# Detection Prevention

## Enable Stealth Mode

By default, the SonicWALL responds to incoming connection requests as either “blocked” or “open”. If you enable **Stealth Mode**, your SonicWALL does not respond to blocked inbound connection requests. **Stealth Mode** makes your SonicWALL essentially invisible to hackers.

## Randomize IP ID

Select **Randomize IP ID** to prevent hackers using various detection tools from detecting the presence of a SonicWALL appliance. IP packets are given random IP IDs which makes it more difficult for hackers to “fingerprint” the SonicWALL appliance.

## Dynamic Ports

- Select **Enable support for Oracle (SQLNet)** if you have Oracle applications on your network.
- Select **Enable Support for Windows Messenger** if you are having problems using Windows Messenger and Windows XP through the SonicWALL. If **Enable Support for Windows Messenger** is selected, it may affect the performance of the SonicWALL.
- Select **Enable SIP Transformations** to transform SIP messaging from the LAN to the WAN. If the SIP proxy is located on the WAN and the SIP clients are on the LAN, the SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) sent to the SIP proxy. Since the IP addresses are unchanged, the SIP proxy cannot return messages to the SIP client. By enabling SIP transformations on the SonicWALL, the appliance changes the private address and port in the SDP to the public address and port. The SIP transformation also controls and opens the RTP/RTCP ports to allow SIP sessions.
- Select **Enable H.323 Transformations** for H.323 protocol-aware packet content inspection and modification by the SonicWALL. The SonicWALL performs any dynamic IP address and transport port mapping, within the H.323 packet, necessary for communication between H.323 parties on the LAN and WAN.
- Select **Enable RTSP Transformations** to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

# Source Routed Packets

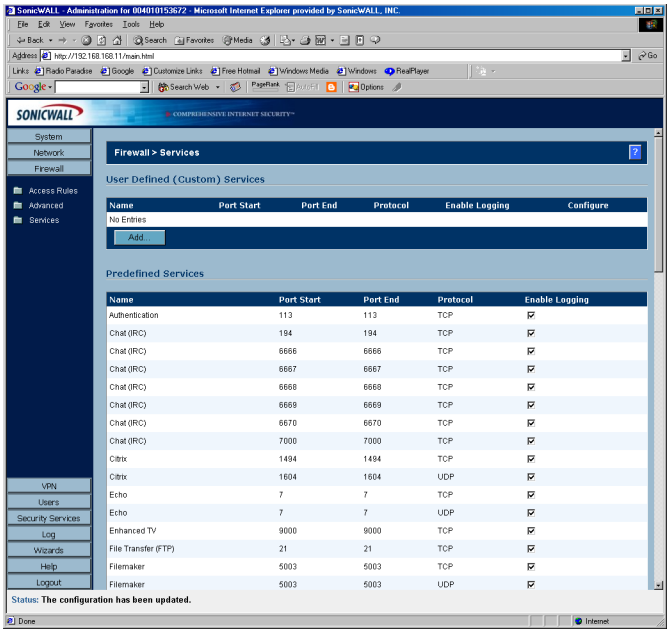
**Drop Source Routed Packets** is selected by default. Clear the check box if you are testing traffic between two specific hosts and you are using source routing.

# TCP Connection Inactivity Timeout

If a connection to a remote server remains idle for more than five minutes, the SonicWALL closes the connection. Without this timeout, Internet connections could stay open indefinitely, creating potential security holes. You can increase the **Inactivity Timeout** if applications, such as Telnet and FTP, are frequently disconnected.

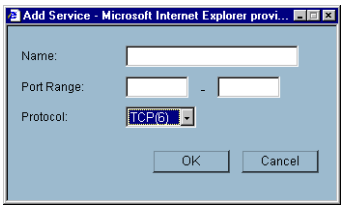
# Firewall>Services

Services are anything a server provides to other computers. A service can be as simple as the computer asking a server for the correct time (NTP) and the server returns a response. Other types of services provide access to different types of data. Web servers (HTTP) respond to requests from clients (browser software) for access to files and data. Services are used by the SonicWALL to configure network access rules for allowing or denying traffic to the network.




## User Defined (Custom) Services

If protocol is not listed in the **Predefined Services** table, you can add it to the User Defined (Custom) Services table by clicking **Add**.




1. Enter the name of the service in the **Name** field.
2. Enter the port number or numbers that apply to the service. A list of well know port numbers can be found in any networking reference.
3. Select the type of protocol, **TCP**, **UDP**, or **ICMP** from the **Protocol** menu.
4. Click **OK**. The service appears in the **User Defined (Custom) Services** table.

# 9 VPN

SonicWALL VPN provides an easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWALL Global VPN Client or Global Security Client and SonicWALL GroupVPN on your SonicWALL.

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

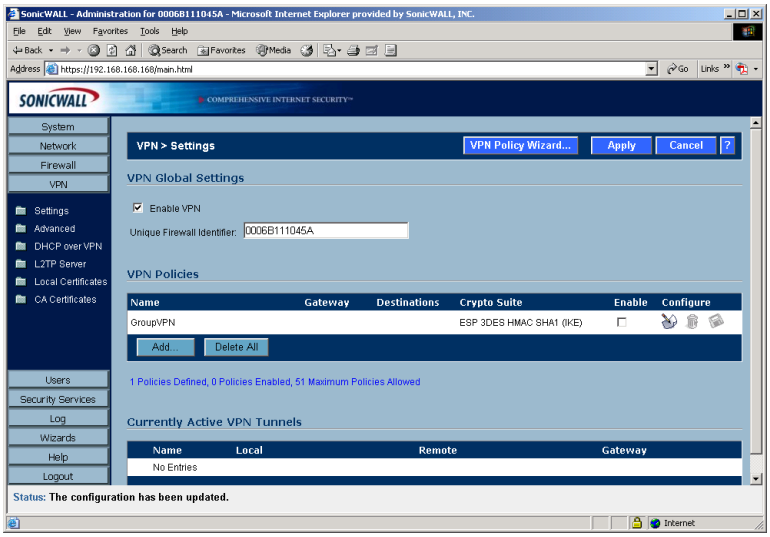
Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections.

Using the SonicWALL intuitive Management Interface, you can quickly create a VPN Security Association (SA) 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, therefore, it is interoperable with other VPN products.

## VPN>Settings

The **VPN>Settings** page provides the SonicWALL features for configuring your site-to-site VPN and your VPN client to SonicWALL VPN policies.




## VPN Global Settings

The **Global VPN Settings** section displays the following information:

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

## VPN Policies

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

- **Name** - user-defined name to identify the Security Association.
- **Gateway** - the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations** - the IP addresses of the destination networks.
- **Crypto Suite** - the type of encryption used
- **Enable** - selecting the check box enables the VPN Policy. Clearing the check box disables it.
- Configure - edit or delete the VPN Policy information. GroupVPN has a **Disk** icon for exporting the configuration for SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table.

## Currently Active VPN Tunnels

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

# Configuring GroupVPN Policy on the SonicWALL

SonicWALL **VPN** defaults to a **Group VPN** setting. This feature facilitates the set up and deployment of multiple VPN clients by the administrator of the SonicWALL. 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 XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

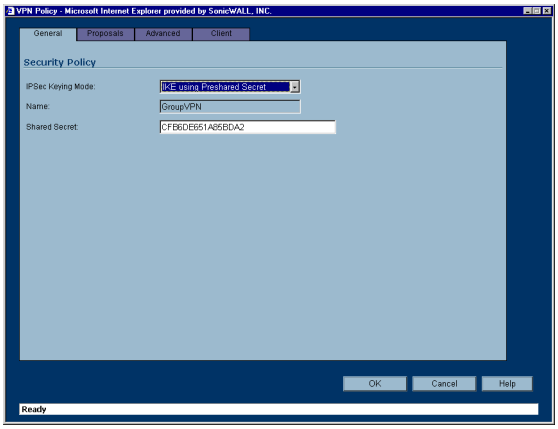
The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

You can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPSec Keying Mode.

## Configuring IKE using Preshared Secret

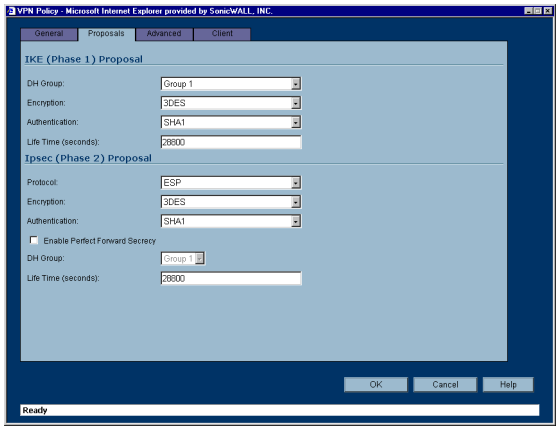
To edit the default settings for Group VPN, follow these steps:

1. Click the **Notepad** icon in the **Group VPN** entry. The **VPN Policy** window is displayed.




## General

2. In the **General** tab, **IKE using Preshared Secret** is the default setting for **IPSec Keying Mode**. A Shared Secret is automatically generated in the **Shared Secret** field, or you can generate your own shared secret. Shared Secrets must be minimum of four characters.




## Proposals

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

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

**Group 2** from the **DH Group** menu.

**3DES** from the **Encryption** menu

**SHA1** from the **Authentication** menu

Leave the default setting, 28800, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

In the **IPSec (Phase 2) Proposal** section, select the following settings:

**ESP** from the **Protocol** menu

**3DES** from the **Encryption** menu

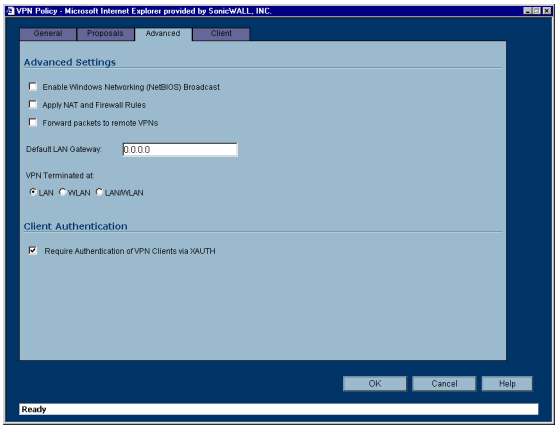
**MD5** from the **Authentication** menu

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

Leave the default setting, 28800, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

## Advanced

4. Click the **Advanced** tab. Select any of the following settings you want to apply to your GroupVPN policy.




- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to 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.

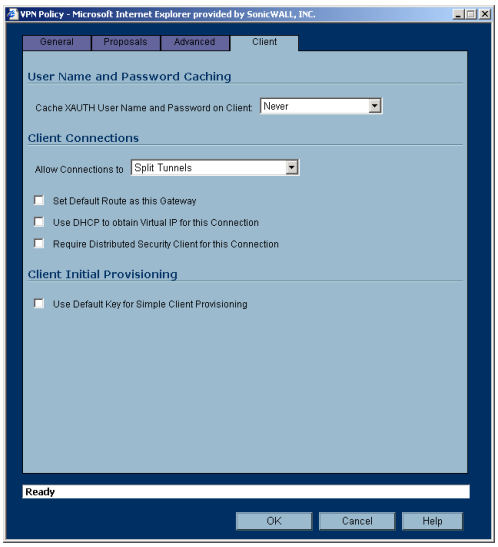
***Alert!*** *Offices can have overlapping LAN IP ranges if the **Apply NAT and Firewall Rules** feature is selected.*

- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can 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 configured on the **Routing** page located in the **Network** 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, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using **Use this VPN Tunnel as default route for all Internet traffic**. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ, or LAN/OPT/DMZ** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ network.

- **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

## Client

5. Click the **Client** tab. Select any of the following settings you want to apply to your GroupVPN policy.




- **Cache XAUTH User Name and Password** - allows the Global VPN Client to cache the user name and password. Select from **Single Session** (default), **Never**, or **Always**.
- **Allow Connections** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select from **Split Tunnels**, **This Gateway Only**, or **All Secured Gateways**.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN Policy. You can only configure one VPN Policy to use this setting.
- **Use DHCP to obtain Virtual IP for this Connection** - allows the VPN Client to obtain an IP address using DHCP over VPN.
- **Require Distributed Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Distributed Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

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

- **Use Default Key for Simple Client Provisoning** - the initial Aggressive mode exchange by the gateway and VPN clients uses a default Preshared Key for authentication.

6. Click **OK**.

# Configuring GroupVPN with IKE using 3rd Party Certificates

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

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

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

## General

2. In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **IPSec Keying Mode** menu. The SA name is **Group VPN** by default and cannot be changed.
3. Select a certificate for the SonicWALL from the **Gateway Certificate** menu.
4. Select one of the following Peer ID types from the **Peer ID Type** menu.

   **E-Mail ID**

   **Distinguished name**

   **Domain name**
5. Enter the Peer ID filter in the **Peer ID Filter** field.
6. Check **All Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the Gateway Certificate menu.

## Proposals

7. Click on the **Proposals** tab.
8. In the **IKE (Phase 1) Proposal** section, select the following settings:

   **Group 2** from the **DH Group** menu.

   **3DES** from the **Encryption** menu.

   **SHA1** from the **Authentication** menu.

   Leave the default setting, **28800**, in the **Life Time (seconds)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.
9. In the **IPSec (Phase 2) Proposal** section, select the following settings:

   **ESP** from the **Protocol** menu.

   **3DES** from the **Encryption** menu.

   **MD5** from the **Authentication** menu.

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

   Leave the default setting, **28800**, in the **Life Time (seconds)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

## Advanced

Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN policy:

**Enable Windows Networking (NetBIOS) broadcast** - to allow access to 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 Transparent Mode network configuration, using this check box applies the firewall access rules and checks for attacks, but not does not apply NAT.

**Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can 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 configured on the Routing page located in the Network 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, select the Forward Packets to Remote VPNs check box. Traffic can travel from a branch office to a branch office via the corporate office.

**Default LAN Gateway** - used at a central site in conjunction with a remote site using the Route all Internet traffic through this SA check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

**VPN Terminated at the LAN, DMZ/OPT, or LAN/DMZ/OPT** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or DMZ/OPT network.

**Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

## Client

10. Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:

**Cache XAUTH User Name and Password** - Allows Global VPN Client to cache any username and password required for XAUTH user authentication. The drop-down list provides the following options:

**Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.

**Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.

**Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.

Client Connections

**Allow Traffic to** - Specifies single or multiple VPN connections. The drop-down list provides the following options:

**This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of this gateway is sent through the VPN tunnel. All other traffic is blocked. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.

**All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with Set Default Route as this Gateway, then Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked. Only one of the multiple gateways can have Set Default Route as this Gateway enabled.

**Split Tunnels** - Allows the VPN user to have both local Internet access and VPN connectivity.

**Set Default Route as this Gateway** - If checked, Global VPN Client traffic that does not match selectors for the gateway's protected subnets must also be tunnelled. In effect, this changes the Global VPN Client's default gateway to the gateway tunnel endpoint. If unchecked, the Global VPN Client must drop all non-matching traffic if Allow traffic to This Gateway Only or All Secured Gateways is selected.

**Use DHCP to Obtain Virtual IP for this Connection** - If set, this allows the Global VPN Client to obtain the IP address and other attributes like DNS and WINS from an external DHCP server on the LAN side of the gateway.

**Require Distributed Security Client for this Connection** - Allows a VPN connection from the remote Global Security Client only if the remote computer is running the SonicWALL Distributed Security Client, which provides policy enforced firewall protection.

**Use Default Key for Simple Client Provisioning** - If set, authentication of initial Aggressive mode exchange uses a default Preshared Key by gateway and all Global VPN Clients. This allows for the control of the use of the default registration key. If not set, then Preshared Key must be distributed out of band.

13. Click **OK**.
14. Click **Apply** to enable the changes.

## Export a GroupVPN Client Policy

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

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

1. Click the **Disk** icon under **Configure** for the **GroupVPN** policy. The **Export VPN Client Policy** window is displayed.
2. **rcf format is required for SonicWALL Global Clients** is selected by default. Files saved in the rcf format can be password encrypted.
3. Click **Yes**. The **VPN Policy Export** window is displayed.
4. If you want to encrypt the exported file, type a password in the **Password** field, re-enter the password in the **Confirm Password** field, and then click **Submit**.
5. If you do not want the exported file encrypted, click Submit. A message appears confirming your choice. Click **OK**.
6. Select the locations to save the file and click **Save**.
7. Click **Close**.

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

# Site to Site VPN Configurations

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

The SonicWALL must have a routable WAN IP Address whether it is dynamic or static.

Be sure that the networks behind the SonicWALLs are unique. The same subnets cannot reside behind two different VPN gateways.

In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site to Site VPN Configurations can include the following options:

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

# VPN Planning Sheet for Site-to-Site VPN Policies

You need the information below before you begin configuring Site-to-Site VPN Policies.

## Site A

**Workstation**

LAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

**SonicWALL**

LAN IP Address: ___.___.___.___

WAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

## Router

Internet Gateway

WAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

DNS Server #1: ___.___.___.___

DNS Server #2: ___.___.___.___

## Additional Information

SA Name:_____

Manual Key, SPI In_____ SPI Out_____

Enc.Key:_____

Auth.Key:_____

If Preshared Secret,

Shared Secret:_____

Phase 1 DH - 1 2 5

SA Lifetime 28800 or _____

Phase 1 Enc/Auth DES 3DES AES-128 AES-256 MD5 SHA1 (circle)

Phase 2 Enc/Auth DES 3DES AES-128 AES-256 MD5 SHA1 (circle)

ARC NULL

# Configuring Site to Site VPN Policies Using the VPN Policy Wizard

The **VPN Policy Wizard** quickly and easily walks you through the steps of configuring a VPN security policy between two SonicWALL appliances.

The **VPN Policy Wizard** allows you to create a **Typical** VPN connection. Using this option, the wizard creates a VPN policy based on **IKE using Preshared Secret**.

Using the **Custom** option in the **VPN Policy Wizard** allow you to create a VPN policy with your own configuration options based on one of the following IPSec Keying Modes:

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

***Note:*** *You need IP addressing information for your local network as well as your remote network. Use the VPN Planning Sheet to record your information.*

## Creating a Typical IKE using Preshared Secret VPN Policy

You can create a **Typical** VPN Policy using the **VPN Policy Wizard** to configure an IPSec VPN security association between two SonicWALL appliances.

1. Click **VPN Policy Wizard** on the **VPN>Settings** page to launch the wizard. Click **Next**.
2. Select **Typical** and click **Next**.
3. Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.
4. Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.
5. Enter a shared secret in the **Shared Secret** field. Use a combination of letters and numbers to create a unique secret. Click **Next**.
6. To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

## Creating a Custom VPN Policy using IKE and a Preshared Secret

To create a custom VPN policy using IKE and a Preshared Secret, follow these steps:

1. Click **VPN Policy Wizard** to launch the wizard. Click **Next** to continue.
2. Select **Custom**, and click **Next**.
3. Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.
4. Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.

***Note:*** *You can add additional networks by editing the VPN policy after it is created in the VPN Policy Wizard.*

5. Select **IKE using Preshared Secret** as the IPSec Keying Mode. Click **Next**.
6. Enter a shared secret in the **Shared Secret** field. Use a combination of letters and numbers to create a unique secret. Click **Next**.
7. Select from the **DH Group** menu. Diffie-Hellman (DH) key exchange (a key agreement protocol) is used during phase 1 of the authentication process to establish pre-shared keys. To compromise between network speed and network security, select **Group 2**.

   Select an encryption method from the **Encryption** list for the VPN tunnel. If network speed is preferred, then select **DES**. If network security is preferred, select **3DES**. To compromise between network speed and network security, select **DES**.

   Select an authentication method from the **Authentication** list. SHA1 is preferred for network security.

   Keep the default value of 28800 (8 hours) as the **Life Time (seconds)** for the VPN Policy. Click **Next**.
8. Select **ESP** from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.

   Select **3DES** from the **Encryption** menu. **3DES** is extremely secure and recommended for use.

   Select **SHA1** from the **Authentication** menu.

   Select **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-Hellman key exchange is performed. **Enable Perfect Forward Secrecy** adds incremental security between gateways.

   If **Enable Perfect Forward Secrecy** is enabled, select the type of Diffie-Hellman (DH) Key Exchange (a key agreement protocol) to be used during phase 2 of the authentication process to establish pre-shared keys.

   Leave the default value, 28800, in the **Life Time (seconds)** field. The keys renegotiate every 8 hours.

   Click **Next**.
9. To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

## Creating a Manual Key VPN Policy with the VPN Policy Wizard

You can create a custom VPN Policy using the VPN Wizard to configure a different IPSec method or configure more advanced features for the VPN Policy.

1. Click **VPN Policy Wizard** to launch the wizard. Click **Next** to continue.
2. Select **Custom**, and click **Next**.
3. Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.
4. Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.

***Note:*** *You can add additional networks by editing the VPN policy after it is created in the VPN Policy Wizard.*

5. Select **Manual Key** from the **IPSec Keying Modes** list. Click **Next**.
6. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length. Or use the default values.

***Alert!*** *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.*

**ESP** is selected by default from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.

**3DES** is selected by default from the **Encryption Method** menu. Enter a 48-character hexadecimal key if you are using 3DES encryption.Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. This encryption key must match the remote SonicWALL's encryption key.

The default 48-character key is a unique key generated every time a VPN Policy is created.

**AH** is selected by default from the **Authentication Key** field. 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.

Click **Next**.

7. To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

## Configuring IKE using 3rd Party Certificates with the VPN Policy Wizard

***Alert!*** *You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate. See “Digital Certificates” on page 55 for more information.*

1. Click **VPN Policy Wizard** to launch the wizard. Click **Next** to continue.
2. Select **Custom**, and click **Next**.
3. Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.
4. Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.
5. Select **IKE using 3rd Party Certificates** from the **IPSec Keying Modes** list. Click **Next**.
6. Select your third party certificate from the **Third Party Certificate** menu. Select the ID type from the **Peer Certificate’s ID Type**, and enter the ID string in the **ID string to match** field. Click **Next**.
7. Select from the **DH Group** menu. Diffie-Hellman (DH) key exchange (a key agreement protocol) is used during phase 1 of the authentication process to establish pre-shared keys. To compromise between network speed and network security, select **Group 2**.

Select an encryption method from the **Encryption** list for the VPN tunnel. If network speed is preferred, then select **DES**. If network security is preferred, select **3DES**. To compromise between network speed and network security, select **DES**.

Select an authentication method from the **Authentication** list. SHA1 is preferred for network security.

Leave the default value of 28800 (8 hours) as the **Life Time (seconds)** for the VPN Policy.

Click **Next**.

8. **ESP** is selected by default from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.

   3DES is selected by default from the **Encryption** menu. Enter a 48-character hexadecimal key if you are using 3DES encryption.Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. This encryption key must match the remote SonicWALL's encryption key.

   The default 48-character key is a unique key generated every time a VPN Policy is created.

   AH is selected by default from the **Authentication Key** field. 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.

   Click **Next**.

9. To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

# Creating VPN Policies Using the VPN Policy Window

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

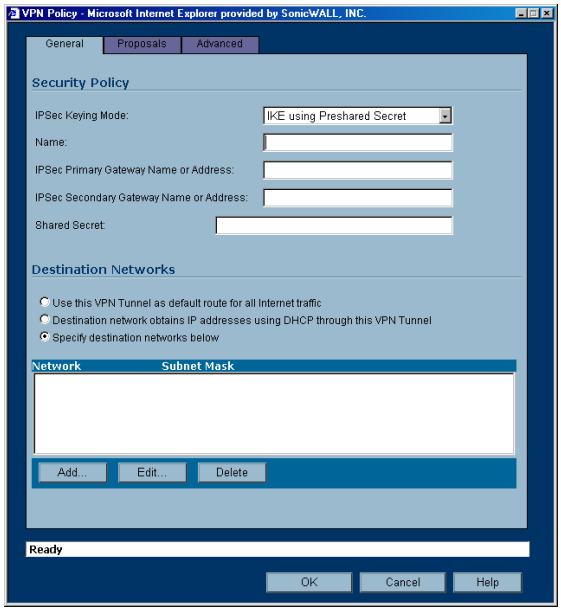
- **IKE using Preshared Key**
- **Manual Key**
- **IKE using 3rd Party Certificates**

***Tip!*** *You can create these policies using the VPN Policy Wizard.*

## Configuring a VPN Policy using IKE with Preshared Secret

To manually configure a VPN Policy using IKE with Preshared Secret, follow the steps below:

1. In the **VPN>Settings** page, click **Add**. The **VPN Policy** window is displayed.




2. In the **General** tab**, IKE using Preshared Secret** is selected by default from the **IPSec Keying Mode** menu.

***Tip!*** *Use the VPN worksheet in this chapter to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.*

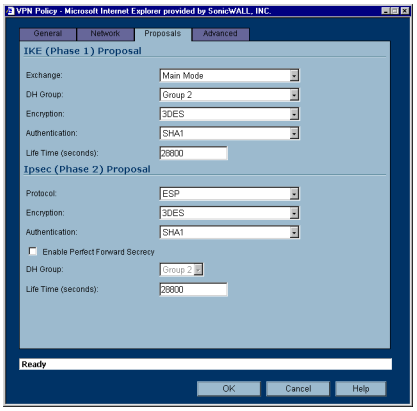
3. Enter a name for the VPN Policy in the **Name** field.
4. Enter the IP address or gateway name of the REMOTE SonicWALL in the **IPSec Primary Gateway Name or Address** field.
5. If you have a second IP address or gateway name, enter it in the **IPSec Secondary Gateway Name or Address** field. If the primary gateway is unavailable, the SonicWALL uses the second gateway to create the VPN tunnel.
6. Enter a combination of letters, symbols, and numbers as the Shared Secret in the **Shared Secret** field.

***Tip!*** *The Shared Secret must be a minimum of four characters.*

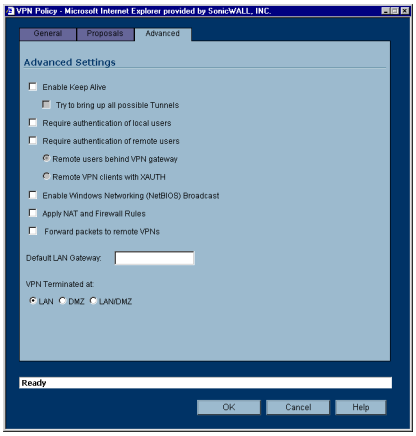
7. Choose from the following options in the **Destination Networks** section:

- **Use this VPN Tunnel as the default route for all Internet traffic** - select this option if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this option.
- **Destination network obtains IP addresses using DCHP through this SA** - select this option if you are managing your network IP address allocation from a central location.
- **Specify destination networks below** - configure the remote destination network for your SA. Click **Add** to add the IP address and subnet mask. You can modify existing destination networks by click **Edit**, and delete networks by selecting the network and clicking **Delete**.

8. Click the **Proposals** tab




9. In the **IKE (Phase 1) Proposal** section, the default settings offer a secure connection configuration, however, the settings can be modified to reflect your preferences. In addition to 3DES, AES-128, AES-192, and AES-256 can be selected for encryption methods.
10. In the **Ipsec (Phase 2) Proposal** section, the default settings offer a secure connection configuration, however, the settings can be modified to reflect your preferences. In addition to 3DES, AES-128, AES-192, and AES-256 can be selected for encryption methods. Selecting **Enable Perfect Forward Secrecy** prevents a hacker using brute force to break encryption keys from obtaining the current and future IPSec keys. During Phase 2 negotiation, an additional Diffie-Hellman key exchange is performed. This option adds an additional layer of security to the VPN tunnel.
11. Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy in the **Advanced Settings** section.




- **Enable Keep Alive -** Select this setting if you want to maintain the current connection by listening for traffic on the network segment between the two connections. If multiple VPN tunnels are configured on the SonicWALL, select **Try to bring up all possible tunnels** to have the SonicWALL renegotiate the tunnels if they lose communication with the SonicWALL.
- **Require authentication of local users** - requires all outbound VPN traffic from this SA is from an authenticated source.
- **Require authentication of remote users** - requires all inbound VPN traffic for this SA is from an authenticated user. Select **Remote users behind VPN gateway** if remote users have a VPN tunnel that terminates on the VPN gateway. Select **Remote VPN clients with XAUTH** if remote users require authentication using XAUTH and are access the SonicWALL via a VPN clients.

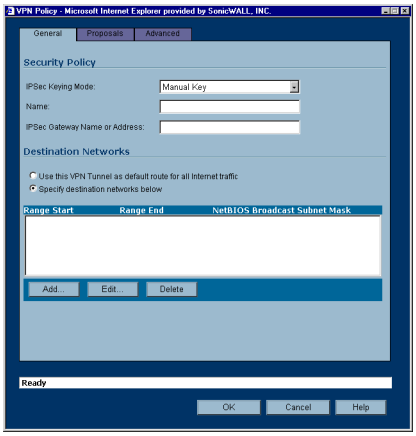
- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- **Apply NAT and Firewall Rules** - This feature allows a remote site's LAN subnet to be hidden from the corporate site, and is most useful when a remote office's 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.
- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can 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 configured on the **Routing** page located in the **Network** 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, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the Route all internet traffic through this SA check box. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ, or LAN/OPT/DMZ** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ network.

12. Click **OK**. Your new VPN policy is displayed in the **VPN Policies** table.

## Configuring a VPN Policy using Manual Key

To manually configure a VPN Policy in the **VPN Policy** window using Manual Key, follow the steps below:

1. In the **VPN>Settings** page, click **Add**. The **VPN Policy** window is displayed.



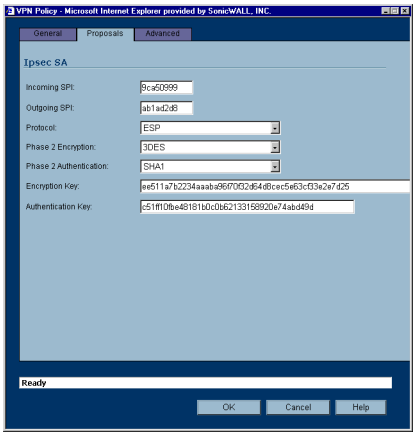

2. Select **Manual Key** from the **IPSec Keying Mode** menu.

***Tip!*** *Use the VPN worksheet at the beginning of this chapter to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.*

3. In the **Security Policy** section, enter a name for the VPN Policy in the **Name** field.
4. Enter the IP address or gateway name of the REMOTE SonicWALL in the **IPSec Gateway Name or Address** field.
5. In the **Destination Networks** section, one of the following options:

- **Use this SA as the default route for all Internet traffic** - select this option if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this option.
- **Specify destination networks below** - configure the remote destination network for your SA. Click **Add** to add the IP address and subnet mask. You can modify existing destination networks by click **Edit**, and delete networks by selecting the network and clicking **Delete**.

6. Click on the **Proposals** tab.



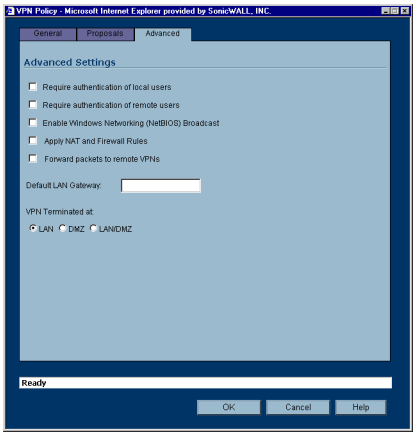

7. In the **Ipsec SA** section, define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length. Or use the default values.

***Alert!*** *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.*

8. **ESP** is selected by default from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.
9. **3DES** is selected by default from the **Phase 2 Encryption** menu. Enter a 48-character hexadecimal key if you are using 3DES encryption.Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. This encryption key must match the remote SonicWALL's encryption key.

   The default 48-character key is a unique key generated every time a VPN Policy is created.
10. **SHA1** is selected by default from the **Phase 2 Authentication** menu. When a new Policy 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.

11. Click on the **Advanced** tab. Select the optional configuration settings you want to apply to your VPN policy from the **Advanced Settings** section.




- **Require authentication of local users** - requires all outbound VPN traffic from this SA is from an authenticated source.
- **Require authentication of remote users** - requires all inbound VPN traffic for this SA is from an authenticated user.
- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to 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.
- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can 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 configured on the **Routing** page located in the **Network** 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, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.

- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the **Use this VPN Tunnel as the default route for all internet traffic**. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this VPN Policy. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. 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.
- **VPN Terminated at the LAN, OPT/DMZ, or LAN/OPT/DMZ** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ network.

12. Click **OK** to add the Manual Key VPN Policy to the SonicWALL.

## Configuring a VPN Policy with IKE using a Third Party Certificate

***Alert!*** *You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate. See "Digital Certificates" on page 55 for more information.*

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

1. In the **VPN>Settings** page, click **Add**. The **VPN Policy** window is displayed.
2. In **General** tab, select **IKE using 3rd Party Certificates**.
3. Type a Name for the Security Association in the **Name** field.
4. Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPSec Primary Gateway Name or Address** field. If you have a secondary remote SonicWALL, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPSec Secondary Gateway Name or Address** field.
5. Select a certificate from the **Third Party Certificate** menu.
6. Select **Distinguished name**, **E-Mail ID**, or **Domain name** from the **Peer Certificate's ID Type** menu.
7. Type an ID string in the **ID string to match** field.
8. In the **Destination Network** section, select one of the following options:

   **Use this VPN Tunnel as default route for all Internet traffic** - select this option if you don't want from any local user to leave the SonicWALL unless it is through a VPN tunnel.

   **Destination network obtains IP addresses using DHCP through this VPN Tunnel** - Select this setting if you want the remote network to obtain IP addresses from your DHCP server.

   **Specify destination networks below** - allows you to add the destination network or networks. To add a destination network, click **Add**. The **Edit VPN Destination Network** window is displayed. Enter the IP address in the **Network** field and the subnet in the **Subnet Mask** field, then click **OK**.
9. Click the **Proposals** tab.
10. In the **IKE (Phase 1) Proposal** section, select the following settings:

    Select **Aggressive Mode** from the **Exchange** menu.

    Select **Group 2** from the **DH Group** menu.

    Select **3DES** from the **Encryption** menu.

    Enter a maximum time in seconds allowed before forcing the policy to renegotiate and exchange keys in the **Life Time** field. The default settings is **28800** seconds (8 hours).

11. In the Ipsec (Phase 2) Proposal section, select the following settings:

    Select **ESP** from the **Protocol** menu.

    Select **3DES** from the **Encryption** menu.

    Select **SHA1** from the **Authentication** menu.

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

    Enter a maximum time in seconds allowed before forcing the policy to renegotiate and exchange keys in the **Life Time** field. The default settings is **28800** seconds (8 hours).

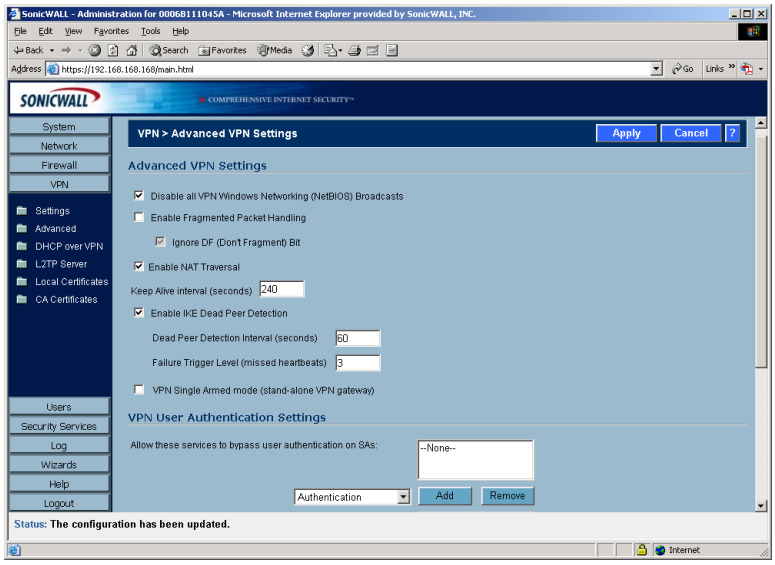
12. Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy in the **Advanced Settings** section.

- **Enable Keep Alive -** Select this setting if you want to maintain the current connection by listening for traffic on the network segment between the two connections. If multiple VPN tunnels are configured on the SonicWALL, select **Try to bring up all possible tunnels** to have the SonicWALL renegotiate the tunnels if they lose communication with the SonicWALL.
- **Require authentication of local users** - requires all outbound VPN traffic from this SA is from an authenticated source.
- **Require authentication of remote users** - requires all inbound VPN traffic for this SA is from an authenticated user. Select **Remote users behind VPN gateway** if remote users have a VPN tunnel that terminates on the VPN gateway. Select **Remote VPN clients with XAUTH** if remote users require authentication using XAUTH and are access the SonicWALL via a VPN clients.
- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to 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.
- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can 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 configured on the **Routing** page located in the **Network** 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, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the Route all internet traffic through this SA check box. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ, or LAN/OPT/DMZ** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ network.

13. Click **OK**. Your new VPN policy is displayed in the **VPN Policies** table.

# VPN>Advanced

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




## Advanced VPN Settings

- **Disable all VPN Windows Networking (NetBIOS) Broadcasts** - Computers running Microsoft Windows® communicate with one another through NetBIOS broadcast packets. Disable this setting access remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Fragmented Packet Handling** - if the VPN log report shows the log message “Fragmented IPSec packet dropped”, select this feature. Do not select it until the VPN tunnel is established and in operation. When you select this setting, the **Ignore DF (Don’t Fragment) Bit** setting becomes active.
- **Enable NAT Traversal** - Select this setting is a NAT device is located between your VPN endpoints. IPSec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPSec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPSec peer.

Selecting **Enable NAT Traversal** allows VPN tunnels to support this protocol, and log messages are generated by the SonicWALL when a IPSec Security Gateway is detected behind a NAT/NAPT device. The following log messages are found on the **View Log** tab:

**Peer IPSec Gateway behind a NAT/NAPT device**

**Local IPSec Security Gateway behind a NAT/NAPT device**

**No NAT/NAPT device detected between IPSec Security**

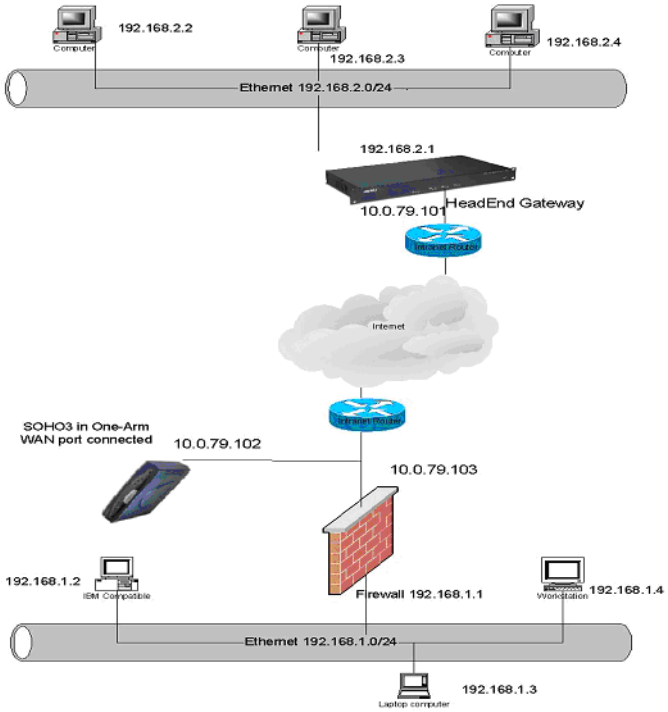
**Peer IPSec Security Gateway doesn't support VPN NAT Traversal**

- **Keep Alive interval (seconds)** - the default value is 240 seconds (4 minutes). If **Enable Keep Alive** is selected on the **Advanced VPN Settings** page, a new negotiation begins if the previous VPN Policy was deleted by Dead Peer Detection (DPD).
- **Enable IKE Dead Peer Detection** - select if you want inactive VPN tunnels to be dropped by the SonicWALL. Enter the number of seconds between "heartbeats" in the **Dead Peer Detection Interval (seconds)** field. The default value is 60 seconds. Enter the number of missed heartbeats in the **Failure Trigger Level (missed heartbeats)** field. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWALL. The SonicWALL uses a UDP packet protected by Phase 1 Encryption as the heartbeat.

## VPN Single-Armed Mode (stand-alone VPN gateway)

VPN Single-Armed Mode allows you to deploy a SonicWALL with single port (WAN) utilized as a VPN tunnel termination point. Clear text traffic is routed to the single interface and the data is encapsulated to the appropriate IPSec gateway.

An example of a deployment is to place the SonicWALL between the existing firewall and the router connected to the Internet. Traffic is sent in clear text to the SonicWALL, then encrypted and sent to the appropriate VPN Gateway.



If **VPN Single-Armed Mode (stand-alone VPN gateway)** is enabled, a warning message appears as follows:


Click **OK** to enable the SonicWALL in VPN Single Armed Mode.

## Configuring a SonicWALL for VPN Single Armed Mode

You have the following information to configure the IP addresses on the firewalls:

| **Remote SonicWALL** | **Corporate SonicWALL** |
|---|---|
| WAN IP Address: 66.120.118.11 | WAN IP Address:66.120.118.25 |
| Subnet Mask: 255.255.255.0 | Subnet Mask: 255.255.255.0 |
| LAN IP Address 192.168.1.1 | LAN IP Address: 192.168.3.1 |
| Subnet Mask: 255.255.255.0 | Subnet Mask: 255.255.255.0 |

**VPN Single Armed Mode SonicWALL**

WAN IP Address: 66.120.118.13

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

To configure a SonicWALL in VPN Single Armed Mode in front of an existing SonicWALL, follow these steps:

1. Configure the Remote and Local SonicWALLs in your preferred networking mode.
2. Configure a VPN SA using IKE and Pre-shared Secret on the Remote SonicWALL using the VPN WAN IP address as the IPSec Gateway, and the Local SonicWALL WAN IP address as the Destination Network.
3. Configure a Static Route on the Local SonicWALL to send network traffic destined for the Remote SonicWALL to the VPN SonicWALL.
4. Configure the VPN SonicWALL in **Standard** networking mode.
5. Click **Advanced**, then **Intranet**. Select the **VPN Single Armed Mode (stand alone VPN gateway)** check box, and click **Update**.
6. A rule is automatically added to the VPN SonicWALL for HTTPS management from the WAN. The LAN port is disabled when you configure a SonicWALL for VPN Single Armed mode.
7. Configure a VPN SA using IKE and Pre-shared Secret on the VPN SonicWALL to securely connect to the Remote SonicWALL. Enter the Remote SonicWALL WAN IP address as the IPSec Gateway and the Remote SonicWALL LAN IP Address range as the Destination Network, if configuring “Many to One NAT”.
8. Click **Advanced**, and then **Routes**. Enter the Corporate SonicWALL WAN IP address in the **Dest**. **Network** field. Enter the subnet mask in the **Subnet Mask** field. Enter the Local SonicWALL WAN IP address as the **Gateway**, and select **WAN** from the **Link** menu. Click **Update**.

- Now that all SonicWALLs are configured, network traffic on the corporate SonicWALL destined for the remote office is routed to the VPN SonicWALL, encrypted, and sent to the remote SonicWALL.

## VPN User Authentication Settings

- **Allow these services to bypass user authentication on SAs** - this feature allows VPN users without authentication to access the specified services. To add a service, select the service from the menu and click **Add**. The service is added to the **Allow these services to bypass user authentication on SAs** list. To remove a service, select the service in the **Allow these services to bypass user authentication on VPN SAs** list and click **Remove**.
- **Allow these address ranges to bypass user authentication on SAs** - this feature allows the specified IP address or IP address range to bypass user authentication on VPN connections. To add an IP address, enter the single IP address in the text box, then click **Add**. To add an IP address range, enter the range starting IP address in the first field and the ending IP address in the text field (up to the last three numbers of the IP address).

## VPN Bandwidth Management

Bandwidth management is a means of allocating bandwidth resources to critical applications on a network. The **VPN Bandwidth Management** section allows you to define the amount of outbound VPN traffic allowed from the SonicWALL. Traffic is then scheduled in Kbps according to **Guaranteed Bandwidth** (minimum) and **Maximum Bandwidth** settings.

To enable VPN Bandwidth Management, follow these steps:

1. Select **Enable VPN Bandwidth Management**.
2. Enter the minimum amount of bandwidth allowed in the **Guaranteed Bandwidth (Kbps)** field.
3. Enter the maximum amount of bandwidth allowed in **Maximum Bandwidth** (Kbps) field.
4. Select VPN bandwidth priority from the **Priority** menu, **0 (highest)** to **7 (lowest)**.
5. Click Apply.

***Tip!*** *Bandwidth management is available only on outbound VPN traffic. You cannot configure individual Security Associations to use bandwidth management.*

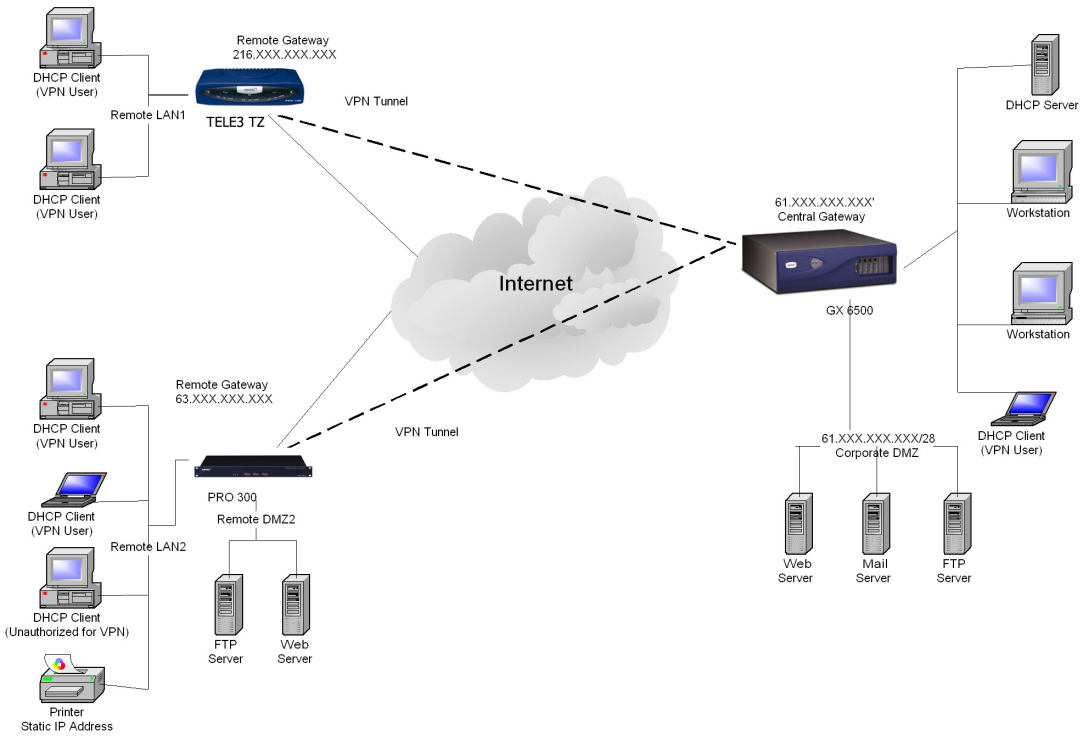
# VPN>DHCP over VPN

**DHCP over VPN** allows a Host (DHCP Client) behind a SonicWALL obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.

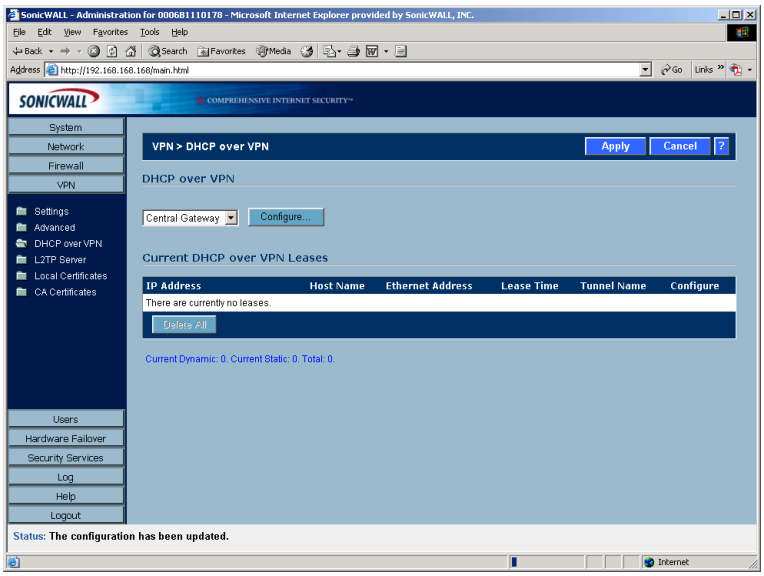
## DHCP Relay Mode

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

DHCP over a VPN Tunnel

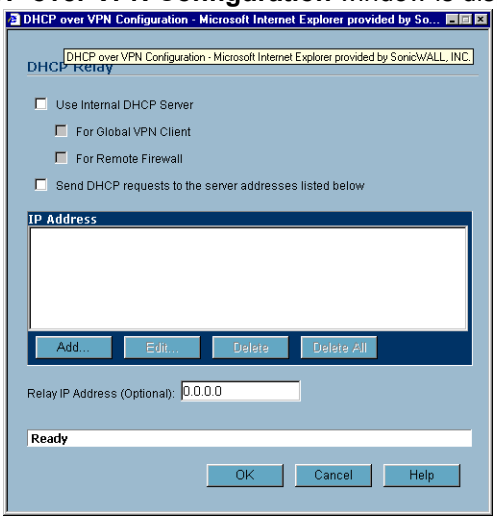


## Configuring the Central Gateway for DHCP Over VPN

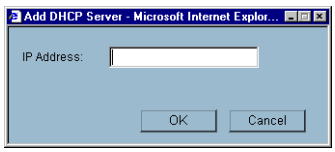



To configure **DHCP over VPN** for the **Central Gateway**, use the following steps:

1. Log into the Management interface, click **DHCP**, and then **DHCP over VPN**.
2. Select **Central Gateway** from the **DHCP Relay Mode** menu.
3. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.




4. Select **Use Internal DHCP Server** to enable the Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information.
5. If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
6. Click **Add**. The IP Address window is displayed.



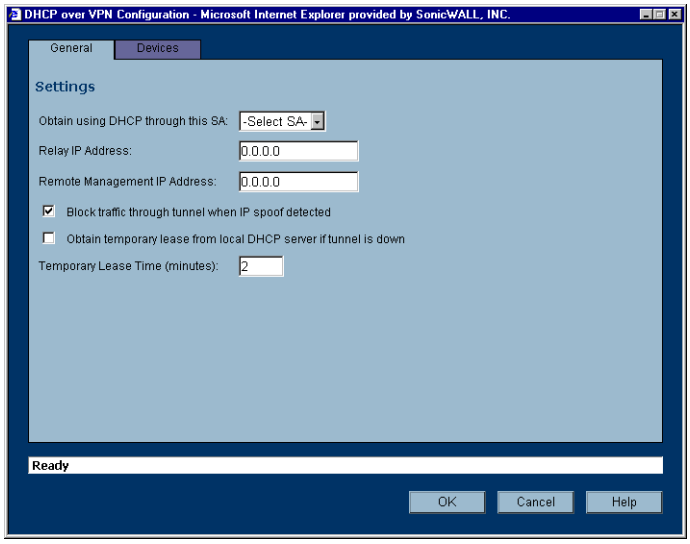

7. Enter the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWALL now directs DHCP requests to the specified servers.

8. Enter the IP address of a relay server in the **Relay IP Address (Optional)** field.

To edit an entry in the **IP Address** table, click **Edit**. To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

## Configuring DHCP over VPN Remote Gateway

1. Select **Remote Gateway** from the **DHCP Relay Mode** menu.
2. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.




3. Select the VPN Security Association to be used for the VPN tunnel from the **Relay DHCP through this VPN Tunnel** menu.

***Alert!*** *Only VPN Security Associations using IKE and terminate on the LAN appear in the Obtain using DHCP through this VPN Tunnel.*

4. The **Relay IP address** is used in place of the Central Gateway address, and must be reserved in the DHCP scope on the DHCP server. The Relay IP address can also be used to manage the SonicWALL remotely through the VPN tunnel behind the Central Gateway.
5. The **Remote Management IP Address,** if entered, can be used to manage the SonicWALL remotely through the VPN tunnel behind the Central Gateway.
6. If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is entered for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL to respond to IP spoofs.
7. If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, enter the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is two (2) minutes.

## Device Configuration

8. To configure **Static Devices on the LAN**, click **Add**, and enter the IP address of the device in the **IP Address** field and then enter the Ethernet Address of the device in the **Ethernet Address** field. An

example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to enter the Ethernet address of a device.

9. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses. Click Add, and enter the Ethernet address in the **Ethernet Address** field.

***Alert!*** *You must configure the local DHCP server on the remote SonicWALL to assign IP leases to these computers.*

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

***Tip!*** *If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.*

## Current DHCP over VPN Leases

The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name. To edit an entry, click the Notepad icon under **Configure** for that entry.

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the Trashcon icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

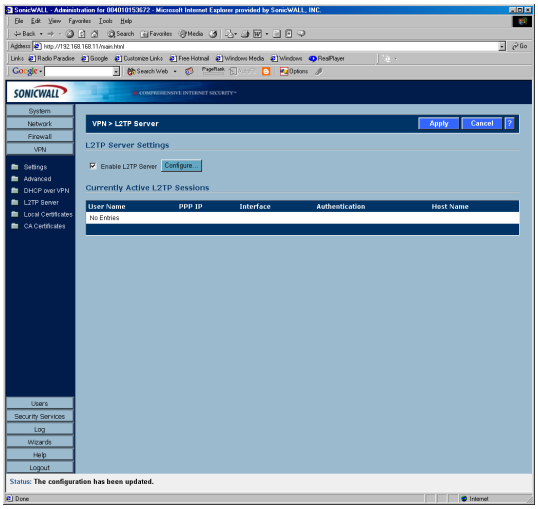
Click **Delete All** to delete all VPN leases.

# VPN>L2TP Server

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the

endpoints of a VPN tunnel to provide additional security, and you can implement it with IPSec to provide a secure, encrypted VPN solution.

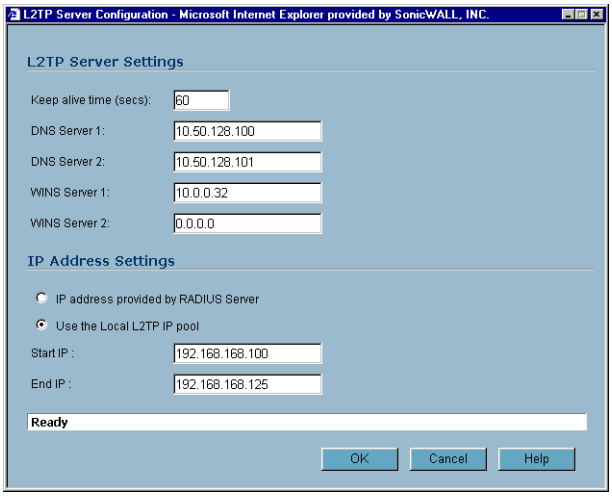



# General

***Note:*** *You must enable Group VPN before configuring the SonicWALL L2TP feature. Also, the encryption method and shared secret must match the L2TP client settings.*

To enable L2TP Server functionality on the SonicWALL, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.

## L2TP Server Settings




Configure the following settings:

1. Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open.
2. Enter the IP address of your first DNS server in the **DNS Server 1** field.
3. If you have a second DNS server, enter the IP address in the **DNS Server 2** field.

4. Enter the IP address of your first WINS server in the **WINS Server 1** field.
5. If you have a second WINS server, enter the IP address in the **WINS Server 2** field.

### IP Address Settings

6. Select **IP address provided by RADIUS Server** if a RADIUS Server provides IP addressing information to the L2TP clients.
7. If the L2TP Server provides IP addresses, select **Use the Local L2TP IP** pool. Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.
8. Click **OK**.

### Adding L2TP Clients to the SonicWALL

To add L2TP clients to the local user database or a RADIUS database, click **Users,** then **Add**. When adding privileges for a user, select **L2TP Client** as one of the privileges. Then the user can access the SonicWALL as a L2TP client.

### Currently Active L2TP Sessions

- **User Name** - the user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - the source IP address of the connection.
- **Interface** - the enter of interface used to access the L2TP Server, whether it's a VPN client or another SonicWALL appliance.
- **Authentication** - enter of authentication used by the L2TP client.
- **Host Name** - the name of the network connecting to the L2TP Server.

# Digital Certificates

## Overview of X.509 v3 Certificates

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWALL has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange VPN policy. IKE is an important part of IPSec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

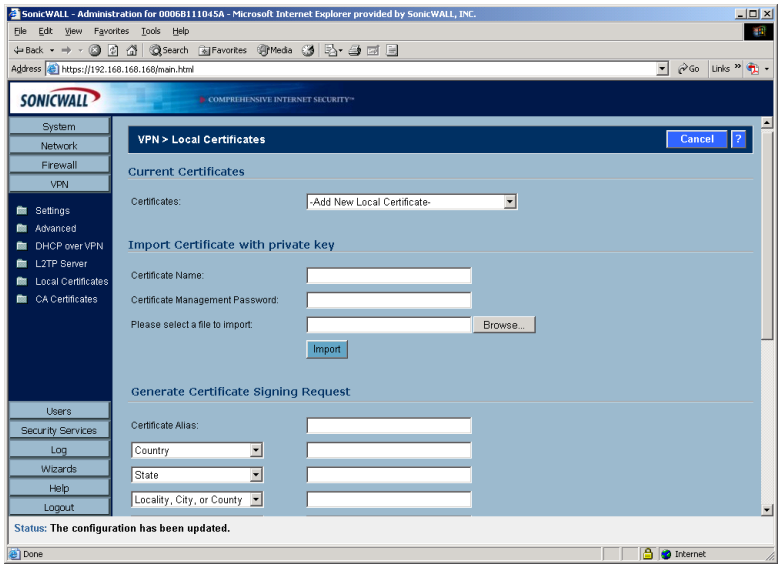
## SonicWALL Third Party Digital Certificate Support

SonicWALL supports third party certificates from the following two vendors of Certificate Authority Certificates:

- VeriSign
- Entrust

To implement the use of certificates for VPN SAs, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWALL to validate your Local Certificates. You import the valid CA certificate into the SonicWALL using the **VPN>CA Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates you add in the **VPN>Local Certificates** page.

# VPN>Local Certificates




After a certificate is signed by the CA and returned to you, you can import the certificate into the SonicWALL to be used as a **Local Certificate** for a VPN Security Association.

***Tip!*** *After you import a local certificate on the SonicWALL, it is recommended you export the certificate to the local disk as a backup. When exporting a local certificate, a password is required.*

## Importing Certificate with Private Key

Use the following steps to import the certificate into the SonicWALL:

1. In the **Import Certificate with private key** section of **Local Certificates**, type the **Certificate Name**.
2. Type the **Certificate Management Password**. This password was created when you exported your signed certificate.
3. Use **Browse** to locate the certificate file.
4. Click **Import**, and the certificate appears in the list of **Current Certificates**.
5. To view details about the certificate, select it from the list of **Current Certificates**.

## Certificate Details

To view details about the certificate, select the certificate from the **Certificates** menu in the **Current Certificates** section. The Certificate Details section lists the following information about the certificate:

- **Certificate Issuer**
- **Subject Distinguished Name**
- **Certificate Serial Number**

- **Expiration On**
- **Alternate Subject Name**
- **Alternate Subject Name Type**
- **Status**

### Delete This Certificate

To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

## Generating a Certificate Signing Request

To generate a local certificate for use with a VPN policy, follow these steps:

***Tip!*** *You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.*

1. Select **Add New Local Certificate** from the **Certificates** menu.
2. In the **Generate Certificate Signing Request** section, enter a name for the certificate in the **Certificate Name** field.
3. Enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

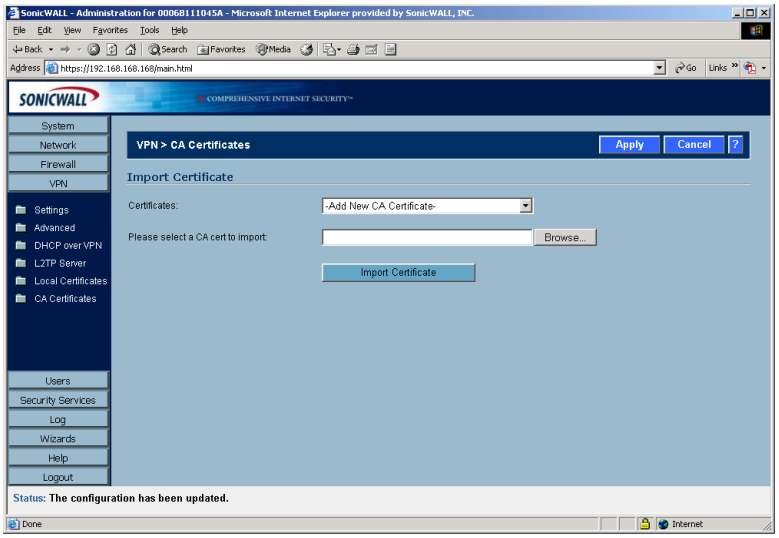
   You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**. You need to provide the proper input for the **Domain Name** (yourcompanyname.com) or **E-mail Address** (abc@yourcompanyname.com) option in the corresponding field.
4. The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.
5. Select a Subject Key size from the **Subject Key Size** menu.

***Note:*** *Not all key sizes are supported by a Certificate Authority, therefore you should check with your CA for support key sizes.*

6. Click **Generate** to create a certificate file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.
7. Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer.

You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

# VPN>CA Certificates




## Importing CA Certificates into the SonicWALL

After your CA service has validated your **CA Certificate**, you can import it into the SonicWALL and use it to validate **Local Certificates** for VPN Security Associations.

To import your **CA Certificate** into the SonicWALL, follow these steps:

1. Select **Add New CA Certificate**.
2. Click **Browse**, and locate the PKCS#7 (*.p7b) or DER (*.der) or *.cer encoded file sent by the CA service.
3. Click **Open** to set the directory path to the certificate
4. Click **Import** to import the certificate into the SonicWALL. Once it is imported, you can view the **Certificate Details**.

## Certificate Details

The **Certificate Details** section lists the following information:

- **Certificate Issuer**
- **Subject Distinguished Name**
- **Certificate Serial Number**
- **Expires On**
- **CRL Status**

The **Certificate Issuer**, **Certificate Serial Number**, and the **Expiration Date** are generated by the CA service. The information is used when a **Generate Certificate Signing Request** is created and sent to your CA service for validation.

### Delete This Certificate

To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

# Certificate Revocation List (CRL)

A **Certificate Revocation List (CRL)** is a way to check the validity of an existing certificate. A certificate may be invalid for several reasons:

- It is no longer needed.
- A certificate was stolen or compromised.
- A new certificate was issued that takes precedence over the old certificate.

If a certificate is invalid, the CA may publish the certificate on a **Certificate Revocation List** at a given interval, or on an online server in a X.509 v3 database using Online Certificate Status Protocol (OCSP). Consult your CA provider for specific details on locating a CRL file or URL.

***Tip!*** *The SonicWALL supports obtaining the CRL via HTTP or manually downloading the list.*

You can import the CRL by manually downloading the CRL and then importing it into the SonicWALL. You can also enter the URL location of the CRL by entering the address in the **Enter CRL's location (URL) for auto-import** field. The CRL is downloaded automatically at intervals determined by the CA service. Certificates are checked against the CRL by the SonicWALL for validity when they are used.

## Importing a CRL List

To import a CRL list, follow these steps:

1. Click **Browse** for **Please select a file to import**.
2. Locate the PKCS#12 (*.p12) or Micorosft (*.pfx) encoded file.
3. Click **Open** to set the directory path to the certificate.
4. Click **Import** to import the certificate into the SonicWALL.

## Automatic CRL Update

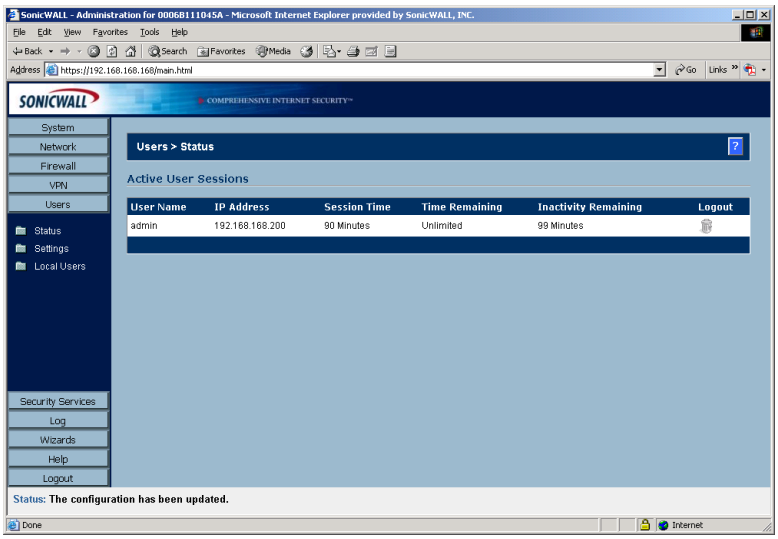
To enable automatic CRL updates to the SonicWALL, type the URL of the CRL server for your CA service in the **Enter CRL's location (URL) for auto-import**, then click Apply.

# 10 Users

The SonicWALL provides a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to bypass content filtering. Also, you can permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

User level authentication can performed using a local user database, RADIUS, or a combination of the two applications. The local database on the SonicWALL can support up to 1,000 users. If you have more than 1,000 users or want to add an extra layer of security for authenticating users to the SonicWALl, use RADIUS for authentication.

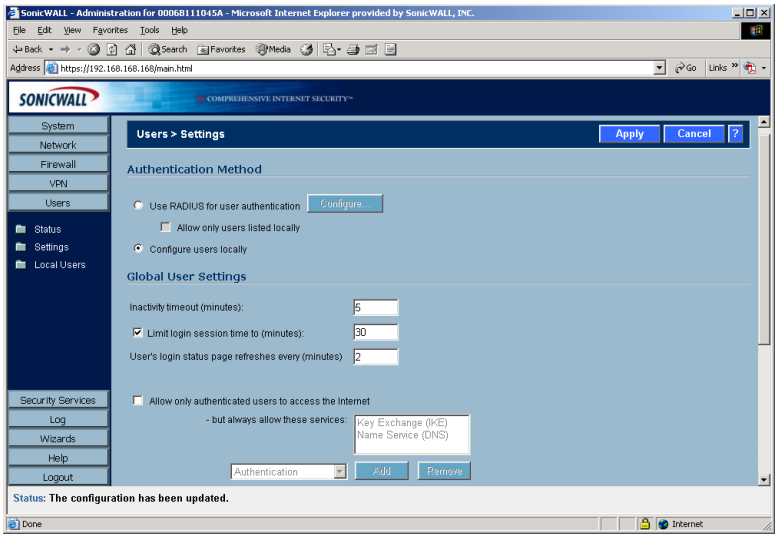
## Users>Status




### Active User Sessions

The Active User Sessions table lists the **User Name**, the **IP Address** of the user, the **Session Time**, **Time Remaining** of the session, and the **Inactivity Remaining** time. You can also click the **Trashcan** icon in the **Logout** column to log a user out of the SonicWALL.

# Users>Settings




On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network. The SonicWALL supports user level authentication using the local SonicWALL database, a RADIUS server, or a combination of the two authentication methods.

## Authentication Method

- **Use RADIUS for user authentication** - if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWALL. If you select Use RADIUS for user authentication, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS. If you select **Use RADIUS for user authentication**, the **Configure** button becomes available.
- **Allow only users listed locally** - enable this setting if you have a subset of RADIUS users accessing the SonicWALL. The user names must be added to the internal SonicWALL user database on the **Users>Local Users** page before they can be authenticated using RADIUS.
- **Configure users locally** - selecting this setting allows you to configure users in the local SonicWALL database using the **Users>Local Users** page.

## Global User Settings

The settings listed below apply to all users when authenticated through the SonicWALL.

- **Inactivity timeout (minutes)** - users can be logged out of the SonicWALL after a preconfigured inactivity time. Enter the number of minutes in this field.
- **Limit login session time to (minutes)** - you can limit the time a user is logged into the SonicWALL by selecting the check box and typing the amount of time, in minutes, in the **Limit login session time to (minutes)** field. The default value is **30** minutes.
- **Allow only authenticated users to access the Internet** - this feature allows Internet access to only users configured on the SonicWALL. There is a corresponding checkbox when adding a user to the local SonicWALL database allowing you to grant
access to the Internet. When you select **Allow only authenticated users to access the Internet, but always allow these services**, the default **Key Exchange (IKE)** and **Name Service (DNS)** services are activated. You can add or remove services available to users. To add a service, select the service from the menu, and click **Add**. To remove a service, select the service in the in the services list, and click **Remove**.
- **And always allow these address ranges** - this feature allows the specified IP address or IP address range to bypass user authentication. To add an IP address, enter the single IP address in the first

field, then click **Add**. To add an IP address range, enter the range starting IP address in the first field and the ending IP address in the next field (up to the last three numbers of the IP address.

## Acceptable Use Policy

An acceptable use policy (AUP) is a policy users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWALL.

**LAN** and **DMZ** are selected automatically from the **Display on login** from section. **WAN** and **VPN** are also available.

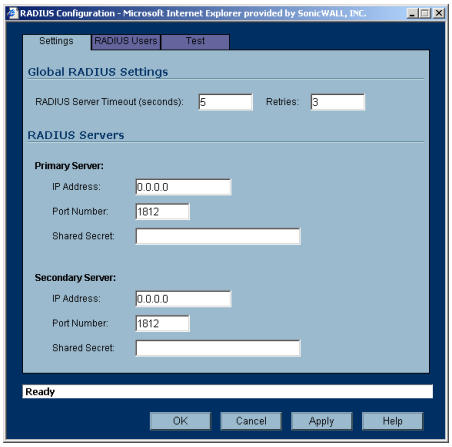
In the **Acceptable Use Policy** field, enter the text of your policy. Click **Apply** to update the configuration.

***Tip!*** *Acceptable Use Policies can use HTML formatting in the body of the message.*

## Configuring RADIUS Authentication

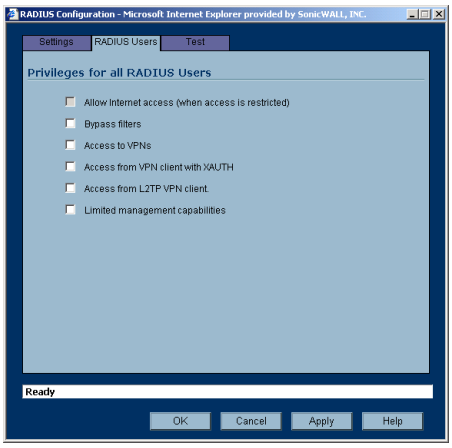
To enable the SonicWALL to use authentication from a RADIUS server, follow these steps:

1. Select **Use RADIUS for user authentication**.
2. Select **Allow only users listed locally** if only the users listed in the SonicWALL database are authenticated using RADIUS.
3. Click **Configure** to set up your RADIUS server settings on the SonicWALL. The **RADIUS Configuration** window is displayed.




4. In the **Global RADIUS Settings** section, define the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of 5.
5. Define the number of times the SonicWALL attempts to contact the RADIUS server in the **Retries** field. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 1 and 10, however 3 RADIUS server retries is recommended.
6. In the **RADIUS Servers** section, specify the settings of the primary RADIUS server in the RADIUS servers section. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.
7. Type the IP address of the RADIUS server in the **IP Address** field.
8. Type the **Port Number** for the RADIUS server.
9. Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

10. If there is a secondary RADIUS server, type the appropriate information in the **Secondary Server** section.
11. Click the **RADIUS Users** tab.




12. Select the default privileges for all RADIUS users in this section.

    **Access to the Internet (when access is restricted)** - If you have selected **Allow only authenticated users to access the Internet**, you can allow individual users to access the Internet.

    **Bypass Filters** - Enable this feature if the user has unlimited access to the Internet from the LAN, bypassing SonicWALL Web, News, Java, and ActiveX blocking.

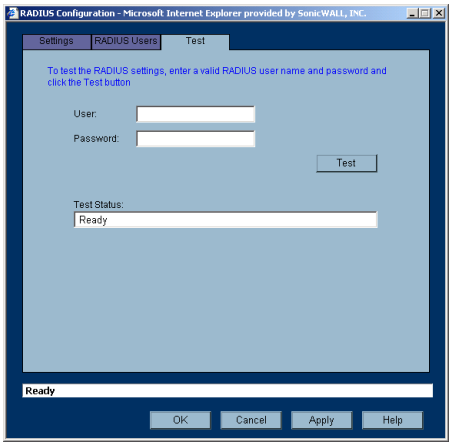
    **Access to VPNs** - Enable feature to allow the user to send information over the VPN connection with authentication enforcement.

    **Access from the VPN Client with XAUTH** - Enable this feature if the user requires XAUTH for authentication and accesses the SonicWALL via a VPN client.

    **Access from L2TP VPN client** - Enable this feature to allow the user to send information using a L2TP VPN Client with authentication enforcement.

    **Limited Management Capabilities** - Enabling this feature allows the user to have limited local management access to the SonicWALL Management Interface. This access is limited to the following pages: **General** (Status, Network, Time); **Log** (View Log, Log Settings, Log Reports); **Diagnostics** (All tools except Tech Support Report).

13. Click **Apply**, then click the **Test** tab.

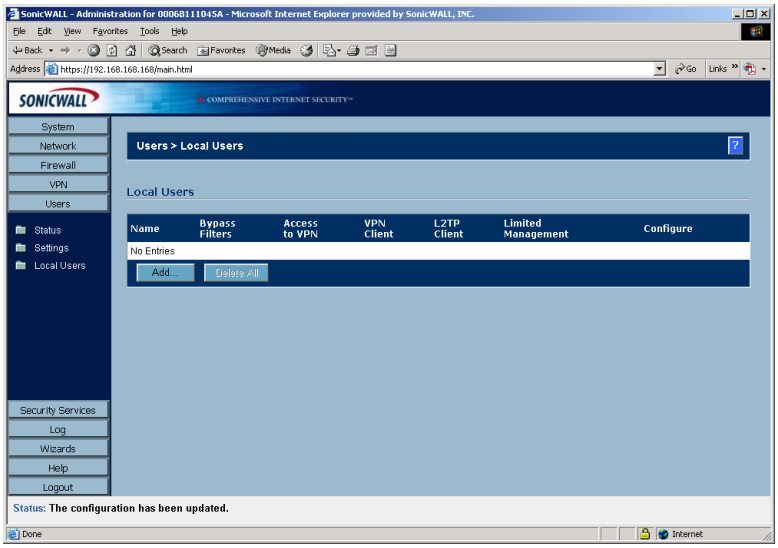



14. Type in a valid user name in the **User** field, and the password in the **Password** field.
15. Click **Test**. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.

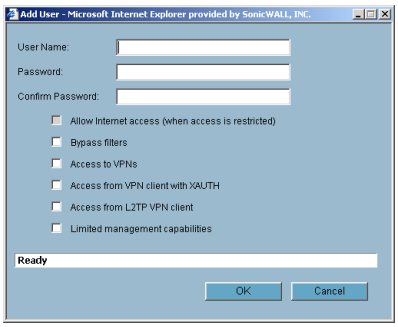
16. Click **OK**.

Once the SonicWALL has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialogue box.

# Users>Local Users




Add local users to the SonicWALL internal database. Click **Add User** to display the **Add User** configuration window. Follow the steps below to add users locally.




## Settings

1. Create a user name and type it in the **User Name** field.
2. Create a password for the user and type it in the **Password** field. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.
3. Confirm the password by retyping it in the **Confirm Password** field.
4. Select from the following list of privileges to assign the user:

   **Access to the Internet (when access is restricted)** - If you have selected **Allow only authenticated users to access the Internet**, you can allow individual users to access the Internet.

   **Bypass Filters** - Enable this feature if the user has unlimited access to the Internet from the LAN, bypassing SonicWALL Web, News, Java, and ActiveX blocking.

   **Access to VPNs** - Enable feature to allow the user to send information over the VPN connection with authentication enforcement.

   **Access from the VPN Client with XAUTH** - Enable this feature if the user requires XAUTH for authentication and accesses the SonicWALL via a VPN client.

**Access from L2TP VPN client** - Enable this feature to allow the user to send information using a L2TP VPN Client with authentication enforcement.

**Limited Management Capabilities** - Enabling this feature allows the user to have limited local management access to the SonicWALL Management Interface. This access is limited to the following pages: **General** (Status, Network, Time); **Log** (View Log, Log Settings, Log Reports); **Diagnostics** (All tools except Tech Support Report).

5. Click **OK**.

The users you add appear in the Local Users table with their privileges listed. Click the **Notepad** icon in the **Configure** column to edit the user information. Click the **Trashcan** to delete a user.

# 11 Security Services

Security Services allows you to manage SonicWALL Security Services and Upgrades for your SonicWALL. SonicWALL, Inc. offers a variety of subscription-based Security Services and Upgrades to enhance the functionality of your SonicWALL. You can activate and manage Security Services directly from the SonicWALL Management Interface or from https://www.mySonicWALL.com. SonicWALL Security Services and Upgrades are designed to integrate seamlessly into your network to provide complete protection.

***Note:*** *For more information on SonicWALL Security Services and Upgrades, please visit <http://www.sonicwall.com.*

This chapter provides an overview of the SonicWALL Security Services listed under Security Services in the SonicWALL Management Interface, which includes:

- SonicWALL Content Filtering Service
- SonicWALL Network Anti-Virus
- SonicWALL E-Mail Filter
- SonicWALL Intrusion Prevention Service

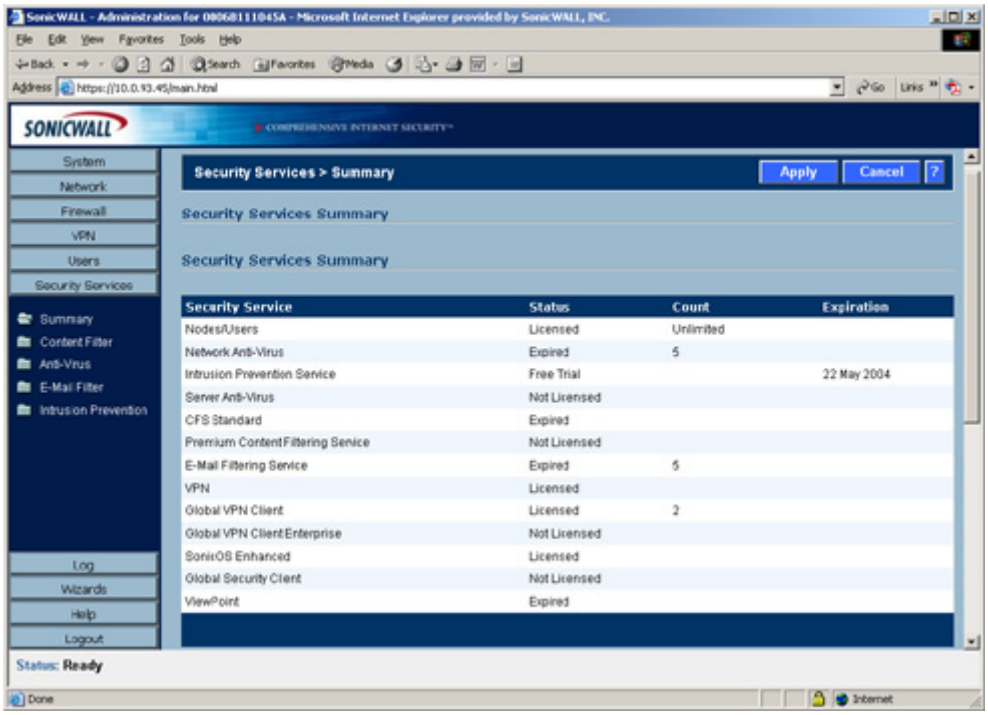
***Tip!*** *You can try FREE TRIAL of these services directly from the SonicWALL Management Interface.*

This chapter also explains how to configure the SonicWALL Restrict Web Features and Trusted Domains features on the **Security Services>Content Filtering** page that are included with SonicOS.

***Note:*** *For complete product documentation for the SonicWALL Security Services in this chapter as well as all SonicWALL Security Services and Upgrades, visit the SonicWALL documentation site at www.sonicwall.com/services/documentation.*

# Security Services>Summary

The **Security Services>Summary** page lists the available SonicWALL security services and upgrades available for your SonicWALL and provides access to mySonicWALL.com to activate services.




## Security Services Summary

A list of currently available services through mySonicWALL.com is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. If the service is limited to a number of users, the number is displayed in the **Count** column. The service expiration date is displayed in the **Expiration** column.

## Manage Services Online

Clicking the **To Activate, Upgrade, or Renew services, click here**. link displays the **mySonicWALL.com Login** page.

Enter your mySonicWALl.com username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System>Licenses** page is displayed with the **Manage Services Online** table. The information in the **Manage Services Online** table is updated from your mysSonicWALL.com account.

***Note:*** *If you have activated SonicWALL Global Security Client on your SonicWALL, a **Policy Editor** button is displayed below the **Manage Services Online** table for configuring security policies. See the **SonicWALL Global Security Client Administrator's Guide** for instructions on configuring the Policy Editor.*

***Note:*** *For more information on activating, upgrading, or renewing a SonicWALL Security Service or Upgrade, see System>Licenses in Chapter 3.*

## If Your SonicWALL is Not Registered

If your SonicWALL is not registered, the **Security Services>Summary** page does not include the **Services Summary** table.

Your SonicWALL must be registered to display the **Services Summary** table. You can register your SonicWALL via the Management Interface on the **System>Status** page. You must have a mySonicWALL.com account to register your SonicWALL via the Management Interface. You can create a mySonicWALL.com account from the Security **Services>Summary** page using the **To Activate, Upgrade, or Renew services, click here**. link, which displays the **mySonicWALL.com Login** page.

Click the **here** link on the **mySonicWALL.com Login** page to display the mySonicWALL account registration form. Complete the form, and click **Submit**.

***Note:*** *For more information on mySonicWALL.com, visit the mySonicWALL.com site at <https://www.mysonicwall.com> and click the question (**?**) icon.*

## Security Services Settings

- **Reduce Anti-Virus and E-mail Filter traffic for ISDN connections** - Selecting this feature enables the SonicWALL Anti-Virus to only check daily (every 24 hours) for updates and reduces the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Synchronize** - Click **Synchronize** to update the licensing and subscription information on the SonicWALL.

# SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. SonicWALL CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWALL CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL informing the user that the site has been blocked according to policy.

With SonicWALL CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWALL CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

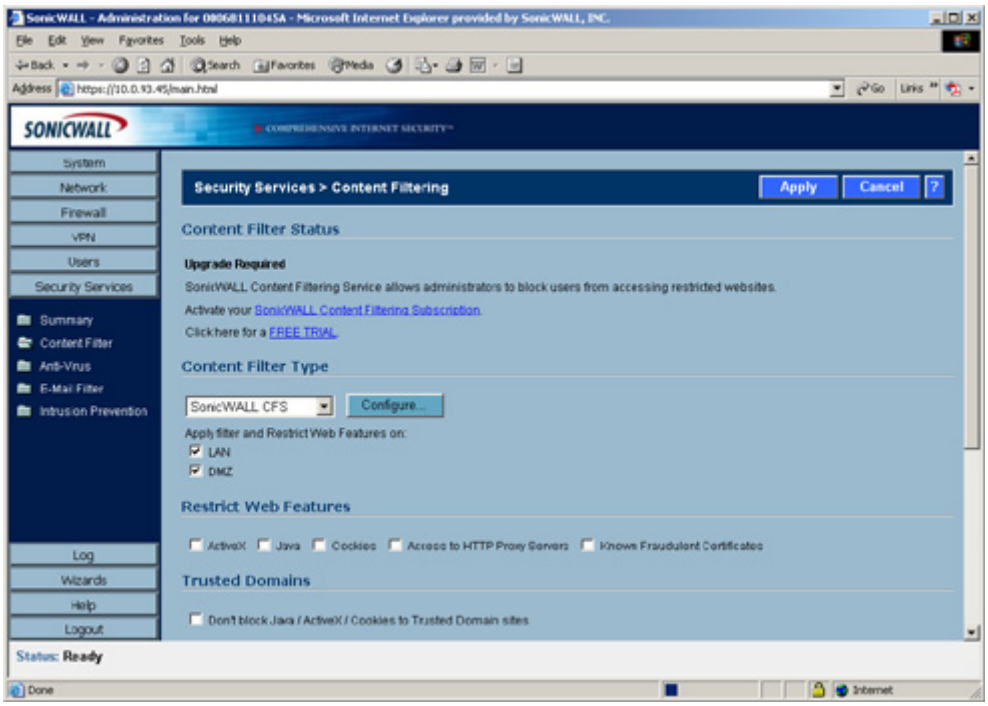
SonicWALL CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL, a customized message is displayed on the user’s screen. SonicWALL Internet Security Appliances can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

- **SonicWALL CFS Standard** blocks 12 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Standard runs on SonicOS Standard 2.0 (or higher).
- **SonicWALL CFS Premium** blocks 56 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Premium provides network administrators with greater control by automatically and transparently enforces acceptable use policies. SonicWALL CFS Premium Productivity Edition and the SonicWALL CFS Premium

Government/Education Edition run on SonicOS Standard 2.1 (or higher) as well as SonicOS Enhanced 2.0 (or higher).

# Security Services>Content Filter

The **Security Services>Content Filter** page allows you to configure the SonicWALL Restrict Web Features and Trusted Domains settings, which are included with SonicOS. You can activate and configure SonicWALL Content Filtering Service as well as two third-party Content Filtering products from the **Security Services>Content Filter** page.




## Content Filter Status

If SonicWALL CFS is activated, the Content Filter Status section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.

You can also access the **SonicWALL CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here**.

If SonicWALL CFS is not activated, you must activate it. If you do not have an Activation Key, you must purchase SonicWALL CFS from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

### Activating SonicWALL CFS

If you have an Activation Key for your SonicWALL CFS subscription, follow these steps to activate SonicWALL CFS:

*Alert!* *You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.*

1. Click the **SonicWALL Content Filtering Subscription** link on the Security **Services>Content Filtering** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS subscription is activated on your SonicWALL.

If you activated SonicWALL CFS at mySonicWALL.com, the SonicWALL CFS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

### Activating a SonicWALL CFS FREE TRIAL

You can try a FREE TRIAL of SonicWALL CFS by following these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL CFS trial subscription is activated on your SonicWALL.

## Content Filter Type

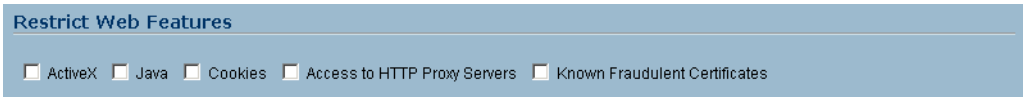
There are three types of content filtering available on the SonicWALL.

- **SonicWALL CFS** - Selecting **SonicWALL CFS** as the **Content Filter Type** allows you to use the SonicWALL Content Filtering Service that is available as an upgrade. You can obtain more information about SonicWALL Content Filtering Service at <http://www.sonicwall.com/products/cfs.html
- **N2H2** - N2H2 is a third party content filter software package supported by SonicWALL. You can obtain more information on N2H2 at <http://www.n2h2.com>.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by SonicWALL. You can obtain more information on Websense Enterprise at <http://www.websense.com>.

**Apply filter and Restrict Web Features on** - Allows you to choose the LAN, WLAN or both for applying content filtering or **Restrict Web Features** protection.

## Restrict Web Features

**Restrict Web Features** enhances your network security by blocking potentially harmful Web applications from entering your network.



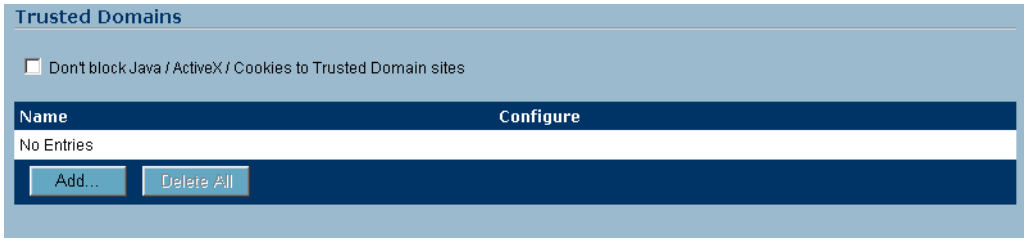
**Restrict Web Features** are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

You can choose the LAN, DMZ or both for applying your **Restrict Web Features** protection from the **Apply filter and Restrict Web Features on** setting in Content Filter Type.

## Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.




If you trust content on specific domains and want them exempt from **Restrict Web Features**, follow these steps to add them

1. Select **Don’t block Java/ActiveX/Cookies to Trusted Domains**.
2. Click **Add**. The **Add Trusted Domain Entry** window is displayed.
3. Enter the trusted domain name in the **Domain Name** field.
4. Click **OK**. The trusted domain entry is added to the Trusted Domain table.

To keep the trusted domain entries but enable Restrict Web Features, uncheck **Don’t block Java/ ActiveX/Cookies to Trusted Domains**.

To delete an individual trusted domain, click on the **Trashcan** icon for the entry.

To delete all trusted domains, click **Delete All**.

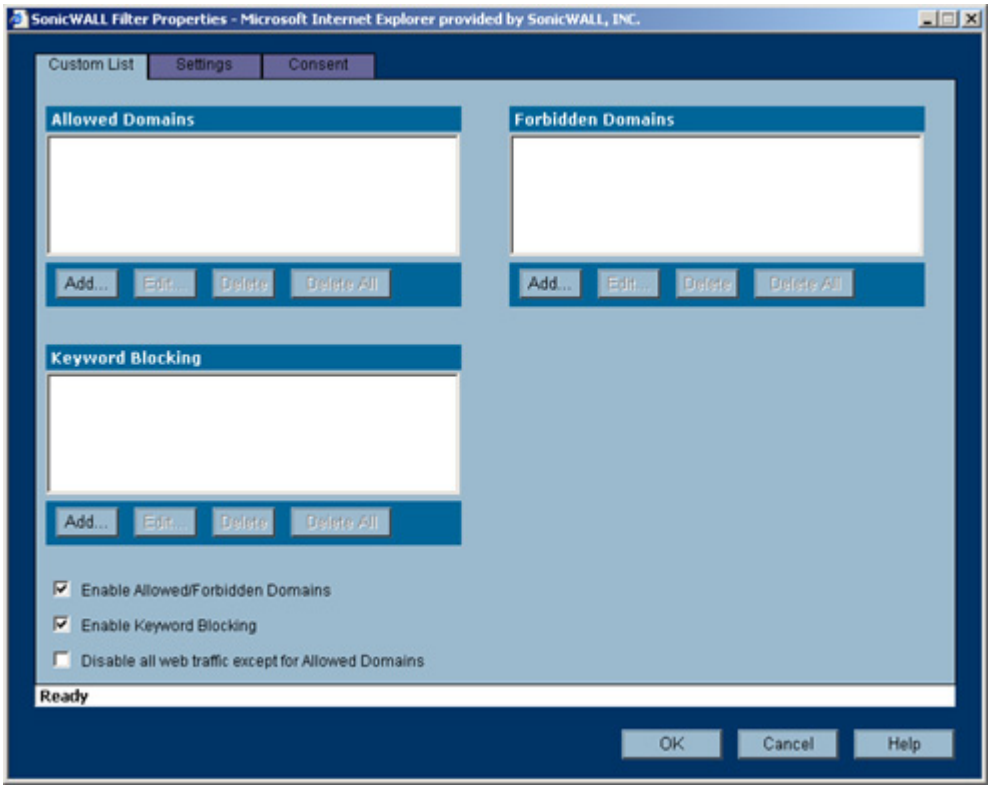
To edit a trusted domain entry, click the **Notepad** icon.

## Message to Display when Blocking

You can enter your customized text to display to the user when access to a blocked site is attempted. The default message is **This site is blocked by the SonicWALL Content Filter Service**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.


# Configuring SonicWALL Filter Properties

You can customize SonicWALL filter features included with SonicOS from the **SonicWALL Filter Properties** window. To display the **SonicWALL Filter Properties** window, select **SonicWALL CFS** from the **Content Filter Type** menu on the **Security Services>Content Filter** page, and click **Configure**. The **SonicWALL Filter Properties** window is displayed.




## Custom List

You can customize your URL list to include **Allowed Domains** and **Forbidden Domains**. By customizing your URL list, you can include specific domains to be accessed, blocked, and include specific keywords to block sites. Select the check box **Enable Allowed/Forbidden Domains** to activate this feature.

To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.

***Alert!*** *Do not include the prefix "http://" in either the Allowed Domains or Forbidden Domains the fields. All subdomains are affected. For example, entering "yahoo.com" applies to "mail.yahoo.com" and "my.yahoo.com".*

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

### Enable Keyword Blocking

To enable blocking using **Keywords**, select **Enable Keyword Blocking**.Click **Add**, and enter the keyword to block in the **Add Keyword** field, and click **OK**.

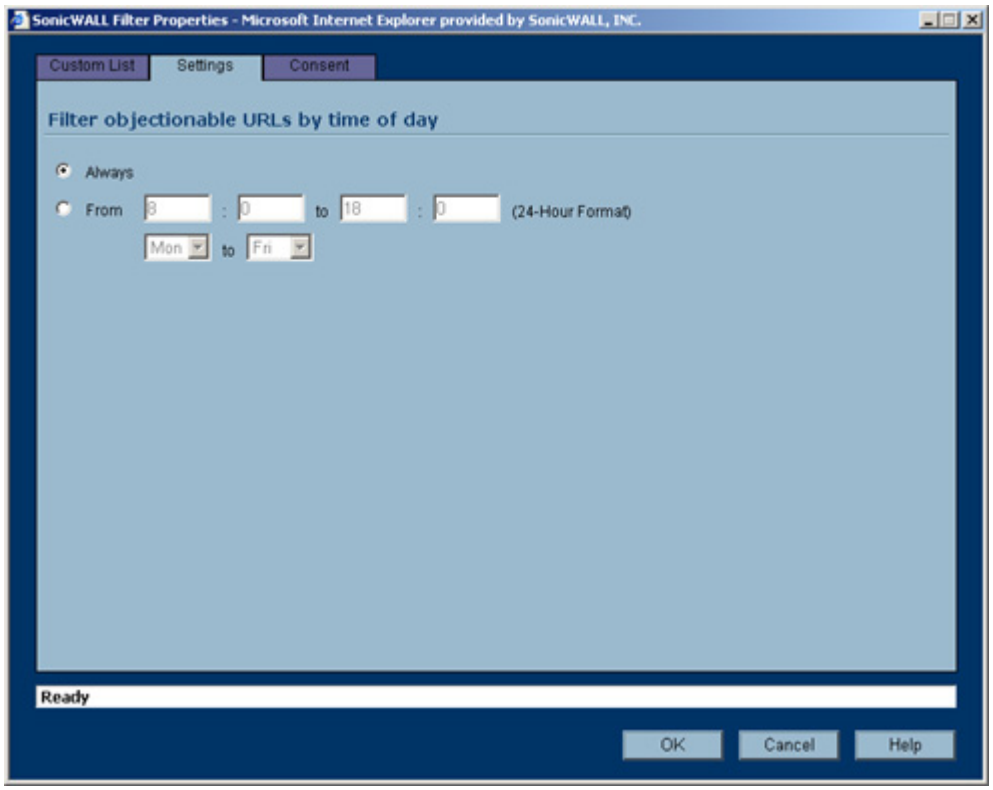
To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.

### Disable all Web traffic except for Allowed Domains

When the **Disable Web traffic except for Allowed Domains** check box is selected, the SonicWALL only allows Web access to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectionable material.

## Settings

The **Time of Day** feature allows you to define specific times when **Content Filtering** is enforced. For example, you could configure the SonicWALL to filter employee Internet access during normal business hours, but allow unrestricted access at night and on weekends.



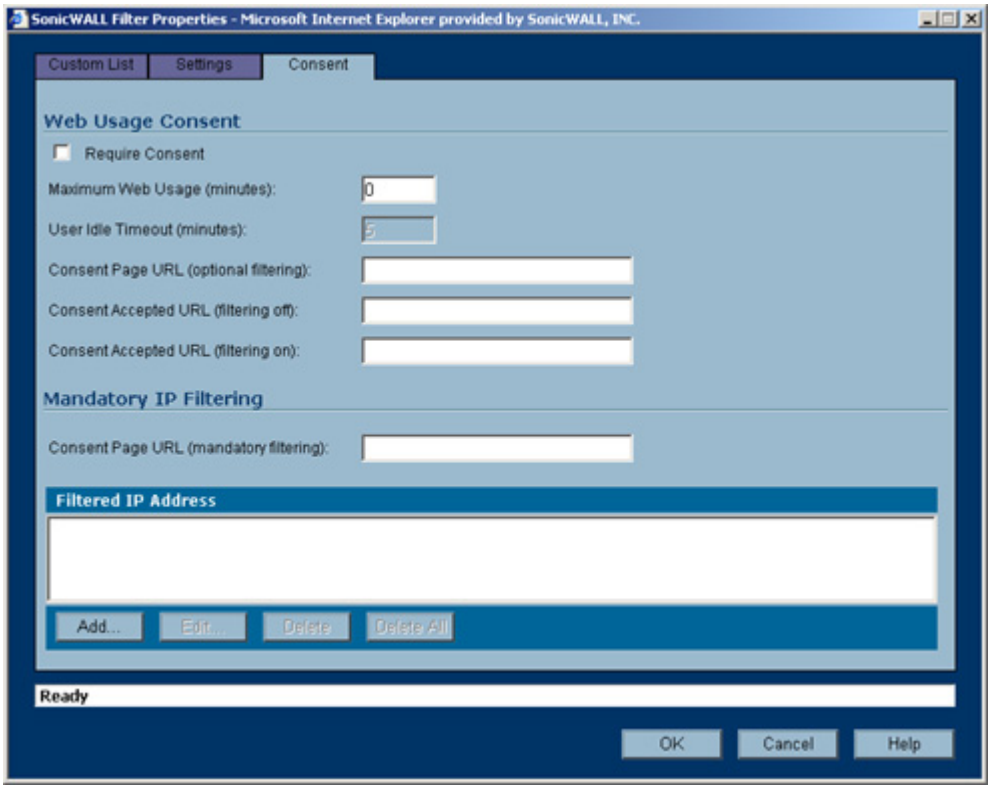

***Tip!*** *Time of Day restrictions only apply to the Content Filtering Service. Customized blocking and Keyword blocking. Consent and Restrict Web Features are not affected.*

- **Always** - When selected, **Content Filtering** is enforced at all times.

- From - When selected, Content Filtering is enforced during the time and days specified. Enter the time period, in 24-hour format, and select the starting and ending day of the week that Content Filtering is enforced.

## Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.




To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes) -** In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.
- User Idle Timeout (minutes) - After a period of Web browser inactivity, the SonicWALL requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.

- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWALL, which, when selected, tell the SonicWALL if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168"\.
- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

## Mandatory Filtered IP Addresses

### Consent Page URL (mandatory filtering)

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL that tells the SonicWALL that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

### Adding a New Address

The SonicWALL can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window.

Enter the IP addresses of these computers in the **Add New Address** field and click **Submit** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete.**

# SonicWALL Network Anti-Virus

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses don't have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Network Anti-Virus prevents occurrences like these and offers a new approach to virus protection. The SonicWALL family of

firewalls constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWALL restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

***Alert!*** *You must purchase an Anti-Virus subscription to enforce Anti-Virus through the SonicWALL.*

# Security Services>Anti-Virus

If SonicWALL Network Anti-Virus is not activated, you must activate it. If you do not have an Activation Key, you must purchase SonicWALL Network Anti-Virus from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

## Activating SonicWALL Network Anti-Virus

If you have an Activation Key for your SonicWALL Network Anti-Virus subscription, follow these steps to activate SonicWALL Network Anti-Virus:

***Alert!*** *You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.*

1. Click the **SonicWALL Network Anti-Virus Subscription** link on the **Security Services>Anti-Virus** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL Network Anti-Virus Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL.

If you activated SonicWALL Network Anti-Virus at www.mySonicWALL.com, the SonicWALL Network Anti-Virus activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

## Activating a SonicWALL Network Anti-Virus FREE TRIAL

You can try a FREE TRIAL of SonicWALL Network Anti-Virus by following these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL.

# Network Anti-Virus E-Mail Filter

The **E-Mail Filter** allows the administrator to selectively delete or disable inbound e-mail attachments as they pass through the SonicWALL. This feature provides control over executable files and scripts, and applications sent as e-mail attachments.

***Note:*** *E-Mail Filter is included with Network Anti-Virus.*

# Intrusion Prevention Service

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

***Note:*** *SonicWALL Intrusion Prevention Service is available for the SonicWALL TZ 170 and PRO Series (PRO 2040, PRO 3060, PRO 4060, and PRO 5060) SonicWALL Internet Security Appliances running SonicOS Standard or Enhanced 2.2 (or higher).*

## SonicWALL IPS Features

- **High Performance Deep Packet Inspection Technology** - SonicWALL's Intrusion Prevention Service features a configurable, high-performance Deep Packet Inspection engine that uses parallel searching algorithms on incoming packets through the application layer to deliver increased attack prevention capabilities over those supplied by traditional stateful packet inspection firewall. By performing all of the matching on packets, SonicWALL IPS eliminates the overhead of having to reassemble the data stream. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL appliances.
- **Inter-Zone Intrusion Prevention** - SonicWALL IPS provides an additional layer of protection against malicious threats by allowing administrator's to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones. This is performed by enabling intrusion prevention on inbound and outbound traffic between trusted zones (SonicOS Enhanced).
- **Extensive Signature Database** - SonicWALL IPS utilizes an extensive database of over 1,700 attack and vulnerability signatures written to detect and prevent intrusions, worms, application exploits, as well as peer-to-peer and instant messaging traffic. The SonicWALL Deep Packet Inspection engine can also read signatures written in the popular Snort format, allowing SonicWALL to easily incorporate new signatures as they are published by third parties. SonicWALL maintains a current and robust signature database by incorporating the latest available signatures from thousands of open source developers and by continually developing new signatures for application vulnerabilities that are not immediately available or provided by open source.
- **Dynamically Updated Signature Database** - SonicWALL IPS includes automatic signature updates delivered through SonicWALL's Distributed Enforcement Architecture (DEA), providing protection

from emerging threats and lowering total cost of ownership. Updates to the signature database are dynamic for SonicWALL firewalls under an active subscription.

- **Scalable** - SonicWALL IPS is a scalable solution for SonicWALL TZ 170 and PRO Series Appliances that secures small, medium and large networks with complete protection from application exploits, worms and malicious traffic.
- **Application Control** - SonicWALL IPS provides the ability to prevent Instant Messaging and Peer-to-Peer file sharing programs from operating through the firewall, closing a potential backdoor that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Simplified Deployment and Management** - SonicWALL IPS allows network administrators to quickly and easily manage the service within minutes. Administrator's can create global policies between security zones and interfaces as well as group attacks by priority, simplifying deployment and management across a distributed network.
- **Granular Policy Management** - SonicWALL IPS provides administrators with a range of granular policy tools to enforce IPS on a global, group, or individual signature level to enable more control and reduce the number of false policies. SonicWALL IPS allows also allows administrators to choose between detection, prevention, or both to tailor policies for their specific network environment.
- **Logging and Reporting** - SonicWALL IPS offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrator's to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System. A hyperlink of the intrusion brings up the signature window for further information from the SonicWALL appliance log.
- **Management by Risk Category** - SonicWALL IPS allows you to enable/disable detection or prevention based on the priority level of attack through High, Medium, or Low predefined priority groups.
- **Detection Accuracy** - SonicWALL IPS detection and prevention accuracy is achieved minimizing both false positives and false negatives. Signatures are written around applications, such as Internet Explorer or SQL Server rather than ports or protocols to ensure that malicious code targeting them are correctly identified and prevented.

## SonicWALL Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWALL Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

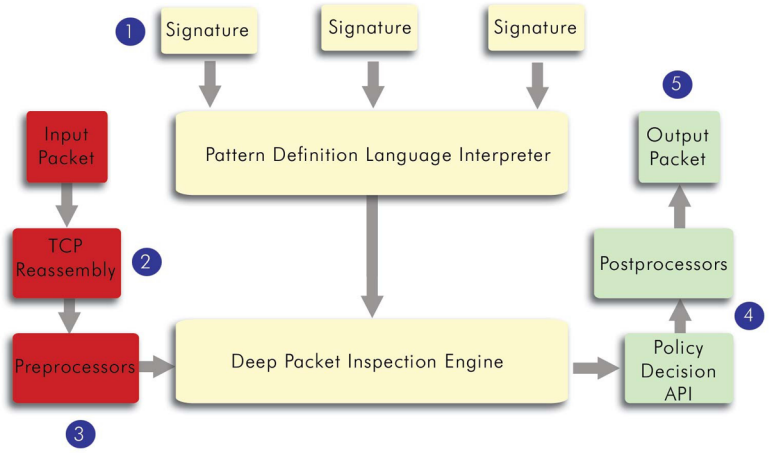
## How SonicWALL's Deep Packet Inspection Architecture Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

The following steps describe how the SonicWALL Deep Packet Inspection Architecture works:

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
4. Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
5. SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

**SonicWALL DEEP PACKET INSPECTION ARCHITECTURE**




## SonicWALL IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Snort** - an open source network intrusion detection system. SonicWALL IPS includes open-source Snort signatures, as well as signatures from other signature databases, and SonicWALL created signatures. SonicWALL does not use the Snort engine.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

# SonicWALL IPS Activation

If you do not have SonicWALL IPS activated on your SonicWALL, you must purchase SonicWALL IPS from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you do not have SonicWALL IPS installed on your SonicWALL, the **Security Services>Intrusion Prevention** page indicates an upgrade is required and includes a link to activate your IPS subscription from the SonicWALL Management Interface or to activate a FREE TRIAL of SonicWALL IPS.

***Note:*** *You must have SonicOS Standard or Enhanced 2.2 (or higher) to activate SonicWALL IPS, and your SonicWALL must be registered on https://www.mySonicwall.com.*

## mySonicWALL.com

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL Internet Security Appliances
- Purchase/Activate SonicWALL Security Services and Upgrades
- Receive SonicWALL firmware and security service updates and alerts
- Manage (change or delete) your SonicWALL security services
- Access SonicWALL Technical Support

Creating a mySonicWALL.com account is easy and free. Simply complete an online registration form. Once your account is created, you can register SonicWALL Internet Security Appliances and activate any SonicWALL Security Services associated with the SonicWALL.

Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

If you activated SonicWALL IPS at mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

## Activating SonicWALL IPS

If you have an Activation Key for your SonicWALL IPS, follow these steps to activate IPS:

1. Click the **SonicWALL IDP Subscription** link on the **Security Services>Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already registered to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL IPS Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL IPS subscription is activated on your SonicWALL.

If you activated the SonicWALL IPS subscription on mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

## Activating the SonicWALL IPS FREE TRIAL

To try a FREE TRIAL of SonicWALL IPS, follow these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL IPS trial subscription is activated on your SonicWALL.

# 12 Log

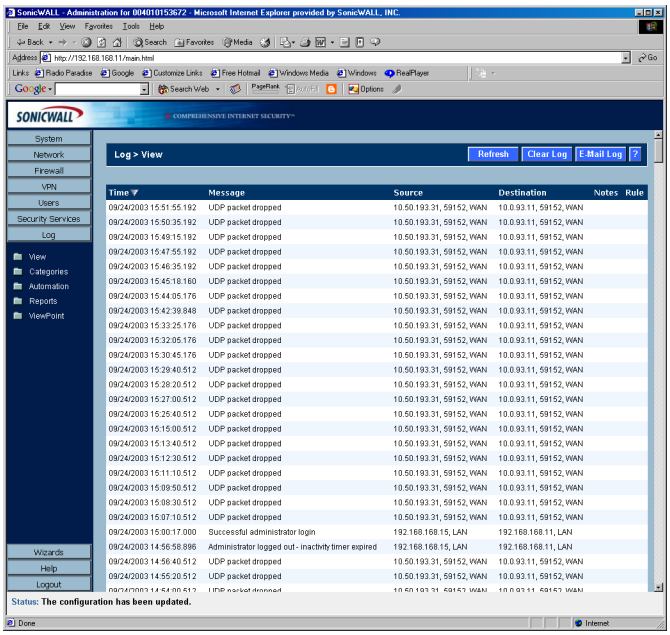
The SonicWALL Internet security appliance provides logging, alerting, and reporting features, which can be viewed in the **Log** section of the SonicWALL Web Management Interface.

## Log>View

The SonicWALL maintains an **Event** log which displays potential security threats. This log can be viewed with a browser using the SonicWALL Web Management Interface, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The SonicWALL can alert you of important events, such as an attack to the SonicWALL. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

Click **Log** on the left side of the browser window. The default view is **Log>View**.



## SonicWALL Log Messages

Each log entry contains the date and time of the event and a brief message describing the event. It is also possible to copy the log entries from the management interface and paste into a report.

- **Dropped TCP, UDP, or ICMP packets**

  When IP packets are blocked by the SonicWALL, dropped TCP, UDP and ICMP messages are displayed. The messages include the source and destination IP addresses of the packet. The TCP or UDP port number or the ICMP code follows the IP address. Log messages usually include the name of the service in quotation marks.

- **Blocked Web Sites**

  When a computer attempts to connect to the blocked site or newsgroup, a log event is displayed. The computer's IP address, Ethernet address, the name of the blocked Web site, and the **Content Filter List Code** is displayed. Code definitions for the 12 Content Filter List categories are displayed in the table below:

| | | |
|---|---|---|
| 1. Violence/Hate/Racism | 5. Weapons | 9. Illegal Skills/Questionable Skills |
| 2. Intimate Apparel/ Swimsuit | 6. Adult/Mature Content | 10. Sex Education |
| 3. Nudism | 7. Cult/Occult | 11. Gambling |
| 4. Pornography | 8. Drugs/Illegal Drugs | 12. Alcohol/Tobacco |

  Descriptions of the categories are available at <http://www.sonicwall.com/products/cfs.html>.

- **Blocked Java, etc**.

  When ActiveX, Java or Web cookies are blocked, messages with the source and destination IP addresses of the connection attempt is displayed.

- **Ping of Death, IP Spoof, and SYN Flood Attacks**

  The IP address of the machine under attack and the source of the attack is displayed. In most attacks, the source address shown is fake and does not reflect the real source of the attack.

***Tip!*** *Some network conditions can produce network traffic that appears to be an attack, even if no one is deliberately attacking the LAN. Verify the log messages with SonicWALL Tech Support before contacting your ISP to determine the source of the attack.*

### Clear Log

Clicking **Clear Log** deletes the contents of the log.

### E-mail Log

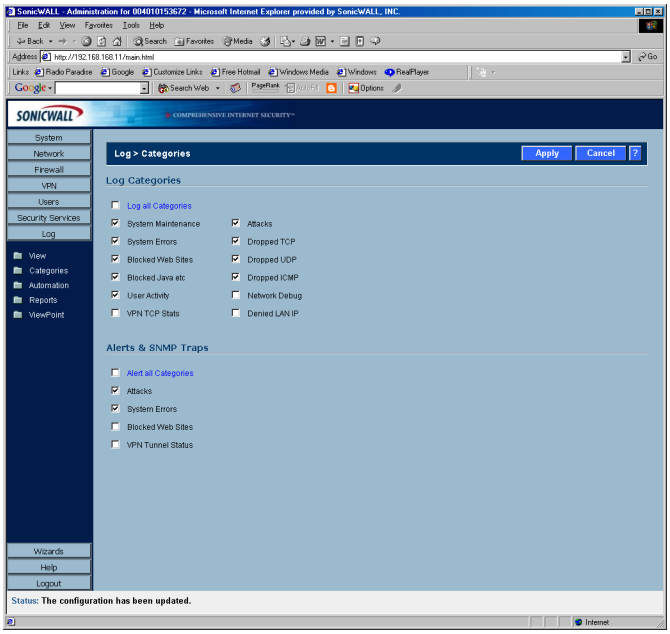
If you have configured the SonicWALL to e-mail log files, clicking **E-mail Log** sends the current log files to the e-mail address specified in the **Log>Automation>E-mail** section.

# Log>Categories

You can define which log messages appear in the SonicWALL **Event Log**.

## Log Categories

All **Log Categories** are enabled by default except **Network Debug**.




- **Log all Categories**
  Select **Log all Categories** to begin logging all event categories.
- **System Maintenance**
  Logs general system activity, such as system activations.
- **System Errors**
  Logs problems with DNS, or e-mail.
- **Blocked Web Sites**
  Logs Web sites or newsgroups blocked by the Content Filter List or by customized filtering.
- **Blocked Java, etc**.
  Logs Java, ActiveX, and Cookies blocked by the SonicWALL.
- **User Activity**
  Logs successful and unsuccessful log in attempts.
- **VPN TCP Stats**
  Logs TCP connections over VPN tunnels.
- **System Environment (PRO 3060)**
  Logs events about fan failure, overheating, and any hardware issues.
- **Attacks**
  Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing.
- **Dropped TCP**
  Logs blocked incoming TCP connections.

- **Dropped UDP**
  Logs blocked incoming UDP packets.
- **Dropped ICMP**
  Logs blocked incoming ICMP packets.
- **Network Debug**
  Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. **Network Debug** information is intended for experienced network administrators.
- **Denied LAN IP**
  Logs all LAN IP addresses denied by the SonicWALL.

## Alerts & SNMP Traps

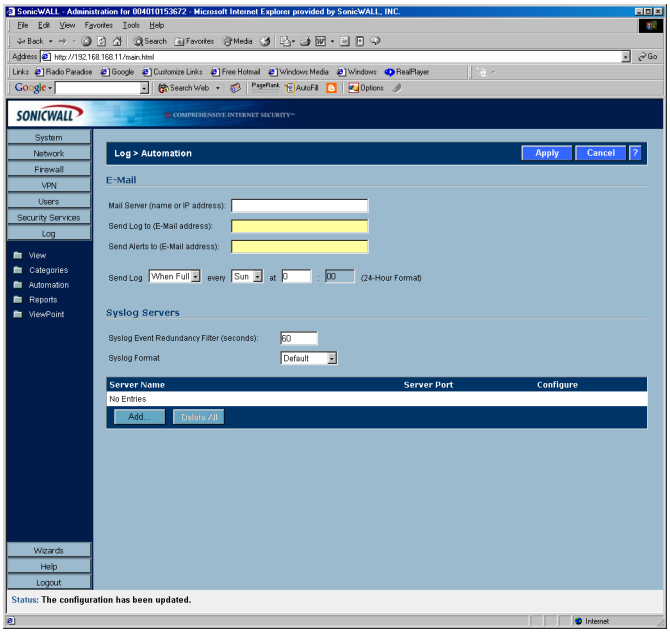
Alerts are events, such as attacks, which warrant immediate attention. When events generate alerts, messages are immediately sent to the e-mail address defined in the **Send alerts to** field. **Attacks** and **System Errors** are enabled by default, **Blocked Web Sites** and **VPN Tunnel Status** are disabled.

- **Alert all Categories**
  Select **Alert all Categories** to begin logging of all alert categories.
- **Attacks**
  Log entries categorized as **Attacks** generate alert messages.
- **System Errors**
  Log entries categorized as **System Errors** generate alert messages.
- **Blocked Web Sites**
  Log entries categorized as **Blocked Web Sites** generate alert messages.
- **VPN Tunnel Status**
  Log entries categorized as **VPN Tunnel Status** generate alert messages.
- **System Environment (PRO 3060)**
  Logs events about fan failure, overheating, and any hardware issues.

Once you have configured the **Log Categories** window, click **Apply**. Once the SonicWALL is updated, a message confirming the update is displayed at the bottom of the browser window.

# Log>Automation

Click **Log**, and then **Automation** to begin configuring the SonicWALL to send log files using e-mail and configuring syslog servers on your network.




## E-mail

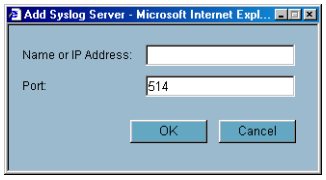
1. **Mail Server** - to e-mail log or alert messages, enter the name or IP address of your mail server in the **Mail Server** field. If this field is left blank, log and alert messages are not e-mailed.
2. **Send Log To** - enter your full e-mail address in the **Send log to** field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL memory. If this field is left blank, the log is not e-mailed.
3. **Send Alerts To** - enter your full e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Enter a standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.
4. **Send Log** / **Every** / **At** - The **Send Log** menu determines the frequency of log e-mail messages: **Daily**, **Weekly**, or **When Full**. If the **Weekly** or **Daily** option is selected, then select the day of the week the e-mail is sent in the **Every** menu. If the **Weekly** or the **Daily** option is selected, enter the time of day when the e-mail is sent in the **At** field.

## Syslog Servers

In addition to the standard event log, the SonicWALL can send a detailed log to an external Syslog server. The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL **Syslog** support requires an external server running a Syslog daemon on UDP Port 514.

Syslog Analysers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyse, and graph the **Syslog** data.

To add syslog servers to the SonicWALL, click **Add**. The **Add Syslog Server** window is displayed.




1. Enter the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL are then sent to the servers. Up to three Syslog Server IP addresses can be added.
2. If your syslog is not using the default port of 514, enter the port number in the **Port Number** field.
3. Click **OK**.

If the SonicWALL is managed by SGMS, however, the **Syslog Server** fields cannot be configured by the administrator of the SonicWALL.

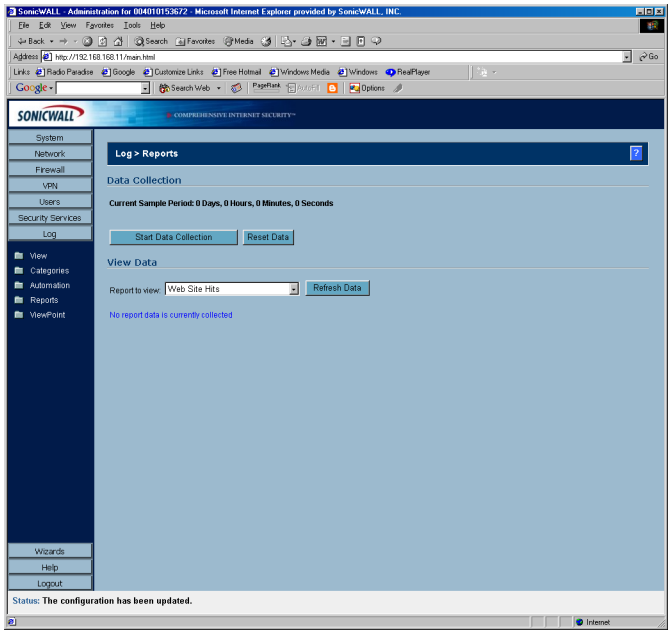
**Syslog Event Redundancy Filter (seconds)** - The **Syslog Event Redundancy Filter** setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred.

The **Syslog Event Redundancy Rate** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.

**Syslog Format** - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.

# Log>Reports

The SonicWALL can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. Click **Log** on the left side of the browser window, and then click the **Reports**.



## Data Collection

The **Reports** page includes the following functions and commands:

- **Start Data Collection**

  Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

- **Reset Data**

  Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the SonicWALL is restarted.

## View Data

Select the desired report from the **Report to view** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analysed by the report is displayed in the **Current Sample Period**.

### Web Site Hits

Selecting **Web Site Hits** from the **Report to view** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites.

### Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report to view** menu displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

### Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from the **Report to view** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

# Log>ViewPoint

## SonicWALL ViewPoint

SonicWALL ViewPoint is a software solution that creates dynamic, Web-based reports of network activity. ViewPoint generates both real-time and historical reports to provide a complete view of all activity through your SonicWALL Internet Security Appliance. With SonicWALL ViewPoint, you are able to monitor network access, enhance network security and anticipate future bandwidth needs.

- Displays bandwidth use by IP address and service.
- Identifies inappropriate Web use.
- Presents detailed reports of attacks.
- Collects and aggregates system and network errors.

***Tip!*** *You can try a FREE trial of ViewPoint. Go to the* ***Security Services>Summary*** *page to access the trial version of ViewPoint*

***Note:*** *For complete instructions on configuring and managing SonicWALL ViewPoint, see the SonicWALL ViewPoint User's Guide, available at www.sonicwall.com/services/ViewPoint_documentation.html.*

# 13 Appendices

## Appendix A - SonicWALL Support Solutions

SonicWALL's powerful security solutions give unprecedented protection from the risks of Internet attacks. SonicWALL's comprehensive support services protect your network security investment and offer the support you need - when you need it.

**Note:** For more information on SonicWALL Support Solutions, please visit <http://www.sonicwall.com/products/services/support.html>.

### Knowledge Base

All SonicWALL customers have immediate, 24X7 access to our state-of-the-art electronic support tools. Power searching technologies on our Web site allow customers to locate information quickly and easily from our robust collection of technical information - including manuals, product specifications, operating instructions, FAQs, Web pages, and known solutions to common customer questions and challenges.

### Internet Security Expertise

Technical Support is only as good as the people providing it to you. SonicWALL support professionals are Certified Internet Security Administrators with years of experience in networking and Internet security. They are also supported by the best in class tools and processes that ensure a quick and accurate solution to your problem.

### SonicWALL Support Programs

SonicWALL offers a variety of support programs designed to get the support you need when you need it. For more information on SonicWALL Support Services, please visit <http://www.sonicwall.com/products/supportservices.html.

### Warranty Support - North America and International

SonicWALL products are recognized as extremely reliable as well as easy to configure, install, and manage. SonicWALL Warranty Support enhances these features with

- 1 year, factory replacement for defective hardware
- 90 days of advisory support for installation and configuration assistance during local business hours
- 90 days of software and firmware updates
- Access to SonicWALL's electronic support and Knowledge Base system.

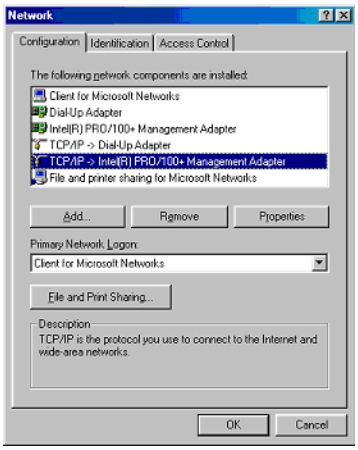
# Appendix B- Configuring the Management Station TCP/IP Settings

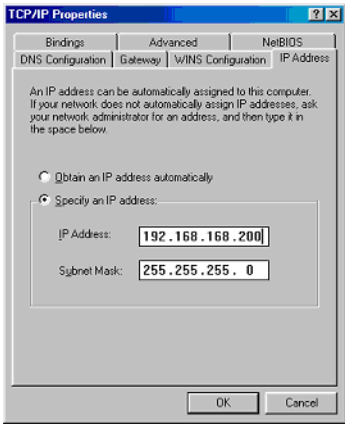
The following steps describe how to configure the Management Station TCP/IP settings in order to initially contact the SonicWALL. It is assumed that the Management Station can access the Internet through an existing connection.

The SonicWALL is pre-configured with the IP address 192.168.168.168. During the initial configuration, it is necessary to temporarily change the IP address of the Management Station to one in the same subnet as the SonicWALL. For initial configuration, set the IP address of the Management Station to 192.168.168.200.

Make a note of the Management Station's current TCP/IP settings. If the Management Station accesses the Internet through an existing broadband connection, then the TCP/IP settings can be helpful when configuring the IP settings of the SonicWALL.

## Windows 98




1.From the **Start** list, highlight **Settings** and then select **Control Panel**.Double-click the **Network** icon in the **Control Panel** window.

2.Double-click **TCP/IP** in the **TCP/IP Properties** window.

3.Select **Specify an IP Address**.

4.Type "192.168.168.200" in the **IP Address** field.

5.Type "255.255.255.0" in the **Subnet Mask** field.

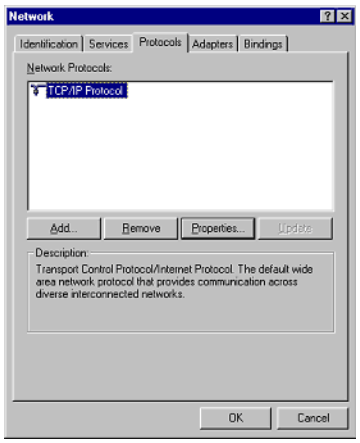
6.Click **DNS Configuration**.

7.Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, type the second one in the **Alternate DNS server** field.

8.Click **OK**, and then click **OK** again.

9.Restart the computer for changes to take effect.

## Windows NT

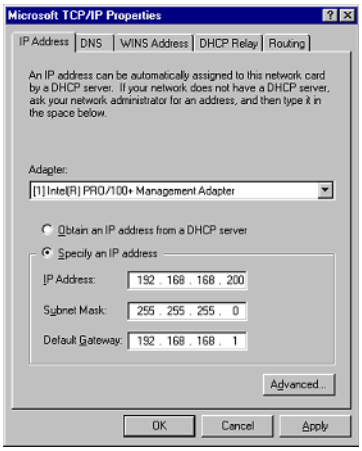



1.From the **Start** list, highlight **Settings** and then select **Control Panel**.

2.Double-click the **Network** icon in the **Control Panel** window.

3.Double-click **TCP/IP** in the **TCP/IP Properties** window.

4.Select **Specify an IP Address**.




5.Type "192.168.168.200" in the **IP Address** field.

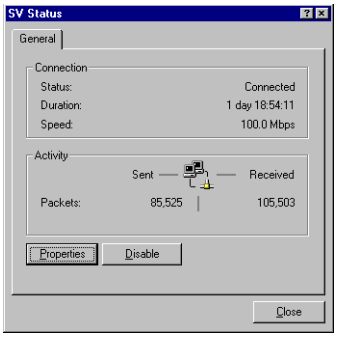
6.Type "255.255.255.0" in the **Subnet Mask** field.

7.Click **DNS** at the top of the window.

8.Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, enter the second one in the **Alternate DNS server** field.

9.Click **OK**, and then click **OK** again.

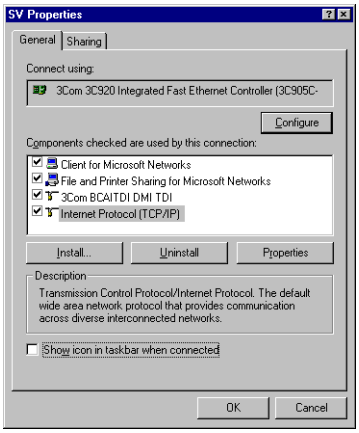
# Windows 2000



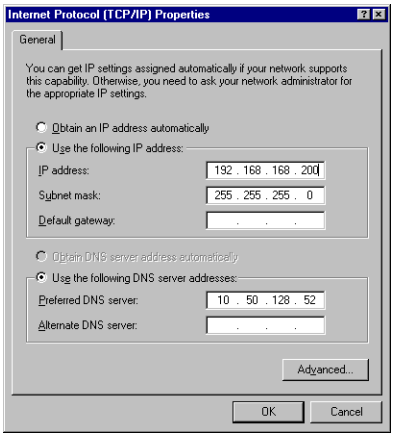

1.In Windows 2000, click **Start**, then **Settings**.

2.Click **Network and Dial-up Connections**. Double-click the network connection name to open the **Status** window.

3.Click **Status** to open the **Properties** window.




4.Double-click **Internet Protocol (TCP/IP)** to open the **TCP/IP properties** window.




5.Select **Use the following IP** address and enter 192.168.168.200 in the **IP address** field.

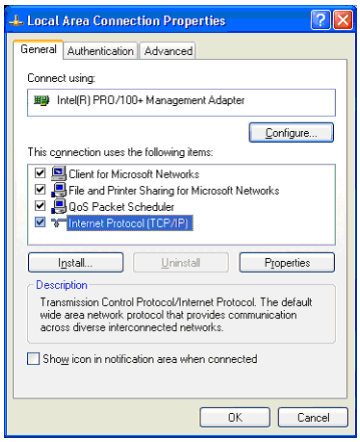
6.Type 255.255.255.0 in the Subnet mask field.

7.Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, enter the second one in the **Alternate DNS server** field.

8.Click **OK**, then **OK** again.

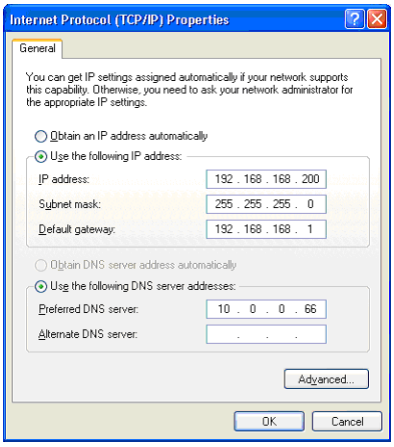
9.Click **Close** to finish the network configuration.

## Windows XP




1.Open the **Local Area Connection Properties** window.

2.Double-click **Internet Protocol (TCP/IP)** to open the **Internet Protocol (TCP/IP) Properties** window.




3.Select **Use the following IP address** and type 192.168.168.200 in the **IP address** field.

4.Type 255.255.255.0 in the **Subnet Mask** field.

5.Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, type the second one in the **Alternate DNS server** field.

6.Click **OK** for the settings to take effect on the computer.

## Macintosh OS 10

From a Macintosh computer, do the following:

1. From the Apple list, choose **Control Panel**, and then choose **TCP/IP** to open the **TCP/IP Control Panel**.
2. From the **Configure** list, choose **Manually**.
3. Type "192.168.168.200" in the **IP address** field.
4. Type the Subnet Mask address in the **Subnet Mask** field.
5. Click **OK**.Follow the SonicWALL Installation Wizard instructions to perform the initial setup of the SonicWALL.

# Index

**W**

**SonicWALL,Inc.**
1143 Borregas Avenue
Sunnyvale,CA 94089-1306

T: 408.745.9600
F: 408.745.9300

www.sonicwall.com



P/ N 232-000497-01
Rev A 04/ 04