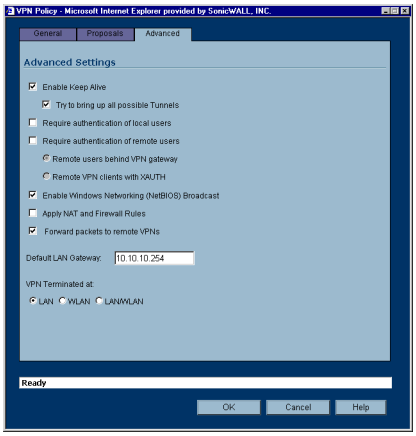
11. Click **OK** to close the window, and then click **Apply** for the settings to take effect on the SonicWALL.

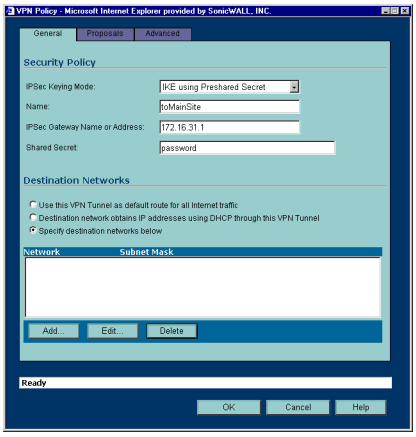


Wireless Bridge VPN Policy

The Wireless Bridge VPN Policy is configured as follows:

1. Click **VPN**, then **Configure**.
2. Select **IKE using Preshared Secret** from the **IPSec Keying Mode** menu.
3. Enter a name for the SA in the **Name** field.
4. Type the IP address of the Access Point in the **IPSec Gateway** field. In our example network, the IP address is 172.16.31.1.
5. Select **Use this VPN Tunnel as default route for all Internet traffic** from the **Destination Networks** section.

Click **OK** to close the window, and then click **Apply** for the settings to take effect on the SonicWALL.



Wireless > WEP Encryption

WEP (Wired Equivalent Protocol) can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWALL. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

WiFiSec should be enabled in addition to WEP for added security on the wireless network.

WEP Encryption Settings

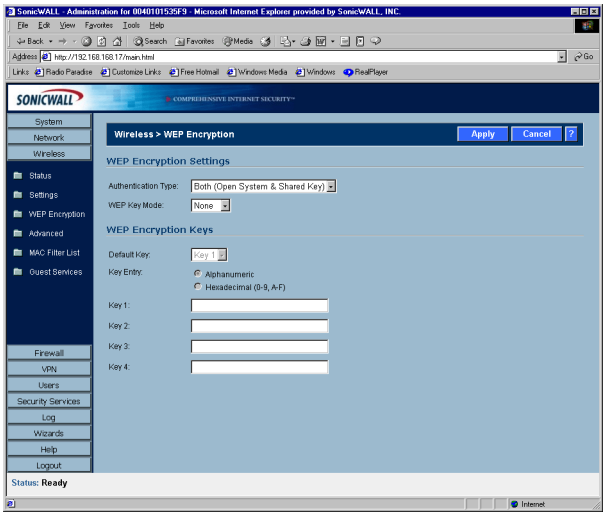
Open-system authentication is the only method required by 802.11b. In open-system authentication, the SonicWALL allows the wireless client access without verifying its identity.

Shared-key authentication uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.

The TZ 170 Wireless provides the option of using **Open System**, **Shared Key**, or both when WEP is used to encrypt data.

If **Both Open System & Shared Key** is selected, the **Default Key** assignments are not important as long as the identical keys are used each field. If **Shared Key** is selected, then the key assignment is important.

To configure WEP on the SonicWALL, log into the SonicWALL and click **Wireless**, then **WEP Encryption**.



1. Select the authentication type from the **Authentication Type** list. **Both (Open System & Shared Key)** is selected by default.
2. Select 64-bit or 128-bit from the **WEP Key Mode**. 128-bit is considered more secure than 64-bit. This value is applied to all keys.

WEP Encryption Keys

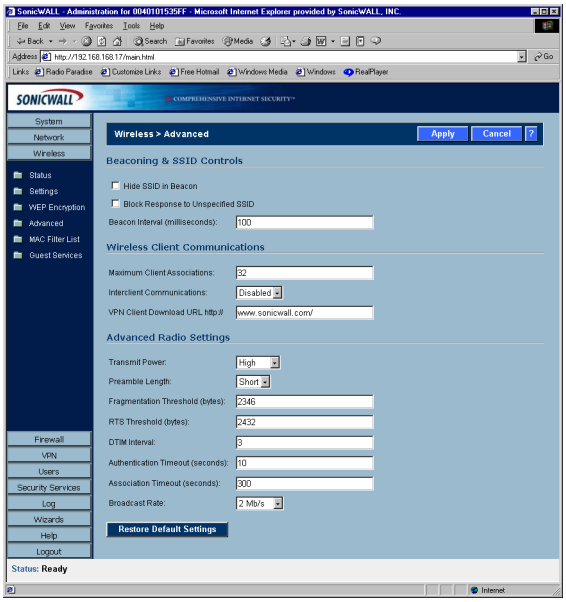
3. Select the key number, 1,2,3, or 4, from the **Default Key** menu.
4. Select the key type to be either **Alphanumeric** or **Hexadecimal**.

WEP - 64-bit	WEP - 128-bit
Alphanumeric - 5 characters (0-9, A-Z)	Alphanumeric - 13 characters (0-9, A-Z)
Hexadecimal - 10 characters (0-9, A-F)	Hexadecimal - 26 characters (0-9, A-F)

5. Type your keys into each field.
6. Click **Apply**.

Wireless>Advanced

To access Advanced configuration settings for the TZ 170 Wireless, log into the SonicWALL, click **Wireless**, and then **Advanced**.



Beaconing & SSID Controls

1. Select **Hide SSID in Beacon**. If you select **Hide SSID in Beacon**, your wireless network is invisible to anyone who does not know your SSID. This is a good way to prevent “drive by hackers” from seeing your wireless connection.
2. Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.

Wireless Client Communications

1. Enter the number of clients to associate with the TZ 170 Wireless in the **Maximum Client Associations** field. The default value is **32** which means 32 users can access the WLAN at the same time. However, an unlimited number of wireless clients can access the WLAN because node licensing does not apply to the WLAN.
2. If you do not want wireless clients communicating to each other, select **Disabled** from the **Interclient Communications** menu. If you want wireless clients communicating with each other, select **Enabled**. Enabling and disabling Interclient communications changes the associated network access rule on the **Firewall > Access Rules** page.
3. Guests on the wireless network can download the SonicWALL Global VPN Client to install on their computer or laptop. Type the URL location for the software in the **VPN Client Download URL http:// /** field. This field can contain up to 128 characters.

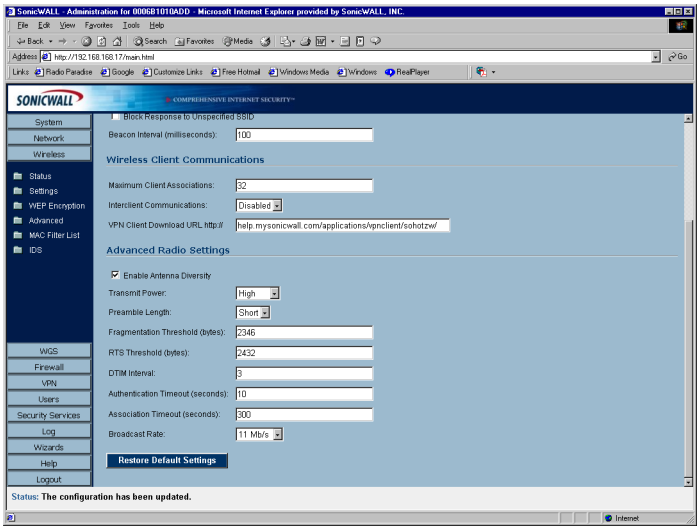
Advanced Radio Settings

Configurable Antenna Diversity

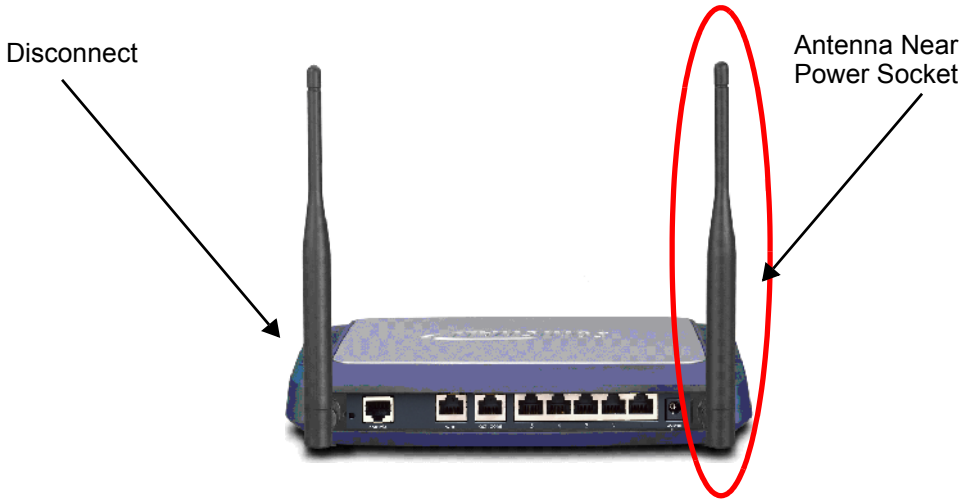
The TZ 170 Wireless employs dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential

receive antenna. As radio signals arrive at both antennas on the TZ 170 Wireless, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal.

To allow for external (e.g. higher gain uni-directional) antennas to be used, antenna diversity can now be disabled from the **Wireless > Advanced > Advanced Radio Settings** section.



Clearing the **Enable Antenna Diversity** checkbox presents a pop-up message indicating that only the antenna nearest the power-socket is active when antenna diversity is disabled. The antenna nearest the serial connector **must be disconnected** when antenna diversity is disabled. The optional antenna should then be connected to the RP-TNC type connector near the power-socket. This antenna is not used exclusively for transmitting and receiving.



Select **High** from the **Transmit Power** menu to send the strongest signal on the WLAN. For example, select **High** if the signal is going from building to building. **Medium** is recommended for office to office within a building, and **Low** or **Lowest** is recommended for shorter distance communications.

4. Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.

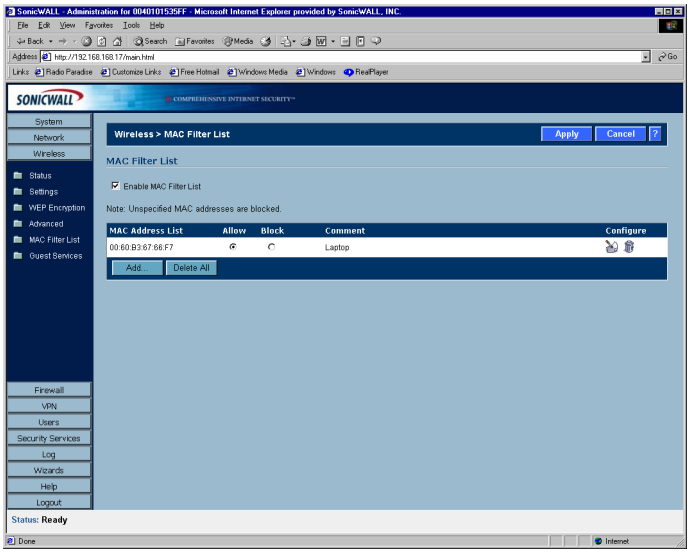
5. The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
6. The **RTS Threshold (bytes)** is 2432 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
7. The default value for the **DTIM Interval** is 3. Increasing the DTIM Interval value allows you to conserve power more effectively.
8. The **Association Timeout (seconds)** is 300 seconds by default. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Authentication Timeout (seconds)** field.

Click **Restore Default Settings** to return the radio settings to the default settings.

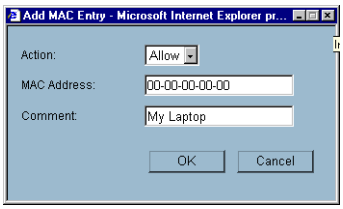
Wireless>MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the TZ 170 Wireless. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card. Unless you enable **Easy WGS MAC Filtering** as a privilege when you configure a User account in **Users > Settings**.

To set up your MAC Filter List, log into the SonicWALL, and click **Wireless**, then **MAC Filter List**.



1. Click **Add** to add a MAC address to the **MAC Filter List**.



2. Select **Allow** from the **Action** menu to allow access to the WLAN. To deny access, select Block.
3. Type the MAC address in the **MAC Address** field. The two character groups should be separated by a hyphen.
4. Type a name or comment in the **Comment** field. The **Comment** field can be used to identify the source of the MAC address.
5. Click **OK** to add the MAC address.

Once the MAC address is added to the **MAC Address List**, you can select **Allow** or **Block** next to the entry. For example, if the user with the wireless card is not always in the office, you can select **Block** to deny access during the times the user is offsite.

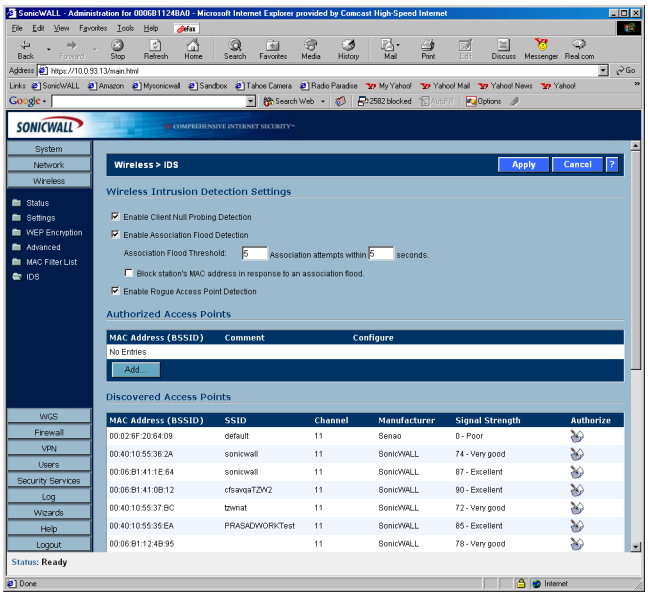
Click on the Notepad icon under **Configure** to edit the entry. Click on the Trashcan icon to delete the entry. To delete all entries, click **Delete All**.

Wireless Intrusion Detection Services

Wireless Intrusion Detection Services (WIDS) greatly increase the security capabilities of the TZ 170 Wireless by enabling it to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. WIDS logging and notification can be enabled under **Log > Categories** by selecting the **WIDS** checkbox under **Log Categories** and **Alerts**.

Wireless Bridge IDS

When the **Radio Role** of the TZ 170 Wireless is set to a Wireless Bridge mode, Rogue Access Point Detection defaults to active mode (actively scanning for other Access Points using probes on all channels).



Access Point IDS

When the **Radio Role** of the TZ 170 Wireless is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the TZ 170 Wireless to perform an active scan, and may cause a brief loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Enable Client Null Probing

The control to block Null probes is not available on the 802.11g card built into the TZ170. Instead, enabling this setting allows the TZ 170 Wireless to detect and log Null Probes, such as those used by Netstumbler and other similar tools.

Sequence Number Analysis

Sequence Number Analysis is an advanced method of wireless intrusion detection enabling the TZ 170 Wireless to recognize malicious wireless client activity designed to gain unauthorized access by means of disassociation attacks and MAC address spoofing. A disassociation attack is a method used to gain unauthorized access to a wireless network by sending an authorized and associated wireless client a disassociation message, causing it to momentarily drop from the network, and then assuming that client's identify via MAC spoofing.

Enable Sequence Number Analysis is selected by default.

Association Flood Detection

Association Flood is a type of Wireless Denial of Service attack intended to interrupt wireless services by depleting the resources of a wireless Access Point. An attacker can employ a variety of tools to establish associations, and consequently association IDs, with an access point until it reaches its association limit (generally set to 255). Once association saturation occurs, the access point discards further association attempts until existing associations are terminated.

Association Flood Detection allows thresholds to be set limiting the number of association attempts a client makes in a given span of time before its activities are considered hostile. Association attempts default to a value of 5 (minimum value is 1, maximum value is 100) within and the time period defaults to a value of 5 seconds (minimum value is 1 second, maximum value is 999 seconds). If association attempts exceed the set thresholds, an event is logged according to log settings.

If the **Block station's MAC address in response to an association flood** option is selected and MAC Filtering is enabled, then in addition to logging actions, the TZ 170 Wireless takes the countermeasure of dynamically adding the MAC address to the MAC filter list. Any future Denial of Service attempts by the attacker are then blocked.

Enable Association Flood Detection is selected by default. The **Association Flood Threshold** is set to **5 Association attempts within 5 seconds** by default.

Rogue Access Point Detection

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The TZ 170 Wireless can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11b channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Active scanning occurs when the TZ 170 Wireless starts up, and at any time **Scan Now** is clicked on the **Wireless > IDS** page. When the TZ 170 Wireless is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the TZ 170 Wireless is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

Alert! *If service disruption is a concern, it is recommended that the **Scan Now** feature not be used while the TZ 170 Wireless is in Access Point mode until such a time that no clients are active, or the potential for disruption becomes acceptable.*

Authorizing Access Points on Your Network

Access Points detected by the TZ 170 Wireless are regarded as rogues until they are identified to the TZ 170 Wireless as authorized for operation. To authorize an access point, it can be manually added to the **Authorized Access Points** list by clicking **Add** and specifying its MAC address (BSSID) along with an optional comment. Alternatively, if an access point is discovered by the TZ 170 Wireless scanning feature, it can be added to the list by clicking the **Authorize** icon.

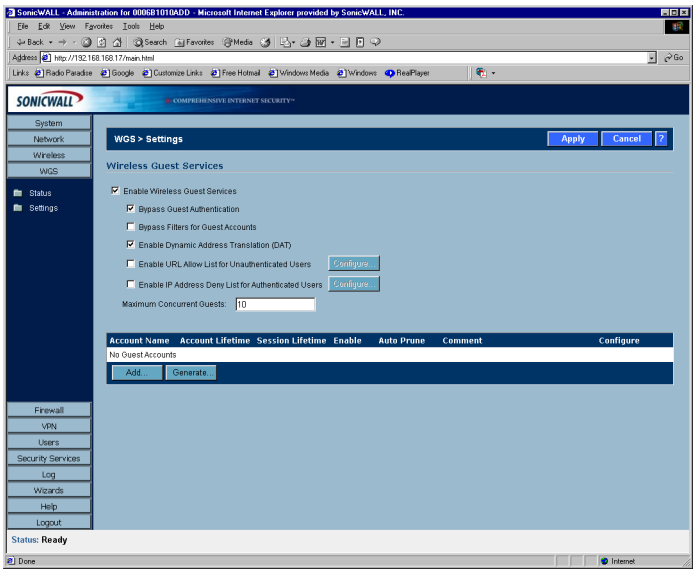
6 Wireless Guest Services

Wireless Guest Services allow you to manage wireless users's access to your network. **Wireless Guest Services** are located under the **WGS** button in the left navigation pane. These include the following:

- **Dynamic Address Translation**
- **Bypass Guest Authentication**
- **URL Allow List**
- **IP Address Deny List**
- **Wireless Guest Services login uniqueness**
- **Account lifetimes and auto-pruning**
- **Automated account generation**
- **Account detail printing**

WGS > Status

The **WGS > Status** page displays the **Active Wireless Guest Sessions**. The table lists the **Account Name**, **MAC Address**, **IP Address**, **Time Remaining**, and **Comment**. The last column, **Configure**, allows you to make changes to the guest account when you click the **Configure** icon next to the account. Wireless Guest Services allow you to create access accounts for temporary use that allow wireless clients to connect from the WLAN to the WAN. To configure Wireless Guest Services, log into the SonicWALL, and click **WGS.**



If Wireless Guest Services are not enabled, Click the link in the Status page to enable the services.

Wireless Guest Services

Select **Enable Wireless Guest Services** to allow configured guest accounts access to the TZ 170 Wireless.

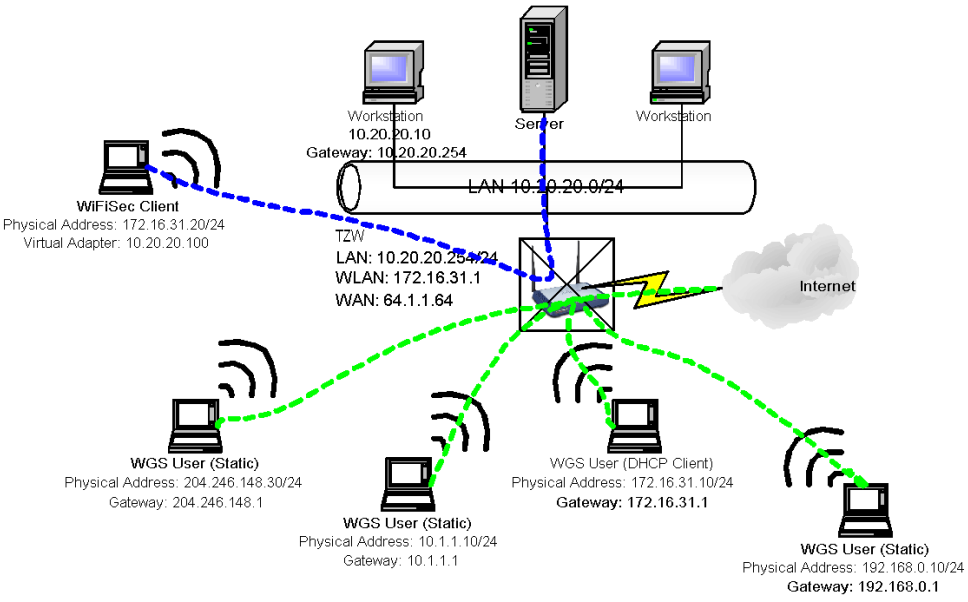
Bypass Guest Authentication

Bypass Guest Authentication feature is designed to allow a TZ 170 Wireless running WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another device upstream of the TZ 170 Wireless is enforcing authentication.

Dynamic Address Translation (DAT)

One of the TZ 170 Wireless key features is Wireless Guest Services (WGS), which provides spur of the moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, WGS allows wireless users to authenticate and associate, obtain IP settings from the TZ 170 Wireless DHCP services, and authenticate using any web-browser. Without DAT, if a WGS user is not a DHCP client, but instead has static IP settings incompatible with the TZ 170 Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values.

Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the TZ 170 Wireless to support any IP addressing scheme for WGS users. For example, the TZ 170 Wireless WLAN interface is configured with its default address of 172.16.31.1, and one WGS client has a static IP Address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.

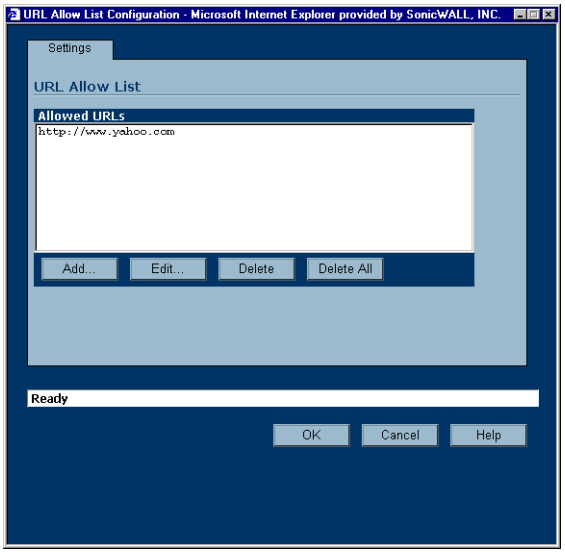


To disable a Guest Account, clear the **Enable** check box in the Guest Account entry line. To edit an existing Guest Account, click on the Notepad icon under **Configure.** To delete a Guest Account, click the Trashcan icon under **Configure**. To delete all Guest Accounts, click **Delete All**.

URL Allow List

Enable URL Allow List for Unauthenticated Users, when selected, allows for the creation of a list of URLs (HTTP and HTTPS only) that WGS users can visit even before they authenticate. This feature could be used, for example, to allow users to reach advertising pages, disclaimer pages, search engines, etc. Entries should be made in URL format, and can be in either Fully Qualified Domain Name (FQDN) or IP address syntax.

1. Select **Enable URL Allow List for Unauthenticated Users**.
2. Click **Configure** to display the **URL Allow List Configuration** window.



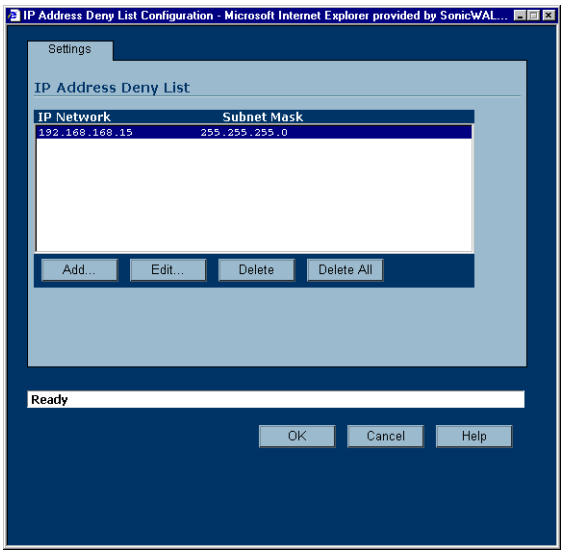
3. Click **Add** to display the **Add URL** dialogue box.
4. Enter the URL in http or https format or domain name. For instance, http://www.yahoo.com or yahoo.com. Click **OK**, then **OK** again.

Tip! *Up to 32 entries consisting of 128 characters each can be added to the TZ 170 Wireless.*

IP Deny List

When **IP Address Deny List for authenticated users** is selected, allows for the specification of IP addresses/subnet masks to which WGS users are explicitly denied access. Individual hosts can be entered by using a 32 bit subnet mask (255.255.255.255), networks can be entered with appropriate subnet mask, or network ranges can be aggregated using CIDR notation or supernetting (e.g. entering 192.168.0.0/255.255.240.0 to cover individual class C networks 192.168.0.0/24 through 192.168.15.0/24).

1. Select **Enable IP Address Deny List for Authenticated Users**.
2. Click **Configure**.



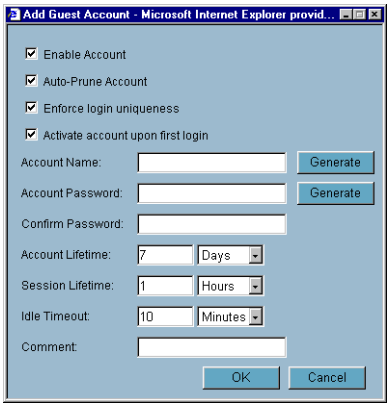
3. Click **Add** to display the **Add IP Address Deny List Entry** window.
4. Type the IP Address in the **IP Network** field. Type the subnet mask in the **Subnet Mask** field.
5. Click **OK**. Then click **OK** again.

The IP address or network range is added to the list.

Tip! *Up to 32 entries consisting of 128 characters each can be added to the TZ 170 Wireless.*

Configuring Wireless Guests

To configure new wireless guest accounts, click **Add**. The **Add Guest Account** window is displayed.



By default, the following settings are selected:

Enable Account

When selected, the wireless guest account is automatically enabled. You can clear the checkbox to disable the account until necessary.

Auto-Prune Account

By default, newly created accounts are set to **Auto-Prune**, automatically deleted when expired. If **Auto-Prune** is cleared, the account remains in the list of WGS accounts with an **Expired** status, allowing it to be easily reactivated.

WGS Login Uniqueness

By enforcing login uniqueness, the TZ 170 Wireless allows only a single instance of a WGS account to be used at any one time. By default, this feature is enabled when creating a new WGS account. If you want to allow multiple users to login with a single account, this enforcement is disabled by clearing the **Enforce login uniqueness** checkbox.

Activate Account Upon First Login

By default, the Activate Account Upon First Login is enabled on the TZ 170 Wireless. The WGS account remains inactive until the user logs in and activates the account.

Automated Account Generation

The task of generating a new WGS account is now easier with the introduction of an automated account generation function with the ability to generate (or re-generate) account name and account password information. Clicking **Generate** in the **WGS > Settings** page creates a fully populated WGS account dialog box. Alternatively, add an account by clicking **Add**, and manually entering account name and password information. Or click the separate **Generate** buttons for account name and account password within this window.

Account Lifetime

This setting defines how long an account remains on the TZ 170 Wireless before the account expires. If **Auto-Prune** is enabled, the account is deleted by the SonicWALL. If the **Auto-Prune** checkbox is cleared, the account remains in the list of WGS accounts with an **Expired** status, allowing easy reactivation.

Session Lifetime

Defines how long a WGS session remains active after it has been activated. By default, activation occurs the first time a WGS user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.

Idle Timeout

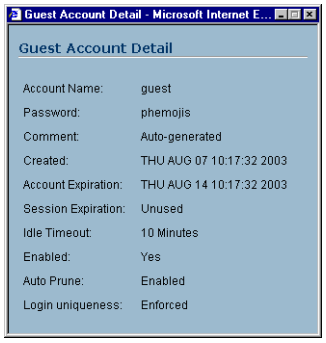
Defines the maximum period of time when no traffic is passed on an activated WGS session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.

Comment

Any text can be entered as a comment in the **Comment** field.

Account Detail Printing

Following the generation of an account, it is possible to click the **Print** icon on the **WGS > Settings** page to send the pertinent account details to the active printer on the administrative workstation for easy distribution to WGS users. Clicking the **Print** icon launches the following window, followed by the administrative workstation's system print dialog.



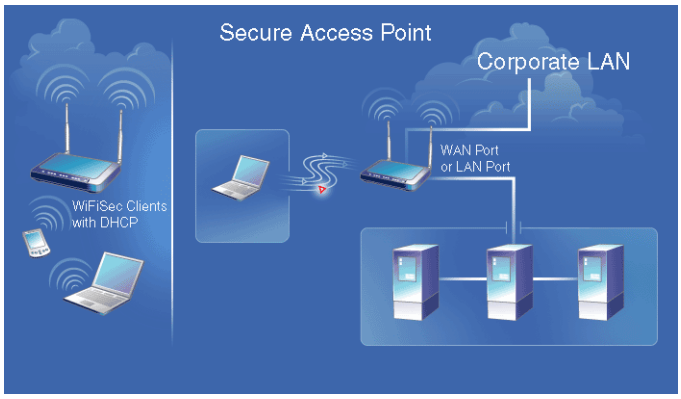
Flexible Default Route

Previously, network traffic from the LAN and WLAN was directed to the WAN interface. With the release of SonicOS Standard, the Default Route can be the WAN, LAN, or WLAN allowing flexible configuration of the TZ 170 Wireless, primarily wireless bridging without WiFiSec and Secure Access Point with Virtual Adapter support.

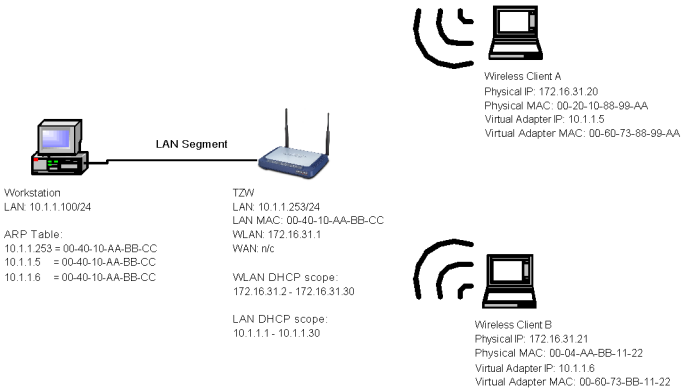
Secure Access Point with Virtual Adapter Support

Secure Access Point deployment previously required the corporate LAN to be connected to the TZ 170 Wireless WAN port, because the default route could only be specified on the TZ 170 Wireless WAN interface. However, the TZ 170 Wireless could not support Wireless Guest Services and SonicWALL Global VPN Clients simultaneously preventing corporate LAN clients from communicating with WLAN

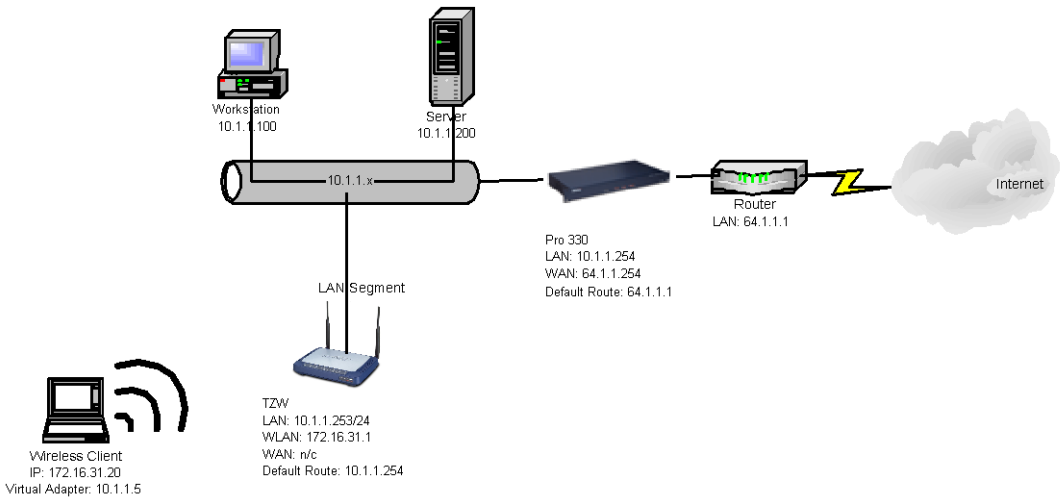
clients, inhibiting crucial functions such as wireless print servers, Microsoft Outlook mail notification, or any other function requiring LAN initiated communications to WLAN clients.



Any LAN clients attempting to resolve an IP address of a Global VPN Virtual Adapter address receives a response from the TZ 170 Wireless LAN.



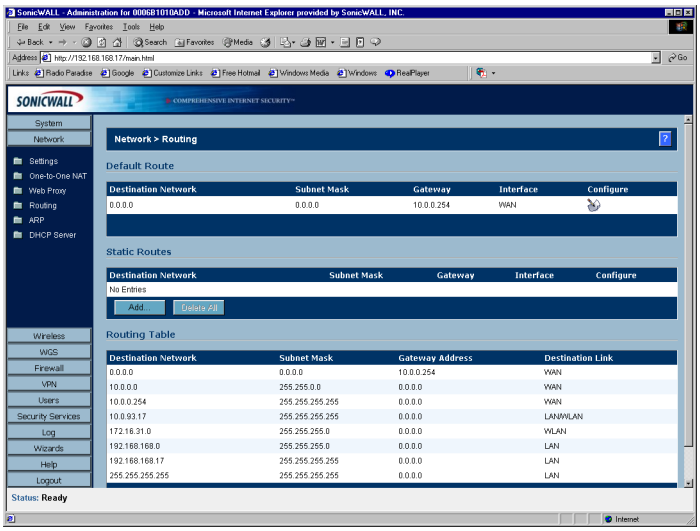
This allows any client on the LAN to communicate directly with WLAN client via the secure WiFiSec link, enabling configurations like the one below.



The above example shows a network configuration with the addition of a TZ 170 Wireless (as a Secure Access Point). The TZ 170 Wireless points to the upstream SonicWALL PRO 330 at 10.1.1.254. Security Services, such as Content Filtering Service and Anti-Virus, are hosted centrally on the PRO 330. In the

example above, PRO 330 does not require a route to the 172.16.31.X as long as the Virtual Adapter is used by all clients.

To configure routing on the TZ 170 Wireless to support the above example, click **Network** and then **Routing**.

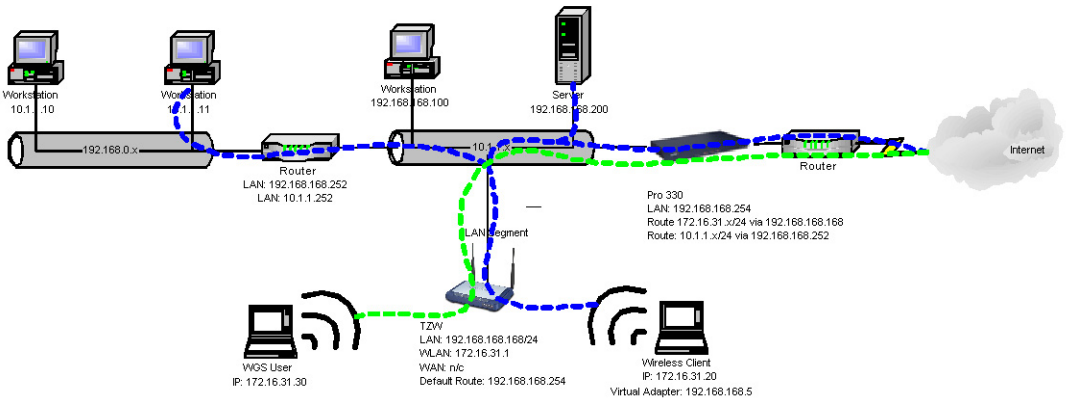


1. Under **Default Route**, click **Configure**. The **Edit Default Route** window is displayed.
2. Enter the IP address in the **Default Gateway** field, and then select **LAN**, **WAN**, or **WLAN** from the **Interface** menu.

Click **OK**. The default gateway is now configured.

Secure Access Point with Wireless Guest Services

If simultaneous Wireless Guest Services support is a requirement, then access to the 172.16.31.x network is necessary. The following diagram portrays such a configuration, and also allows for an introduction to one of the WGS enhancements of SonicOS 2.0, explicit WGS allow and deny lists.



The example above describes a moderately complex network configuration where the TZ 170 Wireless offers both WiFiSec and WGS access via a default route on LAN. As the blue (WiFiSec) and green (WGS) traffic lines indicate, the TZ 170 Wireless allows WGS access only to the Internet, while allowing WiFiSec access to the Internet, the LAN, and to a remote network connected via a LAN router. The Pro 330 in above example requires static routes to the 10.1.1.x (adjacent) network via 192.168.168.252, and to the 172.16.31.x (for WGS) network via 192.168.168.168.

Prior to SonicOS 1.5.0.0, Wireless Guest Services were only available in default route on WAN configurations. This scheme provided an automatic differentiation of destinations for WGS traffic. In other words, WGS traffic bound for the WAN was permitted, but WGS traffic attempting to reach the LAN (local traffic), to cross the LAN (to reach an adjacent network connected via a router) or to cross a VPN tunnel was dropped.

When the TZ 170 Wireless is configured to provide both Secure Access Point and WGS services via a default route on LAN, all traffic exits the LAN interface, eliminating any means of automatically classifying “WGS permissible” traffic. To address this ambiguity, any traffic sourced from a WGS client attempting to reach the default gateway (in our above example, 192.168.168.254) is allowed, but any traffic attempting to traverse a VPN, or reach a LAN resource (for example, 192.168.168.100) is dropped. Finally, to safeguard adjacent networks attached via a router, a WGS **IP Address Deny List** has been added to the **WGS > Settings** page.

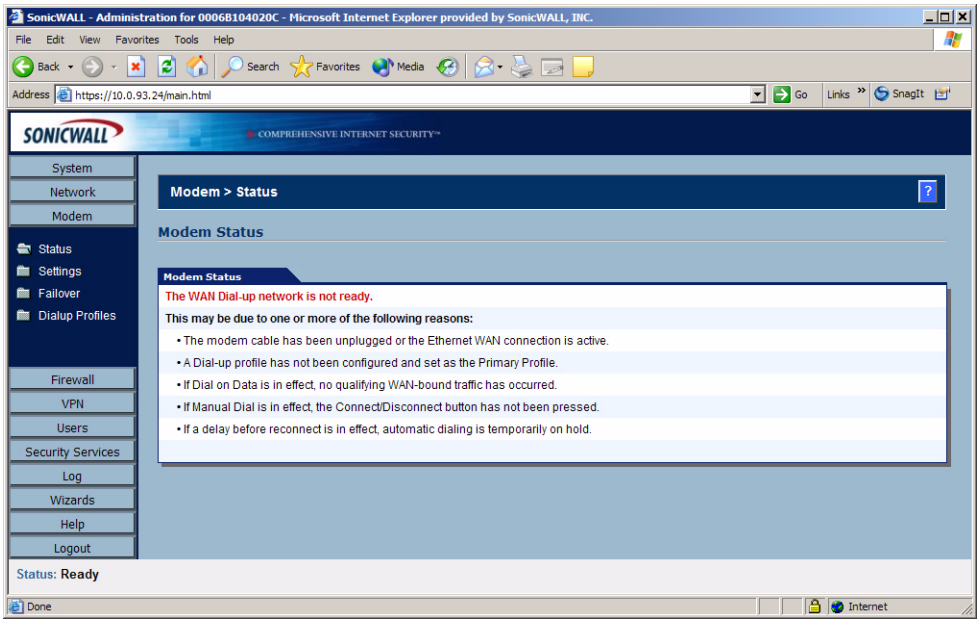
7 Modem

The SonicWALL TZ 170 SP contains a built in modem. You can use the modem as:

- A backup connection for the WAN connection. See **Modem > Failover**.
- The only internet connection for the TZ 170 SP. See **Modem > Settings**

Modem > Status

The Status page displays dialup connection information when the modem is active. You create modem dialup profiles in the Modem Profile Configuration window, which you access from the Modem>Dialup Profiles page.



Modem Status

In the **Modem Status** section, the current active network information from your ISP is displayed when the modem is active:

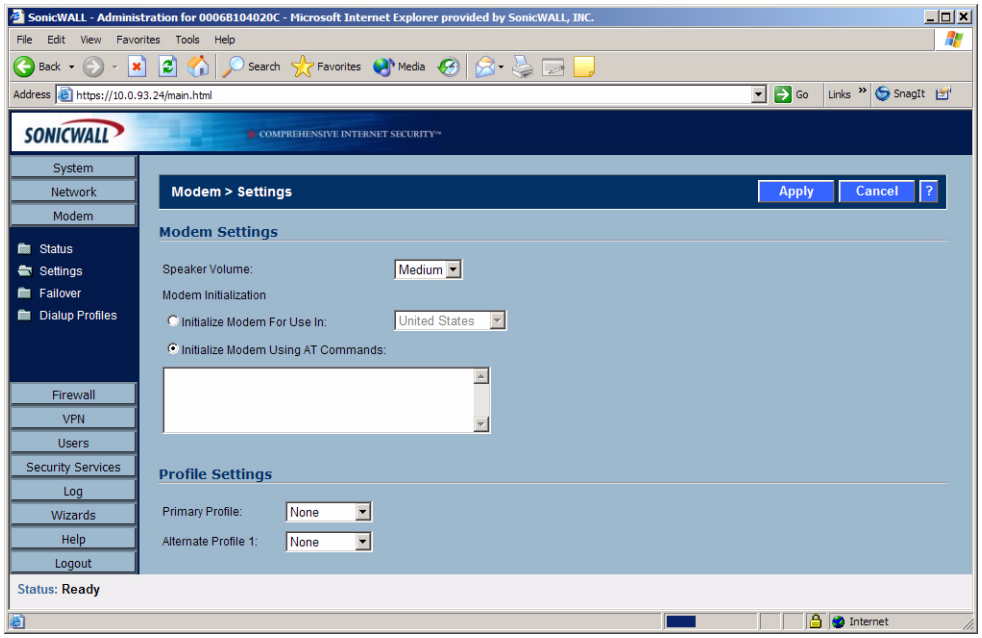
- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**
- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive.

When the modem is active, the network settings from the ISP are used for WAN access. If you select **Modem > Settings**, a message is displayed reminding you that the modem is active and the current network settings are displayed on the **Modem > Status** page.

Modem > Settings

The **Modem > Settings** page lets you select from a list of modem profiles, select the volume of the modem, and also configure AT commands for modem initialization.



Configuring Profile and Modem Settings

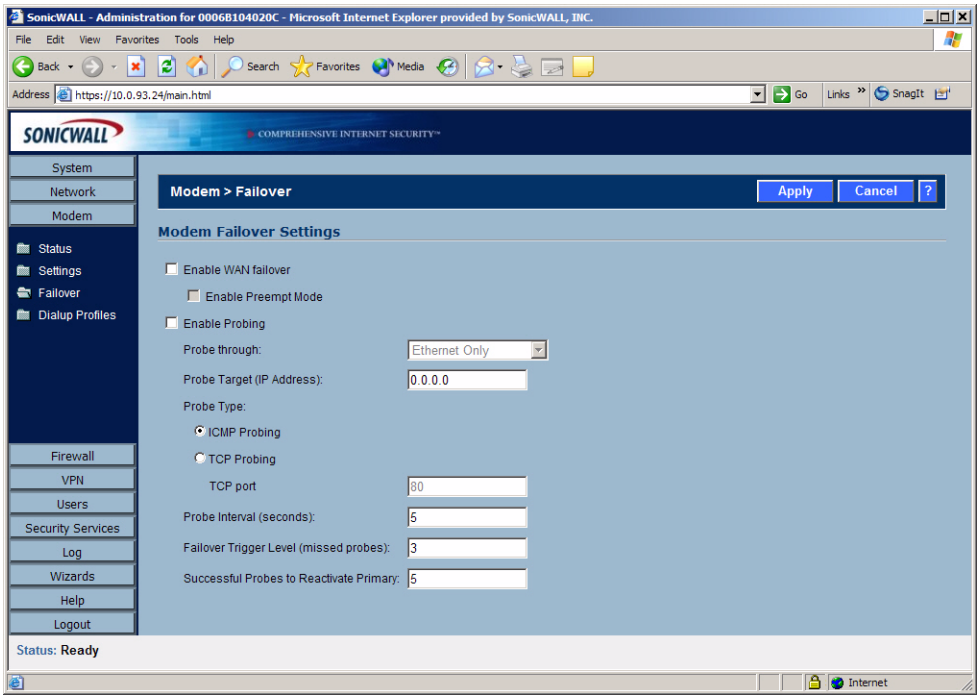
To configure the SonicWALL modem settings, follow these steps:

1. Select the profile you want to use for the primary profile from the **Primary Profile** menu that the SonicWALL uses to access the modem. If you have enabled **Manual Dial** for the **Primary Profile**, the **Alternate Profile 1** is not used.
2. Select the secondary profile from the **Alternate Profile 1** menu. If the **Primary Profile** cannot establish a connection, the SonicWALL uses the **Alternate Profile 1** profile to access the modem and establish a connection.
3. Select the volume of the modem from the **Speaker Volume** menu. The default value is **Medium**.
4. Select **Initialize Modem For Use In** and select the country from the drop down menu. **United States** is selected by default.
5. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands (for modem initialization)** field. AT commands are instructions used to control a modem such as ATS7=30 (allow up to 30 seconds to wait for dialtone), ATS8=2 (set the amount of time the modem pauses when it encounters a "," in the string).

Tip! *The default settings for the modem are generally sufficient for normal operation. The AT Commands (for modem initialization) box is provided for nonstandard situations.*

Modem > Failover

To improve the operational availability of networks and ensure fast recovery from network failures, the **Modem > Failover** page allows you to configure the SonicWALL modem for use as a secondary WAN port. The secondary WAN port can be used in a simple "active/passive" setup to allow traffic to be only routed through the secondary WAN port if the primary WAN port is unavailable. This allows the SonicWALL to maintain a persistent connection for WAN port traffic by "failing over" to the secondary WAN port.



Alert! *Using the WAN failover feature may cause disruption of some features such as One-to-One NAT. See the SonicWALL Administrator's Guide for affected features.*

After configuring your computer on the LAN, you can configure the SonicWALL modem connection for ISP failover or as a primary dial-up access port.

Alert! *You cannot use the WAN failover feature if you have configured the SonicWALL to use Transparent Mode in the* ***Network>Settings*** *page.*

Modem Failover Settings

When you select **Enable WAN Failover**, the SonicWALL modem is used as a failover option when your "always on" DSL or cable connection fails. The SonicWALL automatically detects the failure of the WAN connection and uses the parameters configured for the modem in the Modem>Settings page.

Before you configure your **Modem Failover Settings**, create your dialup profiles in the Modem Profile Configuration window, which you access from the **Modem > Dialup Profiles** page.

Alert! *The SonicWALL modem can only dial out. Dialing into the internal modem is not supported. However, an external modem can be connected to the* ***Console*** *port for remotely accessing the SonicWALL for out-of-band support.*

Configuring Modem Failover

Use the following instructions to configure the **Failover Settings**:

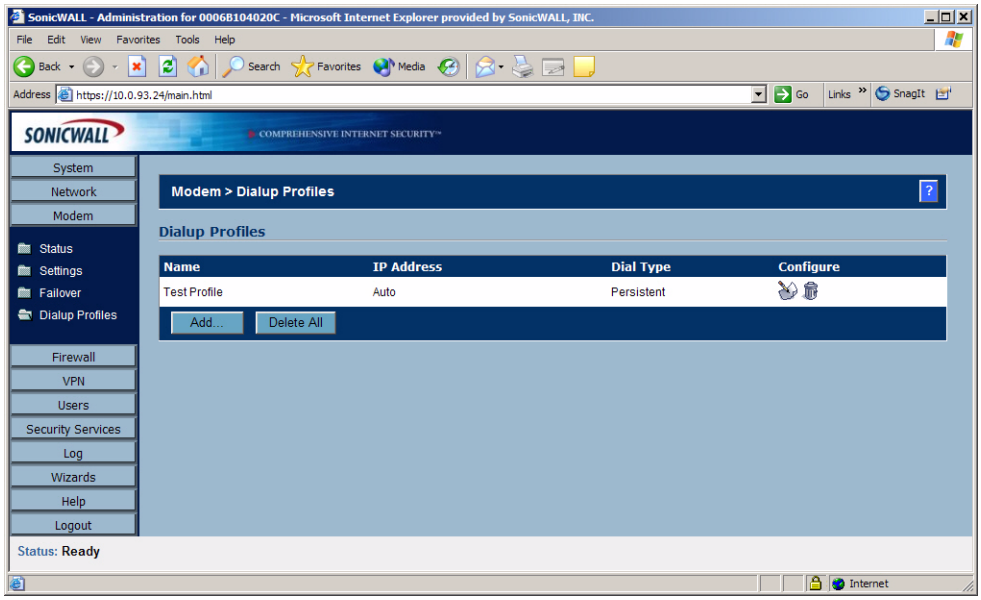
1. Select **Enable WAN Failover**.
2. Select **Enable Preempt Mode** if you want the primary WAN Ethernet interface to take over from the secondary modem WAN interface when it becomes active after a failure. If you do not enable **Preempt Mode**, the secondary WAN modem interface remains active as the WAN interface until you click **Disconnect**.
3. Select **Enable Probing**. Probing for WAN connectivity occurs over the Ethernet connection, the dial-up connection, or both. When probing is disabled on the Ethernet link, the SonicWALL only performs link detection. If the Ethernet connection is lost for a duration of 5-9 seconds, the SonicWALL considers the Ethernet connection to be unavailable. If the Ethernet link is lost for 0-4 seconds, the SonicWALL does not consider the connection to be lost. If you are swapping cables quickly, unnecessary WAN failover does not occur on the SonicWALL. If probing is enabled and the cable is unplugged, the 5-9 seconds link detection does not occur. Instead, the probing rules apply to the connection using the parameters configured for **Probe Interval (seconds)** and **Failover Trigger Level (missed probes)** settings. If probing is enabled on dialup, the dialup connection is terminated and re-established when probing fails over the modem.
4. Select an option from the **Probe through** menu. Select **Ethernet Only** to probe the Ethernet WAN connection and failover to the modem when the connection is lost. Select **Modem Only** to probe a dial-up connection and have the modem redial when the dial-up connection is lost. Select **Modem and Ethernet** to enable both types of probing on the SP.
5. Enter the IP address for the probe target in the **Probe Target (IP Address)** field. The Probe IP address is a static IP address on the WAN. If this field is left blank, or 0.0.0.0 is entered as the address, the Probe Target is the WAN Gateway IP address.

Tip! *The probe is a ping sent to the IP address and is used, along with the response, as a method of determining Internet connectivity.*

6. Select **ICMP Probing** or **TCP Probing** from the **Probe Type** options. If you select **TCP Probing**, enter the TCP port number in the **TCP port** field.
7. In the **Probe Interval (seconds)** field, enter the amount of time between probes to the **Probe Target**. The default value is **5** seconds. To deactivate the Probe Detection feature, enter *0* as the value. In this case, the WAN failover only occurs when loss of the physical WAN Ethernet connection occurs on the SonicWALL.
8. Enter the number of missed probes required for the WAN failover to occur in the **Failover Trigger Level (missed probes)** field.
9. Enter a value for the number of successful probes required to reactivate the primary connection in the **Successful Probes to Reactivate Primary** field. The default value is five (5). By requiring a number of successful probes before the SonicWALL returns to its primary connection, you can prevent the SonicWALL from returning to the primary connection before the primary connection becomes stable.
10. Click **Apply** for the settings to take effect on the SonicWALL.

Modem > Dialup Profiles

The **Modem > Dialup Profiles** page allows you to configure modem profiles on the SonicWALL using your dial-up ISP information for the connection. Multiple modem profiles can be used when you have a different profile for individual ISPs.



Tip! *The SonicWALL supports a maximum of 10 configuration profiles.*

Dial-Up Profiles

The current profile is displayed in the **Dialup Profiles** table, which displays the following dialup profile information:

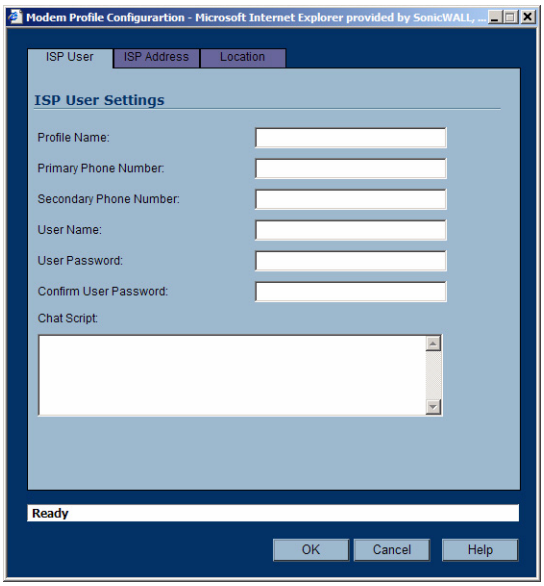
- **Name** - the name you've assigned to the profile. You can use names such as **Home**, **Office**, or **Travel** to distinguish different profiles from each other.
- **IP Address** - the IP address of the Internet connection.
- **Dial Type** - displays Persistent, Dial on Data, or Manual Dial, depending on what you selected in the **Modem Profile Configuration** window for the profile.
- **Configure** - clicking the **Notepad** icon allows you to edit the profile. Clicking on the **Trashcan** icon deletes the profile.

Configuring a Dialup Profile

In the **Modem > Dialup Profiles** page, click the **Add** button. The Modem Profile Configuration window is displayed for configuring a dialup profile.

Modem > Dialup Profiles > Modem Profile Configuration

The **Modem Profile Configuration** window allows you to configure your modem dial-up connections. Once you create your profiles, you can then configure specify which profiles to use for WAN failover or Internet access.



Configuring a Dialup Profile

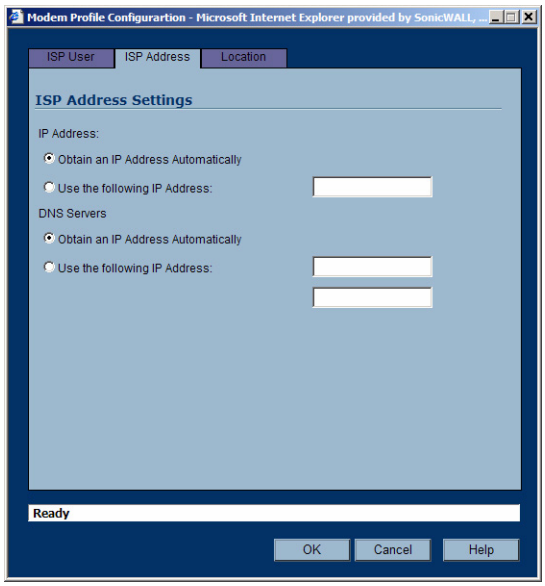
To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

1. In the **ISP User** page, enter a name for your dialup profile in the **Profile Name** field.
2. Enter the primary number used to dial your ISP in the **Primary Phone Number** field.

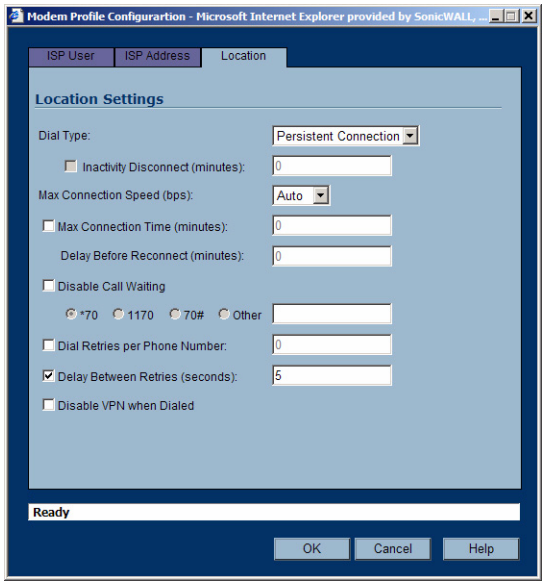
Tip! *If a specific prefix is used to access an outside line, such as 9, &, or , , enter the number as part of the primary phone number.*

3. Enter the secondary number used to dial your ISP in the **Secondary Phone Number** field (optional).
4. Enter your dial-up ISP user name in the **User Name** field.
5. Enter the password provided by your dialup ISP in the **User Password** field.
6. Confirm your dialup ISP password in the **Confirm User Password** field.
7. If your ISP has given you a script that runs when you access your ISP connection, cut and paste the script text in the **Chat Script** field. See the Information on Chat Scripts section for more information on using chat scripts.

8. Click the **ISP Address** tab.



9. In the **ISP Address Setting** section, select **Obtain an IP Address Automatically** if you do not have a permanent dialup IP address from your ISP. If you have a permanent dialup IP address from your ISP, select **Use the following IP Address** and enter the IP address in the corresponding field.
10. If you obtain an IP address automatically for your DNS server(s), select **Obtain an IP Address Automatically**. If your ISP has a specific IP address for the DNS server(s), select **Use the following IP Address** and enter the IP address of the primary DNS server in the corresponding field. You can also add a secondary DNS server address in the field below.
11. Click on the **Location** tab. Use the settings in the page to configure modem dialup behavior.



12. In the **Dial Type** menu select one of the following options:

- **Persistent Connection** - By selecting **Persistent Connection**, the modem stays connected unless you click the Disconnect button on the Network > Settings page. If **Enable WAN Failover** is selected on the Modem>Failover page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.

- **Dial on Data** - Using **Dial on Data** requires that outbound data is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWALL internal applications such as AutoUpdate and Anti-Virus. If **Enable WAN Failover** is selected on the Modem > Failover page, the pings generated by the probe can trigger the modem to dial when no WAN Ethernet connection is detected. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
- **Manual Dial** - Selecting **Manual Dial** for a **Primary Profile** means that a modem connection does not automatically occur. You must click the **Connect** button on the Network>Settings page for the dialup connection to be established. Also, WAN Failover does not automatically occur.

Alert! *If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection.*

Alert! *If you enable Persistent Connection for the modem, the modem connection remains active until the WAN Ethernet connection is reactivated or you force disconnection by clicking **Disconnect** on the **Configure** page.*

13. Enter the number of minutes a dial-up connection is allowed to be inactive in the **Inactivity Disconnect (minutes)** field.
14. Select the connection speed from the **Max Connection Speed (bps)** menu. **Auto** is the default setting as the SonicWALL automatically detects the connection speed when it connects to the ISP or you can select a specific speed option from the menu.
15. Select **Max Connection Time (minutes)** if the connection is terminated after the specified time. Enter the number of minutes for the connection to be active. The value can range from 0 to 1440 minutes. This feature does not conflict with the **Inactivity Disconnect** setting. If both features are configured, the connection is terminated based on the shortest configured time.
16. If you select **Max Connection Time (minutes)**, enter the number of minutes to delay before redialing the ISP in the **Delay Before Reconnect (minutes)**. The value can range from 0 to 1440, and the default value is 0 which means there is no delay before reconnecting to the ISP.
17. If you have call waiting on your telephone line, you should disable it or another call can interrupt your connection to your ISP. Select **Disable Call Waiting** and then select command from the list. If you do not see your command listed, select **Other**, and enter the command in the field.
18. If the phone number for your ISP is busy, you can configure the number of times that the SonicWALL modem attempts to connect in the **Dial Retries per Phone Number** field. The default value is **0**.
19. Enter the number of seconds between attempts to redial in the **Delay Between Retries (seconds)** field. The default value is **5** seconds.
20. Select **Disable VPN when Dialed** if VPN Security Associations (SAs) are disabled when the modem connects to the ISP. Terminating the dial-up connection re-enables the VPN SAs. This is useful if you want to deploy your own point-to-point RAS network and want packets to be sent in the clear to your intranets.
21. Click **OK** to add the dial-up profile to the SonicWALL. The Dialup Profile appears in the **Dialup Profiles** table.

Chat Scripts

Some legacy servers can require company-specific chat scripts for logging onto the dial-up servers.

A chat script, like other types of scripts, automates the act of typing commands using a keyboard. It consists of commands and responses, made up of groups of expect-response pairs as well as additional control commands, used by the chat script interpreter on the TELE3 SP. The TELE3 SP uses a default chat script that works with most ISPs, but your ISP may require a chat script with specific commands to "chat" with their server. If an ISP requires a specific chat script, it is typically provided to you with your dial-up access information. The default chat script for the TELE3 SP has the following commands:

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

The first three commands direct the chat script interpreter to abort if any of the strings **NO CARRIER**, **NO DIALTONE**, or **BUSY**are received from the modem.

The next five commands are AT commands that tell the chat interpreter to wait for nothing as " defines an empty string, and configure the following on the modem: return command responses, don't echo characters, report the connecting baud rate when connected, and return verbose responses.

The next line has **OK** as the expected string, and the interpreters waits for **OK** to be returned in response to the previous command, **ATV1**, before continuing the script. If OK is not returned within the default time period of 50 seconds, the chat interpreter aborts the script and the connection fails. If **OK** is received, the prefix and phone number of the selected dial-up account is dialed. The **\T** command is replaced by chat script interpreter with the prefix and phone number of the dial-up account.

In the last line of the script, **CONNECT** is the expected response from the remote modem. If the modems successfully connect, **CONNECT** is returned from the TELE3 SP modem.The **\D** adds a pause of one second to allow the server to start the PPP authentication. The **\C** command ends the chat script end without sending a carriage return to the modem. The TELE3 SP then attempts to establish a PPP (Point-to-Point Protocol) connection over the serial link. The PPP connection usually includes authentication of the user by using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) from the PPP suite. Once a PPP connection is established, it looks like any other network interface.

Custom Chat Scripts

Custom chat scripts can be used when the ISP dial-up server does not use PAP or CHAP as an authentication protocol to control access. Instead, the ISP requires a user to log onto the dial-up server by prompting for a user name and password before establishing the PPP connection. For the most part, this type of server is part of the legacy systems rooted in the dumb terminal login architecture. Because these types of servers can prompt for a user name and password in a variety of ways or require subsequent commands to initiate the PPP connection, a **Chat Script** field is provided for you to enter a custom script.

If a custom chat script is required by an ISP for establishing a connection, it is commonly found on their web site or provided with their dial-up access information. Sometimes the scripts can be found by using a search engine on the Internet and using the keywords, "chat script ppp Linux <ISP name>".

A custom chat script can look like the following script:

```
ABORT `NO CARRIER'
ABORT `NO DIALTONE'
ABORT `BUSY'
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```

Tip! *The first character of username and password are ignored during PPP authentication.*

The script looks a lot like the previous script with the exception of the commands at the end. There is an empty string (") after **CONNECT** which sends a carriage return command to the server. The chat interpreter then waits for **sername:** substring. When a response is returned, the current PPP account user name, substituting the **\L** command control string, is sent. Then, the chat interpreter waits for the substring assword:, and sends the password, substituting **\P** with the PPP account password. If either the **sername** or **assword** substring are not received within the timeout period, the chat interpreter aborts the dial-up process resulting in a dial-up failure.

8 Firewall

Network Access Rules are management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL.

By default, the SonicWALL's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the "Default" stateful inspection packet rule enabled in the SonicWALL:

- Allow all sessions originating from the LAN to the WAN or OPT/DMZ.
- Allow all sessions originating from the OPT/DMZ to the WAN.
- Deny all sessions originating from the WAN to the OPT/DMZ.
- Deny all sessions originating from the WAN and OPT/DMZ to the LAN.

Additional Network Access Rules can be defined to extend or override the default rules. For example, rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

The custom rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to rules created on the SonicWALL. Network Access Rules take precedence, and can override the SonicWALL stateful packet inspection. For example, a rule that blocks IRC traffic takes precedence over the SonicWALL default setting allowing this type of traffic.

Alert! *The ability to define Network Access Rules is a very powerful tool. Using custom rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting Network Access Rules.*

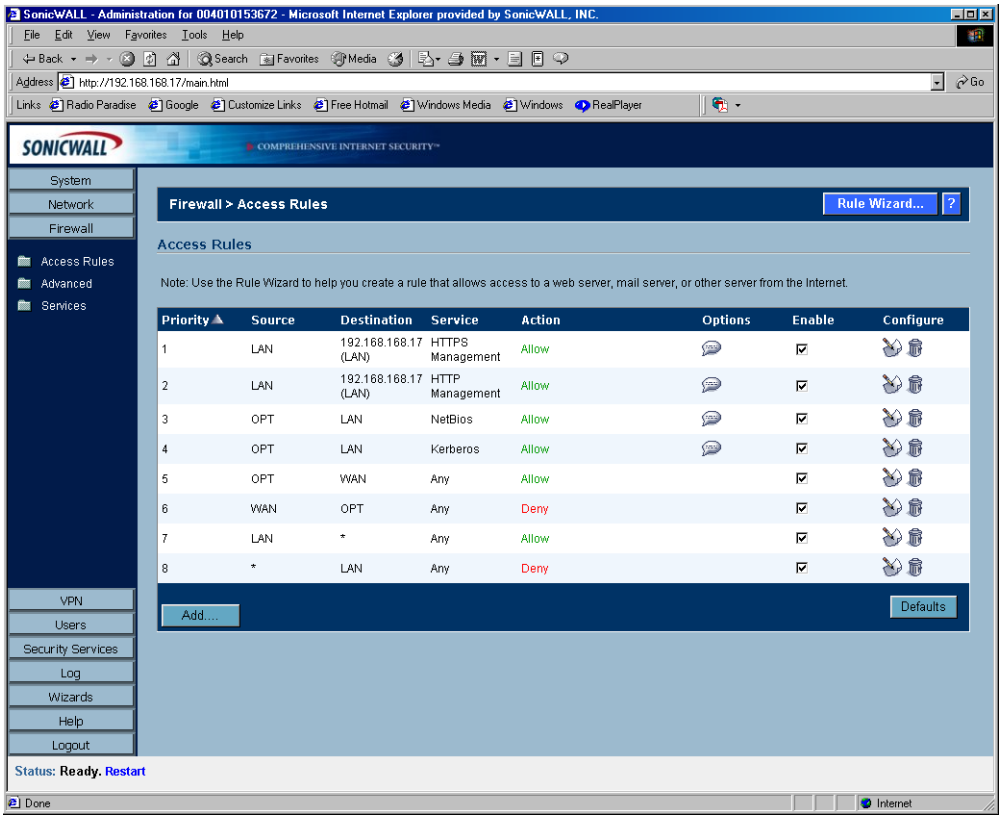
Using Bandwidth Management with Access Rules

Bandwidth management allows you to assign guaranteed and maximum bandwidth to services and also set priorities for outbound traffic. Bandwidth management only applies to **outbound** traffic from the SonicWALL to the WAN or any other destination. The minimum guaranteed bandwidth in Kbps is 20 and the maximum is 100,000 kbps. Any rule using bandwidth management has a higher priority than rules not using bandwidth management. Rules using bandwidth management based the assigned priority and rules without bandwidth management are given lowest priority. For instance, if you create a rule for outbound mail traffic (SMTP) and enable Bandwidth Management with a guaranteed bandwidth of 20 Kbps and a maximum bandwidth of 40 Kbps, priority of 0, outbound SMTP traffic always has 20 Kbps available to it and can get as much as 40 Kbps. If this is the only rule using Bandwidth Management, it has priority over all other rules on the SonicWALL. Other rules use the leftover bandwidth minus 20 Kbps (guaranteed) or minus 40 Kbps (maximum).

Alert! *You must select Bandwidth Management on the **WAN>Ethernet** tab. Click **Network**, then **Configure** in the **WAN** line of the **Interfaces** table, and enter your available bandwidth in the **Available WAN Bandwidth (Kbps**) field.*

Firewall>Access Rules

The **Access Rules** page displays a table of defined Network Access Rules. Rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Default** rule. The Default rule is all IP services except those listed in the **Access Rules** page. Rules can be created to override the behavior of the **Default** rule; for example, the **Default** rule allows users on the LAN to access all Internet services, including NNTP News.



You can enable or disable Network Access Rules by selecting or clearing the check box in the **Enable** column. Clicking the **Notepad** icon allows you to edit an existing rule, or clicking the **Trashcan** icon deletes an existing rule. If the two icons are unavailable, the rule cannot be changed or removed from the list. Rules with a **Funnel** icon are using bandwidth management.

Tip! *You can easily create Network Access Rules using the **Network Access Rule Wizard**.*

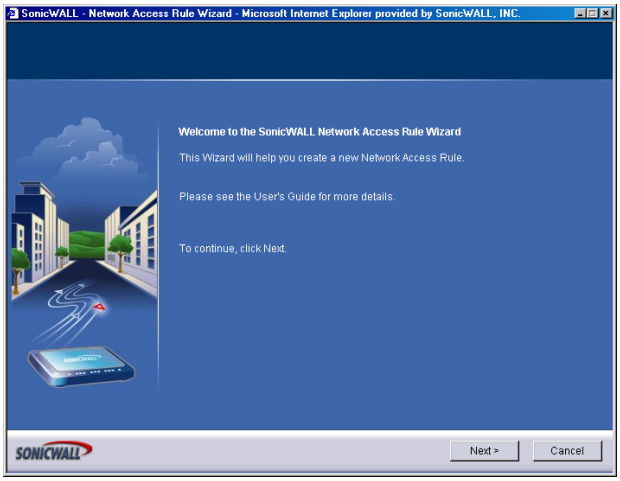
Restoring Default Network Access Rules

The SonicWALL includes a set of default Network Access Rules, which are listed in the **Access Rules** table. You can reset the SonicWALL at any time to restore the Network Access Rules to just the default rules by clicking on the **Defaults** button.

Adding Rules using the Network Access Rule Wizard

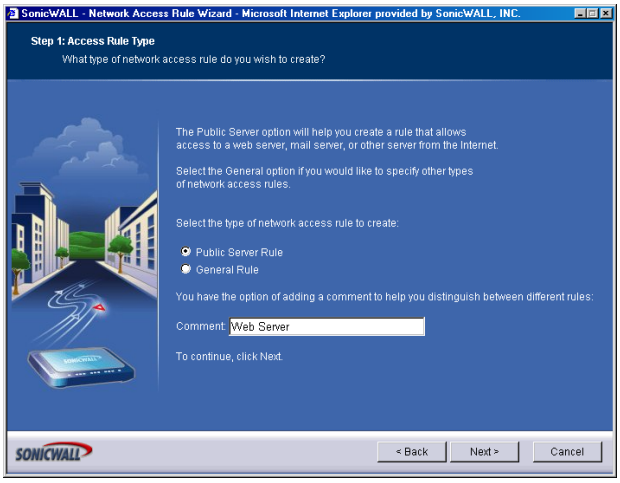
The **Network Access Rule Wizard** takes you step by step through the process of creating network access rules on the SonicWALL. To launch the Access Rules Wizard, click the **Rule Wizard** button at the top right of the **Firewall>Access Rules** page.

Note: *The image on the left pane of the **Network Access Rules Wizard** changes according to the SonicWALL you're using but all the wizard pages are the same for the TZ170, PRO 2040, or PRO 3060.*



1. Read the instructions on the **Welcome** page, and click **Next** to continue.

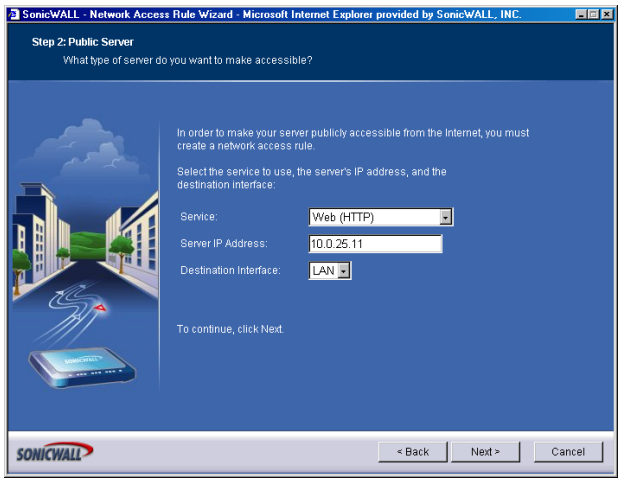
Step 1: Access Rule Type



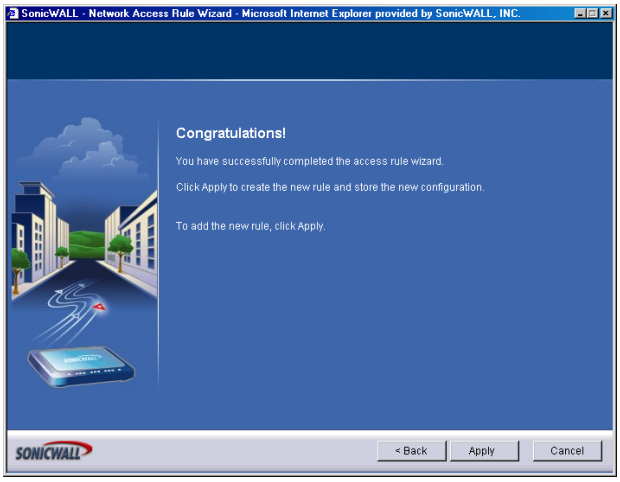
2. Select the type of network access rule you want to create, either **Public Server Rule** or **General**. Select **Public Server Rule**. Click **Next**.

Configuring a Public Server Rule

Step 2: Public Server



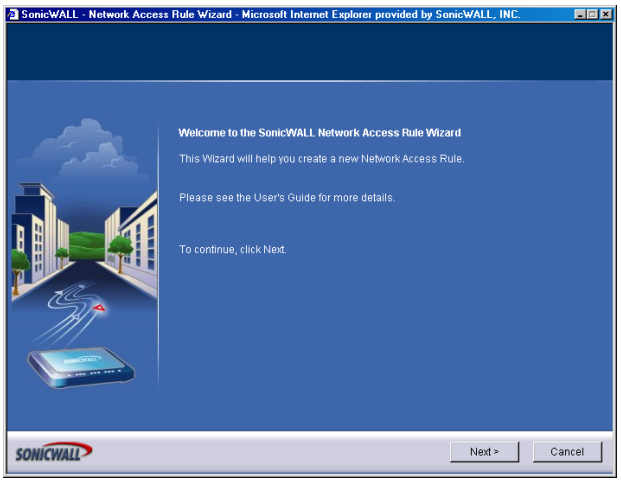
3. Select the type of service for the rule from the **Service** menu. In this example, select **Web** (**HTTP)** to allow network traffic to a Web Server on your LAN.
4. Type the IP address of the mail server in the **IP address** field.
5. Select the destination of the network traffic from the **Destination Interface** menu. In this case, you are sending traffic to the LAN. Select **LAN**.
6. Click **Next**.



7. Click **Apply** to complete the wizard and create a Public Server on your network.

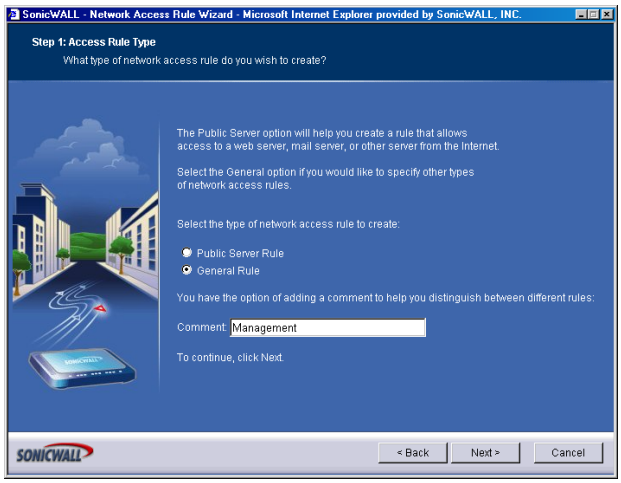
Configuring a General Network Access Rule

To launch the Access Rules Wizard, select the **System>Wizards** page and click the **Rule Wizard** button. The **Network Access Rule Wizard** is displayed.



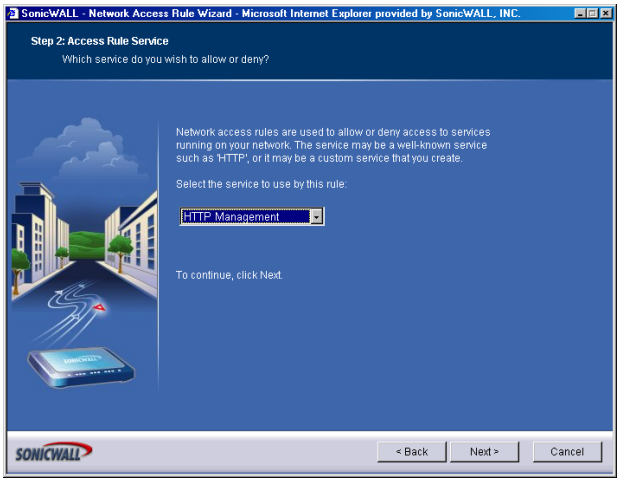
1. To continue, click **Next**.

Step 1: Access Rule Type



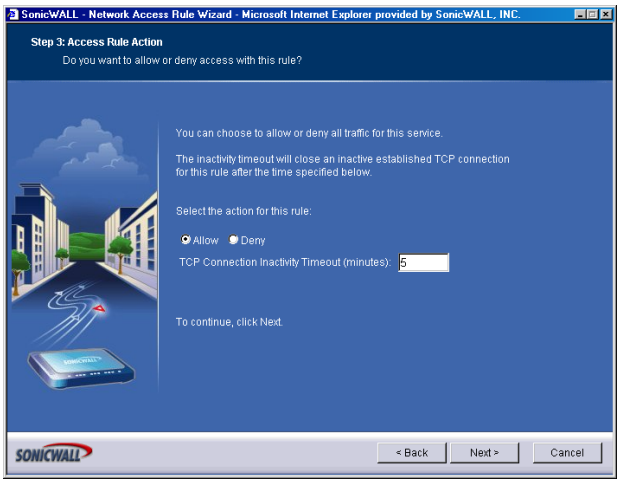
2. Select the type of network access rule you want to create, in this case, **General**. Click **Next**.

Step 2: Access Rule Service



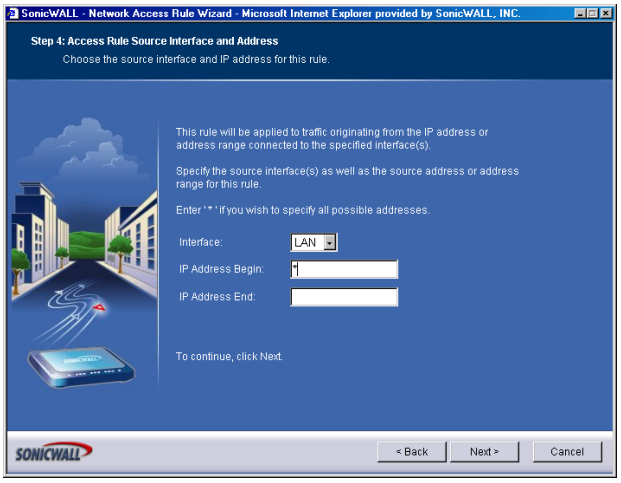
3. Select the type of service for the rule. If you do not see the service in the list, you must add it manually to the list of services on the **Firewall>Services** page. Click **Next**.

Step 3: Access Rule Action



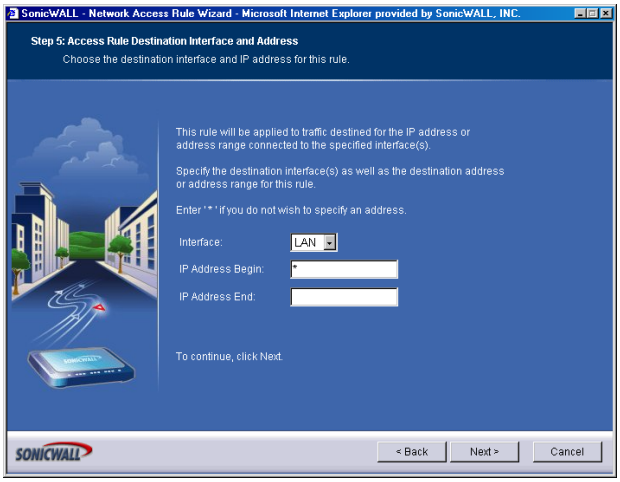
4. Select **Allow** to allow the service to the network, or select **Deny** to disallow the service to the network.
5. Enter a value in minutes in the **Inactivity Timeout (minutes)** field. The default value is 5 minutes.
6. Click **Next**.

Step 4: Access Rule Source Interface and Address



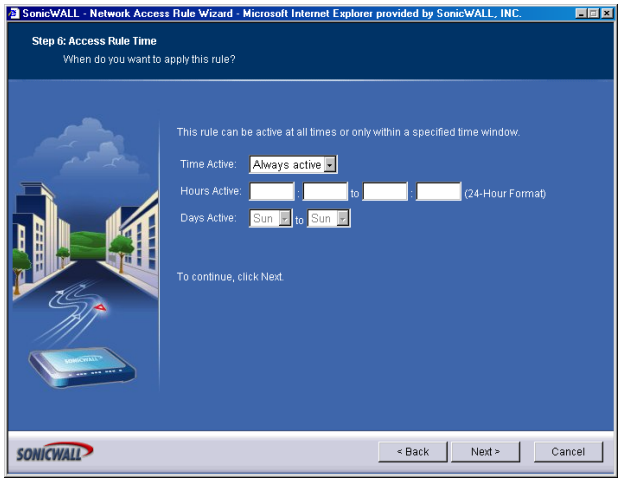
7. If you have a range of IP addresses, enter the first one in the **IP Address Begin** field. If you do not want to specify an IP address, enter "*****" in the **IP Address Begin** field. By typing * (asterisk) in the field, all traffic using the service is either allowed or denied to all computers on the network. Click **Next**.
8. Select the source of the service from the **Interface** menu. If you want to allow or deny the service from the Internet, select **WAN**. To allow or deny the service from any source, select ***** from the **Interface** menu.

Step 5: Access Rule Destination Interface and Address



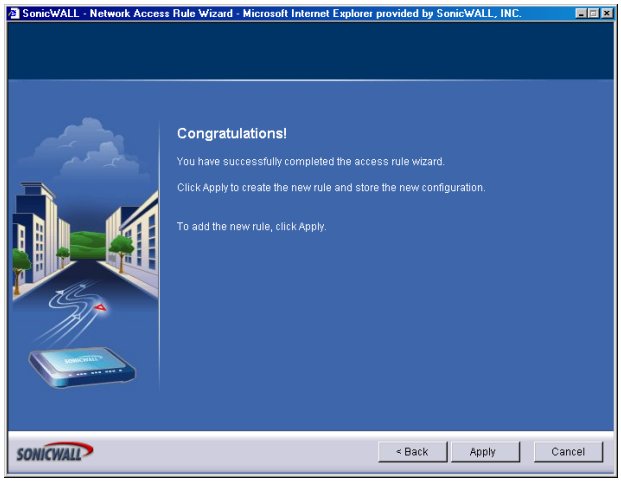
9. If you have a range of IP addresses, enter the first one in the **IP Address Begin** field. If you do not want to specify an IP address, enter "*****" in the **IP Address Begin** field. By typing "*****" in the field, all traffic using the service is either allowed or denied to all computers on the network.
10. Select the source of the service from the **Interface** menu. If you want to allow or deny the service from the Internet, select **WAN**. To allow or deny the service from any source, select ***** from the **Interface** menu. Click **Next**.

Step 6: Access Rule Time



11. The rule is always active unless you specify a time period for the rule to be active. For instance, you can deny access to News (NNTP) between 8 a.m. and 5 p.m. Monday through Friday, but allow access after work hours and on weekends. Click **Next**.

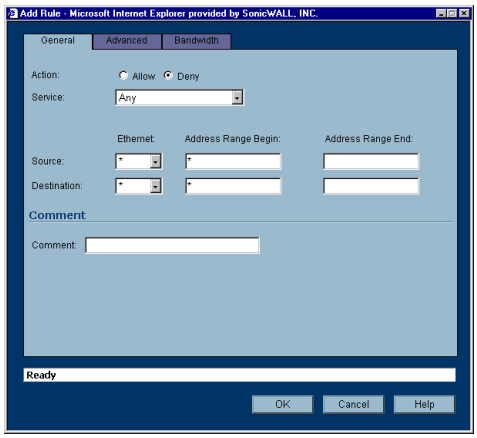
Completing the Network Access Rule Wizard



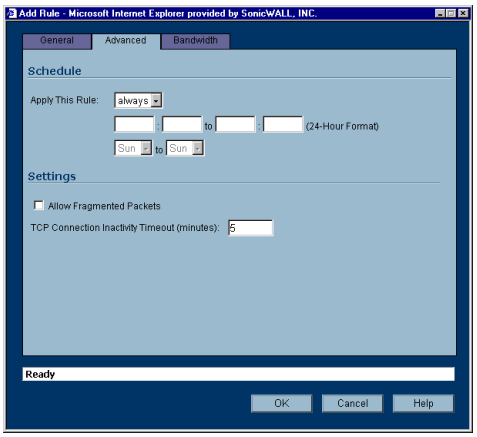
12. Click **Apply** to save your new rule. The new rule is listed in the **Access Rules** table.

Adding Rules Using the Add Rule Window

To add Access Rules to the SonicWALL, click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.



1. Select **Allow** or **Deny** from the **Action** list depending upon whether the rule is intended to permit or block IP traffic.
2. Select the name of the service affected by the Rule from the **Service** list. If the service is not listed, you must define the service in the **Add Service** window. The **Default** service encompasses all IP services.
3. Select the source of the traffic affected by the rule, either **LAN**, **OPT/DMZ** or **WAN**, *(any source), from the **Source Ethernet** list.
4. If you want to define the source IP addresses that are affected by the rule, such as restricting certain users from accessing the Internet, enter the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, enter * in the **Address Range Begin** field.
5. Select the destination of the traffic affected by the rule, either LAN or WAN or *, from the **Destination Ethernet** menu.
6. If you want to define the destination IP addresses that are affected by the rule, for example, to allow inbound Web access to several Web servers on your LAN, enter the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, enter * in the **Address Range Begin** field.
7. Enter any comments to help identify the rule in the **Comments** field.
8. Click the **Advanced** tab.



9. Select **always** from the **Apply this Rule** menu if the rule is always in effect.

10. Select **from** the **Apply this Rule** menu to define the specific time and day of week to enforce the rule. Enter the time of day (in 24-hour format) to begin and end enforcement. Then select the day of the week to begin and end enforcement.

Tip! *If you want to enable the rule at different times depending on the day of the week, make additional rules for each time period.*

11. If you would like for the rule to time out after a period of inactivity, set the amount of time, in minutes, in the **Inactivity Timeout (minutes)** field. The default value is 5 minutes.
12. Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. Because hackers exploit IP fragmentation in Denial of Service attacks, the SonicWALL blocks fragmented packets by default. You can override the default configuration to allow fragmented packets over PPTP or IPSec.
13. Click the **Advanced** tab.
14. Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.
15. Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

Tip! *Rules using Bandwidth Management take priority over rules without bandwidth management.*

16. Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list.
17. Click **OK**.

Tip! *Although custom rules can be created that allow inbound IP traffic, the SonicWALL does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.*

Rule Examples

The following examples illustrate methods for creating Network Access Rules.

Blocking LAN Access for Specific Services

This example shows how to block LAN access to NNTP servers on the Internet during business hours.

1. Click **Add** to launch the **Add** window.
2. Select **Deny** from the **Action** settings.
3. Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must to add it in the **Add Service** window.
4. Select **LAN** from the **Source Ethernet** menu.
5. Since all computers on the LAN are to be affected, enter * in the **Source Address Range Begin** field.
6. Select **WAN** from the **Destination Ethernet** menu.
7. Enter * in the **Destination Address Range Begin** field to block access to all NNTP servers.
8. Click on the **Options** tab.
9. Select **from** the **Apply this Rule** list to configure the time of enforcement.
10. Enter 8:30 and 17:30 in the hour fields.
11. Select **Mon** to **Fri** from the menu.
12. Click **OK**.

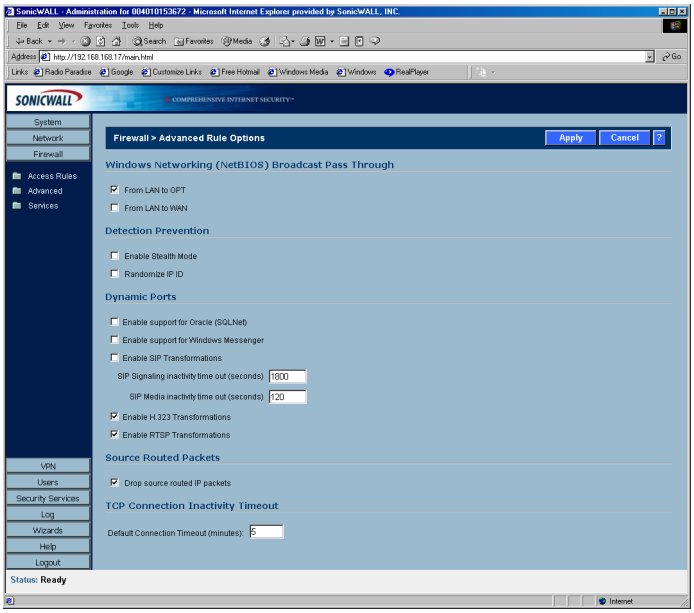
Enabling Ping

By default, your SonicWALL does not respond to ping requests from the Internet. This Rule allows ping requests from your ISP servers to your SonicWALL.

1. Click **Add** to launch the **Add Rule** window.
2. Select **Allow** from the **Action** menu.
3. Select **Ping** from the **Service** menu.
4. Select **WAN** from the **Source Ethernet** menu.
5. Enter the starting IP address of the ISP network in the **Source Address Range Begin** field and the ending IP address of the ISP network in the **Source Address Range End** field.
6. Select **LAN** from the **Destination Ethernet** menu.
7. Since the intent is to allow a ping only to the SonicWALL, enter the SonicWALL LAN IP Address in the **Destination Address Range Begin** field.
8. Click the **Options** tab.
9. Select **Always** from the **Apply this Rule** menu to ensure continuous enforcement.
10. Click **OK**.

Access Rules> Advanced

Click **Advanced** underneath Access Rules.The **Advanced Rule Options** page is displayed.



Windows Networking (NetBIOS) Broadcast Pass Through

Computers running Microsoft Windows communicate with one another through NetBIOS broadcast packets. By default, the SonicWALL blocks these broadcasts. Select **From LAN to OPT/DMZ** to allow broadcasts from the LAN to the OPT/DMZ. Select **From LAN to WAN** to allow broadcasts from the LAN to the WAN.