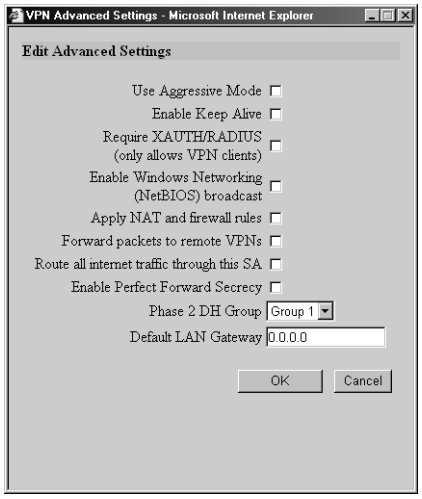
VPN between Two SonicWALLs

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** with **IKE using Pre-shared Secret**. These instructions are followed by an example describing a VPN tunnel between two SonicWALLs.

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 the 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**.

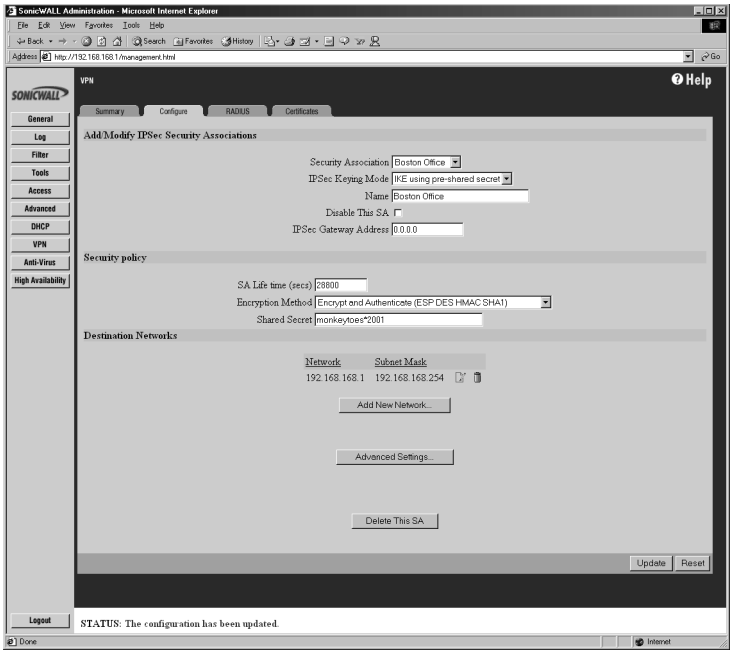
Default LAN Gateway

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.

Creating an IKE Security Association

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. 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**.

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** - 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

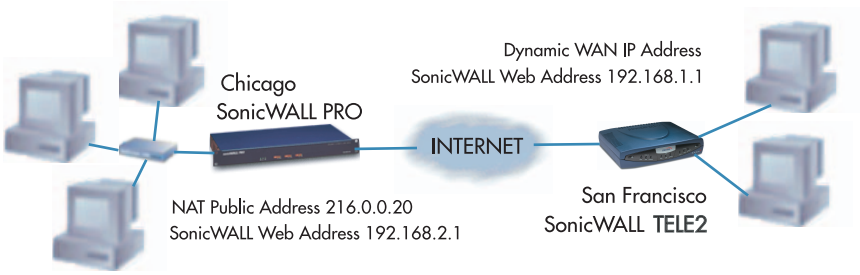
mode messages to be exchanged in Phase One of the SA exchange. **Use Aggressive Mode** is useful when the SonicWALL is located behind another NAT device.

- **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** -
- **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

The following example illustrates the steps necessary to create an IKE VPN tunnel between a SonicWALL PRO and a SonicWALL TELE2.



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 in Chicago and the SonicWALL TELE2 in San Francisco must have corresponding Security Associations.

Configuring a SonicWALL PRO in Chicago

1. Enter the SonicWALL PRO **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 TELE2 does not have a permanent WAN IP address, the SonicWALL PRO must authenticate the VPN session by matching the **Name of the SA** with the TELE2 Unique Firewall Identifier. Enter the TELE2 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 TELE2 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. Enter "86,400" in the **SA Life time (secs)** field to renegotiate IKE encryption and authentication keys every day.
7. Select a VPN method from the **Encryption Method** menu. Since data throughput and security are the primary concern, select **ARCFour**.
8. Define a **Shared Secret**. Write down this key as it is required when configuring the San Francisco Office SonicWALL TELE2.

9. Click **Add New Network...** to open the **VPN Destination Network** window and enter the destination network addresses.

10. 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.*

11. Click **Advanced Settings**. Select the following boxes that apply to your SA:

    - **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.
    - **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 you are 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** - if **Enable Perfect Forward Secrecy** is selected, choose the level of DH Group for the Phase 2 exchange.
    - **Route all internet traffic through this SA** if forcing internet traffic from the WAN to use this SA to access a remote site.

12. **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.

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

Configuring a SonicWALL TELE2 in San Francisco

1. Enter the SonicWALL TELE2 **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 **Unique Firewall Identifier** in the SonicWALL TELE2 **Name** field, in this example, "Chicago Office."
5. Enter the SonicWALL PRO WAN IP Address in the **IPSec Gateway Address** field. This address must be valid, and is the SonicWALL PRO's 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 DH Group** menu.
9. Select a VPN encryption method from the **Phase 2 Encryption/Authentication** menu. The San Francisco office **Phase 2 Encryption/Authentication** must match Chicago, so **ARC Four** must be selected.
10. Enter the same **Shared Secret** used in the Chicago Office SonicWALL PRO into the SonicWALL TELE2 **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** - 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.
    - **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** - if **Enable Perfect Forward Secrecy** is selected, choose the DH Group used for the Phase 2 key exchange.
- **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 TELE2 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.*