SonicWall® Global Management System MANAGE VPN

Administration

SONICWALL®

Contents

1

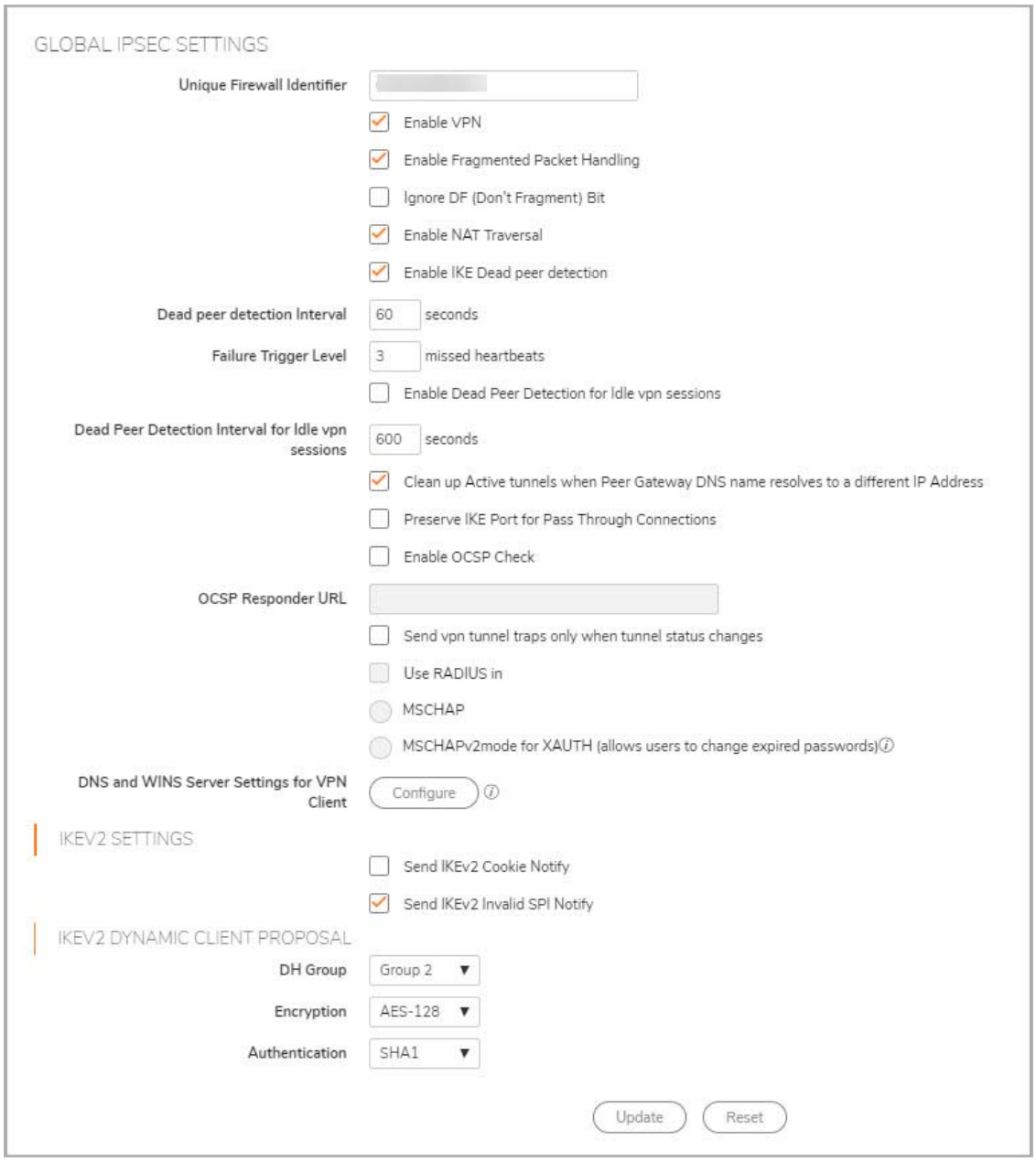
Configuring VPN Settings

Topics:

Enabling VPN

To enable VPN:

1 Navigate to the **VPN** > **Settings** page.



2 The **Unique Firewall Identifier** is an identifier for this SonicWall appliance used for configuring VPN tunnels. The default value is the serial number of the firewall. You can change the Identifier to something meaningful to you.

3 Under **Global IPSec Settings**, select **Enable VPN**. This must be selected to allow VPN policies through the SonicWall security policies.

4 Click **Update**.

Enabling Fragmented Packet Handling

To improve interoperability with other VPN gateways and applications that use a large data packet size, you can enable fragmented packet handling. Packet fragmentation overburdens a network router by resending data packets and causes network traffic to slow down between networks. The **Enable Fragmented Packet Handling** option configures the SonicWall appliance to listen to the intermediate router and, if necessary, send Internet Control Message Protocol (ICMP) messages to the router to decrease the size of the data packets. Enabling this option is recommended when VPN tunnel logs contain a lot of “Fragmented IPSec packets dropped” messages.

To enable fragmented packet handling:

1 Navigate to the **VPN** > **Settings** page.

2 Select **Enable Fragmented Packet Handling**.

3 Click **Update**.

Ignoring the DF Bit in the Packet Header

Some applications can explicitly set the “Don’t Fragment” option in a packet that tells all security appliances to not fragment the packet. The **Ignore DF Bit** option, when enabled, causes the firewall to ignore the option and to fragment the packet regardless.

Setting the Ignore DF bit option:

1 Navigate to the **VPN** > **Settings** page.

2 Select **Ignore DF (Don’t Fragment) Bit**.

3 Click **Update**.

Enabling NAT Traversal

NAT Traversal is an Internet Engineering Task Force (IETF) draft standard that wraps an IPsec packet into a UDP/IP header, allowing NAT devices to change IP addresses without affecting the integrity of the IPsec packet.

To enable NAT traversal:

1 Navigate to the **VPN** > **Settings** page.

2 Select **Enable NAT Traversal**.

3 Click **Update**.

Enabling IKE Dead Peer Detection

To enable detection of a dead peer:

1 Navigate to the **VPN** > **Settings** page.

2 Select **Enable IKE Dead peer detection**.

3 In the **Dead peer detection Interval** field, specify how often the SonicWall appliance should attempt to detect a peer.

4 In the **Failure Trigger Level** field, specify the number of failed attempts that must occur before closing the VPN tunnel.

5 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, select **Enable Dead Peer Detection for Idle vpn sessions**.

6 Click **Update**.

Cleaning Up Active Tunnels

Select the **Clean up Active Tunnels when Peer Gateway DNS names resolves to a different IP Address** option to break down security associations associated with old IP addresses and reconnect to the peer gateway.

To clean up active tunnels:

1 Navigate to the **VPN** > **Settings** page.

2 Select **Clean up Active Tunnels when Peer Gateway DNS names resolves to a different IP Address**.

3 Click **Update**.

Preserving the IKE Port for Pass-Through Connections

To preserve the IKE Port for pass-through connections:

1 Navigate to the **VPN** > **Settings** page.

2 Select **Preserve IKE Port for Pass-Through Connections** to preserve UDP 500/4500 source port and IP address information for pass-through VPN connections.

3 Click **Update**.

Enabling Online Certificate Status Protocol

Use the **Enable OCSP Check** option to enable use of Online Certificate Status Protocol (OCSP) to check VPN certificate status.

To enable use of Online Certificate Status Protocol (OCSP):

1 Navigate to the **VPN** > **Settings** page.

2 Select **Enable OCSP Check**.

3 In the **CSP Responder URL** field, enter the URL of where to check the certificate status.

4 Click **Update**.

Sending Tunnel Traps

By default, the firewall sends traps for VPN up/down status. To minimize email alerts based on VPN traps, use the **Send vpn tunnel traps only when tunnel status changes**. To send tunnel traps when the tunnel status changes.

To send tunnel traps when the tunnel status changes:

1. Navigate to the **VPN** > **Settings** page.
2. Select **Send vpn tunnel traps only when tunnel status changes**.
3. Click **Update**.

Allowing Users to Change Expired Passwords at Login

To allow VPN client users to change their expired passwords at login:

1. Navigate to the **VPN** > **Settings** page.
2. Select **Use RADIUS in**.
3. Select either:
    - **MSCHAP**
    - **MSCHAPv2 mode for XAUTH**.
4. Click **Update**.

Configuring DNS and WINS Server Settings

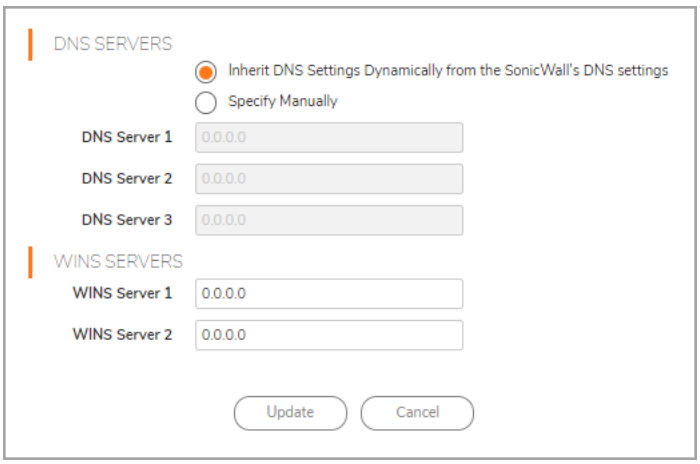
You can configure DNS and WINS server settings for third-party VPN Clients through GroupVPN, or a Mobile IKEv2 Client.

To configure DNS and WINS server settings:

1 Navigate to the **VPN** > **Settings** page.

2 To configure **DNS and WINS server settings for VPN Client**, such as a third-party VPN Client through GroupVPN, or a Mobile IKEv2 Client.

3 Click **Configure** next to **DNS and WINS server settings for VPN Client**. The **Add VPN DNS And WINS Server** dialog displays.



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

4 Click **Update**.

Sending Cookies to IKEv2 Peers

Use the **Send IKEv2 Cookie Notify** option to send cookies to IKEv2 peers as an authentication tool.

To send cookies to IKEv2 peers:

1 Navigate to the **VPN** > **Settings** page.

2 Scroll to the **IKEv2 Settings** section.

3 Select **Send IKEv2 Cookie Notify** to send cookies to IKEv2 peers as an authentication tool.

4 **Click Send IKEv2 Invalid SPI Notify** to send an invalid Security Parameter Index (SPI) notification to IKEv2 peers when an active IKE security association (SA) exists.

5 Click **Update**.

Configuring the Internet Key Exchange (IKE) Attributes

Use the **IKEv2 Dynamic Client Proposal** settings to configure the Internet Key Exchange (IKE) attributes for appliances running GMS, rather than using the default settings.

To configure the Internet Key Exchange (IKE) attributes:

1 Navigate to the **VPN** > **Settings** page.

2 Scroll to the **IKEv2 Dynamic Client Proposal** section.

3 Select a value from the **DH Group** drop-down menu to specify the global IPsec policy for a zero (0.0.0.0) gateway, IKEv2 mode tunnel with dynamic peer gateways from one of these values:

- **Group 1**
- **Group 2**
- **Group 5**
- **Group 14**
- **256-Bit Random ECP Group**
- **384-Bit Random ECP Group**
- **521-Bit Random ECP Group**
- **192-Bit Random ECP Group**
- **224-Bit Random ECP Group**

4 Select a value from the **Encryption** drop-down menu to specify the encryption algorithm in the global IPsec policy for a zero (0.0.0.0) gateway, IKEv2 mode tunnel with dynamic peer gateways whose IP addresses are not static from one of these values:

- **DES**
- **3DES**
- **AES-128**
- **AES-192**
- **AES-256**

5 Select a value from the **Authentication** drop-down menu to specify the authentication algorithm in the global IPsec policy for a zero (0.0.0.0) gateway, IKEv2 mode tunnel with dynamic peer gateways whose IP addresses are not static from one of these values:

- **MD5**
- **SHA1**
- **SHA256**
- **SHA384**
- **SHA512**

If a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPSec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis. The VPN policy on the remote gateway must also be configured with the same settings.

6 Click **Update**.

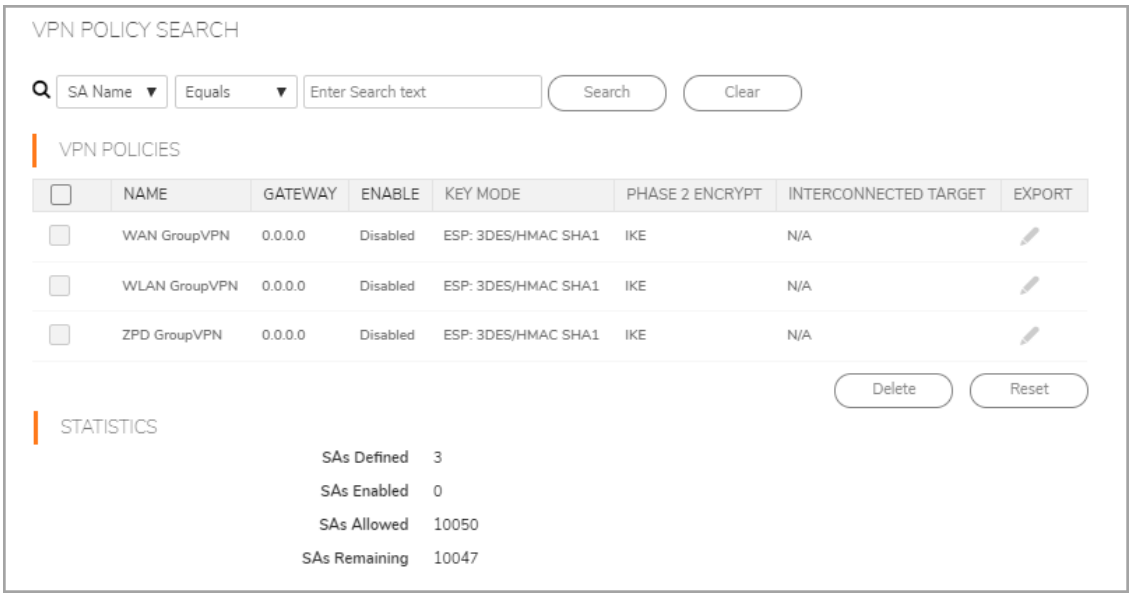
2

Viewing the VPN Summary

To view the VPN summary:

1 Navigate to the **VPN** > **Summary** page. The VPN **Summary** page displays.

NOTE: If VPN is already configured for the SonicWall appliance, a list of current security associations displays. The unique firewall identifier also displays.



When managing VPNs, the VPN Summary Window sometimes can have too many VPNs listed for you to easily find the VPN entry you want to view. Use the **Search** feature to help locate specific gateways or SA names.

Topics:

- Management of VPN Client Users
- VPN Terms and Concepts
- Using OCSP with SonicWall Security Appliances

Management of VPN Client Users

To configure VPN Clients on SonicWall appliances, see the following sections:

- Enabling the VPN Client
- Downloading VPN Client Software

Enabling the VPN Client

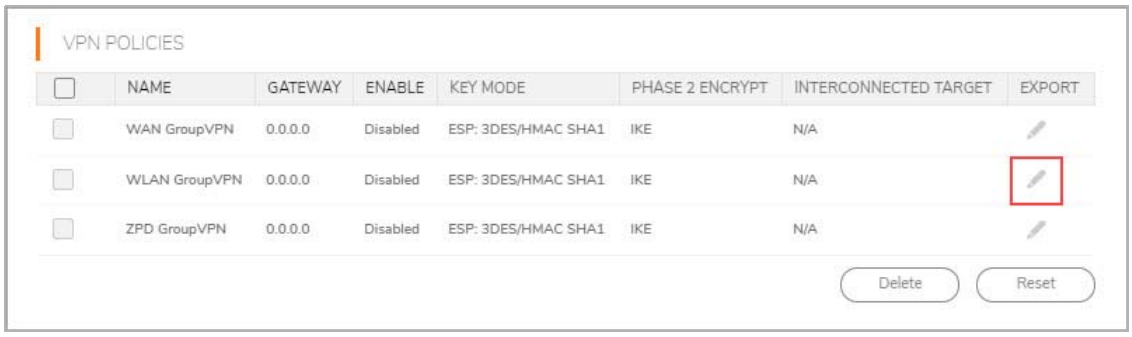
All defined VPN policies are displayed in the VPN Policies table. Each entry displays the following information:

- **Name** – The default name or user-defined VPN policy name.
- **Gateway** – The IP address of the remote firewall. If the wildcard IP address, 0.0.0.0, is used, it is displayed as the IP address.
- **Enable** – Shows whether the policy is enabled. A checked box enables the VPN Policy. Clearing the box disables it.
- **Key Mode** – The IP addresses of the destination networks.
- **Phase 2 Encrypt** – The type of encryption used for the VPN policy.
- **Interconnected Target** – The interconnected appliance.
- **Export** – Exports the VPN policy configuration as a file for local installation by SonicWall Global VPN Clients.

After applying a VPN Client license to one or more SonicWall appliances:

1 Navigate to the **VPN > Summary** page.

2 Click **Export** next to the security association.



3 To email the SPD file to the SonicWall GMS administrator or the VPN Client user, click **Email SPD** file. The file is attached to the email. A task is scheduled for each email.

> **NOTE:** A copy of the SPD file is also stored in the SonicWall Agent's `<GMS_directory\etc` directory.

4 After the SPD file is received, it can be loaded by the VPN Client software on the VPN Client user's computer.

5 If the user does not have the VPN Client software, you can send both the SPD file and the email to the client software by clicking **Email SPD File and VPN Client**.

6 VPN clients use RCF files to import data used to communicate with SonicWall appliances. To send an RCF File to an email address, enter the following information:

- Enter the email address in the **Email Address** field.
- Enter and reenter the RCF File password in the **RCF File Export Password** and **Confirm Password** fields.
- Select whether the file is used for WAN or wireless connections.
- Select from the following:
  - To email the file, click **Email RCF File**.

- To email the file with the Global VPN Client software, click **Email RCF File and Global VPN Client**.

NOTE: Before the VPN client can be emailed to users, it must be downloaded to the `<GMS_directory>\etc` directory from www.MySonicWall.com.

Downloading VPN Client Software

To download the VPN Client software from MySonicWall.com:

1. Navigate to the **Application Configuration Panel | Licenses > Product Licenses** page.
2. Click **Manage**.
3. **Login** using a new window. This opens a new browser into the GMS account on www.MySonicWall.com.
4. Download the VPN Client software from MySonicWall.com to a local directory.
5. Copy the VPN Client software to SonicWall Agent's <*GMS_directory*>\etc directory.
6. Rename the file to `SWVpnClient.zip`.

VPN Terms and Concepts

Before installing and SonicWall VPN, it is important to understand the following basic terms and concepts.

- **Asymmetric vs. Symmetric Cryptography**—Asymmetric and symmetric cryptography refer to the keys used to authenticate, or encrypt and decrypt the data.

  Asymmetric cryptography, or public key cryptography, uses two keys for verification. Organizations such as RSA Data Security and VeriSign support asymmetric cryptography.

  With symmetric cryptography, the same key is used to authenticate on both ends of the VPN. Symmetric cryptography, or secret key cryptography, is usually faster than asymmetric cryptography. Therefore symmetric algorithms are often used when large quantities of data need to be exchanged.

  SonicWall VPN uses symmetric cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- **ARCFour**—ARCFour is used for communications with secure Web sites using the SSL protocol. Many banks use a 40-bit key ARCFour for online banking, while others use a 128-bit key. SonicWall VPN uses a 56-bit key for ARCFour.

  The ARCFour key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9,” and “a” to “f” (such as 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

- **Authentication Header (AH)**—The authentication header is a mechanism for providing strong integrity and authentication for IP packets. The Authentication Header does not offer confidentiality and protection from traffic analysis.

  The IP authentication header provides security by adding authentication information to an IP packet. This authentication information is calculated using all header and payload data in the IP packet. This provides significantly more security than is currently present in IP.

  Use of an AH increases the processing requirements of SonicWall VPN and also increases the communications latency. The increased latency is primarily because of the calculation of the authentication data by the sender and the calculation and comparison of the authentication data by the receiver for each IP packet.

- **Data Encryption Standard (DES)**—When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. The SonicWall DES encryption algorithm uses a 56-bit key.

  The DES Key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9,” and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

- **Encapsulating Security Payload (ESP)**—ESP provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption might be in the form of ARCFour (similar to the popular RC4 encryption method), DES, and so on.

  The use of ESP typically increases the processing requirements and communications latency. The increased latency is primarily because of the encryption and decryption required for each IP packet containing an ESP.

  ESP typically involves encryption of the packet payload using standard encryption mechanisms, such as RC4, ARCFour, DES, or 3DES.

  ESP has no mechanism for providing strong integrity and authentication of the data.

- **Encryption**—Encryption is a mathematical operation that transforms data from “clear text” (something that a human or a program can interpret) to “cipher text” (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric “key” be supplied along with the clear text. The key and clear text are processed by the encryption operation that leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms cipher text to clear text. Decryption also requires a key.

- **Shared Secret**—A shared secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE security association. This field can be any combination of alphanumeric characters with a minimum length of four characters and a maximum of 128 characters. Precautions should be taken when delivering/exchanging this shared secret to assure that a third-party cannot compromise the security of a VPN tunnel.

- **Internet Key Exchange (IKE)**—IKE is a negotiation and key exchange protocol specified by the Internet Engineering Task Force (IETF). An IKE security association automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that are used to pass IP traffic.

- **Key**—A key is an alphanumeric string that is used by the encryption operation to transform clear text into cipher text. A key is composed of hexadecimal characters (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). A valid key would be 1234567890abcdef. Keys used in VPN communications can vary in length, but are typically 16 or 32 characters. The longer the key, the more difficult it is to break the encryption. The reason for this is that most methods used to break encryption involve trying every possible combination of characters, similar to trying to find someone’s telephone number by dialing every possible combination of phone numbers.

- **Manual Key**—Manual keying allows the SonicWall administrator to specify the encryption and authentication keys. SonicWall VPN supports the ability to manually set up a security association as well as the ability to automatically negotiate a security association using IKE.

- **Security Association (SA)**—An SA is the group of security settings needed to create a VPN tunnel. All SAs require an encryption method, an IPSec gateway address, and a destination network address. IKE includes a shared secret. manual keying includes two SPIs and an encryption and authentication key.

  SonicWall PRO appliances supports up to 100 security associations. SonicWall SOHO2 and SonicWall XPRS2 appliances support 10 and 25 security associations, respectively. Different security associations might be created to connect branch offices, allow secure remote management, and pass unsupported traffic.

- **Security Parameter Index (SPI)**—The SPI is used to establish a VPN tunnel. The SPI is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption, and key values that the administrator associated with the SPI to establish the tunnel.

  The SPI must be unique, is from one to eight characters long, and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9,” and “a” to “f” (such as 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, valid SPIs would be 999 or “1234abcd.”

- **Triple Data Encryption Standard (3DES)**—3DES is the same as DES, except that it applies three DES keys in succession and is significantly more secure. However, 3DES has significantly more processing requirements than DES.

  The 3DES Key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9,” and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

- **VPN Tunnel**—Tunneling is the encapsulation of point-to-point transmissions inside IP packets. A VPN Tunnel is a term that is used to describe a connection between two or more private nodes or LANs over a public network, typically the Internet. Encryption is often used to maintain the confidentiality of private data when traveling over the Internet.

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.

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 might or might not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive

response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

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

Topics:

- OpenCA OCSP Responder
- Using OCSP with VPN Policies

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.

NOTE: For GMS to act as an OCSP client to a responder, the CA certificate must be loaded onto the SonicWall system.

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. Then click the VPNs page.

1. Navigate to **VPN > Settings**.
2. Select the radio button next to **Enable OCSP Check**.
3. 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.

3

Configuring VPNs

The GMS uses Address Objects and Address Object Groups to simplify network configuration and interconnection. Address objects are network addresses or hosts. Address object groups are groups of address objects and/or address object groups.

When you configure VPN between Address Object Groups on two SonicWall appliances, the GMS automatically establishes VPN connections between every network within those groups. This saves a lot of configuration time and dramatically simplifies VPN configuration.

Configuring VPNs is supported with IPv6. The configuration procedures for IPv6 and IPv4 are nearly identical, just enter IPv6 addresses in place of IPv4 addresses.

Select from the following:

- Configuring VPNs in Interconnected Mode—For VPNs between two SonicWall appliances.
- Configuring VPNs in Non-Interconnected Mode—For VPN between a SonicWall appliance and another device.

When you have completed the interconnected or non-interconnected configuration procedure, continue on to the following section:

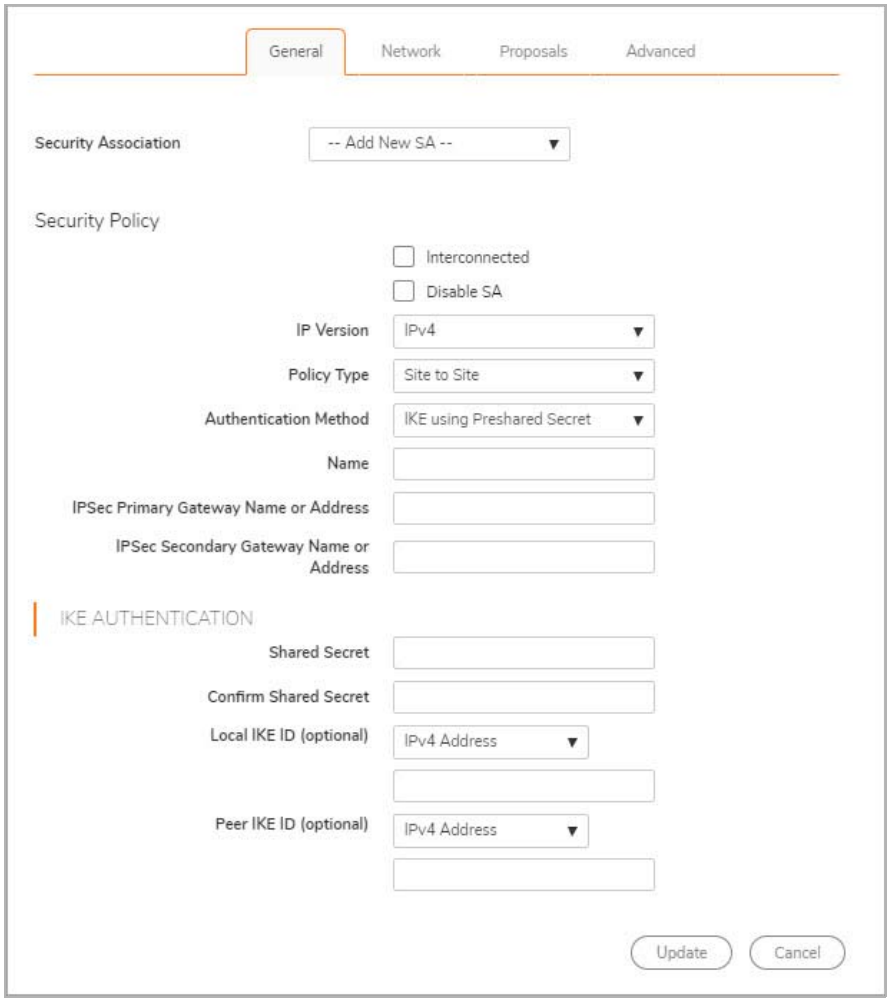
- Generic VPN Configuration

Configuring VPNs in Interconnected Mode

Establishing a VPN between two SonicWall appliances that are being managed by the GMS is easy. Because the GMS is aware of the configuration settings, it automatically configures most of the VPN settings without any user intervention.

To establish VPNs between two SonicWall appliances that are being managed by the GMS:

1 Navigate to the **VPN > Configure** page. The VPN Configure page displays with the **General** view selected.



2 To establish a new security association, select **Add New SA** from the **Security Association** drop-down menu.

3 Select **Interconnected**. The options change.

4 To configure the SonicWall GMS to convert the security associations to non-interconnected mode VPN tunnels, select **Make SAs viewable in Non-Interconnected Mode**.

> **NOTE:** Making a security association viewable in Non-Interconnected mode is not reversible.

5 Select the destination SonicWall appliance by clicking **Select Destination Node** and selecting the node from the dialog box that displays.

6 To initially disable the security association upon creation, select **Disable SA**. This option can always be unchecked later.

7 Select from the following keying modes from the **IPSec Keying Mode** drop-down menu:

> **NOTE:** The SonicWall GMS automatically creates a preshared key, SPI, encryption key, authentication key, or certificate information as applicable, for each mode described as follows.

- **Manual Key**—keys are exchanged in advance. The security association always uses the same encryption and authentication keys. If the keys are compromised by an outside party, they remain compromised until the keys are changed.

- **IKE Using Preshared Secret**—each SonicWall appliance has a shared secret that is used to establish a security association.

  After the security association expires, the SonicWall appliance reestablishes a security association using the same public keys, but does not use the same security and authentication keys. Configure the following:

  - **Local IKE ID**—specifies whether the IP address or SonicWall Identifier is used as the IKE ID for the local SonicWall appliance.
  - **Peer IKE ID**—specifies whether the IP address or SonicWall Identifier is used as the IKE ID for the peer SonicWall appliance.

- **IKE Using 3rd Party Certificates**—the SonicWall appliance and peer device obtain certificates from the third-party certificate authorities. Security and authentication keys are exchanged using public-key cryptography and authenticity of each node is verified by the third-party CA.

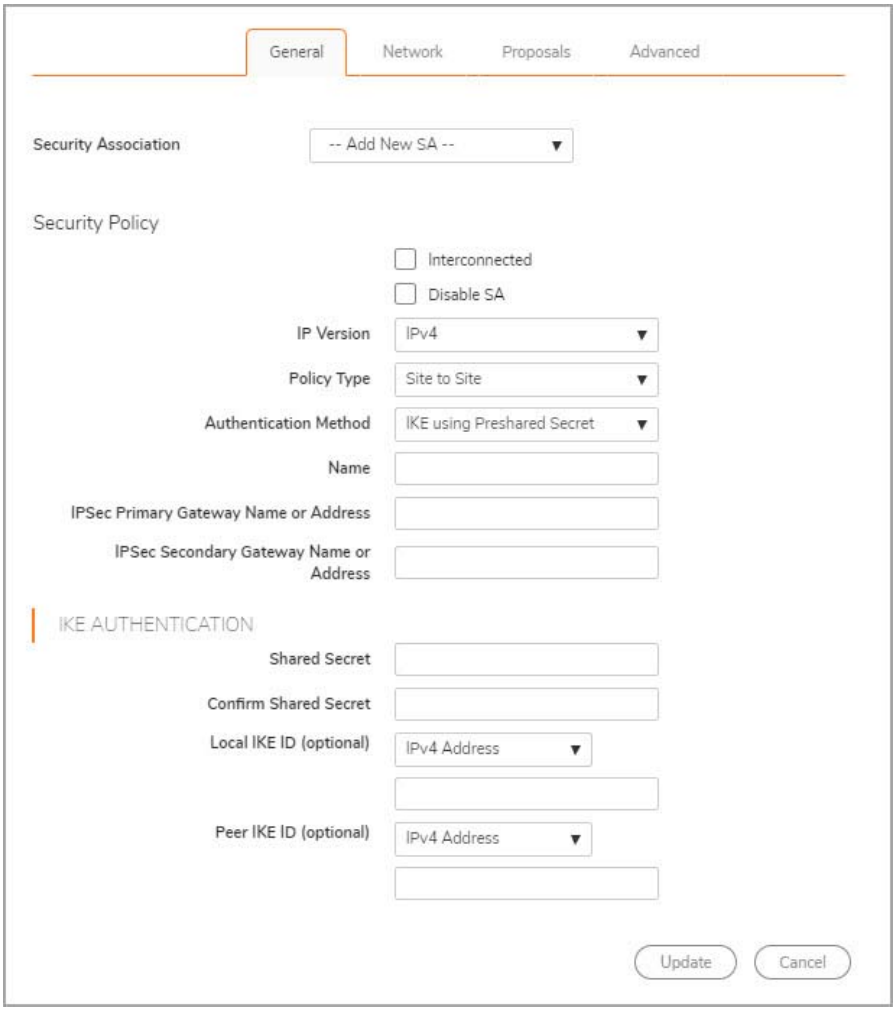
  After the security association expires, the peers reestablish a security association using the same public keys, but do not use the same security and authentication keys.

8 Continue to Generic VPN Configuration.

Configuring VPNs in Non-Interconnected Mode

To establish VPNs between two SonicWall appliances that are being managed by the GMS:

1 Navigate to the **VPN > Configure** page. The VPN Configure page displays with the **General** tab selected. The VPN Configure page displays with the General tab selected.



2 To establish a new security association, select **Add New SA** from the **Security Association** drop-down menu.

3 Deselect **Interconnected**.

4 Select **Disable SA** to initially disable the security association upon creation. This option can be unchecked later.

5 Select from the following keying modes from the **IPSec Keying Mode** drop-down menu:

- **Manual Key**—keys are exchanged in advance. The security association always uses the same encryption and authentication keys. If the keys are compromised by an outside party, they remain compromised until the keys are changed. If you select this option, configure the following:
  - **Name**—specifies the name of the security association.
  - **IPSec Gateway Name or Address**—specifies the name or IP address of the gateway.

- **IKE Using Preshared Secret**—each SonicWall appliance has a shared secret that is used to establish a security association. After the security association expires, the SonicWall appliances reestablishes a security association using the same public keys, but does not use the same security and authentication keys. Configure the following:
    - **Name**—specifies the name of the security association.
    - **IPSec Primary Gateway Name or Address**—specifies the name or IP address of the primary gateway.
    - **IPSec Secondary Gateway Name or Address**—specifies the name or IP address of the secondary gateway.
    - **Shared Secret**—specifies the shared secret used to negotiate the VPN tunnel.
    - **Local IKE ID**—specifies the whether the IP address or SonicWall Identifier is used as the IKE ID for the local SonicWall appliance.
    - **Peer IKE ID**—specifies the whether the IP address or SonicWall Identifier is used as the IKE ID for the peer SonicWall appliance.
- **IKE Using 3rd Party Certificates**—the SonicWall appliance and peer device obtain certificates from the third-party certificate authorities. Security and authentication keys are exchanged using public-key cryptography and authenticity of each node is verified by the third-party CA. After the security association expires, the peers reestablish a security association using the same public keys, but do not use the same security and authentication keys. If you select this option, configure the following:
    - **Name**—specifies the name of the security association.
    - **IPSec Primary Gateway Name or Address**—specifies the name or IP address of the primary gateway.
    - **IPSec Secondary Gateway Name or Address**—specifies the name or IP address of the secondary gateway.
    - **Local Certificate**—specifies the certificate used to establish a security association.
    - **Peer Certificate's ID Type**—specifies the ID type of the peer certificate.
    - **ID string to match**—specifies the string used to establish a security association.

Generic VPN Configuration

To configure the additional options for VPNs in the GMS:

1 Navigate to the **VPN > Configure** page. Click the **Network** view. Select which local networks are establishing VPN connections with the destination networks:
    - **Choose local network from list**—specifies an Address Object that contains one or more networks. For information on creating address objects, refer to the documentation that accompanied the SonicWall appliance.
    - **Local network obtains IP addresses using DHCP through this VPN Tunnel**—indicates that the computers on the local network obtain their IP addresses from the destination network.
    - **Any address**—configures all networks to establish VPN connections with the specified destination networks.

2 Select the destination networks with which the local network connects:
    - **Use this VPN Tunnel as default route for all Internet traffic**—configures all networks on the destination network to use this VPN for all Internet traffic.

- **Destination network obtains IP addresses using DHCP through this VPN Tunnel**—indicates that the computers on the destination network obtain their IP addresses from the local network.
- **Choose destination network from list**—specifies an Address Object that contains one or more networks. For information on creating address objects, refer to the documentation that accompanied the SonicWall appliance.

3 (Optional) Click the **Proposals** view.

4 Select the **IKE (Phase 1) Proposal** Options (Certificates and Preshared Secret only):

- **Exchange**—Select the exchange mode from the **Exchange** drop-down menu. **Aggressive Mode** improves the performance of IKE security association negotiation by only requiring three packet exchanges. However, it provides no identity protection. Otherwise, select **Main Mode**.
- **DH Group**—specifies the Diffie-Hellman group to use when the VPN devices are negotiating encryption and authentication keys.

NOTE: Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.

- **Encryption**—specifies the type of encryption key to use when the VPN devices are negotiating encryption keys.
- **Authentication**—specifies the type of authentication key to use when the VPN devices are negotiating authentication keys.
  - **MD5**
  - **SHA1**
  - **SHA256**
  - **SHA384**
  - **SHA512**
- **Life Time (seconds)**—specifies how long a tunnel remains active before being renegotiated. We recommend a value of 28,800 seconds (eight hours).

5 Select the **IKE (Phase 2) Proposal** options:

- **Protocol**—specifies the type of protocol to use for VPN communications (AH or ESP).
- **Encryption**—specifies the type of encryption key to use when the VPN devices after negotiating encryption keys.
- **Authentication**—specifies the type of authentication key to use when the VPN devices after negotiating authentication keys.
  - **MD5**
  - **SHA1**
  - **SHA256**
  - **SHA384**
  - **SHA512**
  - **AES-XCBC**
  - **None**
- **Enable Perfect Forward Secrecy**—when selected, this option prevents repeated compromises of the same security key when reestablishing a tunnel.

- **DH Group**—specifies the Diffie-Hellman group to use when the VPN devices after negotiating encryption and authentication keys.
- **Life Time (seconds)**—specifies how long a tunnel remains active before being renegotiated. We recommend a value of 28,800 seconds (eight hours).

6 (Optional) Click the **Advanced** view.

7 Configure the following **Advanced** settings:

- **Enable Keep Alive**—configures the VPN tunnel to remain open as long as there is network traffic on the security association.

> **NOTE:** The Allow Advanced Routing, Enable Transport Mode, and Enable Multicast options are available for VPN policies that are configured as follows: Policy Type: Tunnel InterfaceIPSec Keying Mode: IKE using Preshared Secret or IKE using third-party certs.

- **Allow Advanced Routing** - Adds this Tunnel Interface to the list of interfaces in the Advanced Routing table on the **Network > Routing** page. By making this an optional setting, this avoids adding all Tunnel Interfaces to the Advanced Routing table that helps streamline the routing configuration.
- **Enable Transport Mode** - Forces the IPsec negotiation to use Transport mode instead of Tunnel Mode. This has been introduced for compatibility with Nortel. When this option is enabled on the local firewall, it MUST be enabled on the remote firewall as well for the negotiation to succeed.
- **Enable Windows Networking (NetBIOS) Broadcast**—enables NetBIOS broadcasts across the security association.
- **Enable Multicast** - Allows multicast traffic through the VPN tunnel.
- **Permit Acceleration** - Dedicates WXA clustered groups to a VPN and BPR policy.
- **Accept Multiple Proposals for Clients—**enables the system to accept multiple proposals for clients.
- **Enable IKE Mode Configuration—** enables you to configure the IKE Mode feature.
  - **IP Pool for Clients—**select an IP pool type from the drop-down menu.
  - **Address Expiry Time—**enter an expiration time (in seconds) for the address.
- **Apply NAT Policies**—enables NAT for the selected networks.
- **Enable Phase2 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.” The default value is 60 seconds.
  - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWall appliance. The SonicWall appliance uses a UDP packet protected by Encryption as the heartbeat.
- **Management via this SA**—specifies which protocols can be used to manage the SonicWall appliance through this security association. In addition to HTTP, HTTPS, and SNMP, you can enable the SSH management of the device through the IPsec tunnel. When **SSH** is selected in an IPsec Policy, an SSH session can be initiated to the device using the IPsec tunnel for the policy.
- **User login via this SA**—specifies the protocols that users can use to login to the SonicWall appliance through this security association.
- **Default LAN Gateway (optional)** —specifies the default gateway when routing all traffic through this tunnel.

- **Enable OCSP Checking—**enables checking of the Online Certificate Status Protocol.
    - **OCSP Responder URL—**enter the URL for the Online Certificate Status Protocol responder.
- **VPN Policy bound to**—specifies the zone or interface to which the VPN tunnel terminates.
- **Preempt Secondary Gateway**— enables preemption of a secondary gateway to the primary gateway in the IPsec policy. If a secondary gateway is configured in the IPsec Policy, an IPsec tunnel is established with the secondary gateway when the primary gateway is unreachable. If this option is enabled in the policy, a periodic discovery is attempted for the primary gateway and if discovered successfully, tunnels are switched back to the primary gateway from the secondary gateway.
- **Primary Gateway Detection Interval**— specifies the time interval in seconds for the discovery of the primary IPsec gateway if it is unreachable. The minimum value is 120 and the maximum value is 28800.
- **Enable Windows Networking Broadcast**—enables NetBIOS broadcasts across the security association.

8 Click the **Client** view (Group VPNs only).

9 Configure the following **Client** settings:

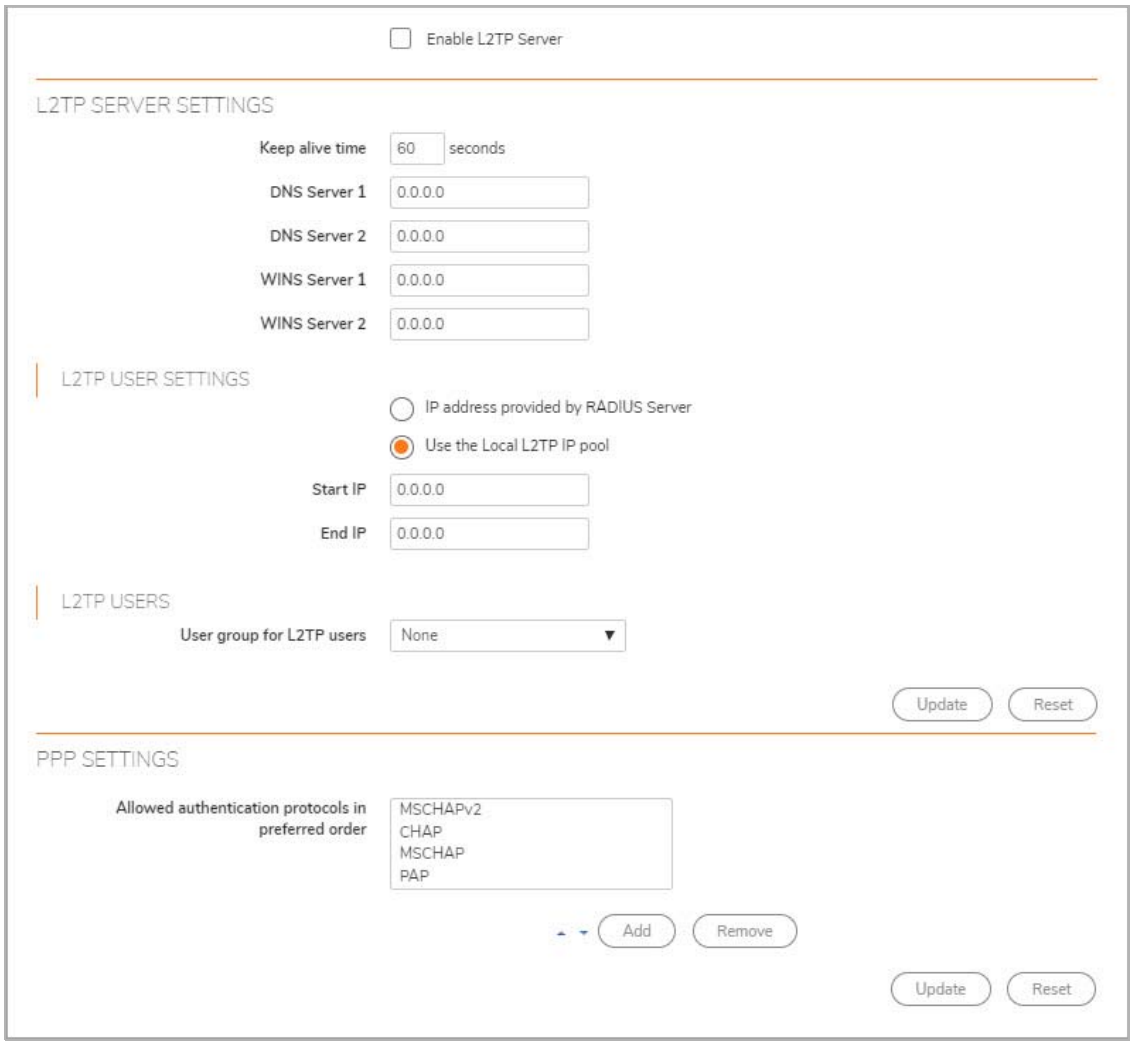
- **Username and Password**—select the settings for the username and password by clicking the drop-down menu and selecting **Never**, **Single Session**, or **Always**.
- **Virtual Adapter Settings**—select the virtual adapter settings from the drop-down menu (**None**, **DHCP Lease**, **DHCP Lease or Manual Configuration**).
- **Allow Connections to**—selects the allowed connections by **Split Tunnels**, **This Gateway Only**, or **All Secure Gateways**.
- **Select Default Route as this Gateway**—select to set the default route as this gateway.
- **Apply VPN Access Control List**—select to apply the VPN Access Control list.
- **Client Initial Provisioning**—select to use the default key for simple client provisioning.

10 When you are finished, click **OK**. The GMS begins establishing VPN tunnels between all specified networks.

Setting up the L2TP Server

To support secure LT2P connections from remote clients:

1 Navigate to the **VPN > L2TP Server** page. The L2TP Server page displays.



2 Select **Enable L2TP Server**.

3 Specify how often the SonicWall appliance issues a Keepalive in the **Keep alive time (secs)** field.

4 Enter the IP addresses of the DNS Servers in the **DNS Server** fields.

5 Enter the IP addresses of the WINS Servers in the **WINS Server** fields.

6 Select from the following:

- To assign IP addresses to L2TP clients that are provided by the RADIUS server, select **IP address provided by RADIUS Server**.

- To use IP addresses from a local L2TP IP address pool, select **Use the Local L2TP IP pool** and enter the starting and ending IP addresses in the **Start IP** and **End IP** fields.

7 Assign appropriate groups using the **User group for L2TP users** drop-down menu.

8 Enter **PPP Settings**.

- Click **Add** to input allowed authentication protocols. Use the arrows to reorder the protocols as you prefer.
- Click **Remove** to remove any unnecessary protocols.

9 When you are finished, click **Update**. To clear all screen settings and start over, click **Reset**.

5

AWS VPN

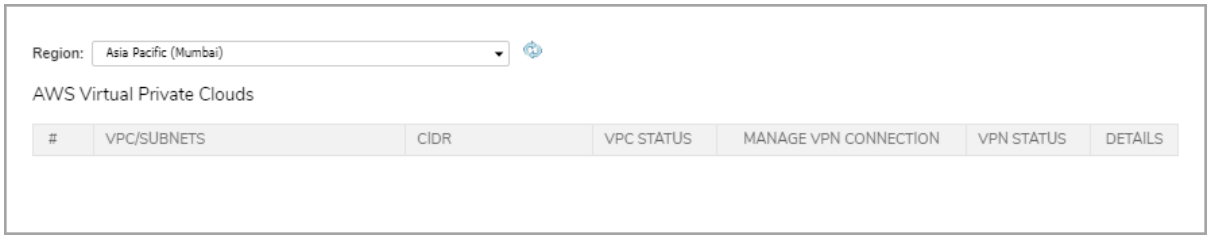
The AWS VPN page makes it easy to create VPN connection from the SonicWall firewall to Virtual Private Clouds (VPCs) on Amazon Web Services (AWS). For more information about Amazon Virtual Private Cloud, refer to https://aws.amazon.com/vpc/.

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

Topics:

Overview

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



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

Creating a New VPN Connection

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

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

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

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

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

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

Reviewing the VPN Connection

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

On the firewall, navigate to **VPN > AWS VPN**. Find the row in the VPC table corresponding to the AWS VPC in question and click **Information**. Details of the VPN connection are shown.

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

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

- Configuration on the Firewall
- Configuration on Amazon Web Services

Configuration on the Firewall

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

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

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

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

Configuration on Amazon Web Services

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

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

Route Propagation

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

- When Creating the VPN Connection

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

- Using checkboxes for each route table

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

- On the AWS Console

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

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

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

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

AWS Regions

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

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

Deleting VPN Connections

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

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

6

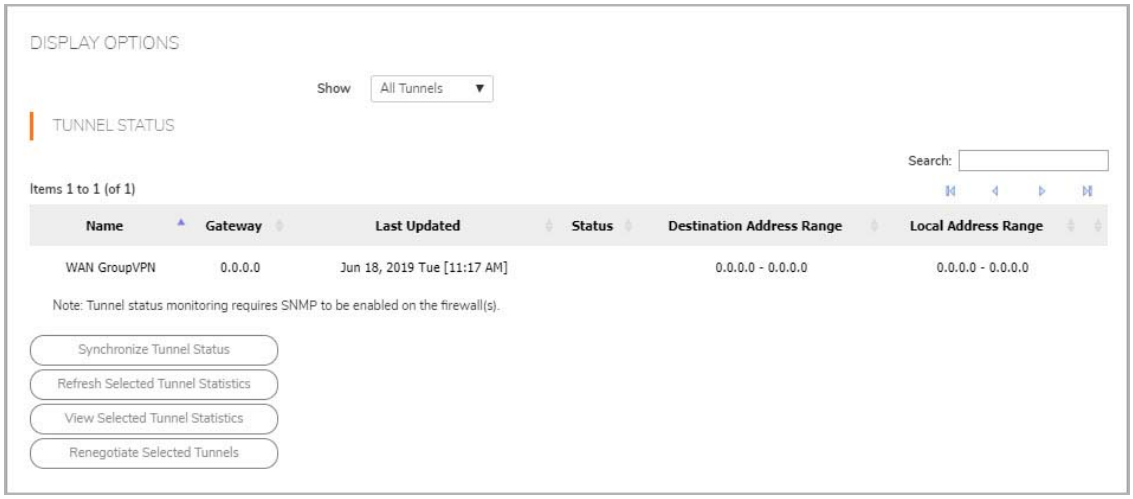
Monitoring VPN Connections

Topics:

Viewing the Tunnel Status

To view the tunnel status:

1 Navigate to the **VPN > Monitor** page.



2 Select the category of tunnels to display the **Display Options** section and click **Refresh Selected Tunnel Statistics**. You can select **Show Up Tunnels**, **Show Down Tunnels, or Show All Tunnels**.

Synchronizing the Tunnel Status Information

To synchronize the tunnel status information:

1 Navigate to the **VPN > Monitor** page.

2 Click **Synchronize Tunnel Status**.

Refreshing the Statistics

To refresh the statistics:

1 Navigate to the **VPN > Monitor** page.

2 Click **Refresh Selected Tunnel Statistics**.

Viewing the Tunnel Statistics

To view the tunnel statistics:

1 Navigate to the **VPN > Monitor** page.

2 Select one or more tunnels and click **View Selected Tunnel Statistics**.

Renegotiating Selected Tunnels

To renegotiate selected tunnels:

1 Navigate to the **VPN > Monitor** page.

2 Select one or more tunnels and click **Renegotiate Selected Tunnels**.

7

SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.SonicWall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.SonicWall.com/support/contact-support.

About This Document

Legend

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

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Global Management System VPN Administration
Updated - October 2019
Software Version - 9.2
232-005126-00 RevA