbox is cleared by default and should only be selected when required for interoperability.

  The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

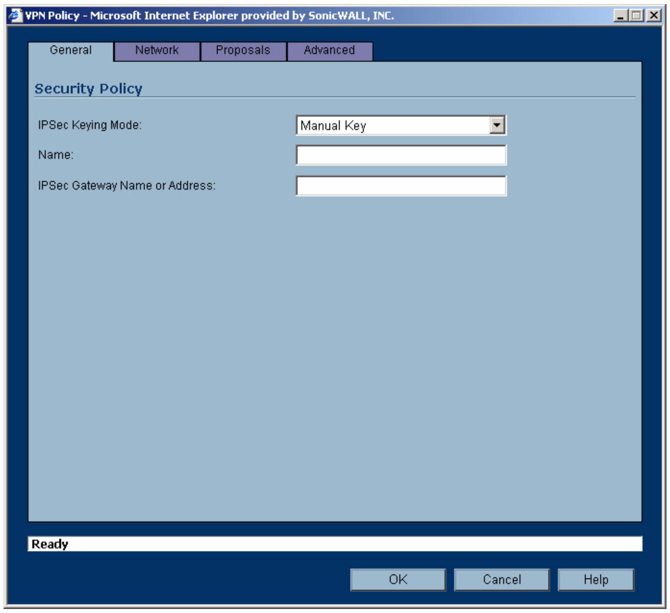
15. Click **OK**.

Configuring a VPN Policy using Manual Key

To manually configure a VPN policy between two SonicWALL appliances using Manual Key, follow the steps below:

Configuring the Local SonicWALL Security Appliance

1. Click **Add** on the **VPN** > **Settings** page. The **VPN Policy** window is displayed.
2. In the **General** tab of the **VPN Policy** window, select **Manual Key** from the **IPsec Keying Mode** menu. The **VPN Policy** window displays the manual key options.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

Security Policy

IPSec Keying Mode: Manual Key

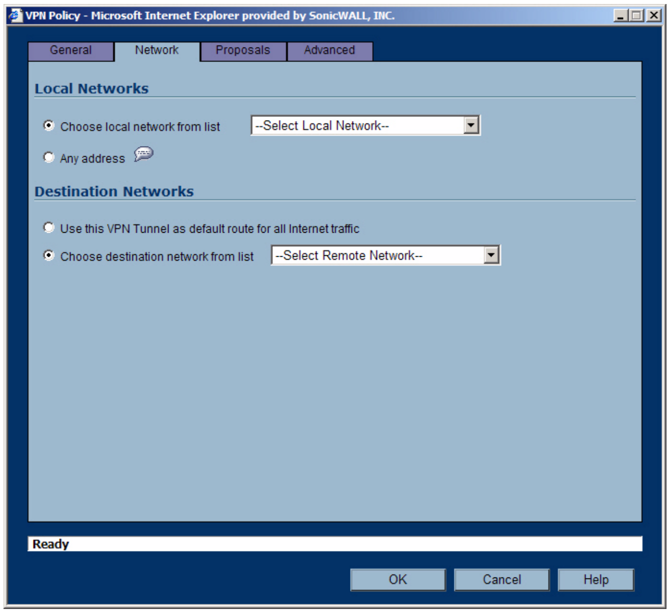
Name:

IPSec Gateway Name or Address:

Ready

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

5. Click the **Network** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Local Networks

● Choose local network from list --Select Local Network--

○ Any address

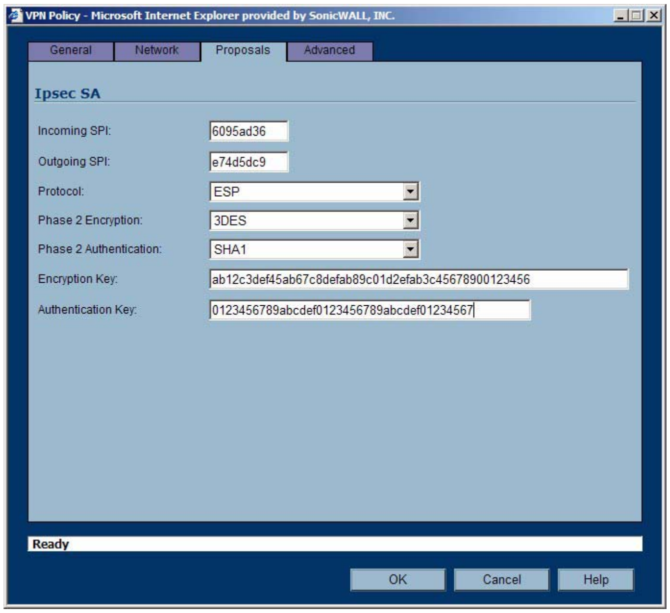
Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

● Choose destination network from list --Select Remote Network--

6. Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Use this option is a peer has **Use this VPN Tunnel as default route for all Internet traffic** selected. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.

7. Click on the **Proposals** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Ipsec SA

Incoming SPI: 6095ad36

Outgoing SPI: e74d5dc9

Protocol: ESP

Phase 2 Encryption: 3DES

Phase 2 Authentication: SHA1

Encryption Key: ab12c3def45ab67c8defab89c01d2efab3c45678900123456

Authentication Key: 0123456789abcdef0123456789abcdef01234567

8. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

Warning **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.**

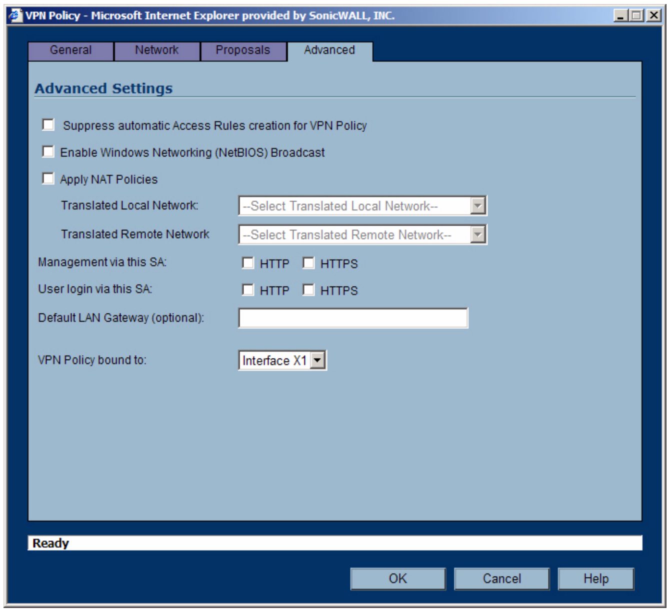
9. The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

Note The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.

10. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the SonicWALL.
11. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the SonicWALL settings.

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.

12. Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Advanced Settings

□ Suppress automatic Access Rules creation for VPN Policy

□ Enable Windows Networking (NetBIOS) Broadcast

□ Apply NAT Policies

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

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

Management via this SA: □ HTTP □ HTTPS

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Interface X1

Ready

- 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.

- Select **Apply NAT Policies** if your want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. 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 local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you 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.

13. Click **OK**.
14. Click **Apply** on the **VPN > Settings** page to update the VPN Policies.

Configuring the Remote SonicWALL Security Appliance

1. Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
2. In the **General** tab, select **Manual Key** from the **IPsec Keying Mode** menu.
3. Enter a name for the SA in the **Name** field.
4. Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.
5. Click the **Network** tab.
6. Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.
7. Click the **Proposals** tab.
8. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

Warning **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.**

9. The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

Note The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.

10. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the remote SonicWALL.
11. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWALL settings.

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.

12. Click the **Advanced** tab and 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.
    - Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. 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.

Warning **You cannot use this feature if you have selected Use this VPN Tunnel as the default route for all Internet traffic on the Network tab.**

- To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you 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.

13. Click **OK**.
14. Click **Apply** on the **VPN > Settings** page to update the VPN Policies.

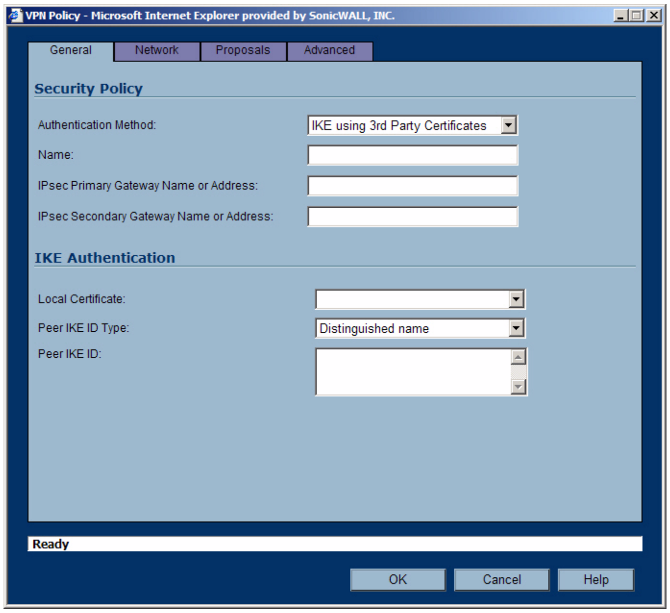
Tip Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers’ or workstations’ remote IP addresses.

Configuring a VPN Policy with IKE using a Third Party Certificate

Warning **You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate.**

To create a VPN SA using IKE and third party certificates, follow these steps:

1. In the **VPN** > **Settings** page, click **Add**. The **VPN Policy** window is displayed.
2. In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**.The **VPN Policy** window displays the 3rd party certificate options.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

Security Policy

Authentication Method: IKE using 3rd Party Certificates

IKE Authentication

Peer IKE ID Type: Distinguished name

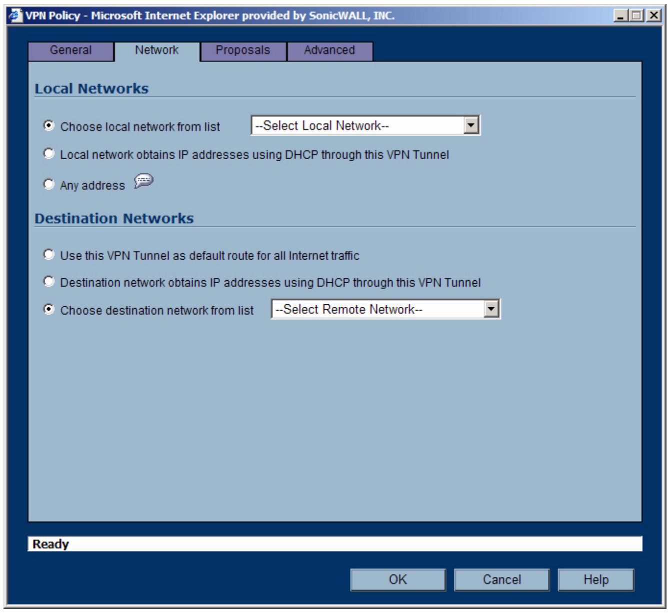
Ready

General
Network
Proposals
Advanced
Name:
IPsec Primary Gateway Name or Address:
IPsec Secondary Gateway Name or Address:
Local Certificate:
Peer IKE ID:
OK
Cancel
Help

3. Type a Name for the Security Association in the **Name** field.
4. Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPsec Primary Gateway Name or Address** field. 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.
5. Under **IKE Authentication**, select a third party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.
6. Select one of the following Peer ID types from the **Peer IKE ID Type** menu:
   – **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail 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, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when Domain Name is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.

  - **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). 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, i.e. c=us.

7. Type an ID string in the **Peer IKE ID** field.
8. Click on the **Network** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Local Networks

● Choose local network from list --Select Local Network--

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

Destination Networks

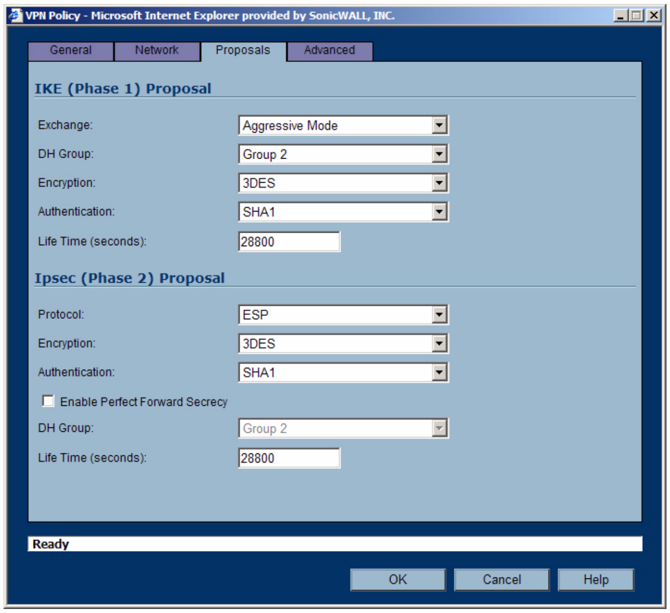
○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list --Select Remote Network--

9. Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.
10. Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

11. Click the **Proposals** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

IKE (Phase 1) Proposal

Exchange: Aggressive Mode
DH Group: Group 2
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 28800

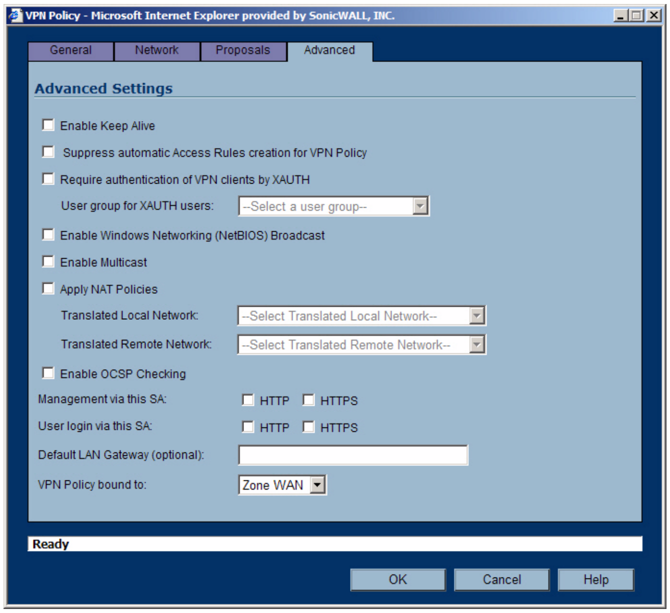
Ipsec (Phase 2) Proposal

Protocol: ESP
Encryption: 3DES
Authentication: SHA1
☐ Enable Perfect Forward Secrecy
DH Group: Group 2
Life Time (seconds): 28800

Ready

12. In the **IKE (Phase 1) Proposal** section, select the following settings:
    - Select **Main Mode** or **Aggressive Mode** from the Exchange menu.
    - Select the desired DH Group from the **DH Group** menu.
    - Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
    - Select the desired authentication method from the **Authentication** menu.
    - 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.
13. In the **IPsec (Phase 2) Proposal** section, select the following settings:
    - Select the desired protocol from the **Protocol** menu
    - Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu
    - Select the desired authentication method from the **Authentication** menu
    - Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.
    - 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.

14. Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Require authentication of VPN clients by XAUTH

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

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Apply NAT Policies

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

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

□ Enable OCSP Checking

Management via this SA: □ HTTP □ HTTPS

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

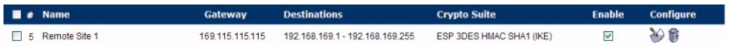
- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. 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** menu. 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 **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See the “Using OCSP with SonicWALL Security Appliances” section in **Chapter 44, Configuring VPN Policies** of the *SonicOS Enhanced 3.2 Administrator’s Guide*.
- To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or Zone from the **VPN Policy bound to** menu. A Zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

15. Click **OK**.

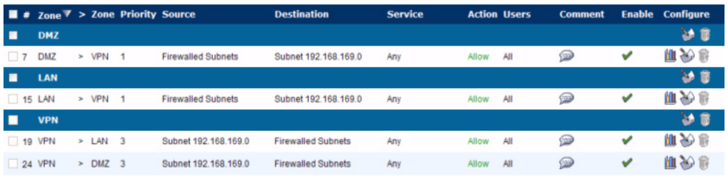
VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS Enhanced auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate Zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet 192.168.169.0. The VPN Policy appears as follows:



■	#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
□	5	Remote Site 1	169.115.115.115	192.168.169.1 - 192.168.169.255	ESP 3DES HMAC SHA1 (IKE)	☑	

And the following Access Rules are added for inbound and outbound traffic:



■	#	Zone	>	Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
■		DMZ											
□	7	DMZ	>	VPN	1	Firewalled Subnets	Subnet 192.168.169.0	Any	Allow	All		✓	
■		LAN											
□	15	LAN	>	VPN	1	Firewalled Subnets	Subnet 192.168.169.0	Any	Allow	All		✓	
■		VPN											
□	19	VPN	>	LAN	3	Subnet 192.168.169.0	Firewalled Subnets	Any	Allow	All		✓	
□	24	VPN	>	DMZ	3	Subnet 192.168.169.0	Firewalled Subnets	Any	Allow	All		✓	

While this is generally a tremendous convenience, there are some instances where is might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke site are addresses using address spaces that can easily be supernetted. For example, assume we wanted to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

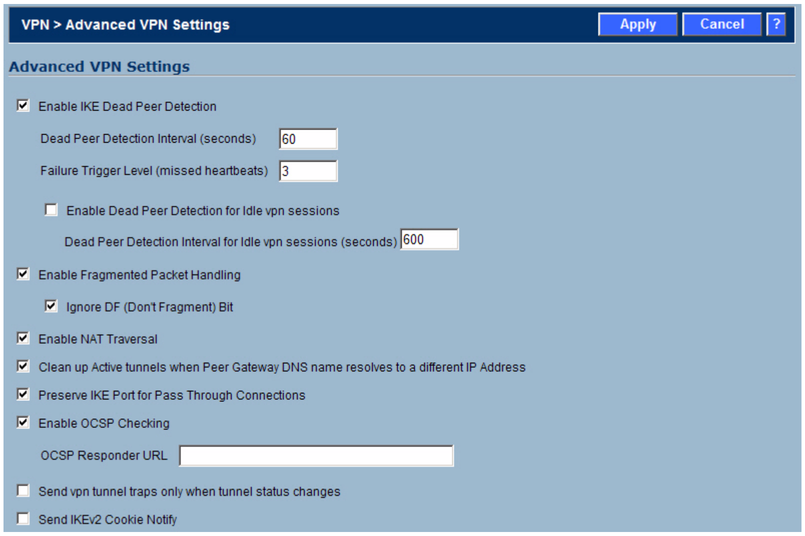
Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just 4 Access Rules to a supernetted or address range representation of the remote sites (More specific allow or deny Access Rules could be added as needed):

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) or
remoteRangeAll=Range 10.0.0.0-10.7.207.255

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** window page offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the checkbox is selected, meaning the accompanying Access Rules will be automatically created, as they've always been. By deselecting the checkbox upon creating the VPN Policy, the administrator will have the ability and need to create custom Access Rules for VPN traffic.

Configuring Advanced VPN Settings

The **VPN** > **Advanced** page includes optional settings that affect all VPN policies.



Advanced VPN Settings

☑ Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds) 60

Failure Trigger Level (missed heartbeats) 3

□ Enable Dead Peer Detection for Idle vpn sessions

Dead Peer Detection Interval for Idle vpn sessions (seconds) 600

☑ Enable Fragmented Packet Handling

☑ Ignore DF (Don't Fragment) Bit

☑ Enable NAT Traversal

☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

☑ Preserve IKE Port for Pass Through Connections

☑ Enable OCSP Checking

OCSP Responder URL

□ Send vpn tunnel traps only when tunnel status changes

□ Send IKEv2 Cookie Notify

Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the SonicWALL.

  Dead Peer Detection Interval - Enter the number of seconds between “heartbeats” in the **Dead peer detection Interval (seconds)** field. The default value is 60 seconds.

  Failure Trigger Level (missed heartbeats) - Enter the number of missed heartbeats in the **Failure Trigger Level (missed heartbeats)** field. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWALL security appliance. The SonicWALL security appliance 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 SonicWALL security appliance 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 - when you select **Enable Fragmented Packet Handling**, the **Ignore DF (Don't Fragment) Bit** setting becomes active.
- **Enable NAT Traversal** - Select this setting is 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.

- **Clean up Active Tunnels when Peer Gateway DNS names resolves to a different IP address** - breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Preserve IKE Port for Pass-Through Connections** - preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.
- **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 Security Appliances.
- **Send IKEv2 Cookie Notify** - sends cookies to IKEv2 peers as an authentication tool.

Using OCSP with SonicWALL Security Appliances

Online Certificate Status Protocol (OCSP) allows you to check VPN certificate status without CRLs. This allows timely updates regarding the status of the certificates used on your SonicWALL.

About OCSP

OCSP is designed to augment or replace Certificate Revocation Lists (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.

Certificate Revocation Lists main disadvantage 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 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 may or may 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 will not 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/ocspd/>. 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 SonicWALL.

1. On the **System** -> **Certificates** page, click on the Import button. This will bring 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.
3. To load a signed local certificate, go to the **System** -> **Certificates** page, click on the **Import** button.
4. Select the **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

The SonicWALL 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 the radio button next to **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.