# 11 SonicWALL VPN

SonicWALL VPN provides secure, encrypted communication to business partners and remote offices at a fraction of the cost of dedicated leased lines. Using the SonicWALL intuitive Web Management Interface, you can quickly create a VPN Security Association to a remote site. Whenever data is intended for the remote site, the SonicWALL automatically encrypts the data and sends it over the Internet to the remote site, where it is decrypted and forwarded to the intended destination.

SonicWALL VPN is based on the industry-standard IPSec VPN implementation, so it is interoperable with other VPN products, such as Check Point FireWall-1 and Axent Raptor. Visit the VPN Center at <http://www.sonicwall.com/vpn-center/vpn-setup.html> SonicWALL VPN is included with the SonicWALL TELE3, the SonicWALL PRO 200 and the SonicWALL PRO 300. It can also be purchased as an upgrade.

This chapter is organized into the following sections:

- **The VPN Summary Tab** describes the **Summary** tab and settings.
- **Enabling Group VPN on the SonicWALL** demonstrates the configuration of SonicWALL Group VPN settings using the Group VPN Security Association.
- **Configuring VPN using Manual Key** describes the configuration of a SonicWALL appliance and a VPN client using the Manual Key Security Association.
- **SonicWALL VPN for two SonicWALLs** describes VPN configuration between two SonicWALL VPN gateways in Manual Key and IKE keying modes, followed by an example VPN Security Association between a SonicWALL PRO 200 and a SonicWALL TELE3.
- **Testing a VPN Tunnel Connection** provides directions for testing a VPN tunnel configuration by using "ping" to send data packets to a remote computer.
- **Enhanced VPN Logging Settings** describes logging settings for both the SonicWALL appliance and the VPN client for troubleshooting VPN problems.
- **XAUTH/RADIUS Server Configuration** describes using a RADIUS server for authentication of VPN Clients.
- **Deleting and Disabling Security Associations** describes deleting and disabling Security Associations for VPN access.
- **Basic VPN Terms and Concepts** provides a glossary defining applicable VPN terms such as encryption methods, authentication methods, and IPSec keying modes.

## VPN Applications

- **Linking Two or More Networks Together**

  SonicWALL VPN is the perfect way for you to connect to your branch offices and business partners over the Internet. SonicWALL VPN offers an affordable, high-performance alternative to leased site-to-site lines. If NAT is enabled, SonicWALL VPN also provides access to remote devices that have been assigned private IP addresses.

- **Remotely Managing the SonicWALL**

  The SonicWALL PRO 200, the SonicWALL PRO 300 and the SonicWALL VPN Upgrade include a free VPN client for remote administration. The SonicWALL VPN client, installed on Windows 95, 98, ME, NT, 2000, and XP, allows you to securely manage the SonicWALL over the Internet.

- **Accessing Network Resources from a VPN Client**

  VPN client remote access allows your employees to connect to your network from any location. The VPN client remote access solution is easy to deploy and supports hundreds of remote users. The SonicWALL PRO 300 includes 50 VPN client licenses for remote access. Please contact your local reseller for information about purchasing additional VPN clients.

**VPN Feature Chart**

| SonicWALL Model | VPN | Security Associations | VPN Clients | Simultaneous VPN Client Connections |
|---|---|---|---|---|
| SonicWALL TELE3 | Included | 5 SAs | | 6,000 VPN Clients |
| SonicWALL SOHO3/10 | Optional | 10 SAs | | 6,000 VPN Clients |
| SonicWALL SOHO3/50 | Optional | 10 SAs | | 6,000 VPN Clients |
| SonicWALL PRO 100 | Optional | 50 SAs | | 6,000 VPN Clients |
| SonicWALL PRO 200 | Included | 1,000 SAs | 1 Included | 30,000 VPN Clients |
| SonicWALL PRO 300 | Included | 2,000 SAs | 51 Included | 128,000 VPN Clients |

***Note**: The values shown in the **Simultaneous VPN Client Connections column** represent the maximum number of VPN clients that should connect to the SonicWALL at the same time. Although the number of VPN clients configured and deployed can exceed this limit, only the number specified in the VPN Feature Chart can connect at the same time without affecting the performance of the SonicWALL.*

# The VPN Interface

Click **VPN** on the left-side of the SonicWALL management station interface. There are four tabs in the VPN interface:

- **Summary**
- **Configure**
- **RADIUS**
- **Certificates**

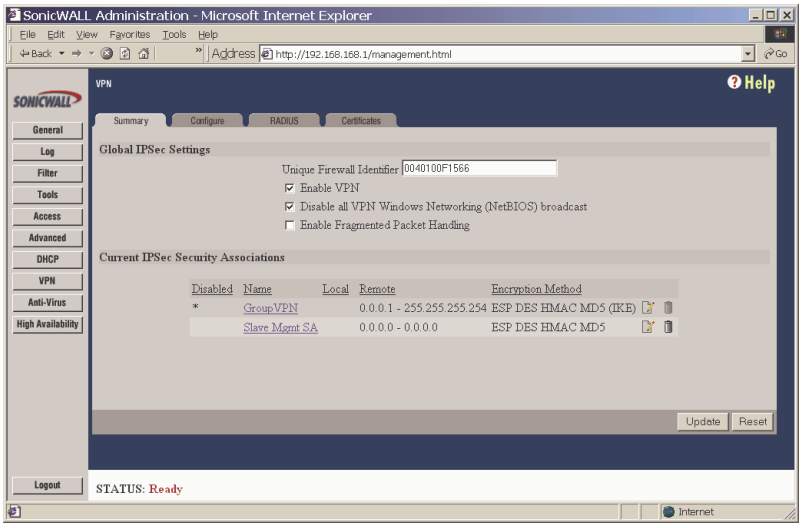
The **Summary** tab has two sections: the **Global IPSec Settings**, and the **Current IPSec Security Associations**.

### Global IPSec Settings

The **Global IPSec Settings** section displays the **Unique Firewall Identifier** which defaults to the serial number of the SonicWALL appliance. You can change the **Identifier**, and use it for configuring VPN tunnels. **Enable VPN** must be selected to allow VPN security associations. **Disable all VPN Windows Networking (NetBIOS) broadcast** is also selected. This check box disables NetBIOS broadcasts for every Security Association configuration. **Enable Fragmented Packet Handling** should be selected if the VPN log report shows the log message "Fragmented IPSec packet dropped". Do not select it until the VPN tunnel is established and in operation.

### Current IPSec Security Associations

This section displays all of the VPN configurations in the SonicWALL appliance. If you click the name of the security association, the security association settings are displayed. The **Security Association**, **Group VPN**, is a default setting.



## SonicWALL VPN Client for Remote Access and Management

This section covers the configuration of SonicWALL VPN and the installation and configuration of the VPN client software. You can create a VPN client Security Association by using **Manual Key Configuration**, **Group Configuration** or **Advanced Configuration**. **Group Configuration**, **Manual Key Configuration,** and **IKE Configuration** (SonicWALL to SonicWALL) are described in this chapter. **Advanced Configuration** is available at the SonicWALL Web site. Before choosing your VPN client configuration, evaluate the differences between the three methods.

**Group Configuration** uses IKE (Internet Key Exchange) and requires fewer settings on the VPN client, enabling a quicker setup. Simple configuration allows multiple clients to connect to a single Security Association (SA), creating a group VPN tunnel. The SonicWALL only supports one **Group Configuration** SA. You can use the Group VPN SA for your single VPN client.

**Manual Key Configuration** requires matching encryption and authentication keys. Because **Manual Key Configuration** supports multiple SAs, it enables individual control over remote users.

**Simple Configuration Using Pre-shared Secret** is a VPN client configuration that is appropriate only for firmware versions 5.1.1 or below.

**Advanced Configuration** requires a complex setup and is therefore not recommended for most SonicWALL administrators. **Advanced Configuration** instructions are available on the Web at the following address: <http://www.sonicwall.com/products/documentation/VPN_documentation.html>.

When you register the SonicWALL PRO 200, the SonicWALL PRO 300, or the SonicWALL VPN Upgrade at <http://www.mysonicwall.com>, you receive a single VPN client for Windows and a VPN Client serial number. Using the VPN client software, you can establish a secure VPN tunnel to remotely manage the SonicWALL. Contact your SonicWALL reseller for information about purchasing additional VPN client licenses for remote access.

## The Configure Tab

The **Configure** tab contains the following sections:

- **Add/Modify IPSec Security Associations**
- **Security Policy**
- **Advanced Settings**
- **VPN Client Configuration File Export (only Group VPN)**

### Add/Modify IPSec Security Associations

In this section, select the type of **Security Association** from the list. Choose either **Group VPN** (default) or **Add New SA**. If you select **Add New SA**, a **Name** field is displayed that allows you to create a name for the SA, such as Boston Office, Corporate Site, etc.

Select the type of security policy for the SA from the **IPSec Keying Mode** menu. You can select **IKE using Preshared Secret**, **Manual Key**, or **IKE using Certificates**.

To disable the SA, select **Disable This SA**. If selected, you can disable a security association temporarily if problems occur with it.

The **IPSec Gateway Address** field is used to configure the gateway for the security association.

### Security policy Settings for IKE using Pre-shared Secret

- **Phase 1 DH Group** - Diffie-Hellman (DH) key exchange (a key agreement protocol) is used during phase 1 of the authentication process to establish pre-shared keys. Select from one of three settings:

  **- Group 1**

  - **Group 2**

  - **Group 5**

  **Groups 1, 2, 5** use Modular-Exponential with different prime lengths as listed below:

| Group Descriptor | Prime Size (bits) |
|---|---|
| Group 1 | 768 |
| Group 2 | 1024 |
| Group 5 | 1536 |

  If network speed is preferred, select **Group 1**. If network security is preferred, select **Group 5**. To compromise between network speed and network security, select **Group 2**.

- **SA Life time (secs) -** This field allows you to configure the length of time a VPN tunnel is active. The default value is 28800 seconds (eight hours).

- **Phase 1 Encryption/Authentication** - You can also select an encryption method from the **Encryption/Authentication** for the VPN tunnel. If you select **IKE using Pre-Shared Secret** for your SA, you can select from one of four encryption methods:

  - **DES & MD5**

  **- DES & SHA1**

  **- 3DES & MD5**

  **- 3DES & SHA1**

  These are listed in order from least secure to most secure. If network speed is preferred, then select **DES & MD5**. If network security is preferred, select **3DES & SHA1**. To compromise between network speed and network security, select **DES & SHA1**.

- **Phase 2 Encryption/Authentication** - Each encryption method is described in the step by step configuration instructions for **Ike using preshared secret**. However, **Phase 2 Encryption/Authentication** is different for the **Group VPN SA**. The VPN Client does not support ArcFour encryption methods, and you cannot disable authentication in the VPN client. The following encryption methods are available for Group VPN and are listed in order from most secure to least secure:

  - **Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)**

  - **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)**

  - **Strong Encrypt and Authenticate (ESP DES HMAC SHA1)**

  - **Strong Encrypt and Authenticate (ESP DES HMAC MD5)**

- If **IKE using Pre-shared Secret** is selected for the **IPSec Keying Mode**, the **Shared Secret** field is displayed and you can type in your shared secret. If **Group VPN using preshared secret** is selected, an alphanumeric key is automatically generated.

**Security Policy Settings using Manual Key**

**Manual Key** is configured differently than **IKE using Pre-shared Secret** or **Group VPN**. It requires an **Incoming** and **Outgoing Security Parameter Index (SPI)** as well as an **Encryption Key** and **Authentication Key**.

- **Incoming SPI** - Enter the Security Parameter Index (SPI) that the remote location transmits to identify the Security Association used for the VPN Tunnel. The SPI may be up to eight characters long and is comprised 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). The hexadecimal characters "0" to "ff" inclusive are reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. These numbers are not accepted by the SonicWALL when entered as an SPI; an error message is displayed at the bottom of the Web browser window when **Update** is pressed. For example, a valid SPI would be 1234abcd.

- **Outgoing SPI** - Enter the Security Parameter Index (SPI) that the local SonicWALL transmits to identify the Security Association used for the VPN Tunnel. The SPI may be up to eight characters long and is comprised 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). The hexadecimal characters "0" to "ff" inclusive are reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. These numbers are not accepted by the SonicWALL when entered as an SPI; an error message is displayed at the bottom of the Web browser window when **Update** is pressed. For example, a valid SPI would be 1234abcd.

***Note**: A Security Association's SPI must be unique when compared to SPIs used in other Security Associations. However, a Security Association's **Incoming SPI** may be the same as the **Outgoing SPI**.*

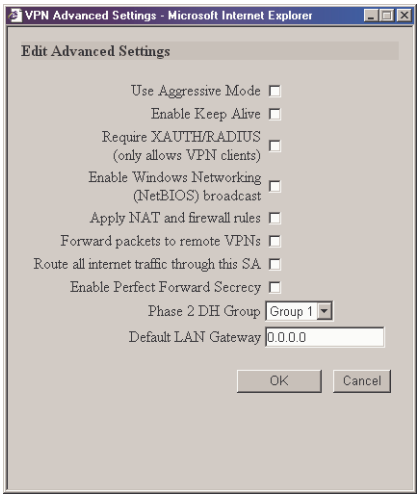
### Destination Networks

In this section, enter the network settings for the remote VPN site. Include the subnet mask which determines broadcast addresses for NetBIOS support.

### VPN Advanced Settings

All of the **Advanced Settings** for VPN connections are accessed by clicking **Advanced Settings** located on the **Configure** tab. The following settings are available in the **Edit Advanced Settings** window:

- **Use Aggressive Mode**
- **Enable Keep Alive**
- **Require XAUTH/RADIUS (only allows VPN clients)**
- **Enable Windows Networking (NetBIOS) broadcast**
- **Apply NAT and firewall rules**
- **Forward packets to remote VPNs**
- **Route all internet traffic through this SA**
- **Enable Perfect Forward Secrecy**
- **Phase 2 DH Group**
- **Default LAN Gateway**




### Use Aggressive Mode

Selecting the **Use Aggressive Mode** check box forces the SonicWALL appliance to use Aggressive Mode to establish the VPN tunnel even if the SonicWALL has a static IP address. Aggressive Mode requires half of the main mode messages to be exchanged in Phase One of the SA exchange. **Use Aggressive Mode** is useful when the SonicWALL is located behind another NAT device. The check box is only available if **IKE using Pre-shared Secret** or **IKE using certificates** (SonicWALL to SonicWALL) is selected as the **IPSec Keying Mode**.

### Enable Keep Alive

Selecting the **Enable Keep Alive** check box allows the VPN tunnel to remain active or maintain its current connection by listening for traffic on the network segment between the two connections. Interruption of the signal forces the tunnel to renegotiate the connection.

### Require XAUTH/RADIUS (only allows VPN Clients)

An IKE Security Association can be configured to require RADIUS authentication before allowing VPN clients to access LAN resources. XAUTH/RADIUS authentication provides an additional layer of VPN security while simplifying and centralizing management. RADIUS authentication allows many VPN clients to share the same VPN configuration, but requires each client to authenticate with a unique user name and password.

### Enable Windows Networking (NetBIOS) broadcast

Computers running Microsoft Windows® communicate with one another through NetBIOS broadcast packets. Select the **Enable Windows Networking (NetBIOS) broadcast** check box to access remote network resources by browsing the Windows® Network Neighborhood.

### Apply NAT and firewall rules

This feature allows a remote site's LAN subnet to be hidden from the corporate site, and is most useful when a remote office's network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN.

If the SonicWALL uses the **Standard** network configuration, using this check box applies the firewall access rules and checks for attacks, but not NAT.

***Note**: You cannot use this feature if you have **Route all internet traffic through this SA** enabled.*

***Note**: Offices can have overlapping LAN IP ranges if this feature is selected.*

### Forward Packets to Remote VPNs

Selecting the **Forward Packets to Remote VPNs** check box for a **Security Association** allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can now be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN specified on the **Routes** tab located under the **Advanced** section.

Enabling this feature allows a network administrator to create a "hub and spoke" network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a "hub and spoke" network, enable the **Forward Packets to Remote VPNs** check box for each Security Association in your SonicWALL. Traffic can travel from a branch office to a branch office via the corporate office.

### Route all internet traffic through this SA

Selecting this box allows a network administrator to force all WAN-destined traffic to go through a VPN tunnel to a central site. Outgoing packets are checked against the remote network definitions for all Security Associations (SA). If a match is detected, the packet is then routed to the appropriate destination. If no match is detected, the SonicWALL checks for the presence of a SA using this configuration. If an SA is detected, the packet is sent using that SA. If there is no SA with this option enabled, and if the destination does not match any other SA, the packet goes unencrypted to the WAN.

***Note:** Only one SA can have this check box enabled.*

### Enable Perfect Forward Secrecy

The **Enable Perfect Forward Secrecy** check box increases the renegotiation time of the VPN tunnel. By enabling **Perfect Forward Secrecy**, a hacker using brute force to break encryption keys is not able to obtain other or future IPSec keys. During the phase 2 renegotiation between two SonicWALL appliances or a Group VPN SA, an additional Diffie-

Hellmen key exchange is performed. **Enable Perfect Forward Secrecy** adds incremental security between gateways.

### Phase 2 DH Group

If Enable Perfect Forward Secrecy is enabled, select the type of Diffie-Hellmen (DH) Key Exchange (a key agreement protocol) to be used during phase 2 of the authentication process to establish pre-shared keys. You can now select from three well-known DH groups:

- **Group 1** - less secure
- **Group 2** - more secure
- **Group 5** - most secure

Groups 1, 2, and 5 use Modular-Exponentiation with different prime lengths as listed below:

| Group Descriptor | Prime Size (bits) |
|---|---|
| 1 | 768 |
| 2 | 1024 |
| 5 | 1536 |

If network connection speed is an issue, select **Group 1**. If network security is an issue, select **Group 5**. To compromise between speed and security, select **Group 2**.

### Default LAN Gateway

A **Default LAN Gateway** is used at a central site in conjunction with a remote site using the **Route all internet traffic through this SA** check box. The **Default LAN Gateway** field 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.

## Advanced Settings for VPN Configurations

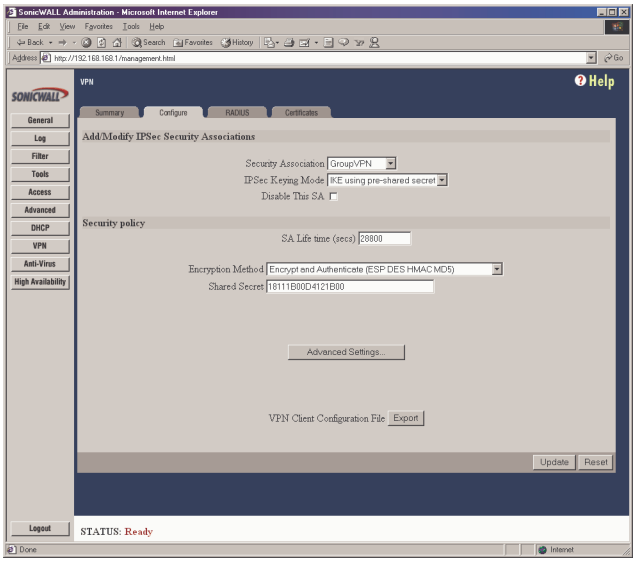
The following table lists the available settings for each VPN configuration. The boxes checked are applicable to the given configuration mode.

| | Group VPN using IKE / Pre-shared Secret | Group VPN using IKE / Certificates | Manual Key* | IKE using Pre-shared Secret | IKE using Certificates |
|---|---|---|---|---|---|
| **Use Aggressive Mode** | | | | ✓ | ✓ |
| **Enable Keep Alive** | | | | ✓ | ✓ |
| **Require XAUTH / RADIUS** | ✓ | | | ✓ | |
| **Enable Windows Networking (NetBIOS) broadcast** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Apply NAT and Firewall Settings** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Forward Packets to Remote VPNs** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Route all internet traffic through this SA** | | | ✓ | ✓ | ✓ |
| **Enable Perfect Forward Secrecy** | ✓ | ✓ | | ✓ | ✓ |
| **Phase 2 DH Group** | ✓ | ✓ | | ✓ | ✓ |
| **Default LAN Gateway** | ✓ | ✓ | ✓ | ✓ | ✓ |

*Default LAN Gateway and Forward Packets to Remote VPN are not configured for VPN Client to SonicWALL appliance connections using Manual Key Exchange.

## Enabling Group VPN on the SonicWALL

Click **VPN** on the left side of the SonicWALL browser window, and then click **Configure**.




The SonicWALL **VPN** tab defaults to a **Group VPN** setting. This feature facilitates the set up and deployment of multiple VPN clients by the administrator of the SonicWALL appliance. Security settings can now be exported to the remote client and imported into the remote VPN client settings. **Group VPN** allows for easy deployment of multiple VPN clients making it unnecessary to individually configure remote VPN clients. **Group VPN** is only available for VPN clients and it is recommended to use **Authentication Service** or XAUTH/RADIUS in conjunction with the **Group VPN** for added security.

To enable **Group VPN**, follow the instructions below:

1. Click **VPN** on the left side of the Management Station interface.
2. Click on **Group VPN**. The **Security Association** default setting is **Group VPN**.
3. Configure the **Group VPN** to use either **IKE using Pre-shared Secrets** or **IKE using Certificates**. To use certificates, an **Authentication Service** upgrade must be purchased.
4. Select **Group 2** from the **Phase 1 DH Group** menu.
5. Enter the **SA Life Time** value in minutes. A value of 28800 seconds (8 hours) is recommended.
6. Select **DES & MD5** from the **Phase 1 Encryption/Authentication** menu.

7. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** from the **Phase 2 Encryption/Authentication** menu.
8. Create and enter a **Shared Secret** in the **Shared Secret** field or use the **Shared Secret** automatically generated by the SonicWALL. The **Shared Secret** should consist of a combination of letters and numbers rather than the name of a family member, pet, etc. It is also case-sensitive.
9. Click **Advanced Settings** to open the window. Select any of the following boxes that apply to your SA:
   - **Require XAUTH/RADIUS (Only allows VPN clients)** if using a RADIUS server.
   - **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
   - **Forward packets to remote VPNs** - if creating a "hub and spoke" network
   - **Enable Perfect Forward Secrecy** - for additional security.
   - **Phase 2 DH Group** - generates a additional key exchange.
   - **Default LAN Gateway** - The **Default LAN Gateway** field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

   ***Note**: It is not necessary to configure the Advanced Settings to get the VPN connection working between the SonicWALL and the VPN client. You can configure the Advanced Settings later, and then re-import the SA into the VPN Client.*
10. Click **Update** to enable the changes.

To export the **Group VPN** settings to remote VPN clients, click on **Export** next to **VPN Client Configuration File**. The security file can be saved to a floppy disk or e-mailed to a remote VPN client. The **Shared Secret**, however, is not exported, and must be entered manually by the remote VPN client. Also, the SA must be enabled to export the configuration file.

***Note**: You must use the **Group VPN Security Association** even if you have only one VPN client to deploy, and you want to use IKE using Pre-shared Secret for your SA. The **Group VPN Security Association** defaults to the **Simple Configuration** previously available in firmware version 5.1.1.*

### Installing the VPN Client Software

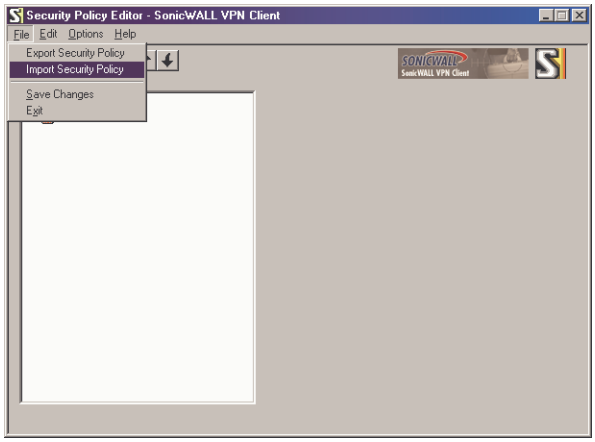
1. When you register your SonicWALL or SonicWALL VPN Upgrade, a unique VPN client serial number and link to download the SonicWALL VPN Client zip file is displayed.
2. Unzip the SonicWALL VPN Client zip file.
3. Double-click **setup.exe** and follow the VPN client setup program step-by-step instructions. Enter the VPN client serial number when prompted.
4. Restart your computer after you have installed the VPN client software.

For detailed instructions on installing the client software, download the **Client Installation Guide** available at http:// www.sonicwall.com/documentation.html.

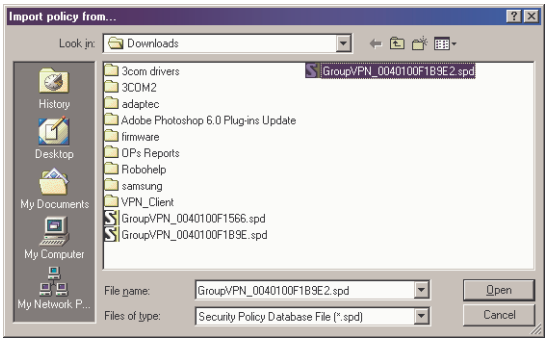
## Group VPN Client Configuration

To import the **Group VPN** security policy into the VPN Client, use the following steps:

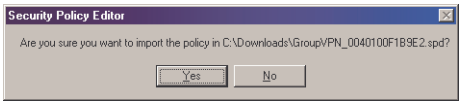
1. Open the **VPN Client**. Click **File**, and then **Import Security Policy**.




2. A file location box appears which allows you to search for the location of the saved security file. Select the file, and click **Open**.

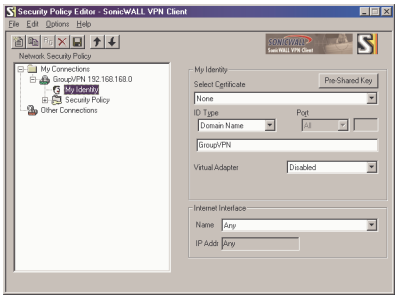


3. A dialogue box asking to import the security file appears.

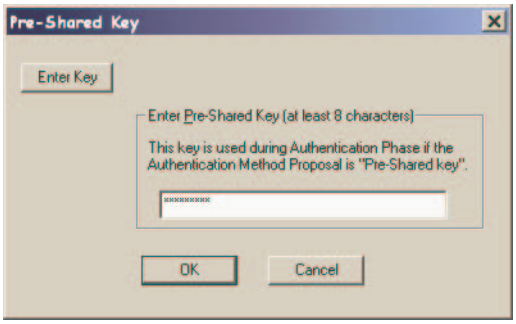



Click **Yes**, and another box appears confirming the file is successfully imported into the client. The client application now has an imported **Group VPN** policy.

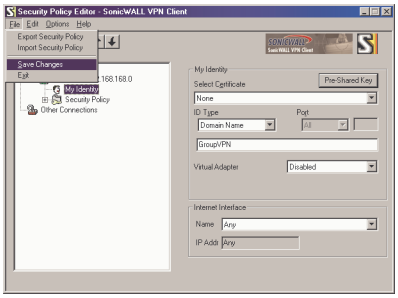

4. Click the **+** sign next to **Group VPN** to reveal two sections: **My Identity** and **Security Policy**. Select **My Identity** to view the settings.




5. Click **Pre-Shared Key** to enter the **Pre-Shared Secret** created in the **Group VPN** settings in the SonicWALL appliance. Click **Enter Key** and enter the pre-shared secret. Then click **OK**.



6. Click **File**, then **Save Changes** to save the settings to the security policy.




It is not necessary to configure the **Security Policy** as it is imported directly into the **Client** application. Exporting the security association to a file facilitates configuration of a large number of VPN clients and you do not have to configure each client individually. You can distribute multiple copies of the configuration file via floppy disk or other distribution means.

**Group VPN** can also be configured using digital certificates in the **Security Association** settings. For more information on **Group VPN** configuration using digital certificates, refer to the **Authentication Service User's Guide** on the SonicWALL website: <http://www.sonicwall.com/vpn-center/vpn-setup.html>.

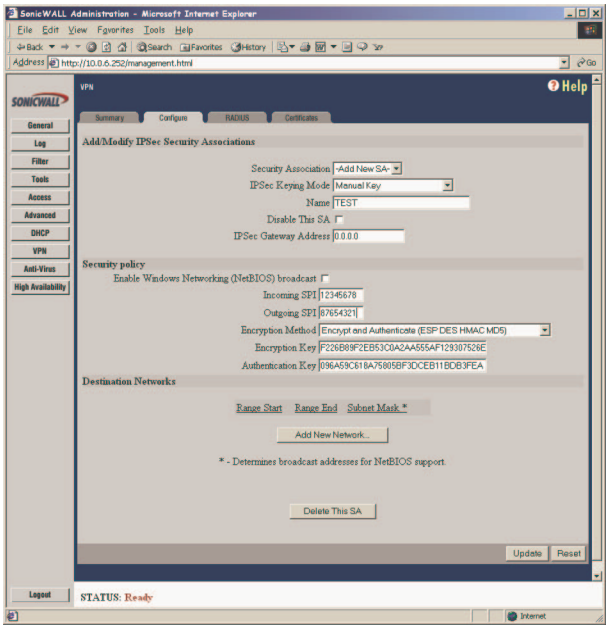
### Verifying the VPN Tunnel as Active

After the Group VPN Policy is active on the VPN Client , you can verify that a secure tunnel is active and sending data securely across the connection. You can verify the connection by verifying the type of icon displayed in the system tray near the system clock. The SonicWALL VPN Client icon is displayed in the System Tray if you are running a Windows operating system. The icon changes to reflect the current status of your communication over the VPN tunnel.

| Icon | Explanation |
|---|---|
| | One of these explanations applies:<br>• The Windows operating system did not start the IREIKE service properly. To start this service, restart your PC. If this icon continues to display, you may need to reinstall SoftRemote.<br>• Your security policy is deactivated—that is, disabled. To reactivate it, go to Reactivate the security policy. |
| | Your computer is ready to establish connections or transmit data. |
| | Your computer has established no secure connections and is transmitting unsecured data. |
| | Your computer has established at least one secure connection, but is not transmitting any data. |
| | Your computer has established at least one secure connection and is transmitting only unsecured data. |
| | Your computer has established at least one secure connection and is transmitting only secured data. |
| | Your computer has established at least one secure connection and is transmitting both secured and unsecured data. |

## Manual Key Configuration for a SonicWALL and VPN Client

To configure the SonicWALL appliance, click **VPN** on the left side of the browser window, and select **Enable VPN** to allow the VPN connection.




1. Select **Disable VPN Windows Networking (NetBIOS) broadcast.** Leave the **Enable Fragmented Packet Handling** unselected until the SonicWALL logs show many fragmented packets transmitted.
2. Click the **Configure** tab and select **Add New SA** from the **Security Association** menu. Then select **Manual Key** from the **IPSec Keying Mode** menu.
3. Enter a descriptive name that identifies the VPN client in the **Name** field, such as the client's location or name.
4. Enter "0.0.0.0" in the **IPSec Gateway Address** field.
5. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

   ***Note**: SPIs should range from 3 to 8 characters in length and include only 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). If you enter an invalid SPI, an error message is be displayed at the bottom of the browser window. An example of a valid SPI is 1234abcd.*

***Note**: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI*.

6. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** from the **Encryption Method** menu.

   ***Note**: It is important to remember the **Encryption Method** selected as you need to select the same parameters in the VPN Client configuration.*

7. 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 client's encryption key, therefore, write it down to use while configuring the client.

8. 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 client settings.

   ***Note:** 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*.

9. Click **Add New Network...** to enter the destination network addresses. Clicking **Add New Network...** automatically updates the VPN configuration and opens the **VPN Destination Network** window.

10. Enter "0.0.0.0" in the **Range Start**, **Range End,** and **Destination Subnet Mask for NetBIOS broadcast** fields.

11. Do not configure **Advanced Settings** at this time.

12. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

## Installing the VPN Client Software

1. When you register your SonicWALL or SonicWALL VPN Upgrade at <http://www.mysonicwall.com>, a unique VPN client serial number and link to download the SonicWALL VPN Client zip file is displayed.

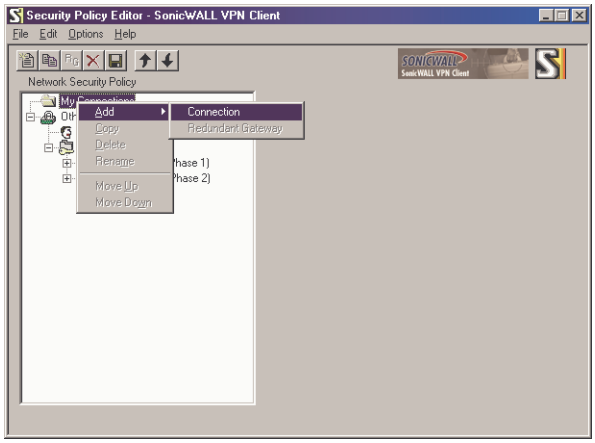
***Note**: SonicWALL PRO 300 lists an additional 50 serial numbers on the back of the SonicWALL VPN Client certificate*.

2. Unzip the SonicWALL VPN Client zip file.
3. Double-click **setup.exe** and follow the VPN client setup program step-by-step instructions. Enter the VPN client serial number when prompted.
4. Restart your computer after installing the VPN client software.

### Launching the SonicWALL VPN Client

To launch the VPN client, select **SonicWALL VPN Client Security Policy Editor** from the **Windows Start** menu, or double-click the icon in the **Windows Task Bar**.

Click **My Connections**, and right click to select **Add > Connection** at the top of the **Security Policy Editor** window.

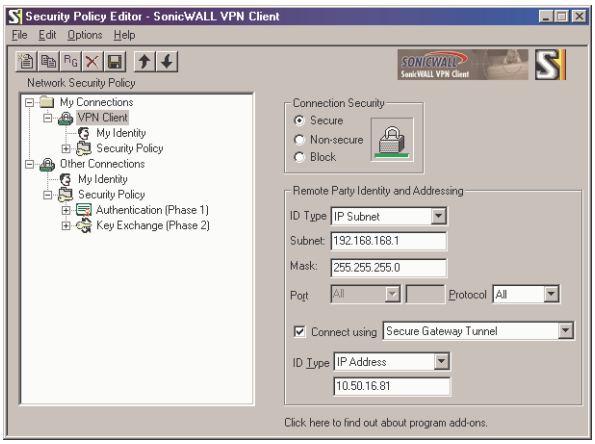



***Note**: The security policy is renamed to match the SA name created in the SonicWALL. You can rename the security policy by highlighting **New Connection** in the **Network Security Policy** box and typing the security policy name.*

### Configuring VPN Security and Remote Identity

1. Select **Secure** in the **Network Security Policy** box on the right side of the **Security Policy Editor** window.
2. Select **IP Subnet** in the **ID Type** menu.
3. Enter the SonicWALL LAN IP Address in the **Subnet** field.

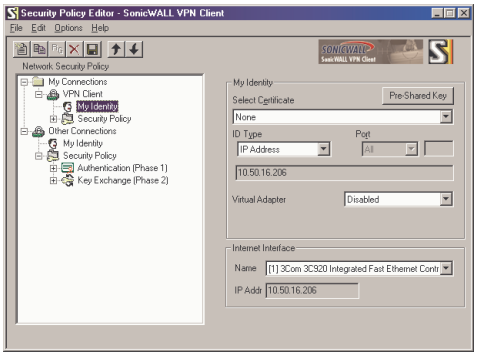
4. Enter the LAN Subnet Mask in the **Mask** field.
5. Select **All** in the **Protocol** menu to permit all IP traffic through the VPN tunnel.
6. Select the **Connect using Secure Gateway Tunnel** check box.
7. Select **IP Address** in the **ID Type** menu at the bottom of the **Security Policy Editor** window.
8. Enter the SonicWALL WAN IP Address in the field below the **ID Type** menu. Enter the NAT Public Address if NAT is enabled.




### Configuring VPN Client Identity

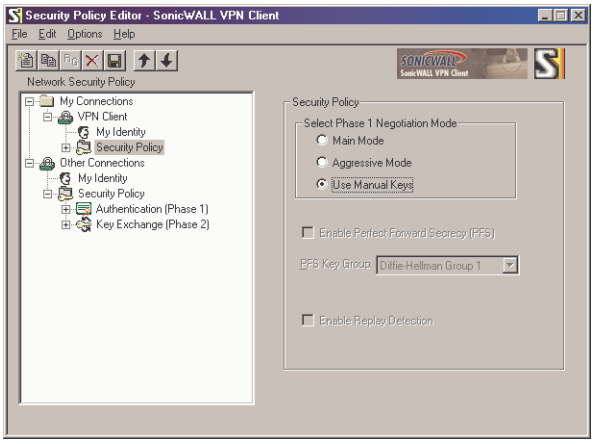
To configure the VPN Client Identity, click **My Identity** in the **Network Security Policy** window.

1. Select **None** from the **Select Certificate** menu.
2. Select the method used to access the Internet from the **Internet Interface** menu. Select **PPP Adapter** from the **Name** menu if you have a dial-up Internet connection. Select the **Ethernet** adapter if you have a dedicated cable, ISDN, or DSL line.

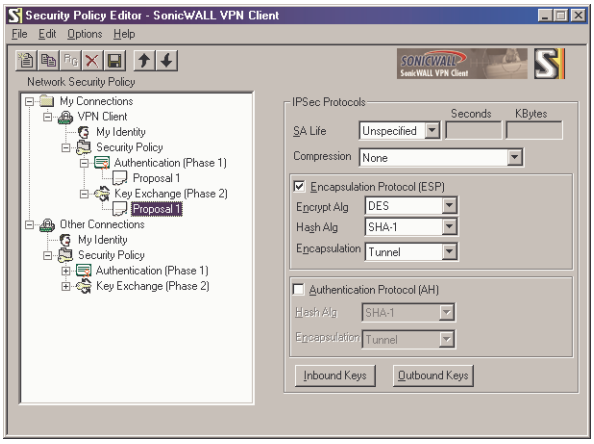


### Configuring VPN Client Security Policy

1. Select **Security Policy** in the **Network Security Policy** window.

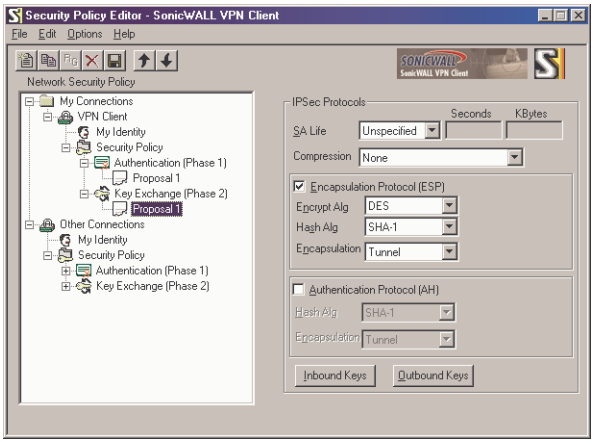



2. Select **Use Manual Keys** in the **Select Phase 1 Negotiation Mode** menu.
3. Click the **+** next to **Security Policy**, and select **Key Exchange (Phase 2)**. Click the **+** next to **Key Exchange (Phase 2),** and select **Proposal 1**.



### Configuring VPN Client Key Exchange Proposal

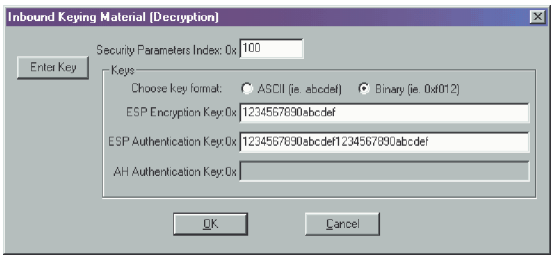
1. Select **Key Exchange (Phase 2)** in the **Network Security Policy** box. Then select **Proposal 1** below **Key Exchange (Phase 2)**.




2. Select **Unspecified** in the **SA Life** menu.
3. Select **None** from the **Compression** menu.
4. Select the **Encapsulation Protocol (ESP)** check box.
5. Select **DES** from the **Encryption Alg** menu.
6. Select **MD5** from the **Hash Alg** menu.
7. Select **Tunnel** from the **Encapsulation** menu.
8. Leave the **Authentication Protocol (AH)** check box unselected.

### Configuring Inbound VPN Client Keys

1. Click **Inbound Keys**. The **Inbound Keying Material box** appears.

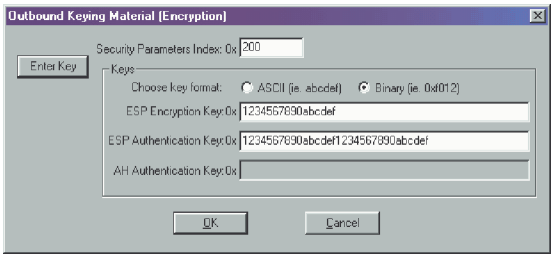



2. Click **Enter Key** to define the encryption and authentication keys.
3. Enter the SonicWALL **Outgoing SPI** in the **Security Parameter Index** field.
4. Select **Binary** in the **Choose key format** options.

5. Enter the SonicWALL 16-character **Encryption Key** in the **ESP Encryption Key** field.
6. Enter the SonicWALL 32-character **Authentication Key** in the **ESP Authentication Key** field, then click **OK**.

### Configuring Outbound VPN Client Keys

1. Click **Outbound Keys**. An **Outbound Keying Material** box is displayed.




2. Click **Enter Key** to define the encryption and authentication keys.
3. Enter the SonicWALL **Incoming SPI** in the **Security Parameter Index** field.
4. Select **Binary** in the **Choose key format** menu.
5. Enter the SonicWALL appliance 16-character **Encryption Key** in the **ESP Encryption Key** field.
6. Enter the SonicWALL appliance 32-character **Authentication Key** in the **ESP Authentication Key** field and then click **OK**.

### Saving SonicWALL VPN Client Settings

Select **Save Changes** in the **File** menu in the top left corner of the **Security Policy Editor** window.

### Verifying the VPN Tunnel as Active

After configuring the VPN Client, you can verify that a secure tunnel is active and sending data securely across the connection. You can verify the connection by verifying the type of icon displayed in the system tray near the system clock.

### Verifying the VPN Client Icon in the System Tray

The SonicWALL VPN Client icon is displayed in the System Tray if you are running a Windows operating system. The icon changes to reflect the current status of your communication over the VPN tunnel.

| Icon | Explanation |
|---|---|
|  | One of these explanations applies:<br>• The Windows operating system did not start the IREIKE service properly. To start this service, restart your PC. If this icon continues to display, you may need to reinstall SoftRemote.<br>• Your security policy is deactivated—that is, disabled. To reactivate it, go to Reactivate the security policy. |
|  | Your computer is ready to establish connections or transmit data. |
|  | Your computer has established no secure connections and is transmitting unsecured data. |
|  | Your computer has established at least one secure connection, but is not transmitting any data. |
|  | Your computer has established at least one secure connection and is transmitting only unsecured data. |
|  | Your computer has established at least one secure connection and is transmitting only secured data. |
|  | Your computer has established at least one secure connection and is transmitting both secured and unsecured data. |

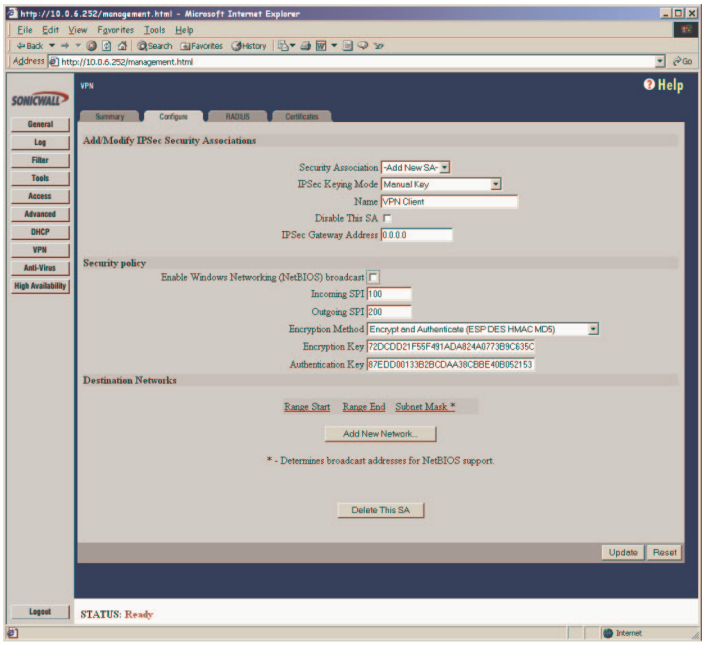
## VPN for Two SonicWALLs

VPN between two SonicWALLs allows users to securely access files and applications at remote locations. The first step to set up a VPN between two SonicWALLs is creating corresponding **Security Associations** (**SAs**). The instructions below describe how to create an **SA** using **Manual Keying and Internet Key Exchange (IKE)**. These instructions are followed by an example illustrating a VPN tunnel between two SonicWALLs. Either **Manual Key** or **IKE using Preshared Secret** can be used to configure a VPN tunnel between two SonicWALLs.

### Manual Key for Two SonicWALLs

Click **VPN** on the left side of the SonicWALL browser window, and then click the **Configure** tab.

1. Select **Manual Key** from the **IPSec Keying Mode** menu.
2. Select **-Add New SA-** from the **Security Association** menu.




3. Enter a descriptive name for the **Security Association**, such as "Chicago Office" or "Remote Management", in the **Name** field.
4. Enter the IP address of the remote VPN gateway, such as another SonicWALL VPN gateway, in the **IPSec Gateway Address** field. This must be a valid IP address and is the remote VPN gateway NAT Public Address if NAT is enabled. Enter "0.0.0.0" if the remote VPN gateway has a dynamic IP address.

5. Define an **SPI** (Security Parameter Index) that the remote SonicWALL uses to identify the **Security Association** in the **Incoming SPI** field.
6. Define an **SPI** that the local SonicWALL uses to identify the **Security Association** in the **Outgoing SPI** field.

   ***Note**: SPIs should range from 3 to 8 characters in length and include only 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). If you enter an invalid **SPI**, an error message will be displayed at the bottom of the browser window. An example of a valid **SPI** is 1234abcd.*

   ***Note**: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association **Incoming SPI** can be the same as the **Outgoing SPI**.*
7. Select an encryption algorithm from the **Encryption Method** menu. The SonicWALL supports the following encryption algorithms:
   - **Tunnel Only (ESP NULL)** does not provide encryption or authentication. This option offers access to computers at private addresses behind NAT and allows unsupported services through the SonicWALL.
   - **Encrypt (ESP DES)** uses 56-bit DES to encrypt data. DES is an extremely secure encryption method, supporting over 72 quadrillion possible encryption keys that can be used to encrypt data.
   - **Fast Encrypt (ESP ARCFour)** uses 56-bit ARCFour to encrypt data. ARCFour is a secure encryption method and has little impact on the throughput of the SonicWALL.
   - **Strong Encrypt (ESP 3DES)** uses 168-bit 3DES (Triple DES) to encrypt data. 3DES is considered an almost "unbreakable" encryption method, applying three DES keys in succession, but it significantly impacts the data throughput of the SonicWALL.
   - **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** uses 168 bit 3DES encryption and HMAC MD5 authentication. 3DES is an extremely secure encryption method, and HMAC MD5 authentication is used to verify integrity. This method significantly impacts the data throughput of the SonicWALL.
   - **Encrypt for Check Point (ESP DES rfc1829)** is interoperable with Check Point Firewall-1. In **Manual Keying** mode, **Encrypt for Check Point** uses 56-bit DES as specified in RFC 1829 as the encryption method.
   - **Encrypt and Authenticate (ESP DES HMAC MD5)** uses 56-bit DES encryption and HMAC MD5 authentication. This method impacts the data throughput of VPN communications. SonicWALL VPN client software supports this method.
   - **Authenticate (AH MD5)** uses AH to authenticate VPN communications but it does not encrypt data.
8. Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. Enter a 48-character hexadecimal key if you are using Triple DES encryption. This encryption key must match the remote SonicWALL's encryption key.

***Note**: 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.*

When a new SA is created, a 48-character key is automatically generated in the **Encryption Key** field. This can be used as a valid key for Triple DES. If this key is used, it must also be entered in the Encryption Key field in the remote SonicWALL. If **Tunnel Only (ESP NULL)** or **Authenticate (AH MD5)** is used, the **Encryption Key** field is ignored.

9. Enter a 32-character, hexadecimal key in the **Authentication Key** field.

   ***Note**: Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef1234567890abcdef is an example of a valid authentication key. If you enter an incorrect authentication key, an error message is displayed at the bottom of the browser window.*

   When a new SA is created, a 32-character key is automatically generated in the **Authentication Key** field. This key can be used as a valid key. If this key is used, it must also be entered in the **Authentication Key** field in the remote SonicWALL. If authentication is not used, this field is ignored.

10. Click **Add New Network...** to enter the destination network addresses. Clicking **Add New Network...** automatically updates the VPN configuration and opens the **VPN Destination Network** window.

11. Enter the beginning IP address of the remote network address range in the **Range Start** field. If NAT is enabled on the remote SonicWALL, enter a private LAN IP address. Enter "0.0.0.0" to accept all remote SonicWALLs with matching encryption and authentication keys.

12. Enter the ending IP address of the remote network's address range in the **Range End** field. If NAT is enabled on the remote SonicWALL, enter a private LAN IP address. Enter "0.0.0.0" to accept all remote SonicWALLs with matching encryption and authentication keys.

13. Enter the remote network subnet mask in the **Destination Subnet Mask for NetBIOS broadcast** field if **Enable Windows Networking (NetBIOS) Broadcast** is selected. Otherwise, enter "0.0.0.0" in the field.

14. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

15. Click **Advanced Settings** and check the boxes that apply to your SA:

    - **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.

- **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
- **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.

16. Click **OK** to close the **Advanced Settings** window. Then click **Update** to update the SonicWALL.

### Configuring the Second SonicWALL Appliance

To configure the second SonicWALL appliance, follow the same configuration steps as the first SonicWALL. You must enter the same SPIs and Encryption keys as the first SonicWALL appliance into the settings of the second SonicWALL appliance.

## Example of Manual Key Configuration for Two SonicWALLs

Widgit, Inc. wants to connect their main office with a branch office on the East Coast. Using a SonicWALL PRO 300 and a TELE3, they can configure a secure VPN tunnel between the two sites. The main office has the following network settings:

- SonicWALL LAN IP address - 192.168.11.1
- LAN subnet mask - 255.255.255.0
- WAN router address - 209.33.22.1
- SonicWALL WAN IP address - 209.33.22.2
- WAN subnet mask - 255.255.255.224

The remote office has the following network settings:

- SonicWALL LAN IP address - 192.168.22.222
- LAN subnet mask - 255.255.255.0
- WAN router address - 207.66.55.129
- SonicWALL WAN IP address - 207.66.55.130
- WAN subnet mask - 255.255.255.248

To configure the main office PRO 300, use the following steps:

1. Configure the network settings for the firewall using the **Network** tab located in the **General** section.
2. Click **Update** and restart the SonicWALL if necessary.
3. Click **VPN**, then the **Configure** tab.
4. Create a name for the main office SA, for example, **Main Office**.
5. Type in the branch office WAN IP address for the **IPSec Gateway Address**.
6. Create an **Incoming SPI** using alphanumeric characters.
7. Create an **Outgoing SPI** using alphanumeric characters.
8. Select **Strong Encrypt (ESP 3DES)** as the **Encryption Method**.
9. Write the **Encryption Key** down or use cut and paste to copy it to a Notepad window.
10. Click **Add New Network**. Type the IP address, “192.168.22.1” in the **Range Start** field. Type the IP address, “192.168.22.255” in the **Range End** field. This **Range End** value is appropriate even if NetBIOS broadcast support is enabled. Leave the subnet mask field blank. Click **Update**.
11. Click **Advanced Settings** and select the features that apply to the SA.
    - **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.
    - **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
    - **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
    - **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
12. Click **OK**, and then click **Update**.

To configure the remote SonicWALL, use the following steps:

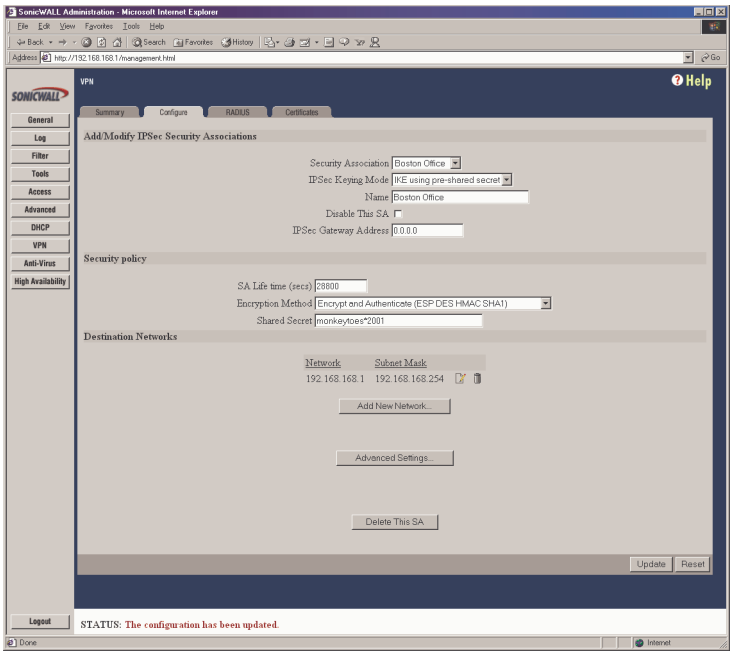
1. Configure the network settings for the firewall using the **Network** tab located in the **General** section.
2. Click **Update** and restart the SonicWALL if necessary.
3. Click **VPN**, then the **Configure** tab.
4. Create a name for the remote office SA, for example, **Remote Office**.
5. Type in the main office WAN IP address for the **IPSec Gateway Address**.
6. Create an **Incoming SPI** using alphanumeric characters.

7. Create an **Outgoing SPI** using alphanumeric characters.
8. Select **Strong Encrypt (ESP 3DES)** as the **Encryption Method**.
9. Enter the **Encryption Key** from the Main Office configuration.
10. Click **Add New Network**. Type the IP address, “192.168.11.1” in the **Range Start** field. Type the IP address, “192.168.11.255” in the **Range End** field. This **Range End** value is appropriate even if NetBIOS broadcast support is enabled. Leave the subnet mask field blank. Click **Update**.
11. Click **Advanced Settings** and select the features that apply to the SA.
    - **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.
    - **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
    - **Forward packets to remote VPNs** - if creating a “hub and spoke” network configuration
    - **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
    - **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
12. Click **OK**, and then click **Update**.

## IKE Configuration for Two SonicWALLs

An alternative to **Manual Key** configuration is **Internet Key Exchange (IKE)**. IKE transparently negotiates encryption and authentication keys. The two SonicWALL appliances authenticate the IKE VPN session by matching preshared keys and IP addresses or Unique Firewall Identifiers.

To create an IKE Security Association, click **VPN** on the left side of the browser window, and then click the **Configure** tab.




1. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
2. Select **-Add New SA-** from the **Security Association** menu.
3. Enter a descriptive name for the **Security Association**, such as "Palo Alto Office" or "NY Headquarters", in the **Name** field.
4. Enter the IP address of the remote SonicWALL in the **IPSec Gateway Address** field. This address must be valid, and should be the NAT Public IP Address if the remote SonicWALL uses Network Address Translation (NAT).

   ***Note**: If the remote SonicWALL has a dynamic IP address, enter "0.0.0.0" in the **IPSec Gateway Address** field. The remote SonicWALL initiates IKE negotiation in Aggressive Mode because it has a dynamic IP address, and authenticates using the SA Names and Unique Firewall Identifiers rather than the IP addresses. Therefore, the SA Name for the SonicWALL must match the opposite SonicWALL Unique Firewall Identifier.*

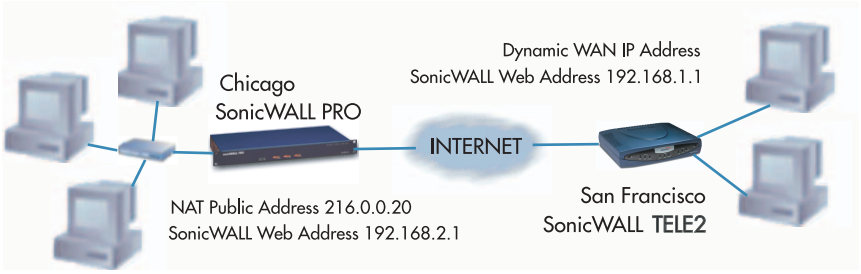
5. Select **Group 2** from the **Phase 1 DH Group** menu.
6. Define the length of time before an IKE Security Association automatically renegotiates in the **SA Life Time (secs)** field. The **SA Life Time** can range from 120 to 9,999,999 seconds.

   ***Note**: A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, users accessing remote resources are disconnected. Therefore, the default SA Life Time of 28,800 seconds (8 hours) is recommended.*
7. Select **DES & SHA1** from the **Phase 1 Encryption / Authentication** menu.
8. Select the appropriate encryption algorithm from the **Phase 2 Encryption / Authentication** menu. The SonicWALL supports the following encryption algorithms:
   - **Tunnel Only (ESP NULL)** does not provide encryption or authentication, but offers access to machines at private addresses behind NAT. It also allows unsupported services through the SonicWALL.
   - **Encrypt (ESP DES)** uses 56-bit DES to encrypt data. DES is an extremely secure encryption method, supporting over 72 quadrillion possible encryption keys that can be used to encrypt data.
   - **Fast Encrypt (ESP ARCFour)** uses 56-bit ARCFour to encrypt data. ARCFour is a secure encryption method, and has less impact on throughput than DES or Triple DES. This encryption method is recommended for all but the most sensitive data.
   - **Strong Encrypt (ESP 3DES)** uses 168-bit 3DES (Triple DES) to encrypt data. 3DES is considered an almost "unbreakable" encryption method, applying three DES keys in succession, but it significantly impacts the data throughput of the SonicWALL.
   - **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** uses 168-bit 3DES encryption and HMAC MD5 authentication. 3DES is an extremely secure encryption method, and HMAC MD5 authentication is used to verify integrity. This method significantly impacts the data throughput of the SonicWALL.
   - **Encrypt for Check Point (ESP DES HMAC MD5)** uses 56-bit DES to encrypt data and is compatible with Check Point Firewall-1. This method impacts the data throughput of the SonicWALL.
   - **Encrypt and Authenticate (ESP DES HMAC MD5)** uses 56-bit DES encryption and HMAC MD5 authentication. This method impacts the data throughput of VPN communications. SonicWALL VPN client software supports this method.
   - **Authenticate (AH MD5)** uses AH to authenticate the VPN communications but it does not encrypt data.
9. Enter a alphanumeric “secret” in the **Shared Secret** field. The **Shared Secret** must match the corresponding field in the remote SonicWALL. This field can range from 4 to 128 characters in length and is case sensitive.

10. Click **Add New Network...** to define the destination network addresses. Clicking **Add New Network...** updates the VPN configuration and opens the **VPN Destination Network** window.
11. Enter the IP address of the remote network in the **Network** field. This address is a private address if the remote LAN has enabled NAT.
12. Enter the subnet mask of the remote network in the **Subnet mask** field.
13. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.
14. Click **Advanced Settings** and select the boxes that apply to your SA:
    - **Use Aggressive Mode** - requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange.
    - **Enable Keep Alive** - if you want to maintain the current connection by listening for traffic on the network segment between the two connections.
    - **Require XAUTH/RADIUS (Only allows VPN clients) -** if you are using a RADIUS server.
    - **Enable Windows Networking (NetBIOS) broadcast** - if remote clients use Windows Network Neighborhood to browse remote networks.
    - **Apply NAT and firewall rules -** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
    - **Forward packets to remote VPNs -** if creating a “hub and spoke” network configuration
    - **Route all internet traffic through this SA** if forcing internet traffic from the WAN to use this SA to access a remote site.
    - **Enable Perfect Forward Secrecy** - if you want to add another layer of security by adding an additional Diffie-Hellman key exchange.
    - **Phase 2 DH Group** - select the level of Phase 2 DH key exchange if **Perfect Forward Secrecy** is enabled.
    - **Default LAN Gateway** - if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
15. Click **OK** to close the **Advanced Settings** window. Click **Update** to upload the changes in the SonicWALL.

## Example: Linking Two SonicWALLs using IKE

The following example illustrates the steps necessary to create an IKE VPN tunnel between a SonicWALL PRO 200 and a SonicWALL TELE3.




A company wants to use VPN to link two offices together, one in Chicago and the other in San Francisco. To do this, the SonicWALL PRO 200 in Chicago and the SonicWALL TELE3 in San Francisco must have corresponding Security Associations.

### Configuring a SonicWALL PRO 200 in Chicago

1. Enter the SonicWALL PRO 200 **Unique Firewall Identifier** in the **VPN Summary** window; in this example, "Chicago Office."
2. Create a new **Security Association** by selecting **-Add New SA-** from the **Security Association** menu in the **VPN Configure** window.
3. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
4. Because the SonicWALL TELE3 does not have a permanent WAN IP address, the SonicWALL PRO 200 must authenticate the VPN session by matching the **Name of the SA** with the TELE3 Unique Firewall Identifier. Enter the TELE3 Unique Firewall Identifier in the **Name** field, in this example, "San Francisco Office."
5. Enter the WAN IP address of the remote SonicWALL in the **IPSec Gateway Address** field. In this example, the San Francisco SonicWALL TELE3 has a dynamic IP address, therefore enter "0.0.0.0" in the **IPSec Gateway Address** field

   ***Note**: Only one of the two IPSec gateways can have a dynamic IP address when using SonicWALL VPN.*
6. Select **Group 2** from the **Phase 1 DH Group** menu.
7. Enter "86400" in the **SA Life time (secs)** field to renegotiate IKE encryption and authentication keys every 24 hours.
8. Select **DES & SHA1** from the **Phase 1 DH Group** menu.

9. Select a VPN encryption method from the **Phase 2 Encryption/Authentication** menu. Since data throughput and security are the primary concern, select **Ecrypt and Authenticate (ESP DES HMAC SHA1)**.
10. Define a **Shared Secret**. Write down this key as it is required when configuring the San Francisco Office SonicWALL TELE3.
11. Click **Add New Network...** to open the **VPN Destination Network** window and enter the destination network addresses.
12. Enter the IP address and subnet mask of the destination network, the San Francisco office, in the **Network** and **Subnet Mask** fields. Since NAT is enabled at the San Francisco office, enter a private LAN IP address. In this example, enter "192.168.1.1" and subnet mask "255.255.255.0."

    ***Note**: The **Destination Network Address** must NOT be in the local network's address range. Therefore, the San Francisco and Chicago offices must have different LAN IP address ranges.*
13. Click **Advanced Settings**. Select the following boxes that apply to your SA:
    - **Use Aggressive Mode** - requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange.
    - **Enable Keep Alive** - if you want to maintain the current connection by listening for traffic on the network segment between the two connections.
    - **Require XAUTH/RADIUS (Only allows VPN clients) -** if you are using a RADIUS server.
    - **Enable Windows Networking (NetBIOS) broadcast** - if remote clients use Windows Network Neighborhood to browse remote networks.
    - **Apply NAT and firewall rules -** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
    - **Forward packets to remote VPNs -** if creating a “hub and spoke” network configuration
    - **Enable Perfect Forward Secrecy** - if you want to add another layer of security by adding an additional Diffie-Hellman key exchange.
    - **Phase 2 DH Group** - select the type of DH key exchange in Phase 2 for **Perfect Forward Secrecy**.
    - **Route all internet traffic through this SA** if forcing internet traffic from the WAN to use this SA to access a remote site.
    - **Default LAN Gateway** - if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
14. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL PRO 200 is updated, a message confirming the update is displayed at the bottom of the browser window.

**Configuring a SonicWALL TELE3 in San Francisco**

1. Enter the SonicWALL TELE3 **Unique Firewall Identifier** in the **VPN Summary** window, in this example, "San Francisco Office."
2. Select **-Add New SA-** from the **Security Association** menu.
3. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
4. Enter the SonicWALL PRO 200 **Unique Firewall Identifier** in the SonicWALL TELE3 **Name** field, in this example, "Chicago Office."
5. Enter the SonicWALL PRO 200 WAN IP Address in the **IPSec Gateway Address** field. This address must be valid, and is the SonicWALL PRO 200 NAT Public Address, or "216.0.0.20."
6. Select **Group 2** from the **Phase 1 DH Group** menu.
7. Enter "86,400" in the **SA Life time (secs)** field to renegotiate keys daily.
8. Select **DES & SHA1** from the **Phase 1 Encryption/Authentication** menu.
9. Select the encryption algorithm from the **Phase 2 Encryption/Authentication** menu. The San Francisco office **Phase 2 Encryption/Authentication** must match Chicago, so **Encrypt and Authenticate (ESP DES HMAC SHA1)** must be selected.
10. Enter the same **Shared Secret** used in the Chicago Office SonicWALL PRO 200 into the SonicWALL TELE3 **Shared Secret** field.
11. Click **Add New Network...** to open the **VPN Destination Network** window and define the destination network addresses.
12. Enter the IP address and subnet mask of the destination network, the Chicago office, in the **Network** and Subnet Mask fields. Since NAT is enabled at the Chicago office, enter a private LAN IP address. In this example, enter "192.168.2.1" and subnet mask "255.255.255.0."
13. Click **Advanced Settings**. Select the following boxes that apply to your SA:
    - **Use Aggressive Mode** - requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange.
    - **Enable Keep Alive** - if you want to maintain the current connection by listening for traffic on the network segment between the two connections.
    - **Require XAUTH/RADIUS (Only allows VPN clients) -** if you are using a RADIUS server.
    - **Enable Windows Networking (NetBIOS) broadcast** - if remote clients use Windows Network Neighborhood to browse remote networks.
    - **Apply NAT and firewall rules -** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
    - **Forward packets to remote VPNs -** if creating a “hub and spoke” network configuration

- **Route all internet traffic through this SA** if forcing internet traffic from the WAN to use this SA to access a remote site.
- **Enable Perfect Forward Secrecy** - if you want to add another layer of security by adding an additional Diffie-Hellman key exchange.
- **Phase 2 DH Group** - select the type of DH key exchange in Phase 2 for **Perfect Forward Secrecy**.
- **Default LAN Gateway** - if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the Route all traffic through this SA check box.

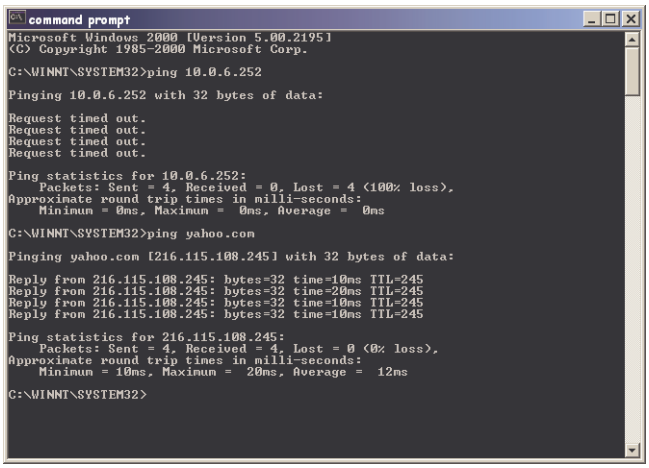
14. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL TELE3 has been updated, a message confirming the update is displayed at the bottom of the browser window.

    ***Note**: 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.*

## Testing a VPN Tunnel Connection Using PING

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

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




If you are unable to ping the remote network, wait a few minutes for the VPN tunnel to become established, and try pinging the network again. If you are still unable to ping the remote network, contact your network administrator.

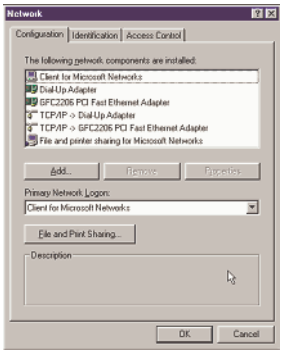
## Configuring Windows Networking

After you have successfully pinged the remote host and confirmed that your VPN tunnel is working, your administrator can ask you to configure your computer for Windows Networking. By configuring your computer for Windows® Networking, you are able to browse the remote network using **Network Neighborhood.** Before logging into the remote network, you must get the following information from your administrator:

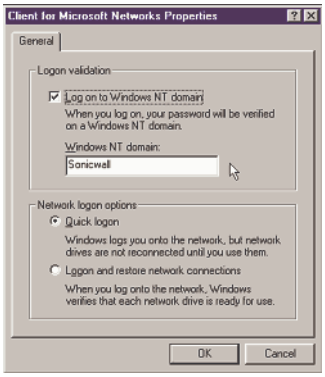
- **NT Account information including your username and password**
- **NT Domain Name**
- **WINS Server IP Address**
- **Internal DNS (optional)**

Use the following steps to configure **Windows Networking** on your computer (Windows98):

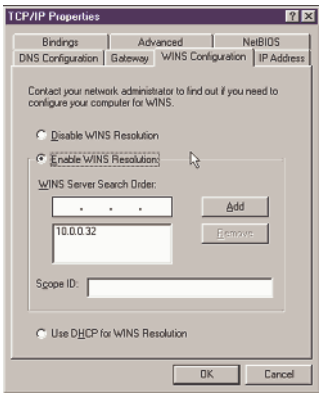
1. Click **Start**, then **Control Panel**. Locate the **Network** icon and double-click it.
2. Select **Client for Microsoft Networks** from the list, and then click **Properties**.



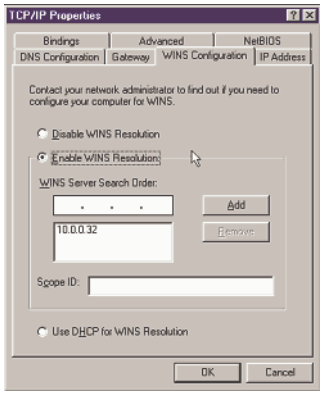

3. Select the **Logon to Windows NT Domain** check box, and enter the domain name provided by your administrator into the **Windows NT domain** text box. Select **Quick Logon** under **Network logon options** section.



4. Click on the **Identification** tab, and enter the domain name provided by your administrator in the **Workgroup** text box.




5. Click on **TCP/IP or Dial-Up Adapter**, and then **Properties**. Click the **WINS Configuration** tab, and select **Enable WINS Resolution**. Enter the WINS server IP address given to you by the administrator, and click **Add**. The WINS server address now appears in the text box below the address entry box.
6. If your administrator has given you an internal DNS address, click the **DNS Configuration** tab and enter the DNS IP address.




7. Windows98® users must restart their computer for the settings to take effect, and then log into the remote domain.

Windows2000® users should consult their network administrators for instructions to set up the remote domain access.

If your remote network does not have a network domain server, you cannot set up a WINS server and browse the network using Network Neighborhood.

To access shared resources on remote computers, you must know the private IP address of the remote computer, and use the **Find** tool in the **Start** menu. Type in the IP address into the **Computer Named** text box, and click **Find Now**. To access the computer remotely, double-click on the computer icon in the box.

## Adding, Modifying and Deleting Destination Networks

You can add, modify or delete destination networks. To add a second destination network, click **Add New Network...** and define the **Network** and **Subnet Mask** fields of the second network segment. To modify a destination network, click the **Notepad** icon to the right of the appropriate destination network entry. Then modify the appropriate fields and click **Update** to update the configuration. To delete a destination network, click the **Trash Can** icon to the far right of the appropriate destination network entry and then click **OK** to confirm the removal.

### Modifying and Deleting Existing Security Associations

The **Security Association** menu also allows you to modify and delete existing **Security Associations**. To delete an **SA**, select it from the list and click the **Delete This SA** button. To modify an **SA**, select it from the list, make the desired changes, and click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the Web browser window. Click **Update** to enable the changes.

### Accessing Remote Resources across a Virtual Private Network

SonicWALL VPN Clients, which cannot transmit NetBIOS broadcasts, can access resources across a VPN by locating a remote computer by IP address. For example, if a remote office has a Microsoft® SQL server, users at the local office can access the SQL server by using the server private IP address.

There are several ways to facilitate connecting to a computer across a SonicWALL VPN:

- Use the **Find Computer** tool
- Create a **LMHOSTS file** in a local computer registry
- Configure a **WINS Server** to resolve a name to a remote IP address.

For more information on accessing remote resources over a VPN, <http://www.sonicwall.com/products/documentation/vpnremotehostswp.html.

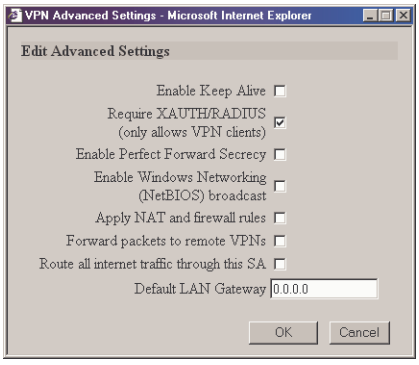
## RADIUS and XAUTH Authentication

An IKE Security Association can be configured to require RADIUS authentication before allowing VPN clients to access LAN resources. This authentication provides an additional layer of VPN security while simplifying and centralizing management. RADIUS authentication allows many VPN clients to share the same VPN configuration, but requires each client to authenticate with a unique user name and password. Because a RADIUS server controls network access, all employee privileges can be created and modified from one location.

***Note**: SonicWALL RADIUS implementation supports Steel-Belted RADIUS by Funk Software. A 30-day demo version of Steel-Belted RADIUS can be downloaded from <http://www.funk.com>. RSA ACE/Server using secure ID tokens can also be used for authentication.*

To enforce RADIUS authentication, complete the following instructions.

1. Click **VPN** on the left side of the browser window and then click the **Configure** tab.
2. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
3. Configure the **Security Association** as specified in the **IKE Configuration** for the **VPN Client** section. Select the **Require XAUTH/RADIUS (only allows VPN clients)** checkbox in the **Advanced Settings** window.



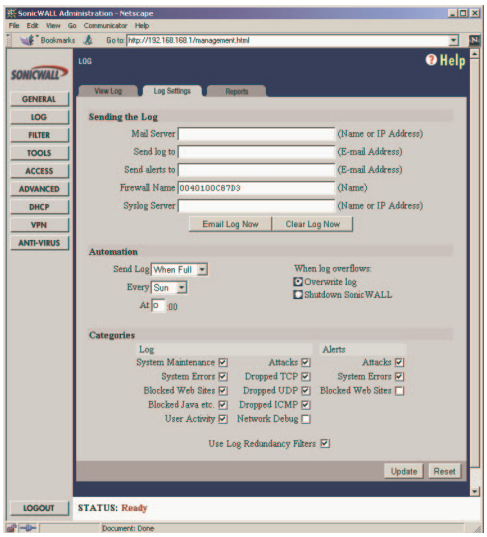

***Note**: Only SonicWALL VPN Clients can authenticate to a RADIUS server. Users tunneling from another VPN gateway, such a second SonicWALL, are not able to complete the VPN tunnel if the Require XAUTH/RADIUS check box is selected.*

## SonicWALL Enhanced VPN Logging

If **Network Debug** is selected in the **Log Settings** tab panel, detailed logs are kept of the VPN negotiations with the SonicWALL appliance. **Enhanced VPN Logging** is useful for evaluating VPN connections when problems can occur with the connections.

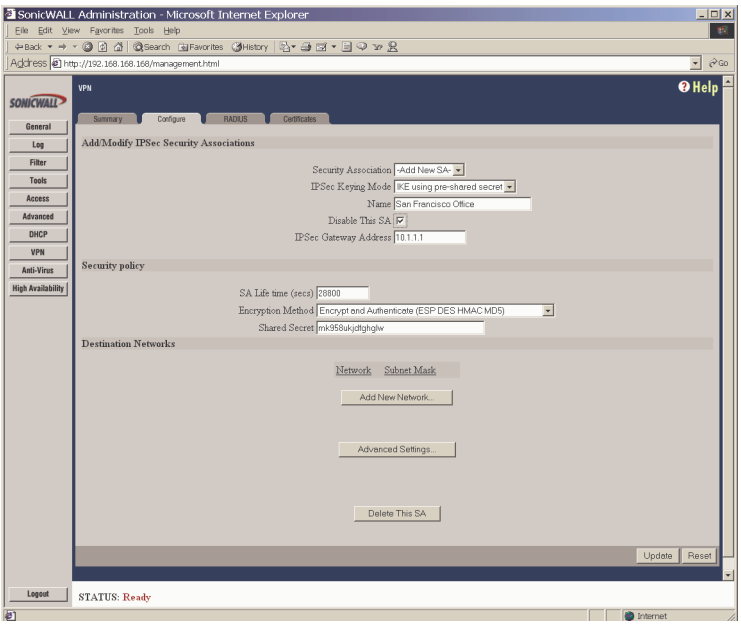
To use the enhanced VPN Logging feature, perform the following steps:

1. Click **Log** on the left side of the management interface.
2. Click on the **Logging Settings** tab, and locate the **Network Debug** check box.
3. Select the **Network Debug** check box, and then click **Update** to enable the **Network Debug** setting.



## Disabling Security Associations

Administrators can choose to disable certain security associations and still allow access by remote VPN clients. The feature is useful if it is suspected that a remote VPN user connection has become unstable or insecure. It can also temporarily block access to the SonicWALL appliance if necessary. Disable the **Security Association** by checking the **Disable this SA** check box. Click **Update** to enable the change to take place.



## Basic VPN Terms and Concepts

- **VPN Tunnel**

  A VPN Tunnel is a term that describes 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.

- **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, which leads to data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms cipher text to clear text.

- **Key**

  A key is an alphanumeric string used by the encryption operation to transform clear text into cipher text. A key is comprised 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 range in length, but typically consist of 16 or 32 characters. The longer the key, the more difficult it is to break the encryption.

- **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 have to be exchanged. SonicWALL VPN uses Symmetric Cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- **Security Association (SA)**

  A Security Association is a group of security settings related to a specific VPN tunnel. A Security Association groups together all of the settings necessary to create a VPN tunnel. Different SAs can be created to connect branch offices, allow secure remote management, and pass unsupported traffic. All Security Associations (SAs) require a specified Encryption Method, IPSec Gateway Address and Destination Network Address. IKE includes a Shared Secret. Manual Keying includes two SPIs and an Encryption and Authentication Key. SonicWALL PRO 300 supports up to 1,000 VPN SAs; SonicWALL PRO 200, 100 SAs; SonicWALL PRO 100, 25 SAs; SonicWALL SOHO3, 10 SAs; and SonicWALL TELE3, 5 SAs.

- **Internet Key Exchange (IKE)**

  IKE is a negotiation and key exchange protocol specified by the Internet Engineering Task Force (IETF). An IKE SA automatically negotiates Phase 1 Encryption/ Authentication Keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that is used to pass IP traffic. The initial exchange occurs on UDP port 500, so when an IKE SA is created, the SonicWALL automatically opens port 500 to allow the IKE key exchange.

- **Manual Key**

  The Manual Key SA allows you to specify the Encryption and Authentication keys as well as Incoming and Outgoing Security Parameter Indices (SPI). SonicWALL VPN supports Manual Key VPN Security Associations.

- **Shared Secret**

  A Shared Secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE SA. This field can be any combination of alphanumeric characters with a minimum length of 4 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.

- **Encapsulating Security Payload (ESP)**

  ESP provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption can be in the form of ARCFour (similar to the popular RC4 encryption method), DES, etc.

  The use of ESP increases the processing requirements in SonicWALL VPN and also increases the communications latency. The increased latency is due to the encryption and decryption required for each IP packet containing an Encapsulating Security Payload.

  ESP typically involves encryption of the packet payload using standard encryption mechanisms, such as RC4, ARCFour, DES, or 3DES. The SonicWALL supports 56-bit ARCFour and 56-bit DES and 168-bit 3DES.

- **Authentication Header (AH)**

  The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet which provides an additional level of security.

  Using AH increases the processing requirements of VPN and also increases the communications latency. The increased latency is primarily due to 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 containing an Authentication Header.

- **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. SonicWALL DES encryption algorithm uses a 56 bit key.

The SonicWALL VPN DES Key must be exactly 16-characters long and is comprised 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.

- **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.

  ARCFour is faster than DES for several reasons. First, it is a newer encryption mechanism than DES. As a result, it benefits from advances in encryption technology. Second, unlike DES, it is designed to encrypt data streams, rather than static storage.

  The SonicWALL VPN ARCFour key must be exactly 16 characters long and is comprised 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.

- **Strong Encryption (TripleDES)**

  Strong Encryption, or TripleDES (3DES), is a variation on DES that uses a 168-bit key. As a result, 3DES is dramatically more secure than DES, and is considered to be virtually unbreakable by security experts. It also requires a great deal more processing power, resulting in increased latency and decreased throughput.

  The SonicWALL 3DES Key must be exactly 24 characters long and is comprised 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 1234567890abcdef12345678.

- **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 keys associated with the SPI to establish the tunnel.

  The SPI must be unique, is from one to eight characters long, and is comprised 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, valid SPIs would be 999 or 1234abcd.