SonicWALL Internet Security Appliances

SonicOS Enhanced
Administrator's Guide

SONICWALL

Contents

Copyright Notice

LIMITED WARRANTY

About this Guide

Thank you for purchasing the SonicWALL Internet Security appliance. The SonicWALL protects your PC from attacks and intrusions, filters objectional Web sites, provides private VPN connections to business partners and remote offices, and offers a centrally-managed defense against software viruses.

This manual covers the configuration of the SonicWALL and its features.

Organization of this Guide

Chapter 1, **Introduction** - describes the features and applications of the SonicWALL.

Chapter 2, **Registering at mySonicWALL.com** - provides details on registering your SonicWALL appliance in the product registration database.

Chapter 3, **System Settings -** describes the configuration of the SonicWALL IP settings, time, and password as well as providing instructions to restart the SonicWALL, import and export settings, upload new firmware, and perform diagnostic tests.

Chapter 4, **Network -** outlines configuring network settings manually for the SonicWALL as well as static routes and RIPv2 advertising on the network. Setting up the SonicWALL to act as the DHCP server on your network is also covered in this chapter.

Chapter 5, **Firewall -** explains how to permit and block traffic through the SonicWALL, set up One-to-One NAT, and configuring automatic proxy forwarding.

Chapter 6, **SonicWALL VPN** - explains how to create a VPN tunnel between two SonicWALLs and creating a VPN tunnel from the VPN client to the SonicWALL.

Chapter 7, **Users** - describes the configuration of user level authentication as well as the setup of RADIUS servers for user authentication.

Chapter 8, **Hardware Failover** - provides configuration instructions for backing up your SonicWALL with another SonicWALL for mission-critical connectivity.

Chapter 9, **Security Services -** provides configuration instructions for SonicWALL Content Filtering Service and Anti-Virus features.

Chapter 10, **Logging and Alerts -** illustrates the SonicWALL logging, alerting, and reporting features.

Chapter 11, **Appendices**

Appendix A, **SonicWALL Support Solutions** - describes available support packages from SonicWALL.

Appendix B, **Configuring TCP/IP Settings** - provides instructions for configuring your Management Station's IP address.

Appendix C, **Configuring RADIUS and ACE Servers** - provides vendor-specific configuration instructions for RADIUS and ACE servers. The appendix also includes a RADIUS Attributes Dictionary.

SonicWALL Technical Support

For fast resolution of technical questions, please visit the SonicWALL Tech Support Web site at <http://www.sonicwall.com/support>. There, you will find resources to resolve most technical issues and a Web request form to contact one of the SonicWALL Technical Support engineers.

Product Information

SonicOS Enhanced 2.0 is the platform for the PRO 4060 and the TZ 170 Unlimited Node SonicWALL Internet Security appliances. It is also supported on the PRO 3060 through a purchased upgrade.

Firmware Version

This manual is updated and released with firmware version SonicOS Enhanced 2.0. Always check <http//:www.sonicwall.com/products/documentation.html> for the latest version of this manual as well as other upgrade manuals.

Icons Used in this Manual

Alert! *Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL.*

Tip! *Useful information about security features and configurations on your SonicWALL.*

Note: *Important information on a feature that requires callout for special attention.*

1 Introduction

Your SonicWALL Internet Security Appliance

The SonicWALL Internet Security Appliance provides a complete security solution that protects your network from attacks, intrusions, and malicious tampering. In addition, the SonicWALL filters objectionable Web content and logs security threats. SonicWALL VPN provides secure, encrypted communications to business partners and branch offices. The SonicWALL Internet Security Appliance uses stateful packet inspection to ensure secure firewall filtering. Stateful packet inspection is widely considered to be the most effective method of filtering IP traffic. MD5 authentication is used to secure communications between your Management Station and the SonicWALL Web Management Interface. MD5 Authentication prevents unauthorized users from detecting and stealing the SonicWALL password as it is sent over your network.

SonicWALL Internet Security Appliance Features

Internet Security

- **ICSA-Certified Firewall**

  After undergoing a rigorous suite of tests to expose security vulnerabilities, SonicWALL Internet security appliances have received Firewall Certification from ICSA, the internationally-accepted authority on network security. The SonicWALL uses stateful packet inspection, the most effective method of packet filtering, to protect your LAN from hackers and vandals on the Internet.

- **Protection from Malicious Network Activity**

  The SonicWALL automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.

Flexible Network and Security Management

- **Network Address Translation (NAT)**

  Network Address Translation (NAT) translates the IP addresses used on your private LAN to a single, public IP address that is used on the Internet. NAT allows multiple computers to access the Internet, even if only one IP address has been provided by your ISP. SonicWALL NAT Policies allows you to configure multiple NAT policies.

- **Configurable Interfaces**

  Six fully configurable 10/100 auto-sensing Ethernet interfaces provide greater network configuration flexibility and internal security.

- **Object/Policy-Based Management**

  Object/Policy-based management enables simple, flexible, and consistent implementation and management of security policies users and groups for access, VPNs, and content filtering.

- **Network Access Rules**

    The default Network Access Rules allow traffic from the LAN to the Internet and block traffic from the Internet to the LAN. You can create additional Network Access Rules that allow inbound traffic to network servers, such as Web and e-mail servers, or that restrict outbound traffic to certain destinations on the Internet.

- **Autoupdate**

    The SonicWALL maintains the highest level of security by automatically notifying you when new firmware is released. When new firmware is available, the SonicWALL Web Management Interface displays a link to download and install the latest firmware.

- **SNMP (Simple Network Management Protocol) Support**

    SNMP is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWALL Internet Security Appliances and receive notification of any critical events as they occur on the network.

- **WAN/WAN Load Balancing**

    This feature gives you the ability to configure a user-assigned port to function as a secondary WAN port. You can choose to divide outbound traffic between the primary WAN port and the secondary WAN port.

Backup and Recovery

- **SonicWALL SafeMode**

    You can easily take a complete "snapshot" of your SonicWALL firmware and configuration preferences for quick disaster recovery. SafeMode also allows you to easily switch between SonicOS versions and configuration preferences.

Content Filtering

- **SonicWALL Content Filtering Service**

    You can use SonicWALL Web Content Filtering to enforce your company's Internet access policies and create custom policies for groups within your company. The SonicWALL blocks specified categories, such as violence or nudity, using the optional SonicWALL Content Filtering Service. Users on your network can bypass the Content Filter Service by authenticating with a unique user name and password.

- **Log and Block or Log Only**

    You can configure the SonicWALL to log and block access to objectionable Web sites, or to log inappropriate usage without blocking Web access.

- **Restrict Web Features**

    In addition to filtering access to Web sites, the SonicWALL can also block Newsgroups, ActiveX, Java, Cookies, and Web Proxies.

Logging and Reporting

- **Log Categories**

You can select the information you wish to display in the SonicWALL event log. You can view the event log from the SonicWALL Web Management Interface or receive the log as an e-mail file.

- **Syslog Server Support**

In addition to the standard screen log, the SonicWALL can write detailed event log information to an external Syslog server. Syslog is the industry-standard method to capture information about network activity.

- **ViewPoint Reporting (optional)**

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. SonicWALL ViewPoint complements the SonicWALL security features by providing detailed and comprehensive reports of network activity.

SonicWALL ViewPoint is a software application that creates dynamic, Web-based network reports. ViewPoint reporting generates both real-time and historical reports to offer a complete view of all activity through your SonicWALL Internet Security Appliance.

- **E-mail Alerts**

The SonicWALL can be configured to send alerts of high-priority events, such as attacks, system errors, and blocked Web sites. When these events occur, alerts can be immediately sent to an e-mail address or e-mail pager.

Dynamic Host Configuration Protocol (DHCP)

- **DHCP Server**

The SonicWALL DHCP Server offers centralized management of TCP/IP client configurations, including IP addresses, gateway addresses, and DNS addresses up to 4,096 hosts or you can bypass the SonicWALL DHCP server and use your existing network DHCP server. Upon startup, each network client receives its TCP/IP settings automatically from the SonicWALL DHCP Server.

- **DHCP Client**

The DHCP Client allows the SonicWALL to acquire TCP/IP settings (such as IP address, gateway address, DNS address) from your ISP. This is necessary if your ISP assigns you a dynamic IP address.

- **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 end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks residing in one IP subnet address space. This facilitates address administration for the networks using VPN tunnels.

IPSec VPN

- **SonicWALL VPN**

SonicWALL VPN provides a simple, secure tool that enables corporate offices and business partners to connect securely over the Internet. By encrypting data, SonicWALL

VPN provides private communications between two or more sites without the expense of leased site-to-site lines.

- **Global VPN Client Software for Windows**

  Mobile users with dial-up Internet accounts can securely access remote network resources with the SonicWALL Global VPN Client. The SonicWALL Global VPN Client establishes a private, encrypted VPN tunnel to the SonicWALL, allowing users to transparently access network servers from any location.

Contact SonicWALL, Inc. for information about **Content Filter Service, Network Anti-Virus** subscriptions, and other upgrades.

Web: http://www.sonicwall.com
E-mail: sales@sonicwall.com
Phone: (408) 745-9600
Fax:(408) 745-9300

2 Registering at mySonicWALL.com

After you complete the initial installation and configuration of your SonicWALL, you should register your SonicWALL Internet Security Appliance at <http://www.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.

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

Alert!   *You must register your SonicWALL on mySonicWALL.com to access technical support. By registering your SonicWALL, you provide the initial information necessary for technical support if any problems arise during installation.*

Creating a New User Account

If you currently have a mySonicWALL.com user account, you can skip this section and proceed to **Adding New Appliances or Services**.

1. Type <https://www.mysonicwall.com> into your Web browser.
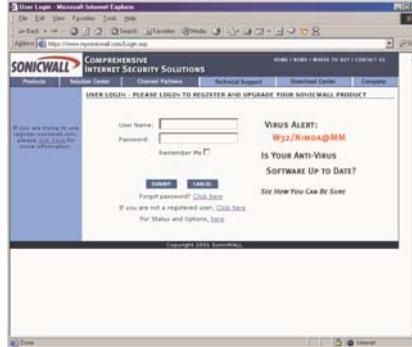
2. As a new user, locate the statement, "If you are not a registered user, <u>click here</u>." Click the link, and an information form appears.

Account Information

3. All field marked with an * are required fields. Be sure to fill out the form completely before submitting to the user database. Create a **User Name** and password for your mySonicWALL account. Confirm the password by typing it in the **Confirm Password** field. For your convenience, you can record the information below.

   User Name:_____ Password:_____

⚠

Alert! *You must remember your user name and password until you have activated your account. If you forget your password before your user account is active, you must create a new user account.*

Tip! *If your security policy doesn't allow you to write down passwords, write down a hint or a prompt for your password.*
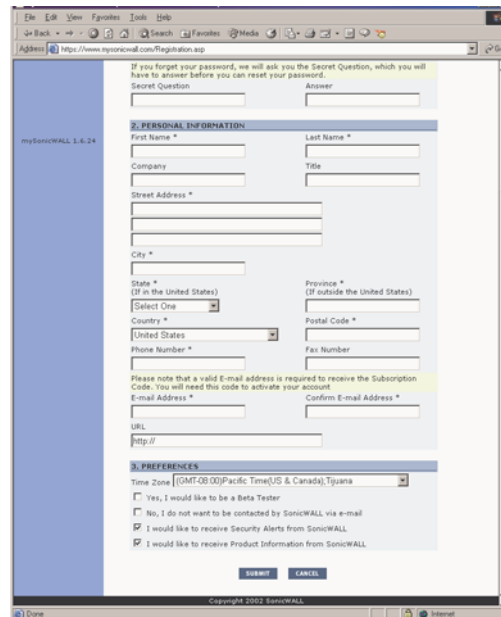
4. Create a **Secret Question and Answer** to prompt you for your password if you forget it.

Personal Information

5. Complete the **Personal Information** section of the Registration form.

Be sure to type the correct e-mail address as the subscription code for your SonicWALL user account is e-mailed to you. The subscription code is necessary to activate your account.

6. Select your time zone from the **Time Zone** menu, and then select any or all of the following options:

   • **Yes, I would like to be a Beta Tester.**
   • **No, I do not want to be contacted by SonicWALL via e-mail.**
   • **I would like to receive security alerts from SonicWALL.**
   • **I would like to receive product information from SonicWALL.**

7. Click **Submit.**

8. Review your information carefully to ensure that it is accurate. Click **Back** on your Web browser navigation bar to go back to the form and re-type any information.
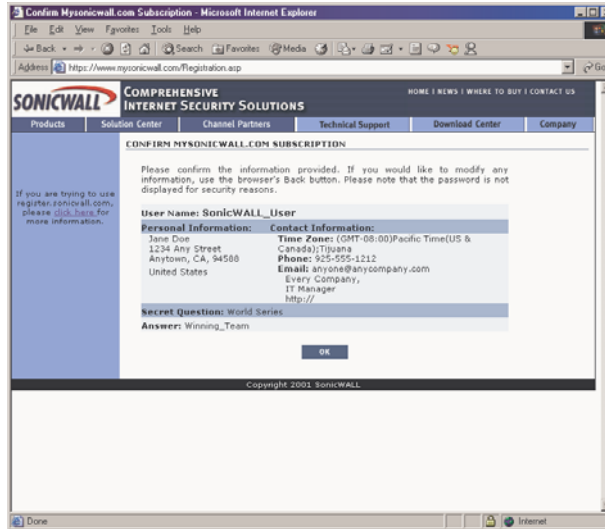
9. If all the information is correct, click **OK**. A confirmation message appears notifying you that your account must be activated within 72 hours of creating it. You also receive an e-mail with your subscription code in it. Write your subscription code below:

    Subscription code:_____
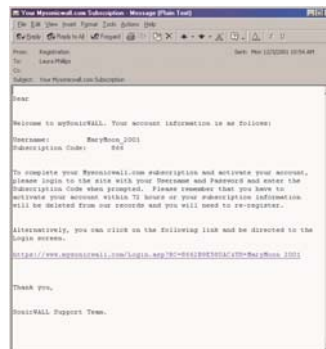
Note: *For security reasons, the subscriber name and part of the subscription code are masked.*

10. Return to the mySonicWALL.com login screen, or alternatively, click on the link in the e-mail message to provide your subscription code to activate your account.

–
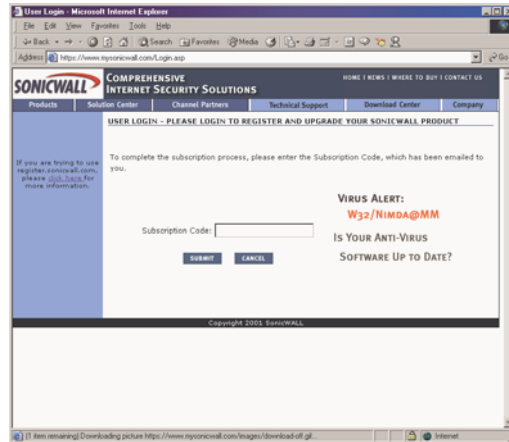
11. Type the subscription code you received via e-mail into the **Subscription Code** field, and click **Submit**.

12. Your Account Management interface appears and you can now register SonicWALL Internet Security Appliances or Services. You can also delete or transfer appliances from your user account.
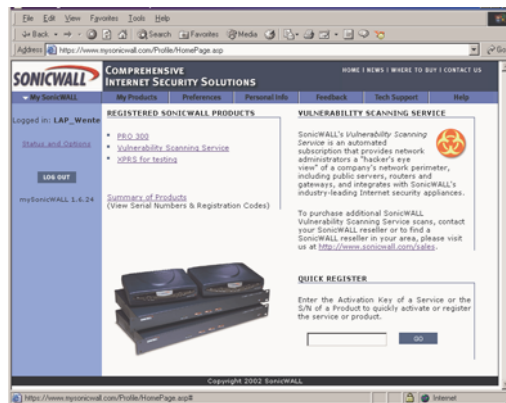
Problems Creating a User Account?

If you're having trouble creating a user account on the mySonicWALL.com Web site, be sure to check the following items in your browser:

- Accept Cookies
- Internet Explorer 5.0 or higher
- Netscape 4.5 or higher
- Allow Java scripts
- Correct Password for mysonicWALL.com

User Name and Password Functions

If you forget your user name, you must send an e-mail message to Tech Support requesting your user name. Be sure to include the e-mail address used to create the mysonicWALL.com account.

If you forget your password, use the **Forget Password? Click here** link to use your **Secret Question and Answer** to remember your password. If you did not set up a **Secret Question and Answer** for your password, a link appears allowing you to reset your password. Be sure to use the same user name and e-mail address as your mysonicWALL.com user account.

Registering Your SonicWALL Internet Security Appliance

To register your SonicWALL Internet Security Appliance, click the hyperlink, **Click Here**, in the **Registered SonicWALL Products** section. Or to quickly register your appliance, type the **Activation Key** of a service, or a SonicWALL Internet Security Appliance serial number into the field in the **Quick Register** section.

Click Here Registration

If you use the hyperlink, **Click Here**, a **My Products** page appears, and you can register your appliance by entering the Serial Number in the **Add New Product** field. You can also create a **Friendly Name**, such as San Francisco Office, to identify the SonicWALL. Using **Friendly Names** can help you to manage multiple SonicWALL appliances.
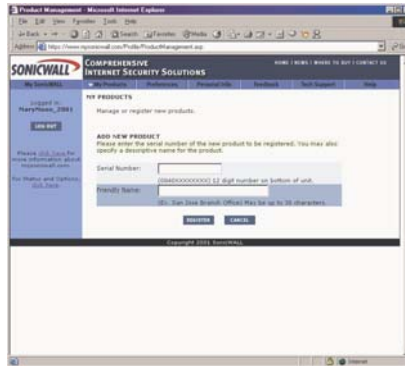
Quick Registration

To quickly register a SonicWALL Internet Security Appliance, type the serial number in the field under the **Quick Register** section, and click **Go**. The serial number automatically appears in the **Serial Number** field. You can then create a **Friendly Name** for the appliance. If you type the incorrect serial number into the **Serial Number** field, a message stating that the appliance is previously registered may be returned. Write your SonicWALL serial number below.

SonicWALL Serial Number:_____
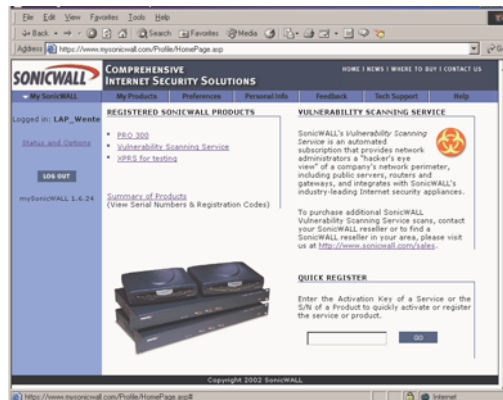
After you register the SonicWALL, the **Friendly Name** appears as a hyperlink under **Registered SonicWALL Products**. Click on the **Friendly Name** to view the services activated on the appliance.
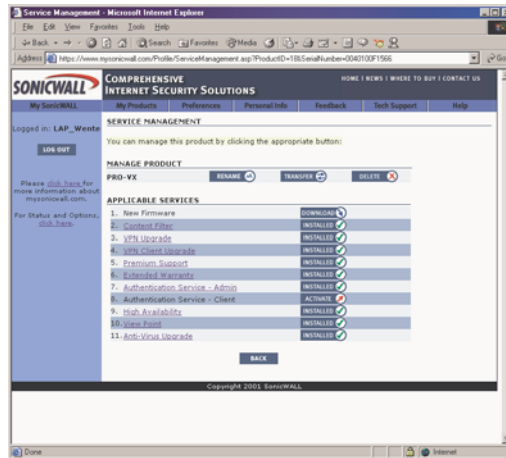
Note: *Services may vary from model to model and may not have the same activated fields as the above appliance. Also, the serial number, registration code, and activation keys are masked for security reasons.*

Status and Options

Click **Status and Options** underneath the login information to search for the status and options relating to a particular SonicWALL appliance. Type the SonicWALL serial number to search for the related information.
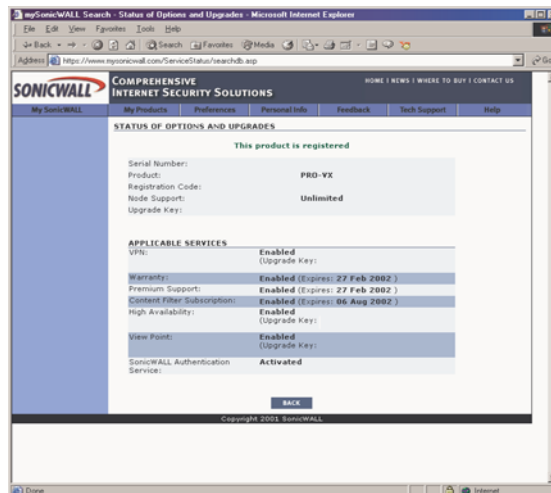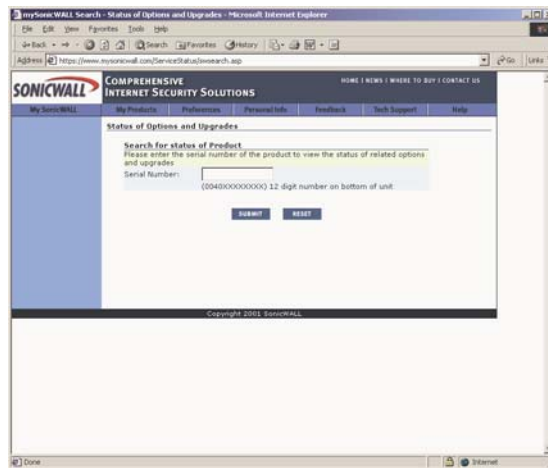
Information displayed includes

- **Serial Number**
- **Product**
- **Registration Code**
- **Node Support Upgrade Key**

There is also a list of applicable services with their activation keys as well as expiration dates for subscriptions.

Managing Your SonicWALL

You can rename your SonicWALL, transfer your SonicWALL, or delete your SonicWALL in this section of **Services Management**.

Renaming Your SonicWALL

You can rename your SonicWALL at any time in order to manage your SonicWALLs. To rename your SonicWALL, click **Rename** in the **Manage Products** section. Type the new name in the **Friendly Name** field, and click **Submit**.
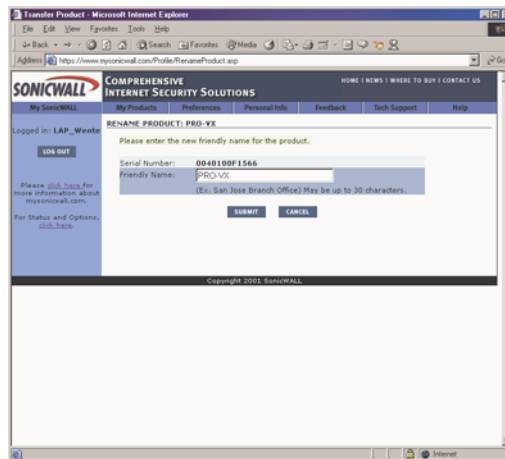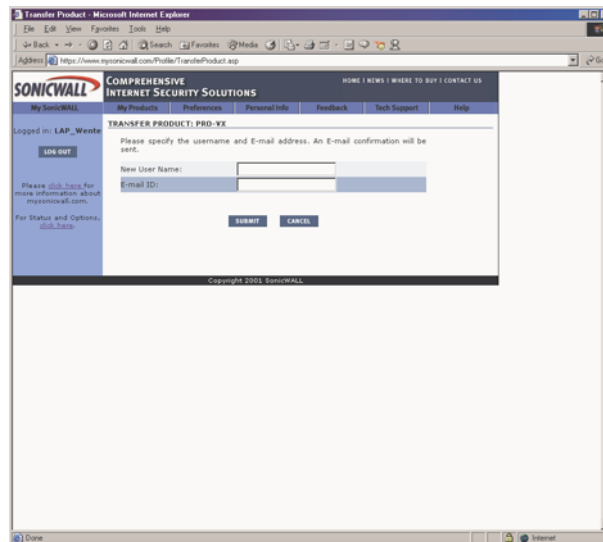
After clicking **Submit**, a new page appears with the message that you have successfully renamed your SonicWALL.
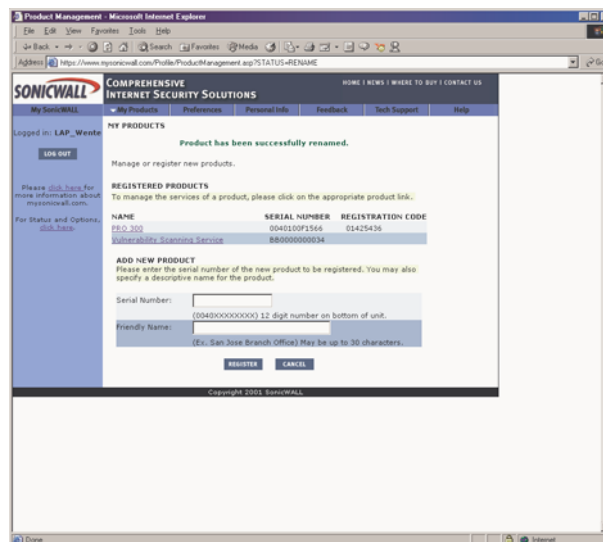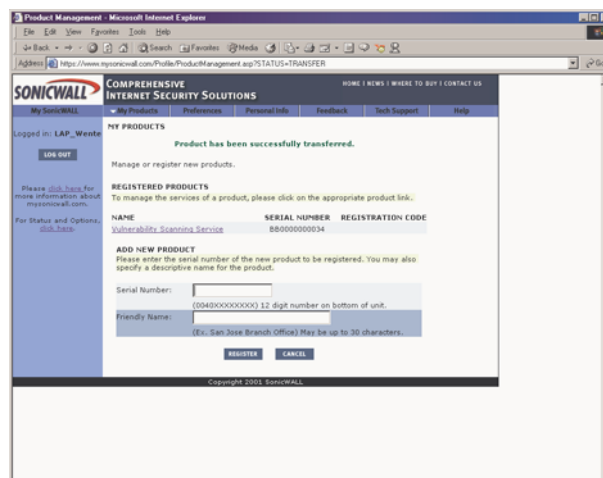
Transferring a SonicWALL Product

You can transfer a SonicWALL to another mySonicWALL.com user at any time. Transferring a SonicWALL is necessary if you sell the appliance to another user, or if you want to transfer it to another person in your company. For example, the sales manager for the East Coast has left, and you were managing the services for his SonicWALL. However, another manager may have an immediate need for the SonicWALL, and requests that you transfer the appliance to him. To transfer a SonicWALL to another user, click **Transfer** in the **Manage Product** section.

Type the **User Name** of the new owner, and the e-mail address ID in the appropriate fields. Click **Submit**. A page is returned with the message that you've successfully transferred the SonicWALL to the new user.

Also, an e-mail message is sent to both the old and new user as a notification that the appliance was transferred.
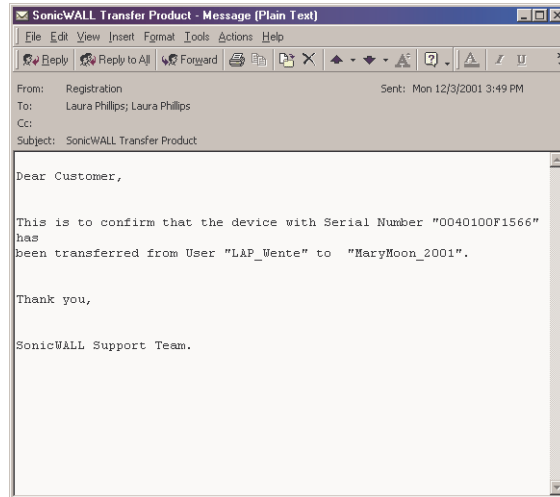
Tip! *You can only transfer a SonicWALL to another registered user of mySonicWALL.com.*

Delete Product

You can also delete a SonicWALL from your mySonicWALL.com user account. Click on the **Friendly Name** for the appliance, and then click **Delete**. A confirmation message appears in the next window, and you have successfully deleted a SonicWALL from your user account. You can add the SonicWALL back to your account at any time.

Managing Services for Your SonicWALL

In the **Applicable Services** section of mySonicWALL.com, a list of installed and inactivated services for your SonicWALL is displayed.
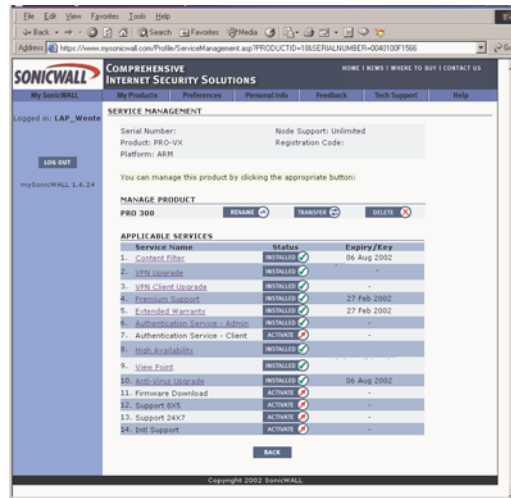
Activated services are indicated by the **Installed** icon with a green check mark.

Inactive services are indicated by the **Activate** icon with a red arrow.

Activated service names are also hyperlinked to an information page with **Activation Status** and the **Expiration Date** of the service. Services can also be renewed by clicking on the name, and entering the activation key into the **Activation Key** field.
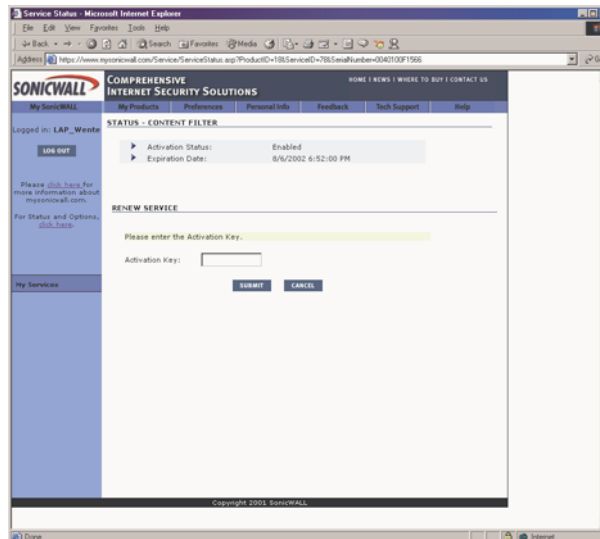
Activating Services Using mySonicWALL.com

To activate a service such as **Content Filter**, use the following steps:

1. Log into mySonicWALL.com using your username and password. Select the appliance to be upgraded with the **Content Filter List** subscription, and click the name.

2. Click **Activate** next to **Content Filter**. The following screen appears with an **Activation Key** field, and a **Terms and Conditions** message.

3. Type the **Activation Key** into the **Activation Key** field, and select **I have read and agreed** to all of the above terms and conditions. Click **Submit**.

4. The **Content Filter List** subscription is now active, and you can download the **Content Filter List** through your SonicWALL appliance.

3 System

All SonicWALL management functions are performed through a Web browser using the SonicWALL management interface. Any computer on the same network as the SonicWALL can be used to access the management interface. A computer used to manage the SonicWALL is referred to as the "Management Station."

The Web browser used to access the management interface must be Java-enabled and support HTTP uploads in order to fully manage the SonicWALL. If your Web browser does not support these functions, certain features such as uploading firmware and saved preferences files are not available.

Tip! *Microsoft Internet Explorer 5.0 or higher, or, Netscape Navigator 4.5 or higher are two recommended Web browsers.*

System>Status

The **Status** page contains five sections: **System Messages, System Information, Security Services, Latest Alerts,** and **Network Interfaces**.

System Messages

Any information considered relating to possible problems with configurations on the SonicWALL such as password, log messages, etc.

System Information

The following information is displayed in this section:
- **Model** - type of SonicWALL product
- **Serial Number** - also the MAC address of the SonicWALL
- **Authentication Code** - the alphanumeric code used to authenticate the SonicWALL on the registration database at <https://www.mysonicwall.com>.
- **Firmware Version** - the firmware version loaded on the SonicWALL.
- **ROM Version** - indicates the ROM version.
- **CPU** - displays the type and speed of the SonicWALL processor.
- **Total Memory** - indicates the amount of RAM and flash memory.
- **Uptime** - the length of time, in days, hours, and seconds the SonicWALL is active.
- **Current Connections** - the number of network connections currently existing on the SonicWALL.

Security Services

A list of available SonicWALL services are listed in this section with the status of unsubscribed or subscribed. Services requiring subscriptions include Content Filtering Service, Anti-Virus, E-mail Filtering, and ViewPoint. Clicking the blue arrow displays the **System>Licenses** page.

Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the blue arrow displays the **Log>Log View** page.

Network Interfaces

The following information is contained in this section:
- **(X0) LAN** - network speed and network address mode
- **(X1) WAN** - network speed, for example 100 Mbps, and devices connected to the WAN link.
- **X2** through **X5** - user-defined interfaces

Clicking the blue arrow displays the **Network>Settings** page.

System>Licenses

The **System>Licenses** page provides links to activate, upgrade, or renew services. It also has links to free trials of SonicWALL services.
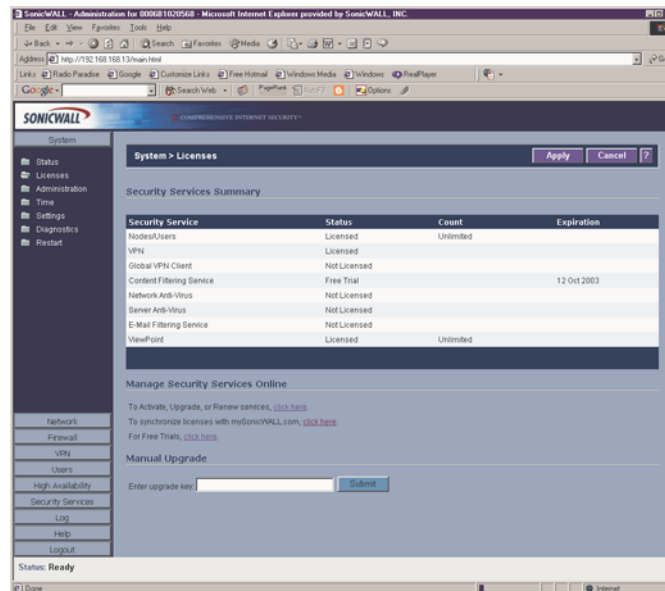
Security Services Summary

The **Security Services Summary** table lists the available and activated security services on the SonicWALL. The Security Service column lists all the available SonicWALL security services and upgrades available for the SonicWALL. The Status column indicates is the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**). The number of nodes/users allowed for the license is displayed in the **Count** column.

The information listed in the Security Services Summary table is updated from your mySonicWALL.com account the next time the SonicWALL automatically synchronizes with your mySonicWALL.com account (once a day) or you can click the link in **To synchronize licenses with mySonicWALL.com click here** in the **Manage Security Services Online** section.

Manage Security Service Online

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**. Click the link in **To synchronize licenses with mySonicWALL.com click here** to synchronize your mySonicWALL.com account with the **Security Services Summary** table.

You can also get free trial subscriptions to SonicWALL Content Filter Service and Network Anti-Virus by clicking the **For Free Trials click here link**. When you click these links, the

mySonicWALL.com Login page is displayed. Enter your mySonicWALL.com account username and password in the **User Name** and Password fields and click Submit. The **Manage Services Online** page is displayed with licensing information from your mySonicWALL.com account.

Manual Upgrade

Manual Upgrade allows you to activate your services by typing the service activation key supplied with the service subscription not activated on mySonicWALL.com. Type the activation key from the product into the **Enter upgrade key** field and click **Submit**.

System>Administration
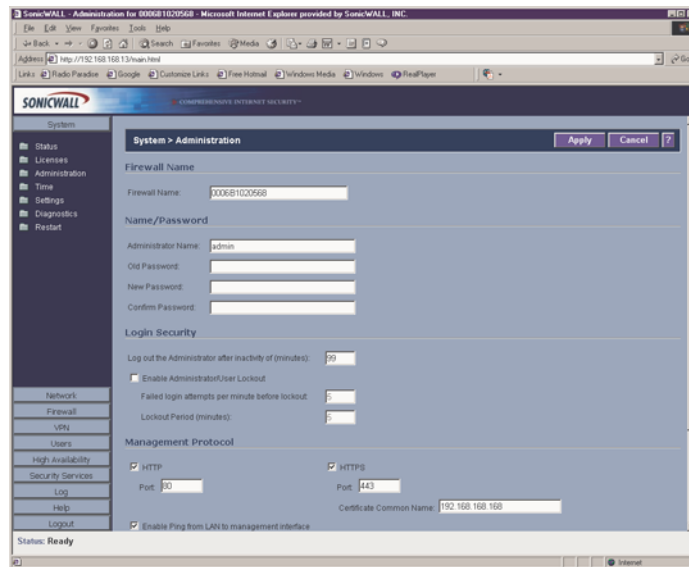
Firewall Name

The **Firewall Name** uniquely identifies the SonicWALL and defaults to the serial number of the SonicWALL. The serial number is also the MAC address of the unit. To change the Firewall Name, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length.

Name/Password

Administrator Name

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length. To create an new administrator name, type the new name in the **Administrator Name** field. Click **Apply** for the changes to take effect on the SonicWALL.

Changing the Administrator Password

To set the password, Type the old password in the **Old Password** field, and the new password in the **New Password** field. Type the new password again in the **Confirm New Password** field and click **Apply**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Login Security

The **Log out the Administrator Inactivity Timeout after inactivity of (minutes)** setting allows you to set the length of inactivity time that elapses before you are automatically logged out of the Management Interface. By default, the SonicWALL logs out the administrator after 5 minutes of inactivity. The inactivity timeout can range from 1 to 99 minutes. Click **Apply**, and a message confirming the update is displayed at the bottom of the browser window.

Tip!   *If the Administrator Inactivity Timeout is extended beyond 5 minutes, you should end every management session by clicking Logout to prevent unauthorized access to the SonicWALL Web Management Interface.*

You can configure the SonicWALL to lockout an administrator or a user if the login credentials are incorrect. Select the **Enable Administrator/User Lockout on login failure** checkbox to prevent users from attempting to log into the SonicWALL without proper authentication credentials. Type the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field. Type the length of time that must elapse before the user attempts to log into the SonicWALL again in the **Lockout Period (minutes)** field.

Alert!   *If the administrator and a user are logging into the SonicWALL using the same source IP address, the administrator is also locked out of the SonicWALL. The lockout is based on the source IP address of the user or administrator.*

Web Management Server

The SonicWALL can be managed using HTTP or HTTPS and a Web browser. Both HTTP and HTTPS are enabled by default. The default port for HTTP is port 80, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Apply**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL. For example, if you configure the port to be 76, then you must type <LAN IP Address>:76 into the Web browser, i.e. <http://192.168.168.1:76>

The default port for HTTPS management is 443, the standard port. You can add another layer of security for logging into the SonicWALL by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you
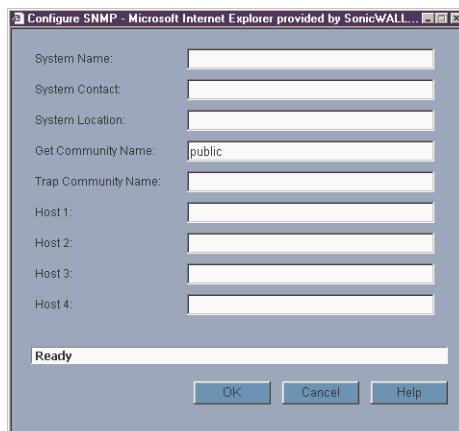
must log into the SonicWALL using the port number as well as the IP address, for example, <https://192.168.168.1:700> to access the SonicWALL.

The **HTTPS Management Certificate Common Name** field defaults to the SonicWALL LAN Address. This allows you to continue using a certificate without downloading a new one each time you log into the SonicWALL.

Advanced Management

Enable SNMP

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWALL and receive notification of critical events as they occur on the network. The SonicWALL supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egp** and **at**. The SonicWALL replies to SNMP Get commands for MIBII via any interface and supports a custom SonicWALL MIB for generating trap messages. The custom SonicWALL MIB is available for download from the SonicWALL Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC. To enable SNMP on the SonicWALL, log into the Management interface and click **System**, then Administration. Select the **Enable SNMP** checkbox, and then click **Configure**.

1. Type the host name of the SonicWALL in the **System Name** field.

2. Type the network administrator's name in the **System Contact** field.

3. Type an e-mail address, telephone number, or pager number in the **System Location** field.

4. Type a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.

5. Type a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.

6. Type the IP address or host name of the SNMP management system receiving SNMP traps in the Host 1 through Host 4 fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.

7. Click **OK**.

Configuring Log/Log Settings for SNMP

Trap messages are generated only for the alert message categories normally sent by the SonicWALL. For example, attacks, system errors, or blocked Web sites generate trap messages.

If none of the categories are selected on the **Log Settings** page, then no trap messages are generated.

Configuring SNMP as a Service and Adding Rules

By default, the SonicWALL responds only to **Get SNMP** messages received on its LAN interface. Appropriate rules must be configured to allow SNMP traffic to and from the WAN interface. SNMP trap messages can be sent via the LAN or WAN. See Chapter 6, **Firewall**, for instructions on adding services and rules to the SonicWALL.

If your SNMP management system supports discovery, the SonicWALL agent automatically discover the SonicWALL appliance on the network. Otherwise, you must add the SonicWALL to the list of SNMP-managed devices on the SNMP management system.

Enable Management Using SonicWALL GMS

You can configure the SonicWALL to be managed by SonicWALL Global Management System (GMS). Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS** window is displayed.

1. Type the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.

2. Type the port in the GMS Syslog Server Port field. The default value is 514.

3. Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.

4. Select **GMS over VPN** if the SonicWALL is managed through a VPN connection. Use the information in the Security Association Information section to configure the SA in GMS.

5. Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.

6. Click **OK**. The SonicWALL is now managed by GMS.

System>Time

Set Time

The SonicWALL uses the time and date feature to timestamp log events, automatically update Content Filtering Services, and other internal purposes.

To configure the time settings on the SonicWALL, click **System**, then **Time**.
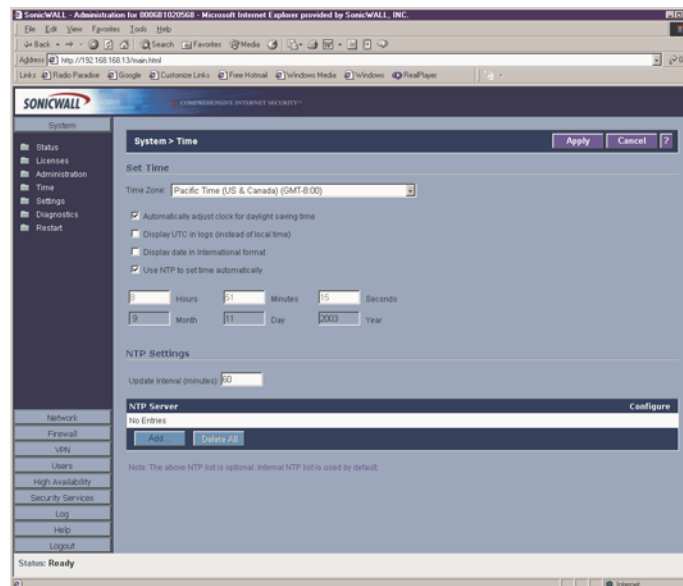
1. Select your time zone from the **Time Zone** list.

2. Click **Apply** to update the SonicWALL.

You can also select **Automatically adjust clock for daylight savings time changes**, **Display UTC in logs (instead of local time)**, **Display time in International format**, and

Use NTP to set time automatically. **Automatically adjust clock for daylight savings time changes** and **Use NTP to set time automatically** are selected by default.

To set the time and date manually, clear the check boxes and type the time, in 24-hour format, and the date.

NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond. The SonicWALL has an internal list of NTP servers so manually entering a NTP server is optional.

Select **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL clock. You can also configure **Update Interval (minutes)** for the NTP server to update the SonicWALL. The default value is 60 minutes.

To add an NTP server to the SonicWALL configuration, click **Add**. The **Add NTP Server** window is displayed. Type the IP address of an NTP server in the **NTP Server** field. Click **Ok**. Then click **Apply** on the **System>Time** page to update the SonicWALL. To delete an NTP server, highlight the IP address and click **Delete**. Or, click Delete All to delete all servers.

System>Settings
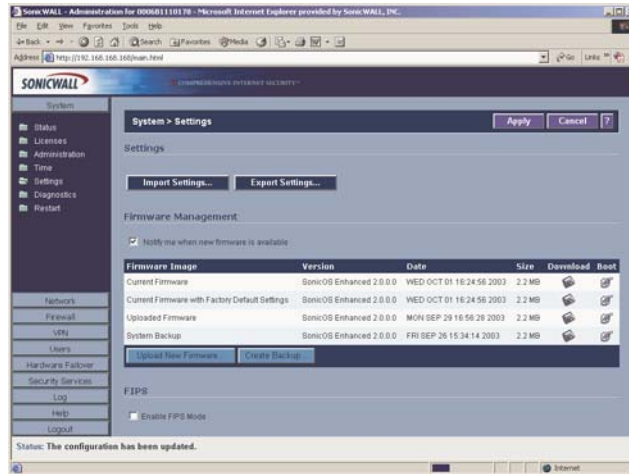
Settings

Import Settings

To import a previously saved preferences file into the SonicWALL, follow these instructions:

1. Click **Import Settings** to import a previously exported preferences file into the SonicWALL. The **Import Settings** window is displayed.

2. Click **Browse** to locate the file which has a *.exp file name extension.

3. Select the preferences file.

4. Click **Import**, and restart the firewall.

Export Settings

To export configuration settings from the SonicWALL, use the instructions below:

1. Click **Export Settings**.

2. Click **Export**.

3. Click **Save**, and then select a location to save the file. The file is named "sonicwall.exp" but can be renamed.

4. Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWALL if it is necessary to reset the firmware.

Firmware Management

The Firmware Management section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.
- Easily return your SonicWALL to the previous system state.

Note: SonicWALL **SafeMode**, which uses the same settings used **Firmware Management**, provides quick recovery from uncertain configuration states. Pressing the Reset button on the SonicWALL for one second launches the SonicWALL into SafeMode, which allows you to select the firmware version to load and reboot the SonicWALL. Once the SonicWALL has entered SafeMode, the SonicWALL SafeMode page provides the functionality of the **Firmware Management** section of the **System>Settings** page.

Automatic Notification of New Firmware

To receive automatic notification of new firmware, select the **Notify me when new firmware is available** check box. If you enable this feature, the SonicWALL sends a status message to the SonicWALL firmware server daily with the following information:

- **SonicWALL Serial Number**
- **Product Type**
- **Current Firmware Version**
- **Language**
- **Currently Available Memory**
- **ROM Version**
- **Options and Upgrades**

Alert! *After the initial 90 days from purchase, firmware updates are available only to registered users with a valid support contract. You must register your SonicWALL at <https://www.mysonicwall.com>.*

If a new firmware version becomes available, the message New SonicWALL Firmware Version is available. Click here for details on this latest release appears in System Messages on the System>Status page. Clicking the here link displays the Release Notes for the new firmware.

Firmware Management Table

The Firmware Management table displays the following information:
- **Firmware Image** - In this column, four types of firmware images are listed:
- **Current Firmware** - firmware currently loaded on the SonicWALL.
- **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the SonicWALL to its default IP addresses, username, and password.
- **Uploaded Firmware** - the latest version uploaded from mySonicWALL.com.
- **System Backup** - a firmware image created by clicking Create Backup.
- **Version** - the firmware version.
- **Date** - the day, date, and time of downloading the firmware.
- **Size** - the size of the firmware file in Megabytes (MB).
- **Download** - clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - clicking the icon reboots the SonicWALL with the firmware version listed in the same row.

⚠️

Alert! Clicking Boot next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image.

Updating Firmware Manually

Click **Upload New Firmware** to upload new firmware to the SonicWALL. The Upload Firmware window is displayed. Browse to the firmware file located on your local drive. Click **Upload** to upload the new firmware to the SonicWALL.

Creating a Backup Firmware Image

When you click **Create Backup**, the SonicWALL takes a "snapshot" of your current system state, firmware and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing **System Backup** firmware image as necessary.

FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWALL supports FIPS-Compliant security. Among the FIPS-compliant features of the SonicWALL include PRNG based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

Select **Enable FIPS Mode** to enable the SonicWALL to comply with FIPS. When you check this setting, a dialog box is displayed with the following message: **Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed**. Click Clicking Boot next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.. The SonicWALL reboots in FIPS Mode.

To return to normal operation, uncheck the **Enable FIPS Mode** check box. The SonicWALL reboots into non-FIPS mode.

⚠️

Alert! When using the SonicWALL for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWALL must remain in place and untouched.

System>Diagnostics

The SonicWALL has several diagnostic tools which help troubleshoot network problems. Click **System** on the menu bar, and then click **Diagnostics**.
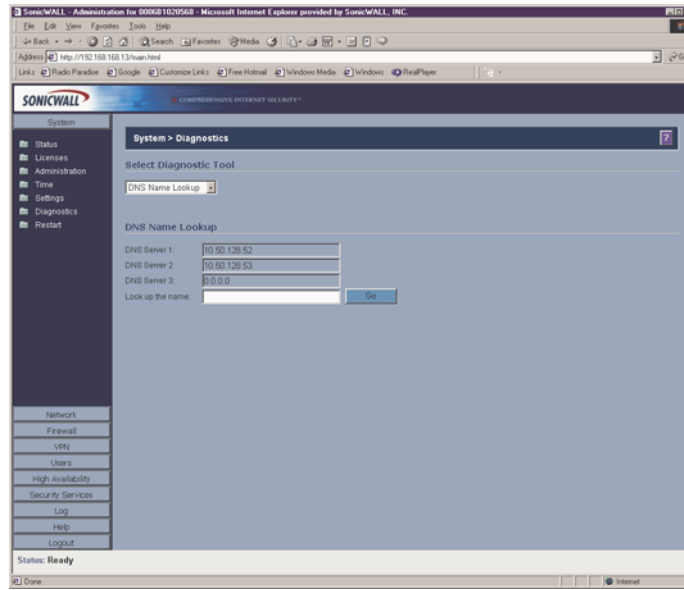
Select Diagnostic Tool

DNS Name Lookup

The SonicWALL has a DNS lookup tool that returns the IP address of a domain name. Or, if you type an IP address, it returns the domain name for that address.

1. Type the host name or IP address in the **Look up name** field. Do not add http to the host name.

2. The SonicWALL queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.

The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the SonicWALL. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network>Settings** page.

Find Network Path

Find Network Path indicates if an IP host is located on the WAN, DMZ, LAN, or other zone. This can diagnose a network configuration problem on the SonicWALL. For example, if the SonicWALL indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured. **Find Network Path** can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

1. Select **Ping** from the **Diagnostic Tool** menu.

2. Type the IP address or host name of the target device and click **Go**.

3. If the test is successful, the SonicWALL returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Packet Trace

The **Packet Trace** tool tracks the status of a communications stream as it moves from source to destination. This is a useful tool to determine if a communications stream is being stopped at the SonicWALL, or is lost on the Internet.

To interpret this tool, it is necessary to understand the three-way handshake that occurs for every TCP connection. The following displays a typical three-way handshake initiated by a host on the SonicWALL LAN to a remote host on the WAN.

1. TCP received on LAN [SYN]

   From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   The SonicWALL receives SYN from LAN client.

2. TCP sent on WAN [SYN]

   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   The SonicWALL forwards SYN from LAN client to remote host.

3. TCP received on WAN [SYN,ACK]

   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)
   To 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

   The SonicWALL receives SYN,ACK from remote host.

4. TCP sent on LAN [SYN,ACK]

   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)
   To 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

   The SonicWALL forwards SYN,ACK to LAN client.

5. TCP received on LAN [ACK]

   From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   Client sends a final ACK, and waits for start of data transfer.

6. TCP sent on WAN [ACK]

   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

   The SonicWALL forwards the client ACK to the remote host and waits for the data transfer to begin.

When using packet traces to isolate network connectivity problems, look for the location where the three-way handshake is breaking down. This helps to determine if the problem resides with the SonicWALL configuration, or if there is a problem on the Internet.

Select **Packet Trace** from the **Diagnostic tool** menu.

Tip!   *Packet Trace requires an IP address. The SonicWALL DNS Name Lookup tool can be used to find the IP address of a host.*

7. Type the IP address of the remote host in the **Trace on IP address** field, and click **Start**. You must type an IP address in the **Trace on IP address** field; do not type a host name, such as "www.yahoo.com". The **Trace is off** turns from red to green with Trace Active displayed.

8. Contact the remote host using an IP application such as Web, FTP, or Telnet.

9. Click **Refresh** and the packet trace information is displayed.

10. Click **Stop** to terminate the packet trace, and **Reset** to clear the results.

Captured Packets

The **Captured Packets** table displays the packet number and the content of the packet, for instance, *ARP Request send on WAN 42 bytes*.

Packet Detail

Select a packet in the **Captured Packets** table to display packet details. Packet details include the packet number, time, content, source of the IP address, and the IP address destination.

Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWALL configuration and status, and saves it to the local hard disk. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.

Alert!   *You must register your SonicWALL on mySonicWALL.com to receive technical support.*

Before e-mailing the Tech Support Report to the SonicWALL Technical Support team, complete a Tech Support Request Form at <https://www.mysonicwall.com>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWALL Technical Support to provide you with better service.

In the **Tools** section, select **Tech Support Report** from the **Select a diagnostic tool** menu. Four **Report Options** are available in the **Tech Support Report** section:

• **VPN Keys** - saves shared secrets, encryption, and authentication keys to the report.

• **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses.

• **DHCP Bindings** - saves entries from the SonicWALL DHCP server.

- **IKE Info** - saves current information about active IKE configurations.

Generating a Tech Support Report

1. Select **Tech Support Report** from the **Choose a diagnostic tool** menu.

2. Select the **Report Options** to be included with your e-mail.

3. Click **Save Report** to save the file to your system. When you click **Save Report**, a warning message is displayed.

4. Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.

Trace Route

Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

Type the IP address or domain name of the destination host. For example, type yahoo.com and click **Go**.

A second window is displayed with each hop to the destination host.

By following the route, you can diagnose where the connection fails between the SonicWALL and the destination.

System>Restart
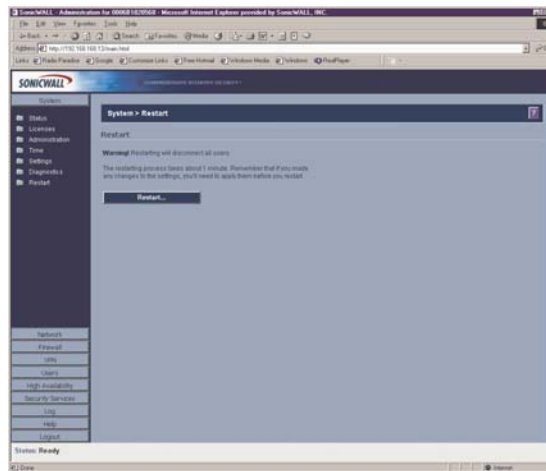
Click **Restart** to display the **System>Restart** page. The SonicWALL can be restarted from the Web Management interface. Click **Restart SonicWALL** and then click **Yes** to confirm the restart.

The SonicWALL takes approximately three minutes to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

4 Network

This chapter describes the Network section of the management interface and the configuration of the SonicWALL Internet Security appliance Network settings. The **Network** menu includes

- **Interfaces** - configure logical interfaces for connectivity.
- **WAN Failover and Load Balancing** - configure one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
- **Zones** - configure security zones on your network.
- **DNS** - set up DNS servers for name resolution.
- **Address Objects** - configure host, network, and address range objects.
- **Routing** - view the **Route Table**, **ARP Cache** and configure static and dynamic routing by interface.
- **NAT Policies** - create NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
- **ARP** - view the ARP settings and clear the ARP cache as well as configure ARP cache time.
- **DHCP Server -** configure the SonicWALL as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.
- **IP Helper** - configure the SonicWALL to forward DHCP requests originating from the interfaces on the SonicWALL to a centralized server on behalf of the requesting client.
- **Web Proxy** - configure the SonicWALL to automatically forward all Web proxy requests to a network proxy server.

Network>Interfaces

After creating a Zone, the next step is to configure an interface. You must configure an interface and bind it to a zone.
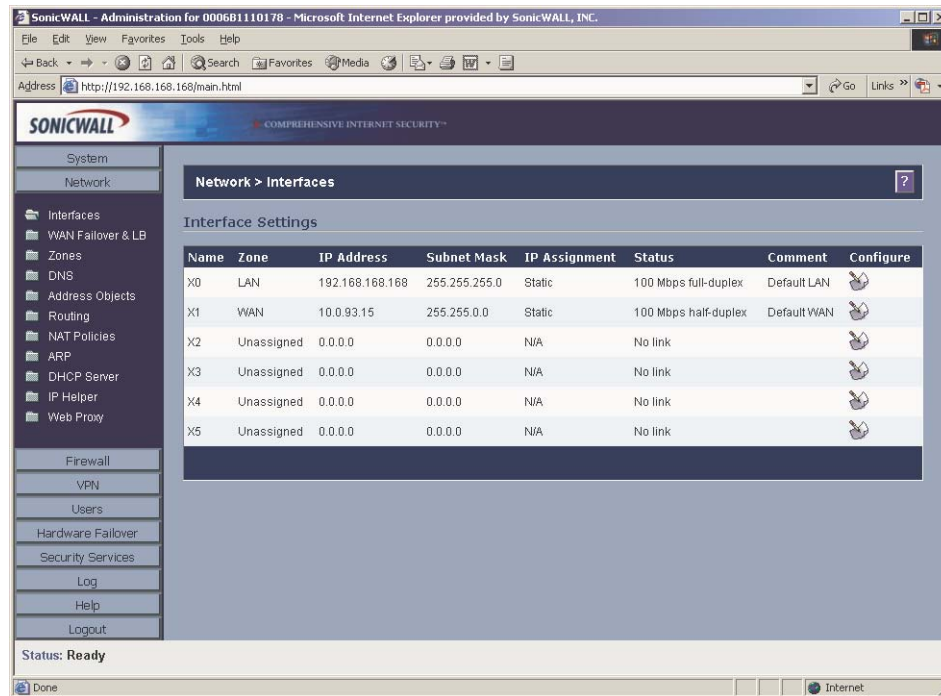
Physical Interfaces

Physical interfaces must be assigned to a Zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

The first two interfaces, X0(LAN) and X1(WAN) are fixed interfaces, permanently bound to the Trusted and Untrusted Zone types. The remaining four interfaces, X2, X3, X4, and X5, can be configured and bound to any Zone type.

Note: *The Untrusted Zone type can only have two members, one of which is the fixed interface, X1.*

Interface Settings

The **Interface Settings** table lists the following information for each interface:

Name - listed as X0, X1, X2, X3, X4, and X5.

Zone - LAN, DMZ and WAN are listed by default. As zones are configured, the names are listed in this column.

IP Address - IP address assigned to the interface.

Subnet Mask - the network mask assigned to the subnet.

IP Assignment - select from **DHCP** or **Static**.

Status - the link status and speed.

Comment - any user-defined comments.

Configure - click the icon to configure any of the interfaces.

Select one of the interfaces from the **Zone** list. The **Edit Interface** window is then populated with the appropriate fields to enter information.

Network > WAN Failover and Load Balancing

With this feature, one of the user-defined interfaces can be configured 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.
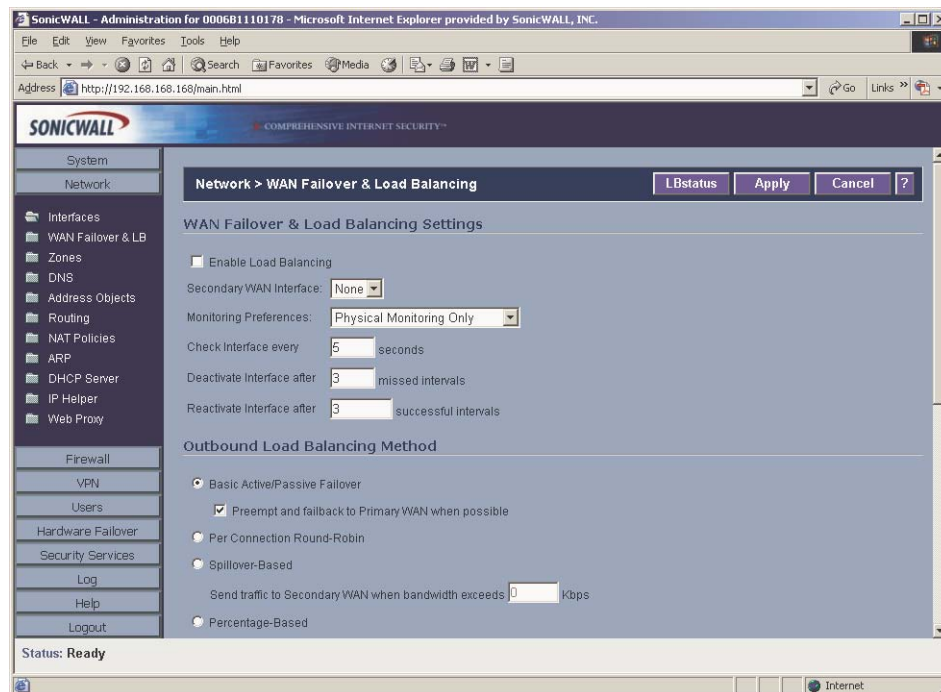
This feature also allows you to perform simple load balancing for the WAN traffic on the SonicWALL. You can select a method of dividing the outbound WAN traffic between the two WAN ports and balance network traffic.

The SonicWALL can monitor WAN traffic using Physical Monitoring which detects if the link is unplugged or disconnected, or Physical and Logical Monitoring, which monitors traffic at a higher level, such as upstream connectivity interruptions.

⚠️
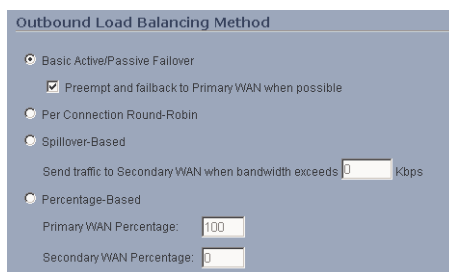
Alert! *Before you begin, be sure you have configured a user-defined interface to mirror the WAN port settings.*

WAN Failover and Load Balancing Settings

To configure the SonicWALL for load balancing, follow the steps below:

1. Select **Enable Load Balancing**.

2. From the **Secondary WAN Interface** menu, select your secondary WAN interface.

3. Enter a number between 5 and 300, in the **Check Interface Every _ Seconds** field. The default value is 5 seconds.

4. In the **Deactivate Interface after _ missed intervals**, enter a number between 1 and 10. The default value is 3. If the default value is used, then the interface is considered inactive after 3 successive attempts at 5 seconds each.

5. Enter a number between 1 and 10 in the **Reactivate Interface after _ successful intervals**. If the default value is used, then the interface is considered active after 3 successive attempts at 5 seconds each.

Outbound Load Balancing Method

By default, **Basic Active/Passive Failover** is selected with **Preempt and failback to Primary WAN when possible** selected. Basic Active Failover only sends traffic through the secondary WAN when the primary WAN becomes inactive. Because **Preempt and failback to Primary WAN when possible** is selected, the secondary WAN becomes inactive when the primary WAN is detected as active.

Selecting **Per Connection Round-Robin** as the **Outbound Load Balancing Method** allows the SonicWALL to load balance outgoing traffic on a per-destination basis by examining source and destination IP addresses.

Tip! *Per Connection Round-Robin can be overridden by specific static route entries.*

Selecting **Spillover-based** as the **Outbound Load Balancing Method** allows you to specify when the SonicWALL starts sending traffic through the secondary WAN interface. Spillover-based load balancing only sends traffic to the secondary WAN port when the primary WAN port traffic exceeds the value set for Kbps. Enter a bandwidth value in the **Send traffic to Secondary WAN when bandwidth exceeds __ Kbp** field.

Tip! *Spillover-based **Outbound Load Balancing Method** can be overridden by specific static route entries.*

Selecting **Percentage-based** as the **Outbound Load Balancing Method** allows you to specify the percentages of network traffic sent through the primary and secondary WAN interfaces. This method allows you to actively utilize both WAN interfaces by entering a percentage in the **Primary WAN Percentage** field. The **Secondary WAN Percentage** field automatically calculates the remaining percentage and populates the field.

Primary WAN Probe Settings

The SonicWALL sends probes to a target IP address to an "always available" target upstream device on the network, such as an ISP-side router, to monitor connectivity. Enter the IP address of the target device in the **Probe Target** field. If you have another target device, enter the IP address in the **Optional Probe** Target field.

If the Probe Target is unable to contact the target device, the interface is deactivated and traffic is no longer sent to the primary WAN.

Secondary WAN Probe Settings

The Secondary WAN Probe Settings are configured in the same manner as the Primary WAN Probe Settings.

Network > Zones

A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. There are four fixed Zone types: **Trusted**, **Untrusted**, **Public**, and **Encrypted**. **Trusted** is associated with LAN Zones. These fixed Zone types cannot be modified or deleted. A Zone instance is created from a Zone type and named accordingly, i.e Sales, Finance, etc.

Only the number of interfaces limits the number of Zone instances for Trusted and Untrusted Zone types. The Untrusted Zone type (i.e. the WAN) is restricted to two Zone instances. The Encrypted Zone type is a special system Zone comprising all VPN traffic and doesn't have any associated interfaces.
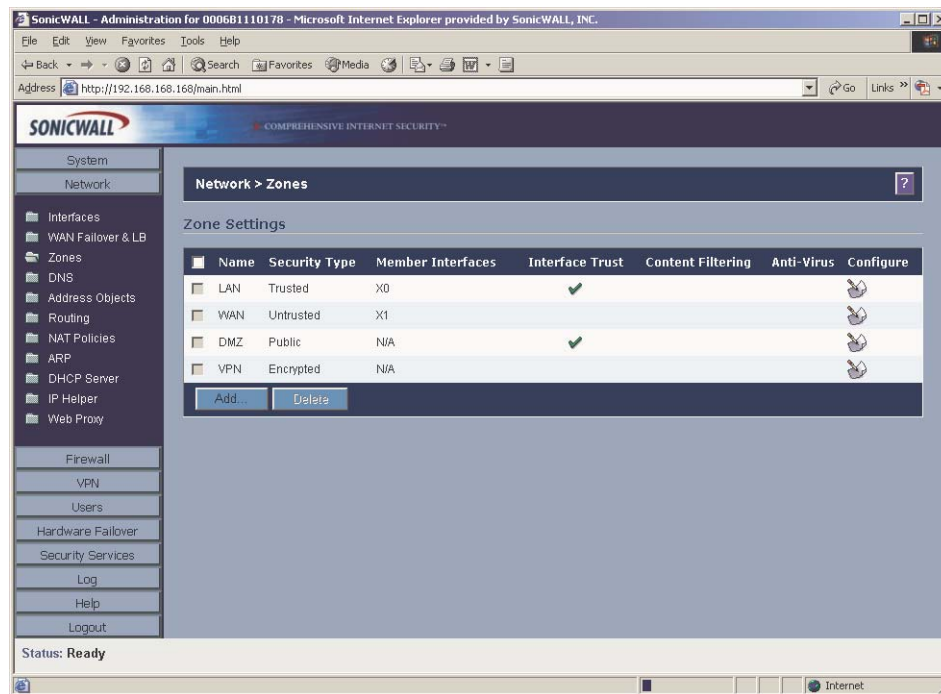
Trusted and Public Zone types offer an option, Interface Trust, to automate the creation of Access Rules to allow traffic to flow between the Interfaces of a Zone instance. For example, if the LAN Zone has interfaces X0, X3, and X5 assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these Interfaces to communicate with each other.

Enforce Content Filtering Service - Select this option to enforce content filtering on multiple interfaces in the same Trusted or Public Zones.

Enforce AV Service - Select this option to enforce anti-virus protection on multiple interfaces in the same Trusted or Public Zones.

Adding a New Zone

To add a new Zone, click **Add** under the **Zone Settings** table.
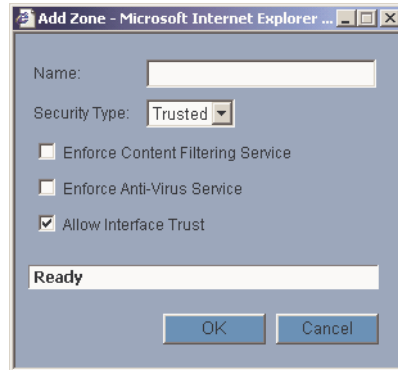
1. Type a name for the new zone in the **Name** field.

2. Select **Trusted** or **Public** from the **Security Type** menu. Use **Trusted** for Zones that you want to assign the highest level of trust, such as internal LAN segments. Use **Public** for Zones with a lower level of trust requirements, such as a DMZ Interface.

3. Select **Enforce Content Filtering Service** to enforce Internet content filtering on the Zone.

Note: *Custom Content Filtering Service policies are specified in the **Users>Local Groups** page.*

4. Select **Enforce AV Service** to enforce anti-virus protection on the Zone.

5. If you want to allow intra-zone communications, select **Allow Interface Trust**. If not, select the **Allow Interface Trust** checkbox.

6. Click **OK**. The new zone is now added to the SonicWALL.

Modifying a Zone

To modify the Zone name, the virtual route, or comments, click the **Notepad** icon next to the Zone to display the **Edit Zone** window. This window has the same settings as the **Add Zone** window. Modify the settings, and click **OK**.

Network > DNS
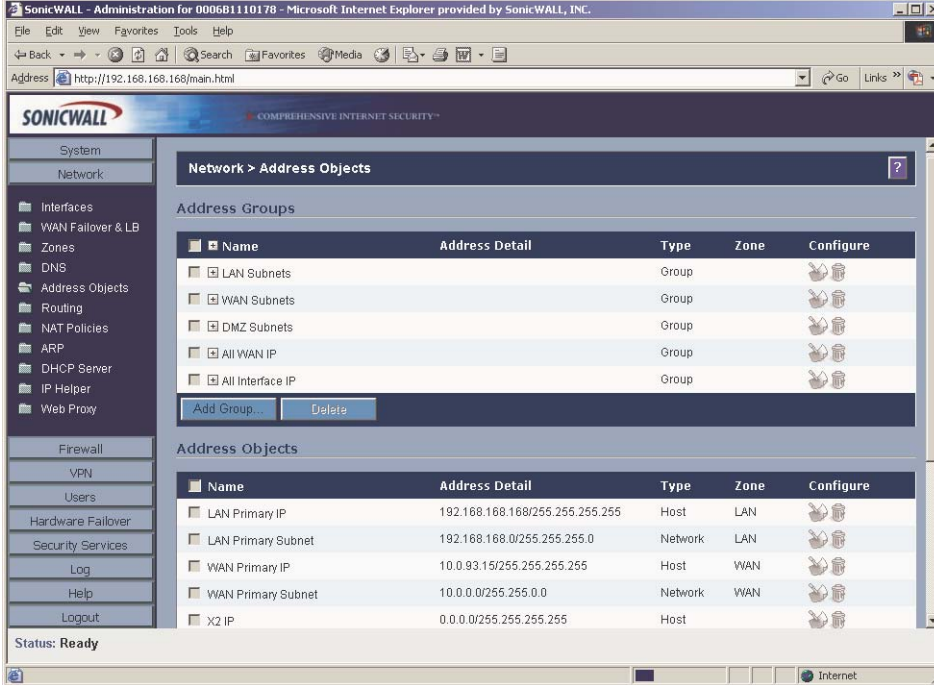
Configure the SonicWALL DNS settings manually on this page if necessary. In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields.
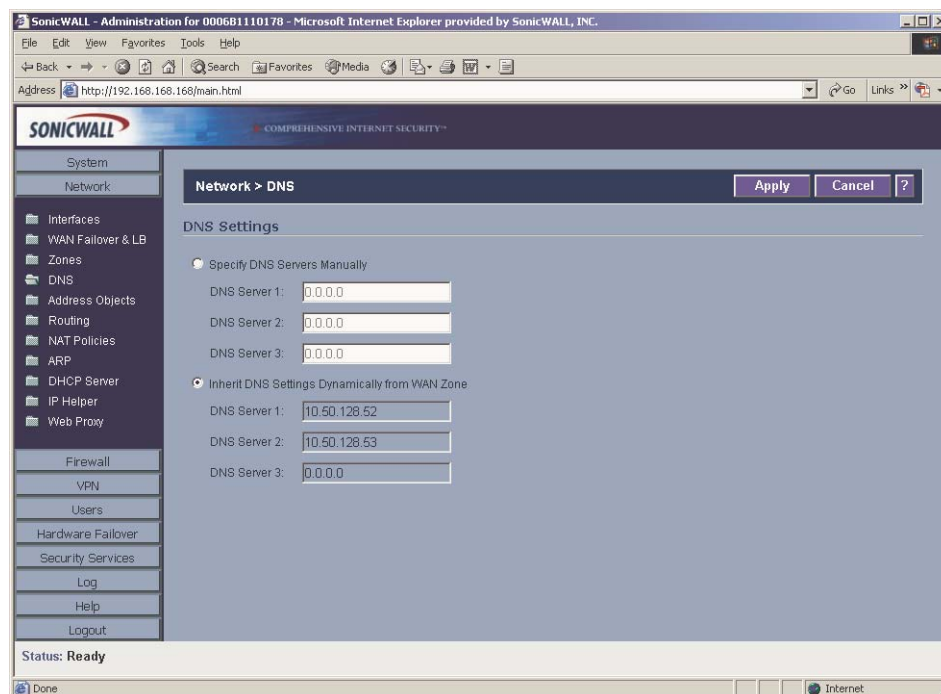
To use the DNS Settings configured for the WAN Zone, select **Inherit DNS Settings Dynamically from the WAN Zone**.

Network > Address Objects

An Address Object consists of a host, a network, or a range of IP addresses. The predefined address objects are **X0-X5 IP Address**, and **X0-X5 Subnet**. These are dynamic address objects which change as the IP address changes. If you change the IP address on an interface, the corresponding address object automatically updates to reflect the change.

Note: *An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.*

Predefined Address Objects and Groups

The Address Objects page displays the following predefined Address Objects and Address Groups:

Default Address Objects
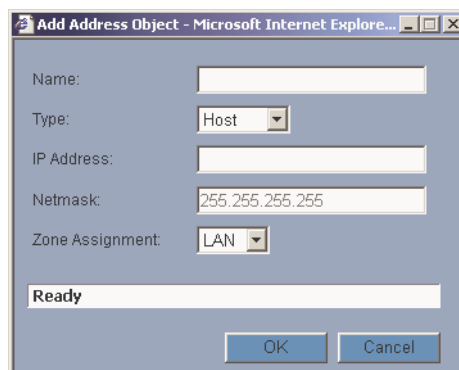
- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Remote Access Networks (VPN)
- VPN DHCP Clients

Default Address Groups

- LAN Subnets
- WAN Subnets
- DMZ Subnets
- All WAN IP
- All Interface IP

Adding an Address Object

To add an **Address Object**, click **Add** to display the **Add Address Object** window.

1. Enter a name for the Network Object in the **Name** field.

2. Select **Host** or **Range** or **Network** from the **Type** menu.

3. If you select **Host**, enter the IP address and netmask in the **IP Address** and **Netmask** fields.

4. If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

5. If you selected Network, enter the network IP address and netmask in the **Network** and **Netmask** fields.

6. Select the zone to assign to the Address Object from the **Zone Assignment** menu.

Creating Group Address Objects

As more and more Address Objects are added to the SonicWALL, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group.

To add a Group of Address Objects, click **Add Group** to display the **Add Address Object Group** window.
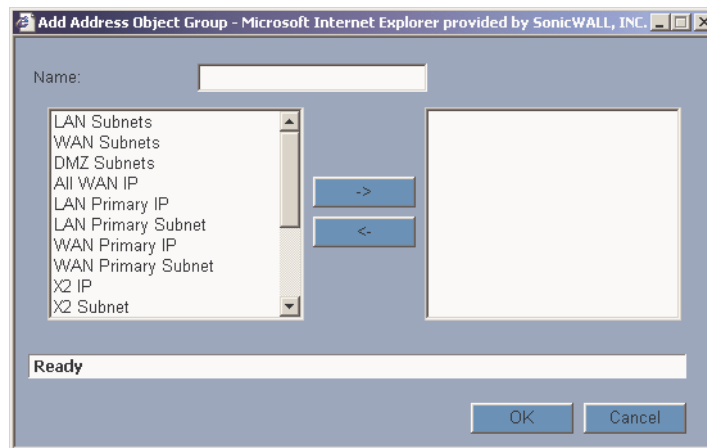
1. Create a name for the group in the **Name** field.

2. Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the Ctrl key allows you to select multiple objects.

3. Click **OK**.

Tip!   *To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.*

Network>Routing

If you have routers on your interfaces, you can configure static routes on the SonicWALL. Static routing means configuring the SonicWALL to route network traffic to a specific, predefined destination.

Static routes must be defined if the LAN, WAN, or other defined interface is segmented into subnets, either for size or practical considerations. For example, a subnet can be created to isolate a section of a company, such as finance, from network traffic on the rest of the LAN, DMZ, or WAN.
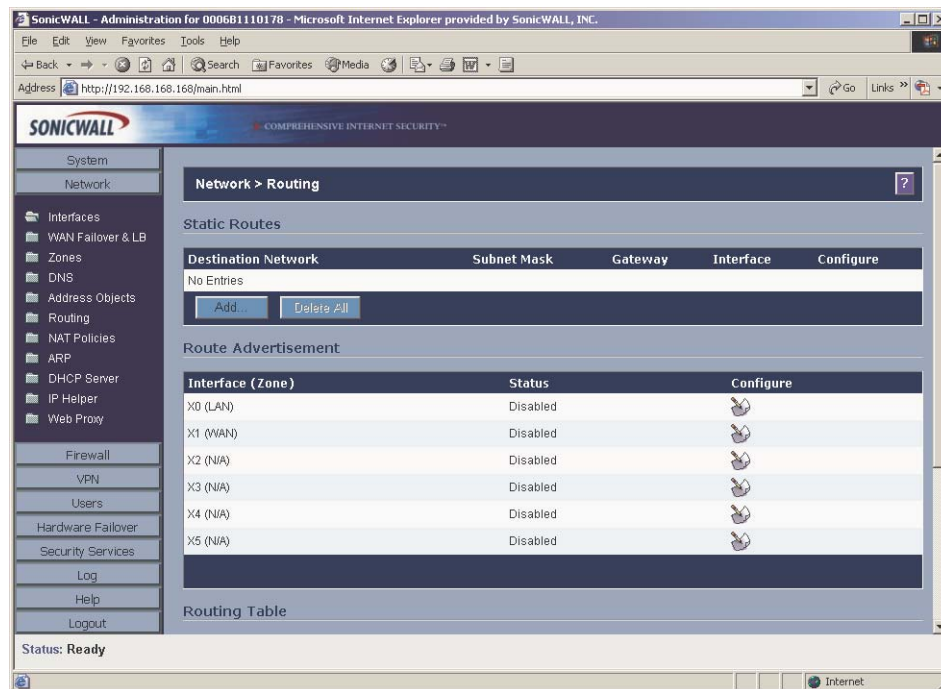
Static Routes

Static Routes are configured when network traffic is directed to subnets located behind routers on your network. For instance, you have a router on your network with the IP address of 192.168.168.254, and there is another subnet on your network with IP address range of 10.0.5.0 with a subnet mask of 255.255.255.0. To configure a static route to the 10.0.5.0 subnet, follow these instructions:

1. Click **Network**, then **Routing**.

2. Click **Add** in the **Static Routes** section.

3. Type 10.0.5.0 in the **Destination Network** field.

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

5. Type 192.168.168.254 in the **Default Gateway** field. This is the IP address of the router.

6. Select **LAN** from the **Interface** menu.

7. Click **OK.**

💡

Tip!   *You can configure up to 512 routes on the SonicWALL.*

Static Route Configuration Example

Static Route configurations allow for multiple subnets separated by an internal (LAN) router to be supported behind the sonicwall LAN. This option is only be used when the secondary subnet is accessed through an internal (LAN) router that is between it and the SonicWALL LAN port. Once static routes are configured, network traffic can be directed to these subnets.

Key terms:

- **Destination Network**: the network IP address of the remote subnet. The address usually ends in 0, i.e 10.0.5.0.
- **Subnet Mask**: the subnet mask of the remote network (i.e. 255.255.255.0)
- **Gateway**: the IP address of the Internal (LAN) router that is local to the sonicwall.

For example:

SW LAN IP ADDRESS: 192.168.168.1
Subnet mask: 255.255.255.0
Router IP ADDRESS: 192.168.168.254
Secondary Subnet: 10.0.5.0
Subnet mask: 255.255.255.0

If you have an Internal (LAN) router on your network with the IP address of 192.168.168.254, and there is another subnet on your network with IP address range of 10.0.5.0 - 10.0.5.254 with a subnet mask of 255.255.255.0. To configure a static route to the 10.0.5.0 subnet, follow these instructions:

Click **Network**, and then **Routing**.

1. Click **Add** in the **Static Routes** section.

2. Type 10.0.5.0 in the **Destination Network** field.

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

4. Type 192.168.168.254 in the **Default Gateway** field. This is the IP address of the internal (LAN) router that is local to the SonicWALL.

5. Select **LAN** from the **Interface** menu.

6. Click **OK**.

💡
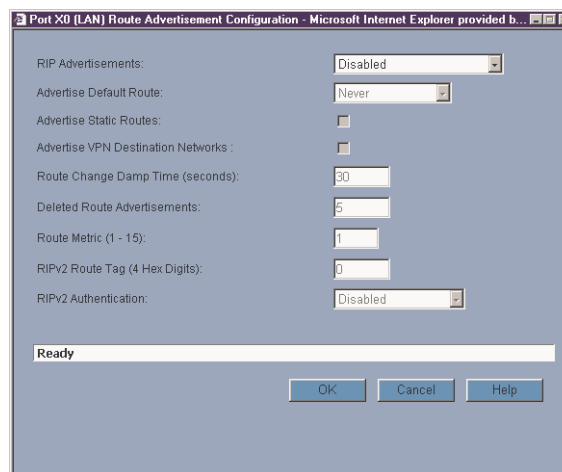
Tip!   *Make sure the Internal (LAN) router is configured as follows:*
If the SonicWALL has a NAT Policy on the WAN, the internal (LAN) router needs to have a route of last resort (i.e. gateway address) that is the SonicWall LAN IP address.

Route Advertisement

The SonicWALL uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWALL and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

To enable Route Advertisement, click the Notepad icon in the **Configure** column for each interface.

1. Select one of the following types of RIP Advertisements:

   - **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
   - **RIPv2 Enabled (multicast)** - to send route advertisements using multicasting (a single data packet to specific notes on the network).
   - **RIPv2 Enabled (broadcast)** - to send route advertisements using broadcasting (a single data packet to all nodes on the network).

2. Select **Never**, or **When WAN is up**, or **Always** from the **Advertise Default Route** menu.

3. **Advertise Static Routes** - If you have static routes configured on the SonicWALL, enable this feature to exclude them from Route Advertisement.

4. **Advertise VPN destination networks** - select to advertise VPN networks.

   - **Route Change Damp Time (seconds**) - is the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of a temporary change in a VPN tunnel status. Enter a value in seconds between advertisements

broadcasted over the network in the Route Change Damp Time (seconds) field. The default value is 30 seconds. A lower value corresponds with a higher volume of broadcast traffic over the network.

5. **Deleted Route Advertisements** - enter the number of advertisements that a deleted route broadcasts until it stops in the Deleted Route Advertisements field. The default value is 5.

6. **Route Metric (1-15)** - Enter a value from 1 to 15 in the Route Metric field. This is the number of times a packet touches a router from the source IP address to the destination IP address.

7. **RIPv2 Route Tag (4 Hex Digits**) - If RIPv2 is selected from the Route Advertisements menu, you can enter a value for the Route Tag. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.

8. **RIPv2 Authentication** You can enable RIPv2 Authentication by selecting the type of authentication from the menu:

   • **User defined** - Enter 4 hex digits in the Authentication Type (4 hex digits) field. Enter 32 hex digits in the Authentication Data (32 Hex Digits) field.
   • **Cleartext Password** - Enter a password in the Authentication Password (Max 16 Chars) field. A maximum of 16 characters can be used to define a password.
   • **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the Authentication Key (32 hex digits) field, or use the generated key.

Routing Table

The **Route Table** is a list of destinations that the IP software maintains on each host and router. The network IP address, subnet mask, gateway address, and the corresponding link are displayed. Most of the entries are the result of configuring LAN and WAN network settings. The SonicWALL LAN and WAN IP addresses are displayed as permanently published at all times.

Network > NAT Policies

When two hosts communicate using TCP/IP on the internet, there are four parameters used in any TCP or UDP connection: Source (IP) Address, Source (TCP/UDP) Port, Destination (IP) Address, and Destination (TCP/UDP) Port. There are other protocols used on the internet which don't use port numbers; ICMP has types and they typically don't get translated in NAT policies.

For example, if Host A with a Web browser with an IP address of 192.168.168.100 communicates using HTTP with Server B, a web server on the Internet with an IP address of 64.0.0.1, the connection is from Source Address 192.168.168.1 with Source Port, possibly a dynamic value 6082, to Destination Address 64.0.0.1 with Destination Port 80, a well-known HTTP port.

This communication will not work unless the NAT device does a translation of the source IP address. If the Pro4060 has a WAN IP address of 65.5.5.5, then a default NAT policy is used to change the original source IP address of 192.168.168.100 into the routable address on the outside (65.5.5.5), required for the web server's responses to get back to the computer with the web browser. This default NAT policy for outbound traffic is explained in detail later.

You can create customized NAT policies that manipulate of the three out of the four parameters in order satisfy a number of networking requirements:

- Source IP address
- Destination IP address
- Destination Service or Port Number (called 'Service' in the NAT Policies screens).

This features allows you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously, including One-to-One, Many-to-One, Many-to-Few, and Many-to-Many, as well as IP port redirection.

- **One-to-One NAT Policy** - one IP address maps directly to another IP address. This is useful for hosting publicly accessible servers and maintaining private IP addressing.
- **Many-to-One NAT Policy** - commonly used to allow multiple hosts on your LAN to communicate with hosts on the Internet by sharing the WAN public IP address. Distinct sessions are possible via port uniqueness and NAT is maintained using a dynamic state table.This policy is enabled by default on the SonicWALL.
- **Many-to-Many NAT Policy** - a group of IP addresses maps to another group of IP addresses. This policy supports extremely large numbers of connections and can enable IP address rotation.

The NAT Policies page allows you to view your NAT Policies by **Custom Policies**, **System Policies**, or **All Policies**.

⚠️
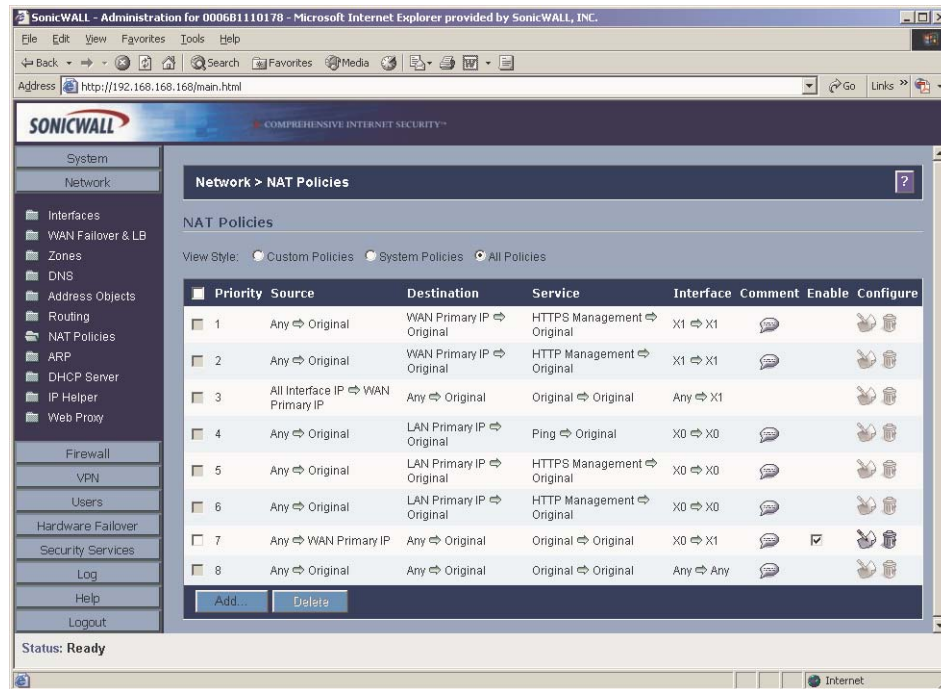
Alert!   *Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.*

💡
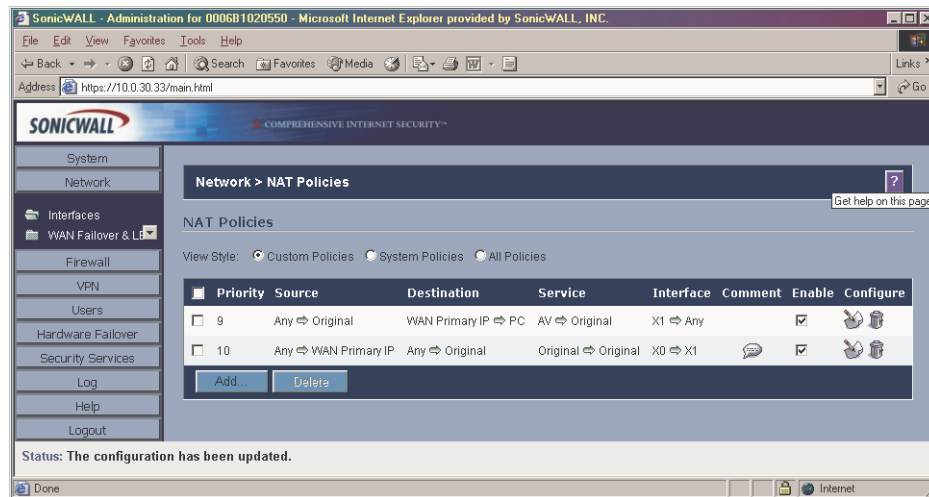
Tip!   *By default, LAN to WAN has a NAT policy predefined on the SonicWALL.*

The Default Many-to-One Outbound NAT Policy

The default Many-to-One Outbound NAT policy is visible as Any -> WAN Primary IP in either Custom Policies or All Policies. It translates any source to the WAN Primary IP as the traffic goes out to the Internet. The Destination and Service are not translated. The default policy is listed also with a source interface of X0 and a destination interface of X1. This policy allows your computers on internal interfaces in the LAN and DMZ zones to communicate with hosts on the Internet by sharing the WAN public IP address. This policy is always available, even if you want to run customized NAT policies for certain services or for certain address objects or interfaces, but it can be changed, disabled or deleted. There are other default NAT Policies created automatically which relate to the network interfaces, and to IKE VPNs. If the user has chosen make the interfaces accessible by ping, SNMP, HTTP, and/or HTTPS, or if they have enabled GroupVPN or other VPN configurations which use IKE (Key Exchange)..

There are other default NAT Policies created automatically which relate to the network interfaces, and to IKE VPNs. If the user has chosen make the interfaces accessible by ping, SNMP, HTTP, and/or HTTPS, or if they have enabled GroupVPN or other VPN configurations which use IKE (Key Exchange). The figure below shows how your System Policies page might look:
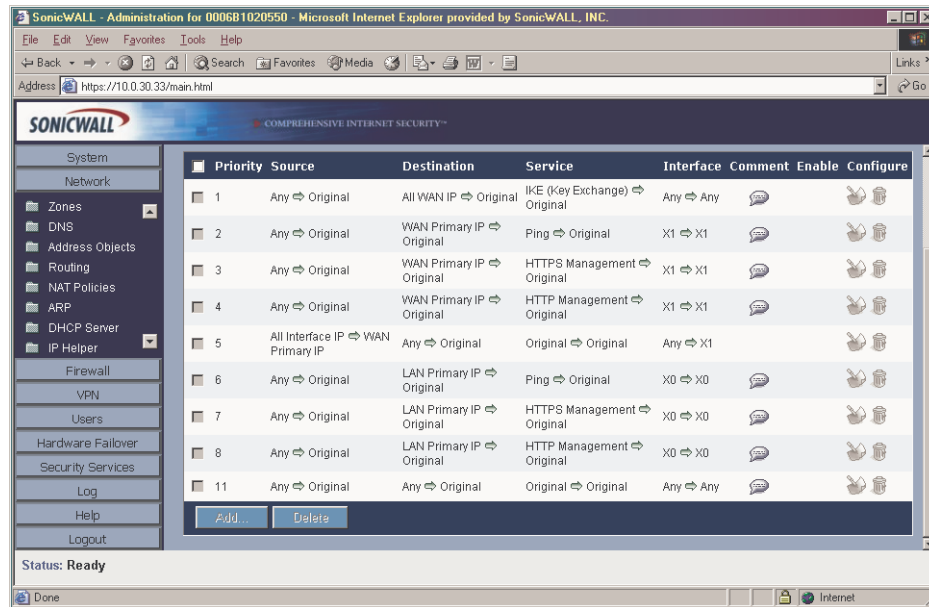
Configuring an Inbound Many-to-One NAT Policy

This is a policy for inbound traffic that forwards traffic coming in from the WAN Primary IP address to an address object on the inside (LAN or DMZ zone). This example is for a web server sitting on the X0 interface, with an address object name of '**WWWserver**.

To configure this policy, click **Network**, then **NAT Policies**. Click **Add** to display the **NAT Policy** window.

1. Select **WAN Primary IP** from the **Original Destination** menu.

2. Select **WWWserver** from the **Translated Destination** menu.

3. Select **HTTP** from the **Original Service** menu.

4. Select **Original** from the **Translated Service** menu.

5. Select **X1** from the **Source Interface** menu.

6. Select **Any** from the **Destination Source** menu.

7. Click **OK** to add the NAT policy to the SonicWALL.

Note: *The NAT policies window will not allow you to specify a destination interface when you translate the destination.*

Configuring a One-to-One NAT Policy

One-to-One NAT requires configuring two policies: one for inbound traffic and one for outbound traffic. In this example, two Address Objects are used: server_IP_private and server_IP_Public.
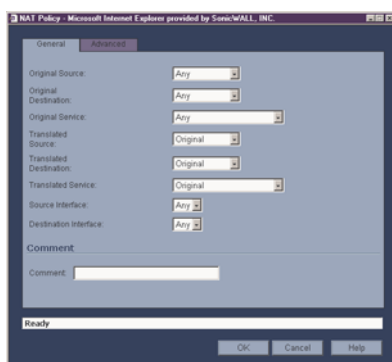
Creating an Outbound Traffic Policy

To configure a One-to-One NAT Policy, click **Network**, then **NAT Policies**. Click **Add** to display the **NAT Policy** window.

1. Select **server_IP_private** from the **Original Source** menu.

2. Select **server_IP_Public** from the **Translated Source** menu.

3. Select the physical interface for the private server from the **Source Interface** menu.

4. Select the physical interface for the public server from the **Destination Source** menu.

5. Click **OK** to add the NAT policy to the SonicWALL.

Creating an Inbound Traffic Policy

1. From the **Original Destination** menu, select **server_IP_public**.

2. Select **server_IP_private** from the **Translated Destination** menu.

3. Select **SMTP** from the **Original Service** menu.

4. Select **Original** from the **Translated Service** menu.

5. Select **X1** from the **Source Interface** menu.

6. Select **Any** from the **Destination Interface** menu.

7. Click **OK** to add the NAT policy to the SonicWALL.

Note: *The NAT policies page does not allow you to specify a destination interface when you translate the destination.*

Tip! **Enable** *is selected by default. Clear the checkbox to disable the policy after creating it.*

Network>ARP

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.
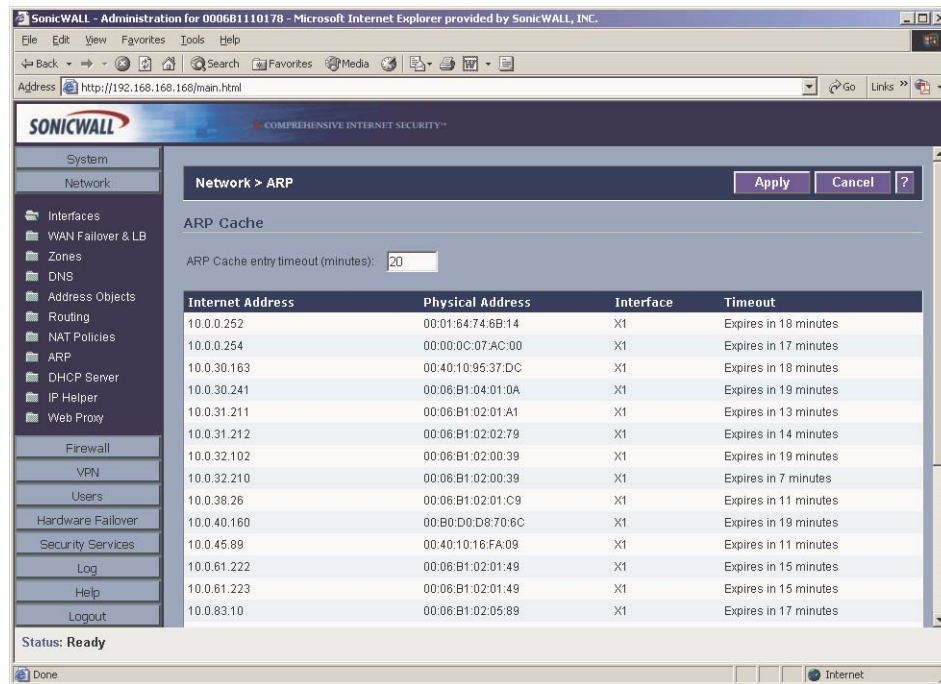
It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP** Cache to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.

Network>DHCP Server

The SonicWALL DHCP Server distributes IP addresses, subnet masks, gateway addresses, and DNS server addresses to the computers on your network.
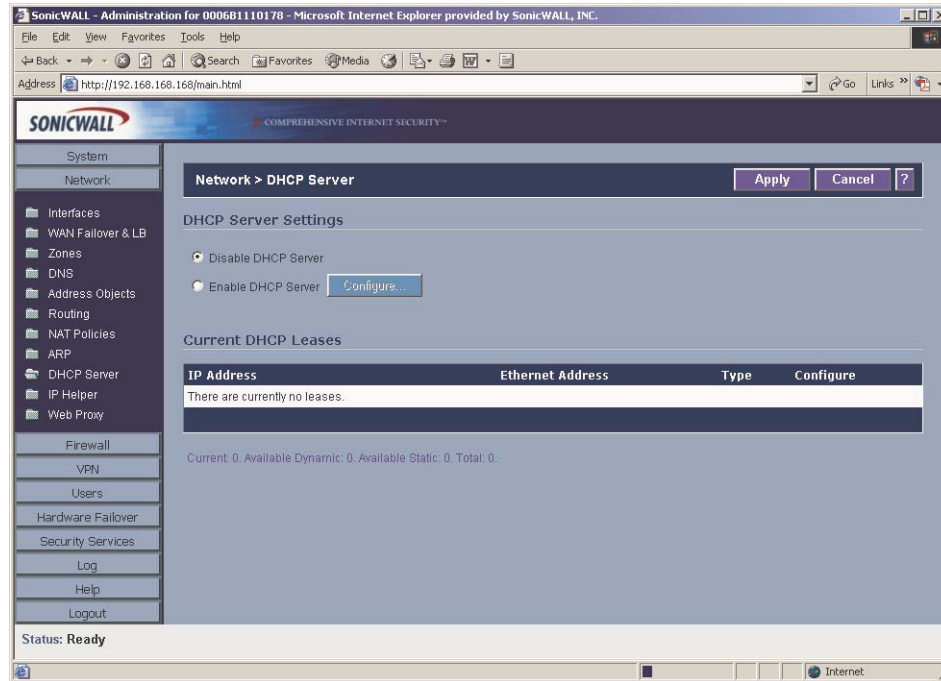
DHCP Settings

To enable the DHCP Server feature on the SonicWALL, select **Enable DHCP Server**, and click **Configure**. The **DHCP Server Configuration** window is displayed.
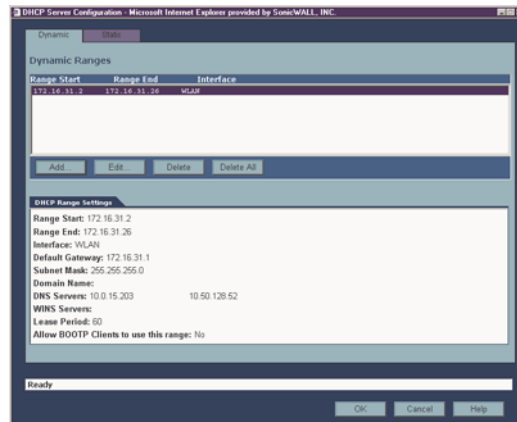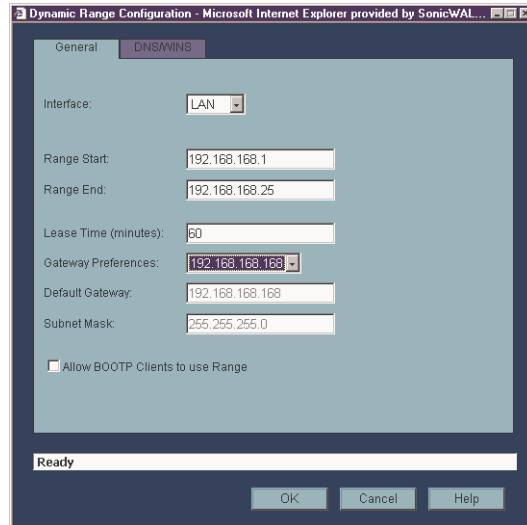
Configuring DHCP Server

The Dynamic Tab

In the **Dynamic Ranges** table, the **Range Start**, **Range End**, and **Interface** information is displayed. To add ranges to the table, click **Add**.

The **Dynamic Ranges Configuration** window is displayed.

The General Tab

1. Select interface, X0 - X5, from the Interface menu. The IP addresses are in the same private subnet as the selected interface.

💡

Tip!   *To select an interface from the Interface menu, it must first be fully configured and it must be of the Zone type, LAN or DMZ.*

---
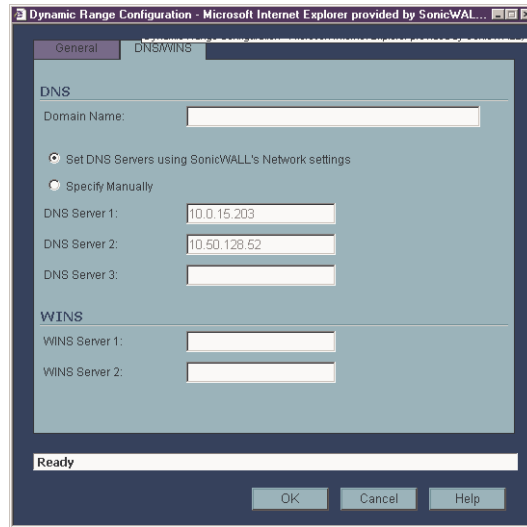
2. Type the beginning IP address in the **Range Start** field. The default IP address is appropriate for most networks.

3. Type the last IP address in the **Range End** field. If there are more than 25 computers on your network, type the appropriate ending IP address in the **Range End** field.

4. Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. 60 minutes is the default value.

5. Select the gateway from the **Gateway Preferences** menu. The LAN IP address is the default value, but you can select **Other** and type a different IP address for the gateway.

6. If you select the SonicWALL LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields

are available for you to type the Default Gateway and Subnet Mask information into the fields.

7. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

8. Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

The DNS/WINS Tab

9. If you have a domain name for the DNS Server, type it in the **Domain Name** field.

10. **Set DNS Servers using SonicWALL's Network Settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

11. If you do not want to use the SonicWALL network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You must specify at least one DNS server.

12. If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field.

13. Click **OK** to add the settings to the SonicWALL.

14. Then click **Apply** for the settings to take effect on the SonicWALL.

Configuring Static DHCP Entries

Click the **Static** tab to add static DHCP entries to the SonicWALL. Static entries are IP addresses assigned to servers requiring permanent IP settings.

TIP! Static DHCP entries should not be configured for computers with IP addresses configured in Network
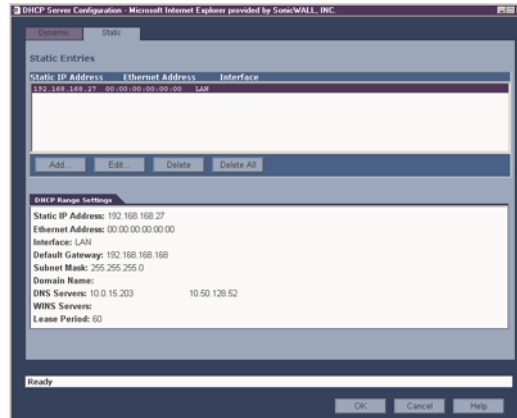
To configure static entries, click **Add**.

The General Tab

1. Select **LAN**, **DMZ,** or other interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.

2. Type the device IP address in the **Static IP Address** field.

3. Type the device Ethernet (MAC) address in the **Ethernet Address** field.

4. Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. 60 minutes is the default value.

5. Select the gateway from the **Gateway Preferences** menu. The LAN IP address is the default value, but you can select **Other** and type a different IP address for the gateway.

6. If you select the SonicWALL LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the Default Gateway and Subnet Mask information into the fields.

7. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

8. Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

The DNS/WINS Tab

9. If you have a domain name for the DNS Server, type it in the **Domain Name** field.

10. **Set DNS Servers using SonicWALL's Network Settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

11. If you do not want to use the SonicWALL network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You must specify at least one DNS server.

12. If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field.

13. Click **OK** to add the settings to the SonicWALL.

Then click **Apply** for the settings to take effect on the SonicWALL.

Tip!   *The SonicWALL DHCP server can assign a total of 64 address ranges with 64 IP addresses each or a total of 4096 IP addresses.*

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding displays the IP address and the Ethernet address along with the type of binding, Dynamic, Dynamic BOOTP, or Static BOOTP. To delete a binding, which frees the IP address on the DHCP server, click the Trashcan icon next to the entry. To edit an entry, click the Notepad icon next to the entry.

Network > IP Helper

IP Helper allows a SonicWALL to forward DHCP requests originating from the interfaces on a SonicWALL to a centralized DHCP server on the behalf of the requesting client. The SonicWALL then returns the DHCP server response and/or lease information back to the client.

This feature is extensively used in networks incorporating VLAN environments where a DHCP server is not available for each interface or the layer 3 routing mechanism is not capable of acting as a DHCP server.

To configure IP Helper, click **Network**, then **IP Helper**.
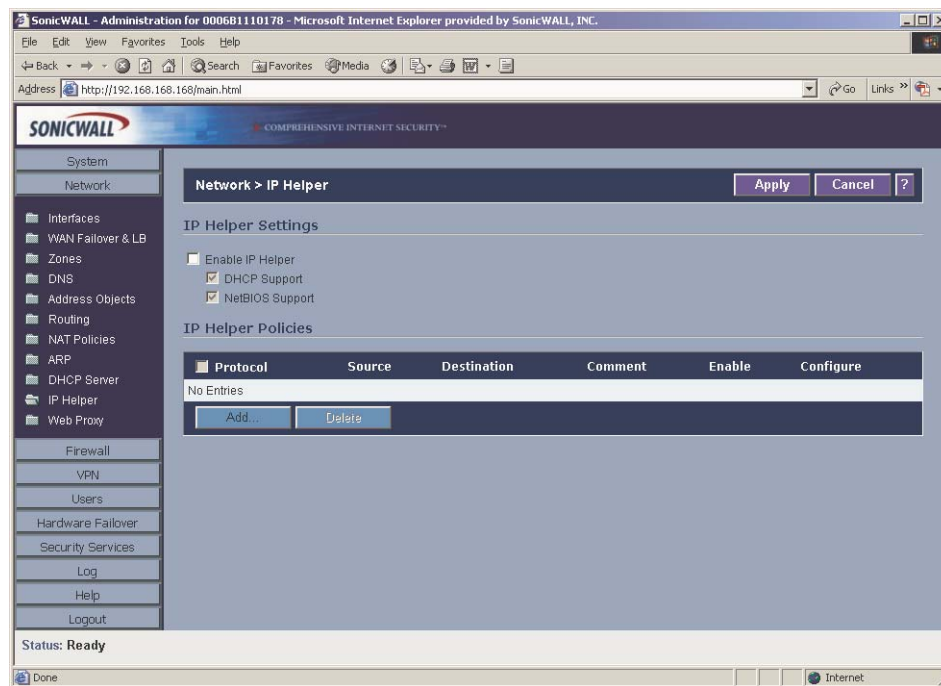
IP Helper Settings

To enable IP Helper on the SonicWALL, select **Enable IP Helper**. To enable DHCP Support, select **DHCP Support**. The SonicWALL now forwards DHCP requests to your central DHCP server.

⚠️
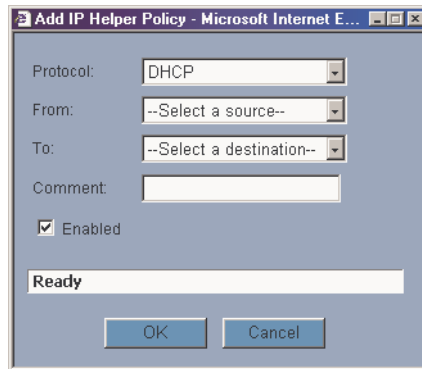
Alert!   *The SonicWALL DHCP Server feature must be disabled before you can enable DHCP Support.*

Select **NetBIOS Support** to allow NetBIOS broadcasts with the DHCP client requests. NetBIOS is required to allow Windows operating systems to browse for resources on a network.

IP Helper Policies

IP Helper Policies allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface. Click **Add**.

1. Select **DHCP** or **NetBIOS** from the **Protocol** menu.

2. Select a source IP address or IP subnet from the **From** menu.

3. Select a destination IP address or subnet from the **To** menu.

4. Enter a comment in the **Comment** field.

5. The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.

6. Click **OK** to add the policy to the **IP Helper Policies** table.

Network > Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests.

Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN and enable Web Proxy Forwarding. The SonicWALL automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.

Configuring Automatic Proxy Forwarding (Web Only)

⚠️

Alert! *The proxy server must be located on the WAN; it can not be located on the LAN.*

To configure a Proxy Web sever, click **Firewall**, and then **Web Proxy**.
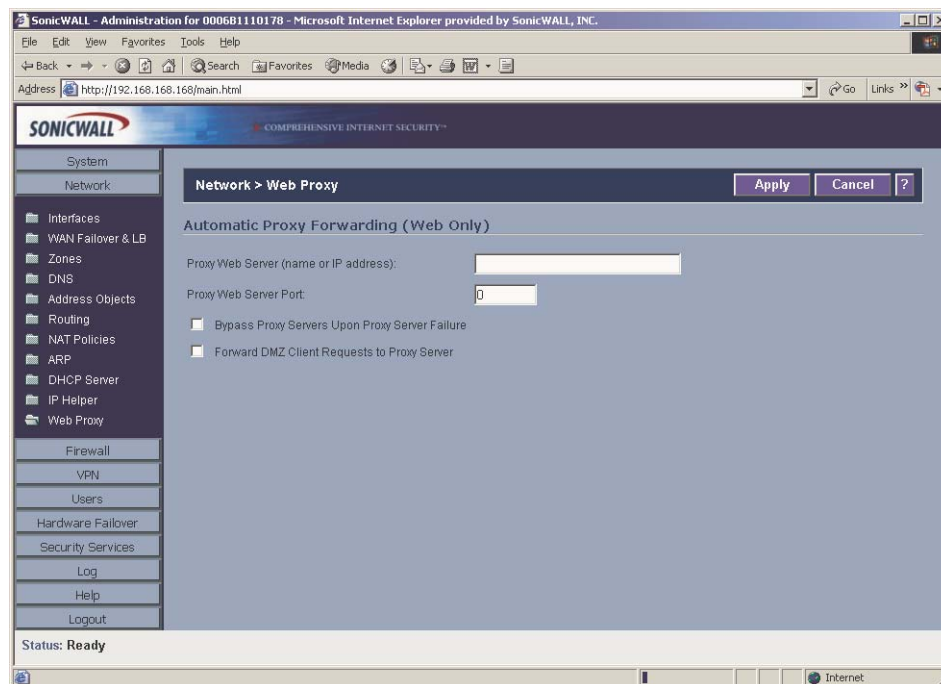
1. Connect your Web proxy server to a hub, and connect the hub to the SonicWALL WAN port.

2. Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.

3. Type the proxy IP port in the **Proxy Web Server Port** field.

4. To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.

5. Select **Forward DMZ Client Requests to Proxy Server** if you have clients configured on the DMZ.

6. Click **Apply**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Firewall>Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the SonicWALL to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.

5 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 and DMZ.

* Allow all sessions originating from the DMZ to the WAN.

* Deny all sessions originating from the WAN to the DMZ.

* Deny all sessions originating from the WAN and 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.

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's stateful packet inspection. For example, a rule that blocks IRC traffic takes precedence over the SonicWALL default setting of 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 prioritize the outbound traffic. Bandwidth management only applies to **outbound** traffic from the SonicWALL to the WAN or any other destination. 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 percent and a maximum bandwidth of 40 percent, priority of 0, outbound SMTP traffic always has 20 percent of available bandwidth available to it and can get as much as 40 percent of available bandwidth. 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 percent of bandwidth or minus 40 percent of bandwidth.

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

Firewall>Access Rules
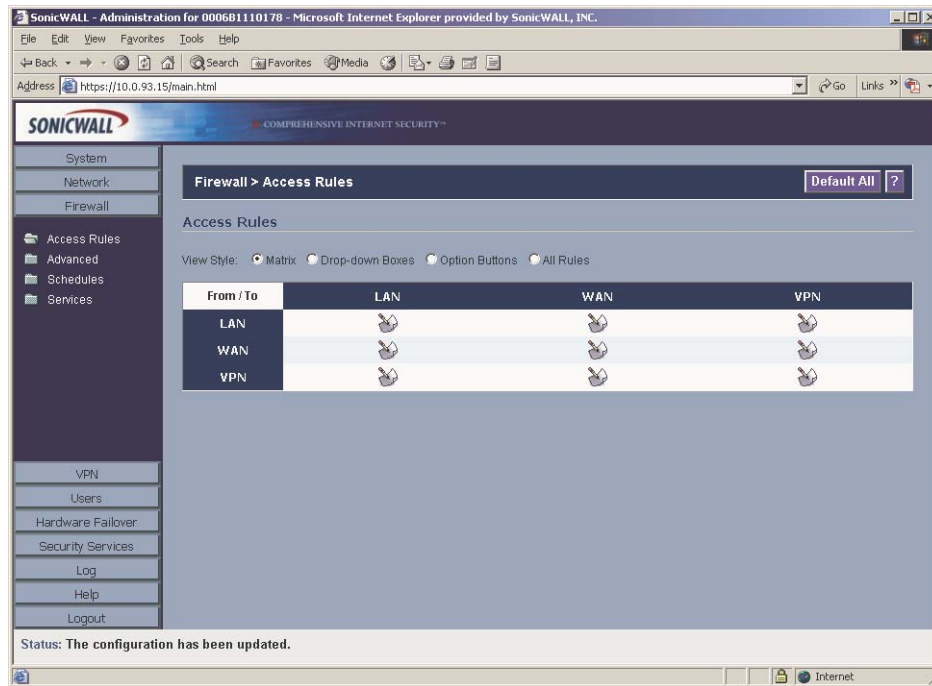
View Styles

Multiple ways of displaying Access Rules is available in SonicOS Enhanced. Select the type of view from the selections in the **View Style** section. The following **View Styles** are available:

- **Matrix** - displays as From/To with LAN, WAN, VPN, or other interface in the **From** row, and LAN, WAN, VPN, or other interface in the **To** column. Select the Notepad icon in the table cell to view the rules.
- **Drop-down Boxes** - displays two pull-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and rules defined for the two interfaces are displayed.
- **Option Buttons** - Select LAN, WAN, VPN, ALL from the **From Zone** column. Then select LAN, WAN, VPN, ALL from the **To Zone** column. Click **OK** to display the rules.
- **All Rules** - selecting **All Rules** displays all rules configured on the SonicWALL.

Each view displays a table of defined Network Access Rules. For example, selecting **All Rules** displays all the Network Access Rules for all Zones.

The 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 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.

Adding Rules

To add Access Rules to the SonicWALL, click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.
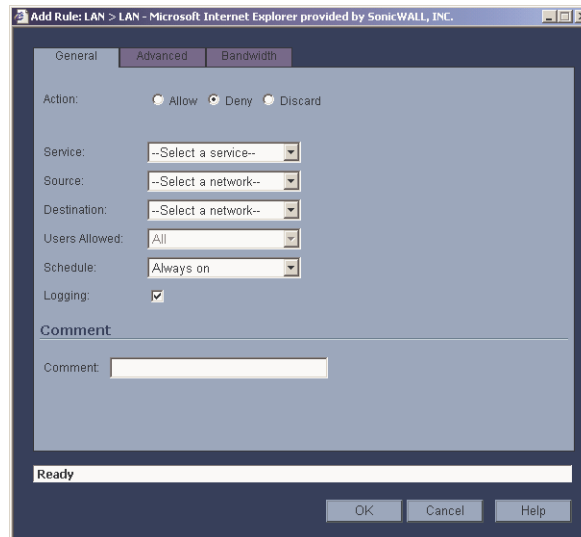
1. Select **Allow**, **Deny,** or **Discard** from the **Action** list depending upon whether the rule is intended to permit or block IP traffic.

2. Select the service or group of services 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.Selecting **Create New Service** or **Create New Group** displays the **Add Service** window or **Add Service Group** window.

3. Select the source of the traffic affected by the rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.

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, type 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, type * in the **Address Range Begin** field.

5. Select the destination of the traffic affected by the rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.

6. From the **Users Allowed** menu, add the user or user group affected by the rule.

7. Select a schedule from the Schedule menu. The default schedule is **Always on**.

8. Enter any comments to help identify the rule in the **Comments** field.

9. Click the **Advanced** tab.
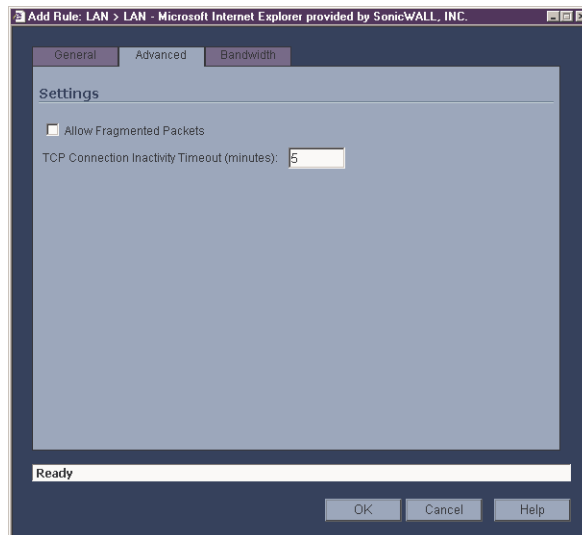
10. Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. Because hackers exploit IP fragmentation in Denial of Service attacks, the SonicWALL blocks fragmented packets by default. You can override the default configuration to allow fragmented packets over PPTP or IPSec.

11. If you would like for the rule to timeout 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. Click the **Bandwidth** tab. Select **Enable Outbound Bandwidth Management ('allow' rules only)**, and enter the **Guaranteed Bandwidth** in Kbps.

13. Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

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

Adding New 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 **Any** from the **Source** menu.
5. Select **X1** from the **Destination** menu.
6. Select the schedule from the **Schedule** menu.
7. Enter any comments in the **Comment** field.
8. 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 **X1** from the **Source** menu.
5. Select **X0** from the **Destination** menu.
6. Select All from the **Users Allowed** menu.
7. Enter any comments in the **Comment** field.
8. Select **Always** from the **Schedule** menu to ensure continuous enforcement.

9. Click **OK**.

Firewall > Advanced

Click **Advanced** under Firewall. The **Advanced Rule Options** page is displayed.
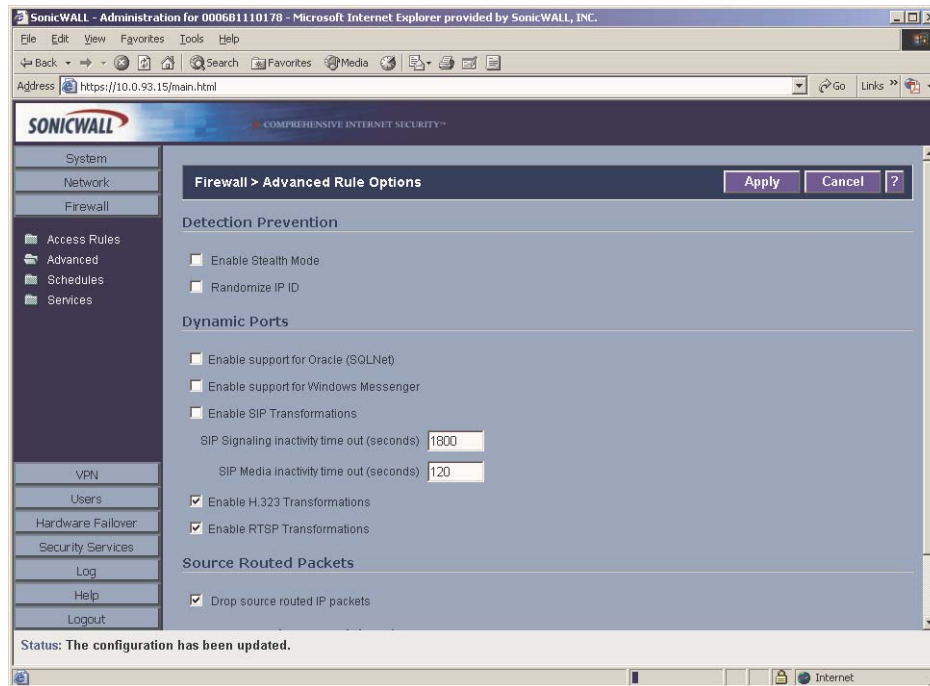
Advanced Rule Option

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 through the SonicWALL. If **Enable Support for Windows Messenger** is selected, it may affect the performance of the SonicWALL.

Select **Enable support for H.323** if you are having problems with videoconferencing. H.323 promotes compatibility for videoconferencing over IP networks as well as interoperability in audio, video and data transmissions.

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 > Schedules

Schedules

The SonicWALL has the flexibility to create and add schedules for Access Rules or Access Rule Groups.
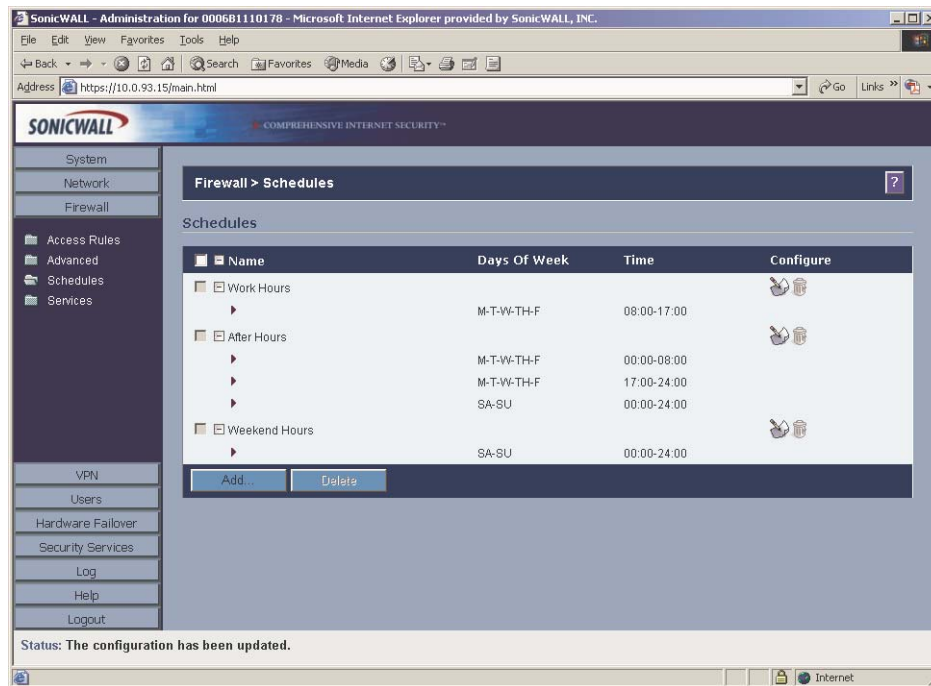
In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. You can modify these schedule by clicking on the **Notepad** icon in the **Configure** column.

Adding a Schedule

To create schedules, click **Add**. The **Add Schedule** window is displayed.

1. Enter a name for the schedule in the **Name** field.

2. Select the days of the week to apply to the schedule or select **All**.

3. Enter the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, i.e. 17:00 for 5 p.m.

4. Enter the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, i.e. 17:00 for 5 p.m.

5. Click **Add**.

6. Click **OK** to add the schedule to the **Schedules** table.

7. To delete existing days and times, select the schedule and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Deleting Schedules

To delete individual Schedules, select the checkbox next to the Schedule, the **Delete** button becomes enabled. Click **Delete**. To delete all Schedules, select the checkbox next to **Name** to select all Schedules. Click **Delete**.

Firewall>Services

Services are anything a server provides to other computers. A service can be as simple as the computer asking the 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. The SonicWALL includes **Default Services** that are predefined services and also allows you to create **Custom Services**.
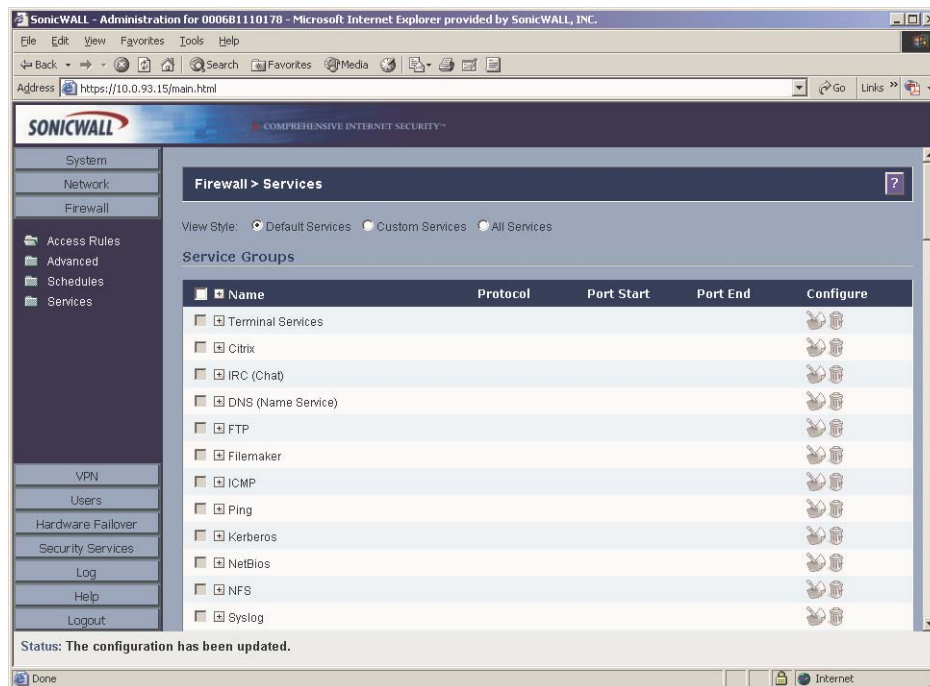
Default Services

The **Default Services** view displays the SonicWALL default services in the **Services** table and **Service Groups** table that displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Services** table displays the following attributes of the services that are currently defined:

- **Name** - the name of the service.
- **Protocol** - the protocol of the service (TCP, UDP, or ICMP).
- **Port Start** - the starting port number for the service.
- **Port End** - the ending port number for the service.
- **Configure** - Displays the unavailable Notepad and Trashcan icons, indicating these Default Services cannot be edited or deleted.

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the + to the left of the Default Service Groups entry, displays all the individual Default Services included in the group. For example, the **DNS (Name Service)** entry has two services labeled **DNS (Name Service) TCP** for port 53 and **DNS (Name Service) UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

Custom Services

All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement.

Adding Custom Services

If a protocol is not listed in the **Default Services** table, you can add it to the Custom Services table by clicking **Add**.
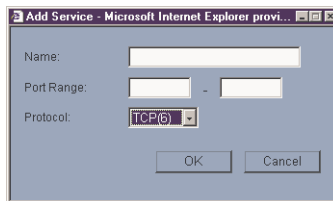
1. Enter the name of the service in the **Name** field.
2. Enter the port number or numbers that apply to the service. A list of well-known port numbers can be found in any networking reference.
3. Select the type of protocol, **TCP**, **UDP**, or **ICMP** from the **Protocol** menu.
4. Click **OK**. The service appears in the **Custom Services** table.

Click the **Enable Logging** checkbox to disable or enable the logging of the service activities.

Editing Custom Services

Click the **Notepad** icon under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

Deleting Custom Services

Click the **Trashcan** icon to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

Custom Services Groups

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only

during certain hours or days of the week by adding the two services as a Custom Service Group. To create a **Custom Services Group**, click **Add Group**.
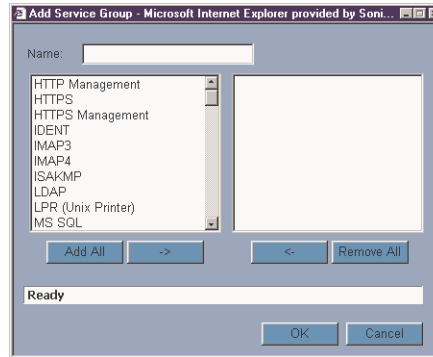
1. Enter a name for the custom group in the name field.

2. Select individual services from the list in the left column. You can also select multiple services by pressing the Ctrl key and clicking on the services.

3. Click **-** > to add the services to the group.

4. To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.

5. Click < - to remove the services.

6. When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking+ on the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

Editing Custom Services Groups

Click the **Notepad** icon under **Configure** to edit the custom service group in the **Edit Service Group** window, which includes the same configuration settings as the **Add Service Group** window.

Deleting Custom Services Groups

Click the **Trashcan** icon to delete the individual custom service group entry. You can delete all custom service groups by clicking the Delete button.

6 SonicWALL VPN

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

SonicWALL VPN is based on the industry-standard IPSec VPN implementation, so it is interoperable with other VPN products, such as Check Point FireWall-1 and Axent Raptor. Basic VPN terminology definitions are located in Appendix F-Basic VPN Terms and Concepts.

Before You Start Configuring VPN Tunnels

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.

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

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: ___.___.___.___

Site B

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:_____
Local IKE ID and Remote IKE ID
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
Local Network in a VPN Policy
__ Choose local network from list
__ Local network obtains IP addresses using DHCP through this VPN tunnel
__ Any address
Remote Networks
__ Use this VPN tunnel as a default route for all Internet traffic
__ Destination network obtains address using DHCP through this VPN tunnel
__ Choose destination network from list

VPN>Settings

To begin configuring VPN Security Associations, log into the SonicWALL and click **VPN**. The default page is **VPN>Settings**.
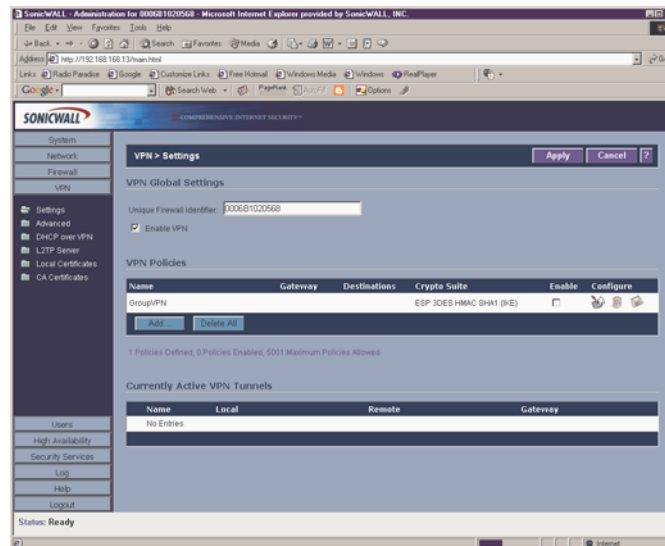
Global Settings

The **Global VPN Settings** section displays the following information:
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL appliance. You can change the Identifier, and use it for configuring VPN tunnels.
- **Enable VPN** must be selected to allow VPN policies.

VPN Policies

💡

Tip!   *VPN Policies can be edited at any time by clicking on the Notepad icon in the table entry.*

All existing VPN security policies are displayed in the **VPN Policies** table. Each entry displays the following information:
- **Name** - user-defined name to identify the VPN policy.
- **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 Security Association information. Group VPN has a **File** icon for exporting the configuration to Global VPN Clients.

The number of SAs defined, SAs enabled, and the maximum number of SAs allowed is displayed below the table.

Currently Active SAs

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

Adding VPN SAs to the SonicWALL

Configuring Group VPN 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 appliance. Security settings can now be exported to the remote client and imported into the remote VPN client settings. **Group VPN** allows for easy deployment of multiple VPN clients making it unnecessary to individually configure remote VPN clients. **Group VPN** is only available for VPN clients and it is recommended to use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.
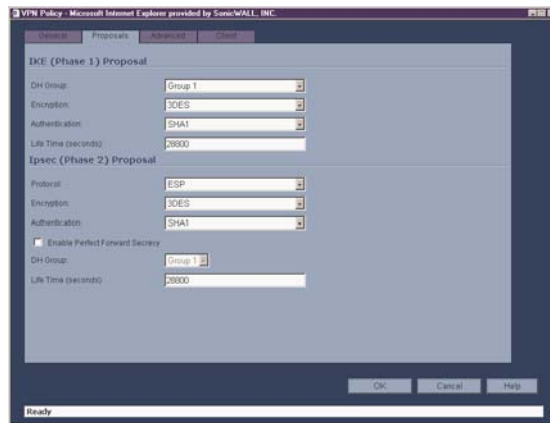
To edit the default settings for Group VPN, click the Notepad icon in the **Group VPN** entry. The **VPN Policy** window is displayed.
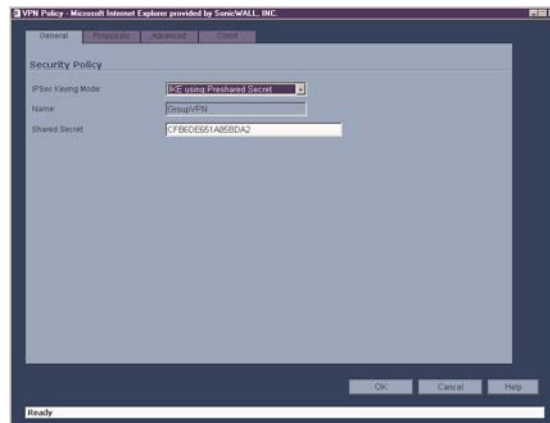
VPN Policy>General

IKE using Preshared Secret is the default setting for IPSec Keying Mode. You can also use Third Party Certificates for authentication. Group VPN is the default policy name and cannot be changed. 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. Click the **Proposals** tab to continue the configuration process.

VPN Policy>Proposals

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

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

2. **3DES** from the **Encryption** menu

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

4. 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:

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

6. **3DES** from the **Encryption** menu

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

8. 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.

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

10. Click the **Advanced** tab.

VPN Policy>Advanced

💡
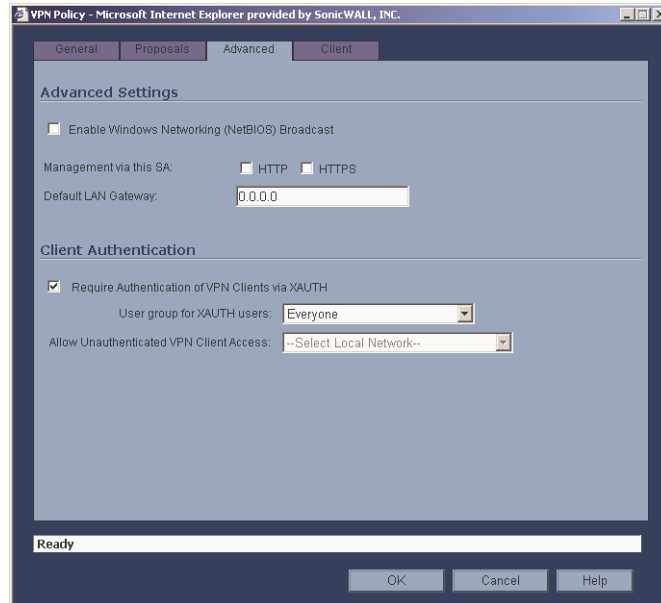
Tip!   *These settings are optional and are not required for VPN tunnel configuration.*

- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- **Management via this SA**: - If using the VPN SA to manage the SonicWALL, select the management method, either **HTTP** or **HTTPS**.
- **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.

Client Authentication
- **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. Select a user group or Everyone from **User Group for XAUTH users**.

VPN Policy>Client

Client Cache
- **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**.

Client Connections
- **Allow Traffic to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select from **Any Destination**, **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 SA. You can only configure one SA 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.

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

Configuring a VPN SA using Manual Key

To manually configure a VPN SA between two SonicWALL appliances using Manual Key, follow the steps below:

Local SonicWALL

1. Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.

2. Select **Manual Key** from the **IPSec Keying Mode** menu.
3. Enter a name for the policy in the **Name** field.
4. Enter the host name or IP address of the remote connection in the **IPSec Gateway Name or Address** field. Click the **Network** tab.

5. Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select Use this VPN Tunnel as default route for all Internet traffic if all remote

VPN connections access the Internet through this SA. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group. Click **Proposals**.

Proposals

6. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

⚠️

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.*

7. The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

📝

Note: *The values for **Protocol, Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.*

8. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the SonicWALL.

9. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the SonicWALL settings.

💡

Tip! *Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a,b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter*

an incorrect encryption key, an error message is displayed at the bottom of the browser window.

10. Click **Advanced**.

11. Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

12. **Apply NAT Policies** - Use this feature to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

13. To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**

14. Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

15. If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.

16. Select an interface from the **VPN Policy bound to** menu.

17. Click **OK**.

18. Click **Apply** on the **VPN >Settings** page to update the VPN Policies.

Remote SonicWALL

1. Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
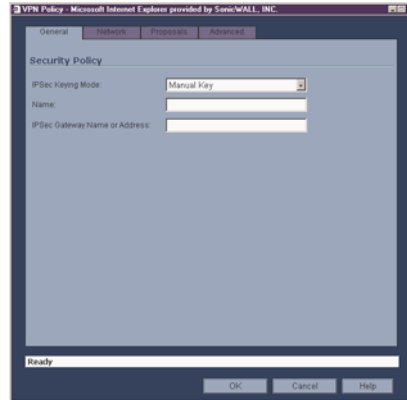
2. Select **Manual Key** from the **IPSec Keying Mode** menu.
3. Enter a name for the SA in the **Name** field.
4. Enter the host name or IP address of the local connection in the **IPSec Gateway Name or Address** field. Click the **Network** tab.

5. Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group. Click **Proposals**.

Proposals

6. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

⚠️

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.*

7. The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

📝

Note: *The values for **Protocol, Phase 2 Encryption,** and **Phase 2 Authentication** must match the values on the remote SonicWALL.*

8. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the remote SonicWALL.

9. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWALL settings.

💡

Tip! *Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a,b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.*

10. Click **Advanced**.

11. Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

12. **Apply NAT Policies** - Use this feature to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

⚠

Alert!   *You cannot use this feature if you have selected* **Use this VPN Tunnel as the default route for all Internet traffic** *on the* **Network** *tab.*

13. To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**

14. Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

15. If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.

16. Select an interface from the **VPN Policy bound to** menu.

17. Click **OK**.
18. Click **Apply** on the **VPN >Settings** page to update the VPN Policies.

Note: *Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.*

Configuring a VPN SA with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE), follow the steps below:

1. Click **Add** on the **VPN>Settings** page. The **VPN Policy** window is displayed.

2. Select **IKE using Preshared Secret** from the **IPSec Keying Mode** menu.
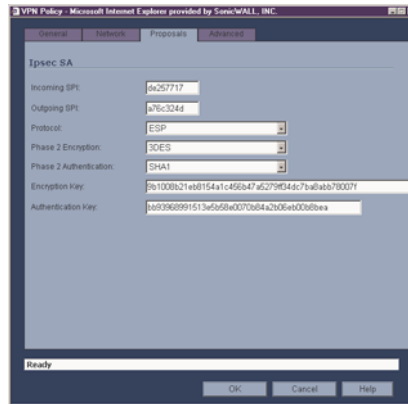
3. Enter a name for the policy in the **Name** field.

4. Enter the host name or IP address of the remote connection in the I**PSec Primary Gateway Name or Address** field.

5. If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPSec Secondary Gateway Name or Address** field.

6. Enter a Shared-Secret password to be used to setup the SA in the **Shared Secret** field. The password must be at least 4 characters long, and should comprise both numbers and letters.

7. Optionally, specify a Local and IKE Peer ID for this Policy. By default, the IP Address (ID_IPv4_ADDR) will be used for Main Mode negotiations, and the SonicWALL Identifier (ID_USER_FQDN) will be used for Aggressive Mode.

8. Click the **Network** tab.
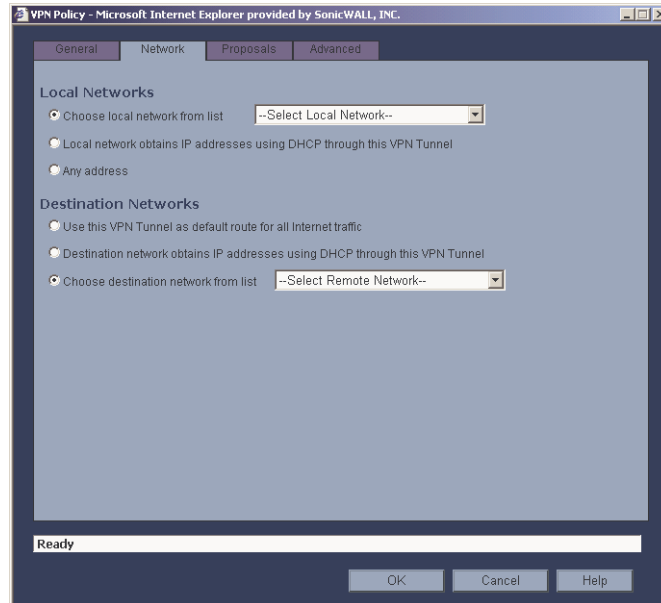
9. Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.

10. Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

11. Click **Proposals**.
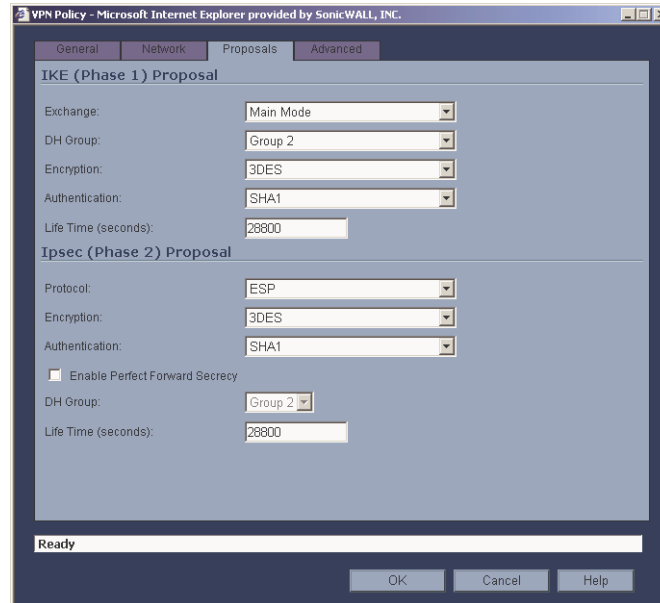
12. Under **IKE (Phase 1) Proposal**, select either **Main Mode** or **Aggressive Mode** from the **Exchange** menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned.

13. Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

14. **Under IPSec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group**, and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

15. Click **Advanced**.
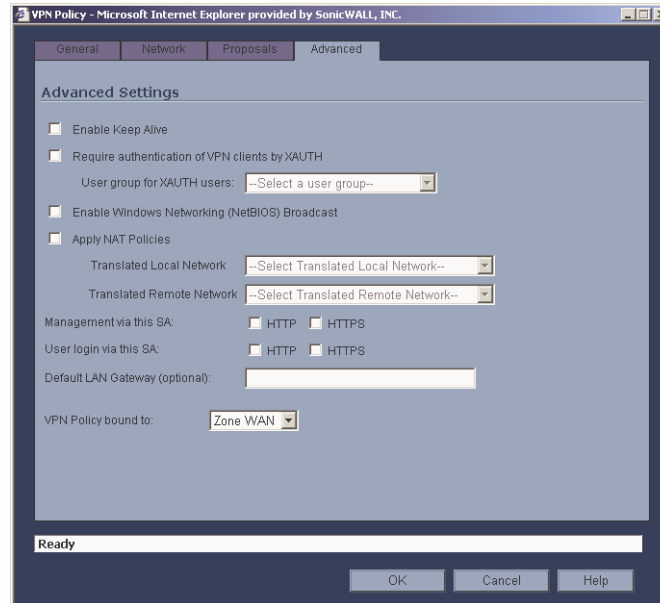
16. Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

17. To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.

18. Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote

19. network resources by browsing the Windows® Network Neighborhood.

20. **Apply NAT Policies** - Use this feature to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

21. To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

22. If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel**

as default route for all Internet traffic, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

23. Select an interface or Zone from the **VPN Policy bound to** menu. A Zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

24. Click OK.

25. Click Apply on the **VPN>Settings** page to update the VPN Policies.

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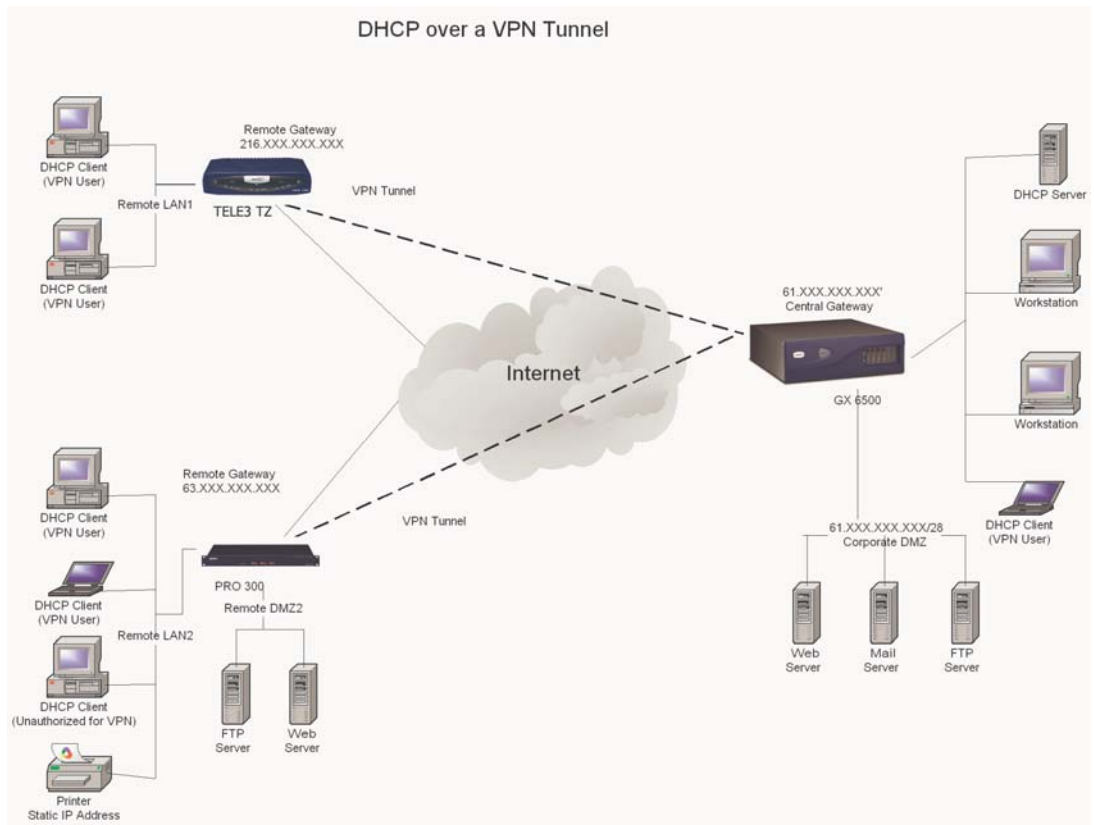
Configuring the Central Gateway for DHCP Over VPN
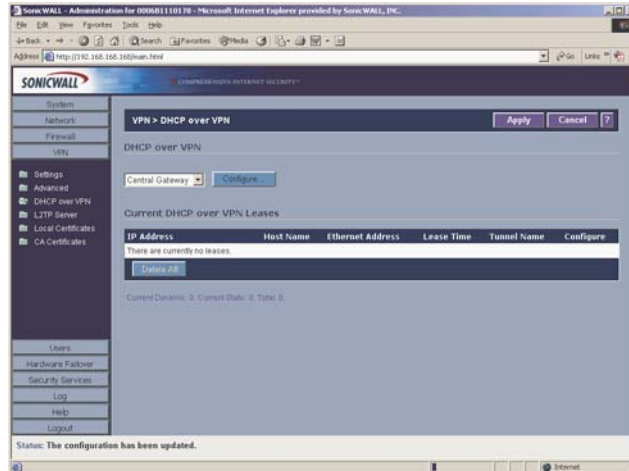
To configure **DHCP over VPN** for the **Central Gateway**, use the following steps:

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.
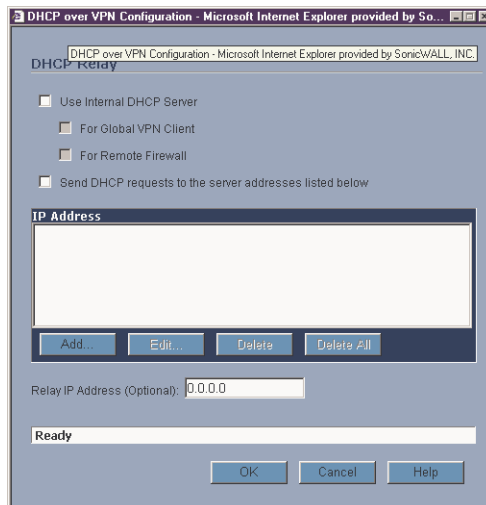
4. Select **Use Internal DHCP Server** to enable the Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information.

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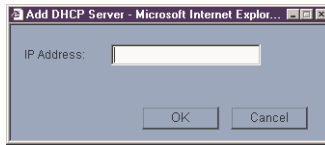
7. Type the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWALL now directs DHCP requests to the specified servers.

8. Type 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.
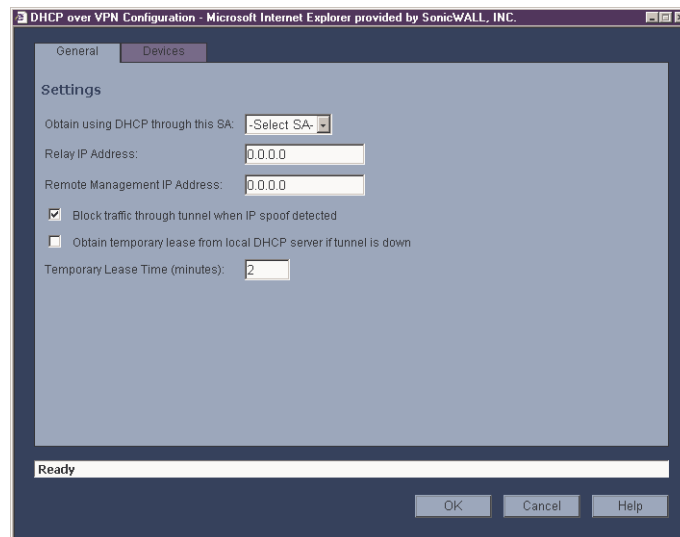
3. Select the VPN Security Association to be used for the VPN tunnel from the **Obtain using DHCP through this SA** menu. When a VPN Policy has a selection, the local network obtains IP addresses using DHCP through this VPN tunnel. The policy name is automatically displayed in **Obtain using DHCP through this SA** field on the **DHCP over VPN** page for Remote Gateway.

⚠️

Alert!   *Only VPN Security Associations using IKE can be used as VPN tunnels for DHCP.*

4. The **Relay IP address** is a static IP address from the pool of specific IP addresses on the **Central Gateway**. It should not be available in the scope of DHCP addresses. The SonicWALL can also be managed through the Relay IP address.

5. 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 typed 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.

6. 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, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is two (2) minutes.

Device Configuration

7. To configure **Static Devices on the LAN**, click **Add**, and type the IP address of the device in the **IP Address** field and then type 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 type the Ethernet address of a device.

8. 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 type 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.
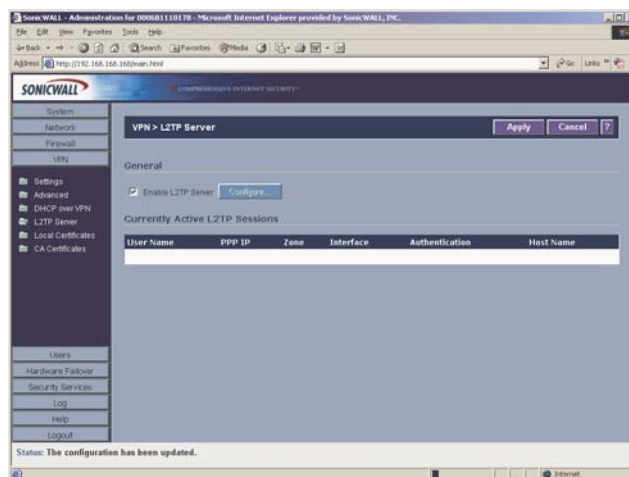
General

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, type 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, type 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.

L2TP Users

8. If you have configured a specific user group for using L2TP, select it from the **User Group for L2TP users** menu. You can also select **Everyone**.

9. 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 type of interface used to access the L2TP Server, whether it's a VPN client or another SonicWALL appliance.
- **Authentication** - type of authentication used by the L2TP client.
- **Host Name** - the name of the network connecting to the L2TP Server.

SonicWALL Third Party Digital Certificate Support

Tip *This section assumes that you are familiar with Public Key Infrastructure (PKI) and the implementation of digital certificates with VPN.*

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). SonicWALL now supports third party certificates in addition to the existing Authentication Service. The difference between third party certificates and the SonicWALL Authentication Service is the ability to select the source for your CA certificate. Using **Certificate Authority Certificates** and **Local Certificates** is a more manual process than using the SonicWALL Authentication Service; therefore, experience with implementing Public Key Infrastructure (PKI) is necessary to understand the key components of digital certificates.

Internet Key Exchange (IKE) is an important part of IPSec VPN solutions, and it can use digital signatures to authenticate peer devices before setting up security associations. Without digital signatures, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices using digital signatures do not require configuration changes every time a new device is added to the network.

SonicWALL has implemented X.509v3 as its certificate form and CRLv2 for its certificate revocation list.

SonicWALL supports the following two vendors of Certificate Authority Certificates:

- **VeriSign**
- **Entrust**

Overview of Third Party Digital Certificate Support

X.509 Version 3 Certificate Standard

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 a VPN SA.

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.

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.

Current Certificates

Both **Certificate Requests** and validated **Certificates** appear in the list of **Current Certificates**. The **Certificate Details** section lists the same information as the **CA Certificate Details** section, but a **Status** entry now appears in the details. If a certificate is valid and ready to be used with a VPN Security Association, the **Status** is **Verified**. If the certificate is not signed by the CA, the **Status** is **Request Generated**. You can also import the corresponding **Signed Certificate** in this section. Additionally, **Certificate Signing Requests** can be exported and deleted in the **Certificate Details** section of a **Request Generated** certificate.

Importing Certificate with private key

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. 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

Both **Certificate Requests** and validated **Certificates** appear in the list of **Current Certificates**. The **Certificate Details** section lists the same information as the **CA Certificate Details** section, but a **Status** entry now appears in the details. If a certificate is valid and ready to be used with a VPN Security Association, the **Status** is **Verified**. If the certificate is not signed by the CA, the **Status** is **Request Generated**. You can also import the corresponding **Signed Certificate** in this section. Additionally, **Certificate Signing Requests** can be exported and deleted in the **Certificate Details** section of a **Request Generated** certificate.

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 locating the URL and then importing it into the SonicWALL. Certificates are checked against the CRL by the SonicWALL for validity when they are used. You can also type a URL location of the CRL by typing the address in the **Enter CRL's location for this CA (URL)** field. The CRL is downloaded automatically at intervals determined by the CA service.

Importing a Signed Local Certificate

When the CA service returns the signed certificate request generated locally, import it into the SonicWALL using the following steps:

1. In the **Current Certificates** section of **Local Certificates**, select the corresponding request from the **Certificates** menu.

2. Click **Browse**, and select the *.der from the **Choose File** dialogue box.

3. Click **Import Certificate**.

4. The certificate is now updated to **Verified**, and you can now use it for a VPN SA using a third party certificate.

Configuring a VPN Security Association using IKE and a Third Party Certificate

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

1. Click **VPN**, then **Add**.

2. Type a Name for the Security Association in the **Name** field.

3. Select a certificate from the **Select Certificate** list.

4. Type the Gateway address in the **IPSec Gateway Address** field.

5. In the **Security Policy** section, select the type of DH group from the **Phase 1 DH Group** menu.

6. The **SA Lifetime (secs)** automatically defaults to 28800 seconds (8 hours).

7. Select the type of **Phase 1 Encryption/Authentication** from the menu.

8. Select the type of **Phase 2 Encryption/Authentication** from the menu.

9. In the **Peer Certificate's ID** section, you must select the ID Type from the **ID Type** menu. You can select **Distinguished Name**, **E-mail ID**, or **Domain Name** from the menu. Then cut and paste the information from the Local Certificate into the text field.

10. In the **Destination Networks** section, select the type of destination for the VPN tunnel:

    - Use this SA as default route for all Internet traffic can be used for only one SA, and routes all VPN traffic destined for the WAN through the SA.

    - Destination network obtains IP addresses using DHCP through this SA to allow computers at the VPN destination to obtain IP addresses using DHCP over VPN.

    - Specify destination network below If the VPN destination is a specific IP address.

11. Click **Add New Network...** type the network IP address and subnet mask in the fields, and click **OK**.

Creating a Certificate Signing Request

To create a certificate for use with a VPN SA, follow these steps:

> 💡
>
> **Tip!** *You should create a Certificate Policy to 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. Click **VPN**, then **Local Certificates**.

2. In the **Generate Certificate Signing Request** section, type a name for the certificate in the **Certificate Name** field. Using the drop down menus, type information for the certificate request. As you type information in the Request fields, the Distinguished Name (DN) is created. You may also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**.

3. The **Subject Key** type is preset as an RSA algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

4. Select a Subject Key size from the from the **Subject Key Size** menu.

5. Not all key sizes are supported by a Certificate Authority, therefore you should check with your Certificate Authority for supported key sizes.

6. Click **Generate** to create a certificate file.

7. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.

8. Click **Export** to download the file to your computer, and then click **Save** to save it to a directory on your computer.

Now that you have generated the **Certificate Request**, you can send it to your CA service 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, use the following steps:

1. Click **VPN**, then **CA Certificates**.

2. Click **Browse**, and locate the PKCS#7 or DER encoded file sent by the CA service.

3. Click **Open** to set the directory path to the certificate, and then click **Import** to import the certificate into the SonicWALL. Once it is imported, you can view the **Certificate Details**.

7 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 1000 users. If you have more than 1000 users, you must use RADIUS for authentication

Users>Status

.The **Users>Status** page displays **Active User Sessions** on the SonicWALL. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, and **Logout**. To logout a user, click the Trashcan icon next to the user's entry.r
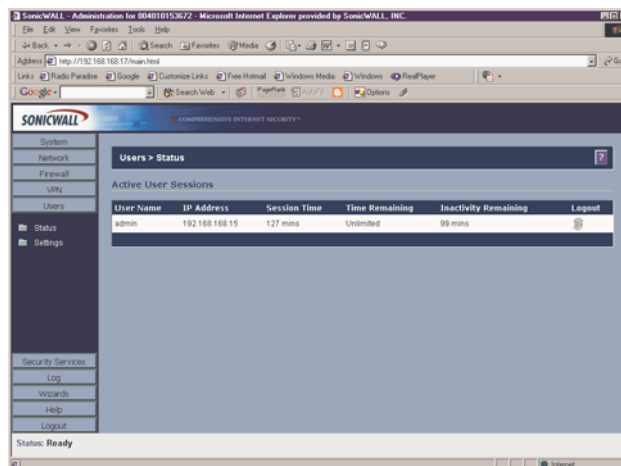
User Settings

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.
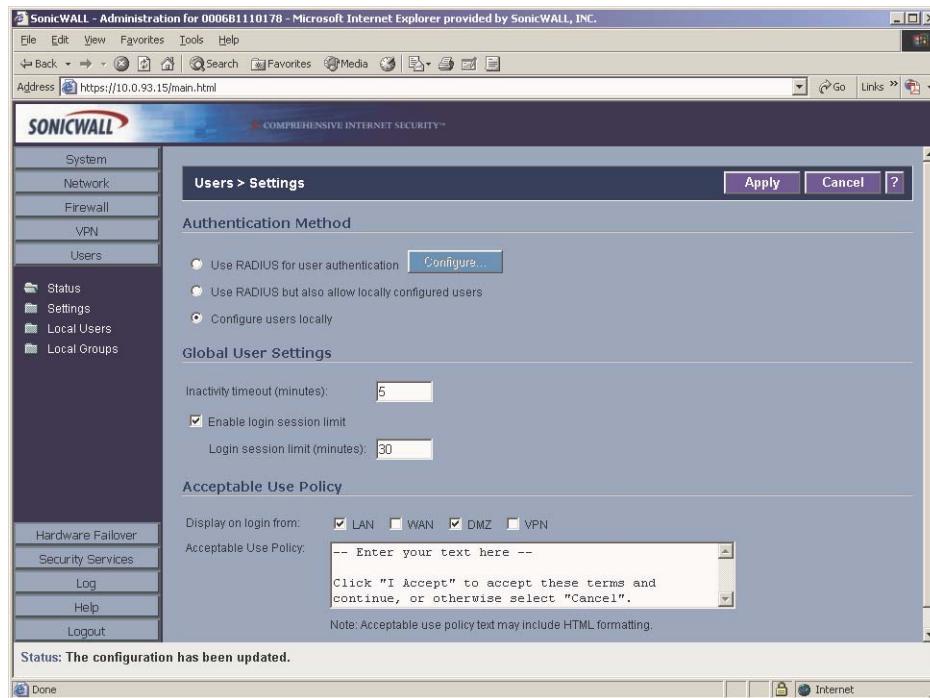
Authentication Method
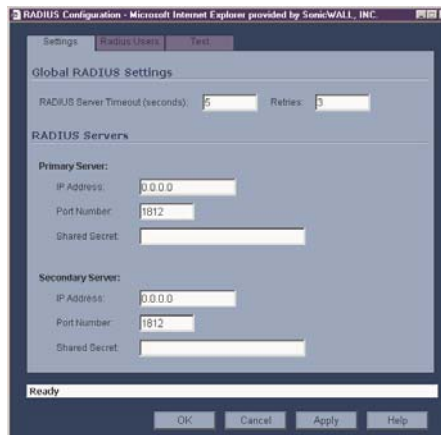
Select **Use RADIUS for user authentication** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWALL. If you select Use RADIUS for user authentication, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS.

Select **Use RADIUS but also allow locally configured users** if you want to use both RADIUS and the SonicWALL local user database for authentication.

Select **Configure users locally** to configure users in the local database using the Users>Local Users and Users>Local Groups pages.

If you selected **Use RADIUS for user authentication** or U**se RADIUS but also allow locally configured users**, the **Configure** button becomes available.

Click **Configure** to set up your RADIUS server settings on the SonicWALL. The **RADIUS Configuration** window is displayed.

1. Define the **RADIUS Server Timeout in Seconds**. The allowable range is 1-60 seconds with a default value of 5.

2. Define the number of times the SonicWALL attempts to contact the RADIUS server in the **RADIUS Server 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.

RADIUS Servers

3. 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.

4. Type the IP address of the RADIUS server in the **IP Address** field.

5. Type the **Port Number** for the RADIUS server.

6. 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.

7. If there is a secondary RADIUS server, type the appropriate information in the **Secondary Server** section.

8. 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.

RADIUS Users

Click the **RADIUS Users** tab..
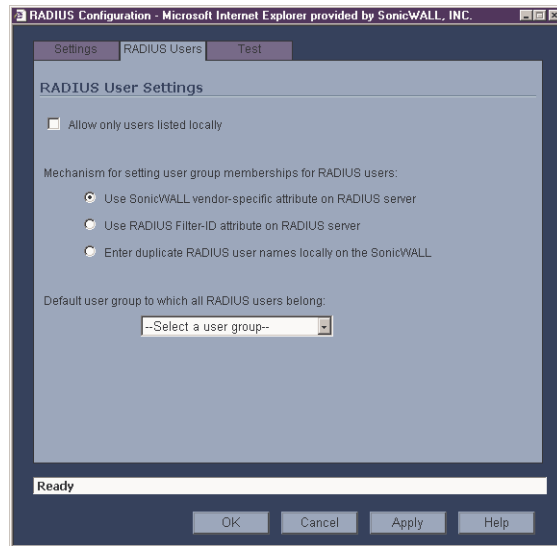
RADIUS Users Settings

Select **Allow only users listed locally** if only the users listed in the SonicWALL database are authenticated using RADIUS.
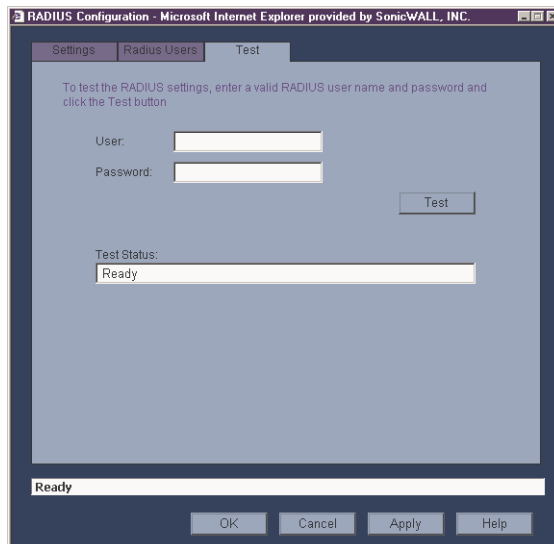
Select the mechanism used for setting user group memberships for RADIUS users from the following list:

- **Use SonicWALL vendor-specific attribute on RADIUS server -** select to apply specific attributes from the RADIUS server.
- **Use RADIUS Filter-ID attribute on RADIUS server**
- **Enter duplicate RADIUS user names locally on the SonicWALL**

If you have previously configured User Groups on the SonicWALL, select the group from the **Default user group to which all RADIUS user belong** menu.

RADIUS Client Test

You can test your RADIUS Client user name and password by typing in a valid user name in the **User** field, and the password in the **Password** field.

If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**. 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.

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 field.
- **Allow unauthenticated VPN users to access DNS** - selecting this check box allows unauthenticated users access to DNS servers across a VPN tunnel with authentication enforcement.

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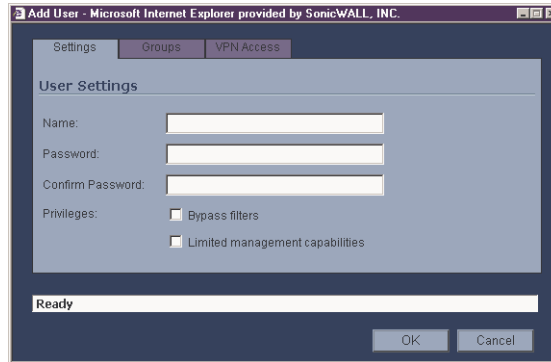
Tip!   *Acceptable Use Policies can use HTML formatting in the body of the message.*

User>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.

   • **Bypass Filters** - select **Bypass Filters** if the user has unlimited access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.

   • **Limited Management Capabilities** - By enabling this check box, the user has limited local management access to the SonicWALL Management interface. The access is limited to the following pages:

     • **General** - Status, Network, Time

     • **Log** - View Log, Log Settings, Log Reports

     • **Tools** - Restart, Diagnostics minus Tech Support Report

Groups

To add the user to a User Group, select one or more groups, and click ->. The user then becomes a member of the selected groups. To remove a group, select the group from the Member of column, and click <-.
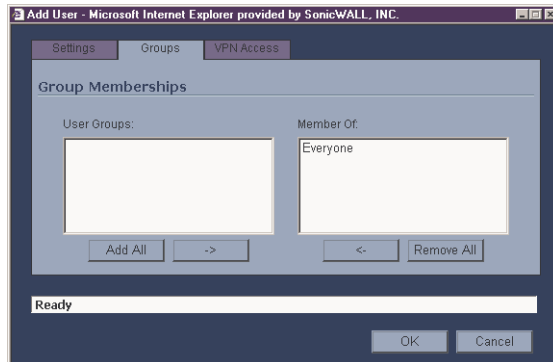
VPN Access

To allow users to access networks using a VPN tunnel, select the network from the **Networks** list and click -> to move it to the **Access List.**
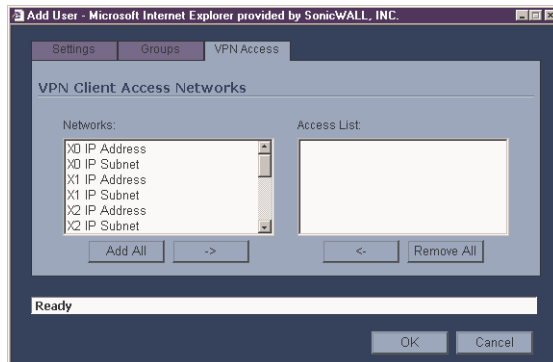
To remove a network from the **Access List**, select the network and click <-. Click **OK** to complete the user configuration.

Users > Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **Bypass Filters**, **Limited Admin**, **VPN Access**, and **Configure**. A default group, **Everyone**, is listed in the first row of the table. Click the Notepad icon in the **Configure** column to review or change the settings for **Everyone**.
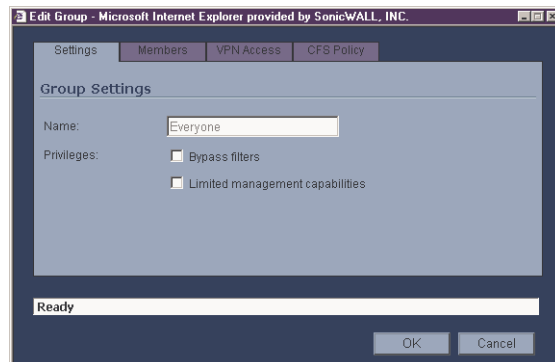
Creating a Local Group

1. Click the Add Group button to display the Add Group window.

2. Create a user name and type it in the **User Name** field.

3. Select any of the following options from the Group Settings section:

   • **Bypass Filters** - select **Bypass Filters** if the user has unlimited access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.

   • **Limited Management Capabilities** - By enabling this check box, the user has limited local management access to the SonicWALL Management interface. The access is limited to the following pages:

      • **General** - Status, Network, Time

      • **Log** - View Log, Log Settings, Log Reports

      • **Tools** - Restart, Diagnostics minus Tech Support Report

4. To add non-Members Users and Groups, click the **Members** tab. Select the non-member user or group from the **Non-Members Users and Groups** list and click ->.
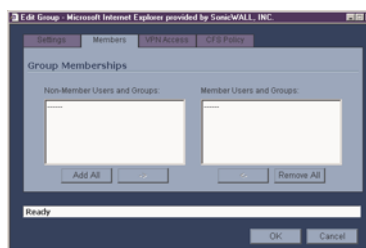
5. To allow users in this group to access networks using a VPN tunnel, click the **VPN Access** tab, select the network from the **Networks** list and click -> to move it to the **Access List.**

6. To enforce a custom Content Filtering Service policy for this group, click on the **CFS Policy** tab. Select the CFS policy from the **Policy** menu.

Note: *You create custom Content Filtering Service policies in the **Security Services>Content Filter** page.*

7. Click **OK**.

8 Hardware Failover

A reliable Internet connection has become a mission critical requirement for today's modern business. Internet connections today are used for accessing important real-time data for decision-making, reaching E-commerce customers, connecting with business partners, and extending communications across the distributed enterprise.

The loss of this mission critical connection can have serious, and sometimes disastrous, consequences on an organization.The following applications are examples of the mission critical nature of an Internet connection today:

- An Internet connection that provides customer access to an e-commerce site. In this case, connection downtime results in lost revenue.
- An Internet connection used to connect to business partners or an application service provider (ASP). Connection downtime can significantly disrupt business activities.
- Internet connections that provide access to critical resources for remote offices, telecommuters and mobile workers. Connection downtime can result in lower productivity for remote users.

Given the critical nature of many Internet connections, each element of the Internet connection needs to be highly reliable. SonicWALL **Hardware Failover** feature adds to the award-winning SonicWALL Internet security solution by assuring a highly reliable and secure connection to the Internet.

SonicWALL **Hardware Failover** eliminates network downtime by allowing the configuration of two SonicWALL appliances (one primary and one backup) as a **Hardware Failover** pair. In this configuration, the backup SonicWALL monitors the primary SonicWALL and takes over operation in the event of a failure. This ensures a secure and reliable connection between the protected network and the Internet.

Before Configuring Hardware Failover

Before attempting to configure two SonicWALL appliances as a **Hardware Failover** pair, check the following requirements:

- You have two (2) identical SonicWALL Internet Security Appliances. The **Hardware Failover** pair must consist of two identical SonicWALL models.
- You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (2) valid, static IP addresses are required to remotely manage both the primary SonicWALL and the backup SonicWALL.

⚠️

Alert!   *SonicWALL Hardware Failover does not support dynamic IP address assignment from your ISP.*

- Each SonicWALL in the **Hardware Failover** pair must have the same firmware version installed.
- Each SonicWALL in the **Hardware Failover** pair must have the same upgrades and subscriptions enabled. If the backup unit does not have the same upgrades and

subscriptions enabled, these functions are not supported in the event of a failure of the primary SonicWALL.

- All SonicWALL ports being used must be connected together with a hub or switch. If each SonicWALL has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

Tip!   *The two SonicWALL s in the Hardware Failover pair send "heartbeats" on their X5 Interfaces, which is a dedicated Hardware Failover link.*

Configuring Hardware Failover on the Primary SonicWALL

Click **Hardware Failover** on the menu bar to open the **Hardware Failover>Settings** page.
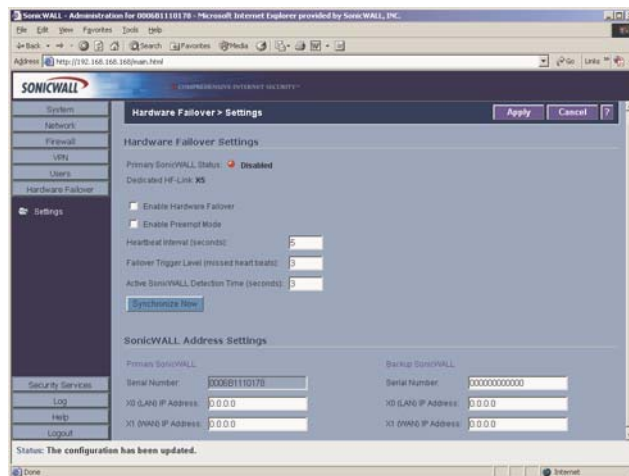
Hardware Failover Settings

The left half of the **SonicWALL Address Settings** section displays the primary SonicWALL serial number and network settings. The right half of the **SonicWALL Address Settings** section displays the primary and backup SonicWALL information. To configure **Hardware Failover**, follow the steps below:

1. Connect the primary SonicWALL and the backup SonicWALL to the network, but leave the power turned off on both units.

2. Turn on the primary SonicWALL unit and wait for the diagnostics cycle to complete. Configure all of the settings in the primary SonicWALL before configuring **Hardware Failover**.

3. Select **Enable Hardware Failover**.

4. Check the **Enable Preempt Mode** checkbox if you want the primary SonicWALL to take over from the backup SonicWALL whenever the primary becomes available (for example,

after recovering from a failure and restarting). If this option is not used, the backup SonicWALL remains the active SonicWALL.

Alert! *The primary and backup SonicWALL appliances use a "heartbeat" signal to communicate with one another. This heartbeat is sent between the SonicWALL appliances over the network segment connected to the LAN ports of the two SonicWALL appliances. The interruption of this heartbeat signal triggers the backup SonicWALL to take over operation from the primary unit of the Hardware Failover pair. The time required for the backup SonicWALL to take over from the primary unit depends on the Heartbeat Interval and the Failover Trigger Level.*

5. Enter the **Heartbeat Interval** time in seconds. Use a value between 3 seconds and 255 seconds. This interval is the amount of time in seconds that elapses between heartbeats passed between the two SonicWALLs in the **Hardware Failover** pair.

6. Enter the **Failover Trigger Level** in terms of the number of missed heartbeats. Use a value between 2 and 99 missed heartbeats. When the backup unit detects the number of consecutive missed heartbeats, the backup SonicWALL takes over operation from the primary unit.

   Example: Assume that the **Heartbeat Interval** and the **Failover Trigger Level** are 5 seconds and 2 missed heartbeats respectively. Based on these values, the backup SonicWALL takes over from the primary unit after 10 seconds in the event of a primary unit failure.

7. Enter the **Active SonicWALL Detection Time** in seconds using a value between 0 and 300. The default value of 0 is correct in most cases.When any SonicWALL (primary or backup) becomes active after bootup, it looks for an active SonicWALL configured for Hardware Failover on the network. If another SonicWALL is active, the SonicWALL that is booting up transitions to the **Idle** mode. In some cases, there may be a delay in locating another SonicWALL due to network delays or problems with hubs or switches.You can configure either the primary or backup SonicWALL to allow an increment of time (in seconds) to look for another SonicWALL configured for **Hardware Failover** on the network. You may enter a value between 0 and 300 seconds, but the default value of 0 seconds is sufficient in most cases.

Tip! *Synchronize Now is used for diagnostics and troubleshooting purposes and is not required for initial configuration.*

SonicWALL Address Settings

Primary SonicWALL

- **Serial Number** - The Primary SonicWALL serial number cannot be changed unless it is changed in **System >Administration**.
- **LAN IP Address** - This is a unique IP address for accessing the primary SonicWALL from the LAN whether it is **Active** or **Idle**.

⚠️

Alert! *This IP address is different from the IP address used to contact the SonicWALL in the Network settings.*

- **WAN IP Address** - This is a unique WAN IP address used to remotely manage the primary SonicWALL whether it is **Active** or **Idle**.

8. Configure the backup SonicWALL settings as follows:

- **Serial Number** - Enter the serial number of the backup SonicWALL.
- **LAN IP Address** - The unique LAN IP address used to access and manage the backup SonicWALL whether it is **Active** or **Idle**.

⚠️

Alert! *This IP address is different from the IP address used to contact the SonicWALL in the Network settings.*

- **WAN IP Address (Optional)** - This is a unique WAN IP address used to remotely manage the primary SonicWALL whether it is **Active** or **Idle**.

9. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

⚠️

Alert! *It is important during initial configuration that the backup SonicWALL has not been previously configured for use. If the backup SonicWALL has previous network settings, it is recommended to reset the SonicWALL to the factory default settings. Additionally, the password must be changed back to the default password of "password."*

10. Power on the backup SonicWALL used for **Hardware Failover**. After completing the diagnostic cycle, the primary SonicWALL auto-detects the presence of the backup SonicWALL and synchronizes the settings.

11. To confirm that the synchronization is successful, check the primary SonicWALL log for a **Hardware Failover** confirmation message. Alternatively, you can log into the backup SonicWALL using its unique LAN IP address and confirm that it is the backup SonicWALL.

If the primary SonicWALL fails to synchronize with the backup, an error message is displayed at the bottom of the screen. An error message also appears on the **System>Status** page. To view the error message on the **System>Status** page, click **System** on the left side of the browser.

To check the backup SonicWALL firmware version or serial number, log into the backup SonicWALL, click **System** on the left side of the browser window. Both the firmware version and the SonicWALL serial number are displayed at the top of the window.

If the backup SonicWALL serial number was incorrectly specified in the primary SonicWALL Web Management Interface, log into the primary SonicWALL and correct the backup SonicWALL Serial Number field.

At this point, you have successfully configured your two SonicWALLs as a **Hardware Failover** pair. In the event of a failure in the primary unit, the backup unit takes over operation and maintains the connection between the protected network and the Internet.

Configuration Changes

Configuration changes for the **Hardware Failover** pair can be made on the primary or the backup SonicWALL. The primary and backup SonicWALL appliances are accessible from their unique IP addresses. A label indicates which SonicWALL appliance is accessed.

⚠️
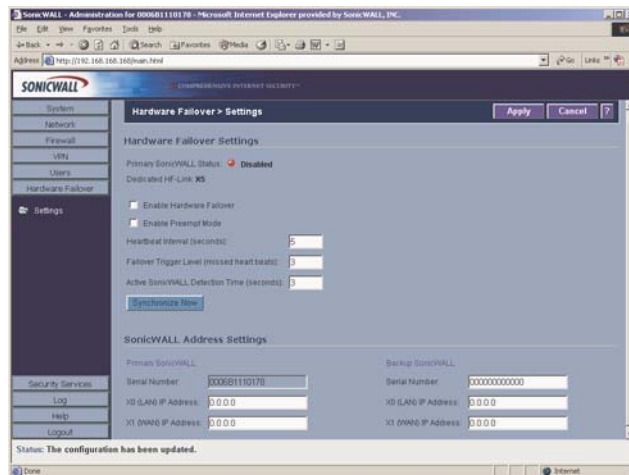
Alert! *You can change the IP address of either SonicWALL for the X0 or X1 interfaces as long as they're in the same subnet as the Primary and Backup Hardware Failover WAN/LAN IP address.*

Synchronizing Changes between the Primary and Backup SonicWALLs

Changes made to the **Primary** or **Backup** firewall are synchronized automatically between the two firewalls. If you click **Synchronize Now**, the Backup SonicWall restarts and becomes temporarily unavailable for use as a backup firewall.

Hardware Failover Status

If failure of the primary SonicWALL occurs, the backup SonicWALL assumes the primary SonicWALL LAN and WAN IP Addresses. There are three primary methods to check the status of the High Availability pair: the Hardware Failover Status window, E-mail Alerts and View Log. These methods are described in the following sections.

- **Hardware Failover Status** - One method to determine which SonicWALL is active is to check the Hardware Failover Settings Status indicator on the Hardware Failover>Settings page. If the primary SonicWALL is active, the first line in the page indicates that the primary SonicWALL is currently Active. It is also possible to check the status of the backup SonicWALL by logging into the LAN IP Address of the backup SonicWALL. If the primary SonicWALL is operating normally, the status indicates that the backup SonicWALL is currently Idle. If the backup has taken over for the primary, the status indicates that the backup is currently Active. In the event of a failure in the primary SonicWALL, you can access the Management Interface of the backup SonicWALL at the primary SonicWALL LAN IP Address or at the backup SonicWALL LAN IP Address. When the primary SonicWALL restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the primary SonicWALL becomes the active firewall and the backup firewall returns to Idle status.

- **E-mail Alerts Indicating Status Change** - If you have configured the primary SonicWALL to send E-mail alerts, you receive alert e-mails when there is a change in the status of the Hardware Failover pair. For example, when the backup SonicWALL takes over for the primary after a failure, an e-mail alert is sent indicating that the backup has transitioned from Idle to Active. If the primary SonicWALL subsequently resumes operation after that failure, and Preempt Mode has been enabled, the primary SonicWALL takes over and another e-mail alert is sent to the administrator indicating that the primary has preempted the backup.

- **View Log** - The SonicWALL also maintains an event log that displays the Hardware Failover events in addition to other status messages and possible security threats. This log may be viewed with a browser using the SonicWALL Management Interface or it may be automatically sent to the administrator's E-mail address. To view the SonicWALL log, click Log on the left side of the management interface.

Forcing Transitions

In some cases, it may be necessary to force a transition from one active SonicWALL to another – for example, to force the primary SonicWALL to become active again after a failure when **Preempt Mode** has not been enabled, or to force the backup SonicWALL to become active in order to do preventive maintenance on the primary SonicWALL.

To force such a transition, it is necessary to interrupt the heartbeat from the currently active SonicWALL. This may be accomplished by disconnecting the active SonicWALL's LAN port, by shutting off power on the currently active unit, or by restarting it from the Web Management Interface. In all of these cases, heartbeats from the active SonicWALL are interrupted, which forces the currently **Idle** unit to become **Active**.

To restart the active SonicWALL, log into the primary SonicWALL LAN IP Address and click **Tools** on the left side of the browser window and then click **Restart** at the top of the window. Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **Hardware Failover** pair takes over operation.

⚠️

Alert! *If the Preempt Mode checkbox has been checked for the primary SonicWALL, the primary unit takes over operation from the backup unit after the restart is complete.*

Configuration Notes

- If you are configuring the SonicWALL in **Transparent Mode** on the network, an additional IP address is necessary for the **Hardware Failover** configuration.
- For firmware upgrades, the Primary SonicWALL should be upgraded first. And during the upgrade, the backup SonicWALL should be disconnected from the LAN or turned off. When the firmware upgrade is performed on the backup SonicWALL, the Primary SonicWALL should be disconnected from the network or turned off.
- Changes made to the backup SonicWALL do not get updated on the Primary SonicWALL until synchronization takes place between the two units.

9 Security Services

SonicWALL, Inc. offers a variety of Security Services and upgrades to enhance the functionality of your SonicWALL. This chapter explains how to configure SonicWALL Content Filtering Service and SonicWALL Anti-Virus on your SonicWALL.

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

Security Services>Summary

The **Security Services>Summary** page provides a status listing of Security Services currently activated on your SonicWALL or available for activation.
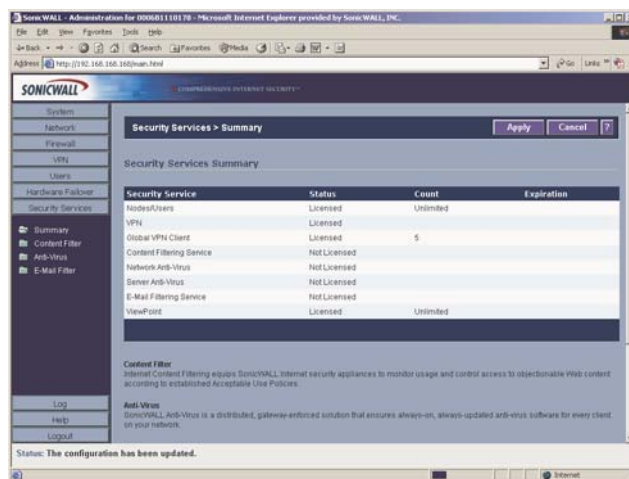
Security Services Summary

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.

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.

Security Services>Content Filtering

The SonicWALL Content Filtering Service (SonicWALL CFS) helps organizations increase productivity and reduce legal and privacy risks by automatically enforcing acceptable use policies while minimizing administration overhead. Integrated with SonicWALL's line of Internet Security Appliances, the SonicWALL Content Filtering Service enables organizations such as businesses, schools and libraries to maintain Internet access policies tailored to their specific needs.

With SonicWALL Content Filtering Service, 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. The SonicWALL Content Filtering Service automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWALL Content Filtering Service can 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 Filter List, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

Note: *Creating content filtering policies requires on the SonicWALL requires SonicWALL CFS Premium service.*

To activate a subscriptions, see the SonicWALL Content Filtering Service User's Guide located at <http://www.sonicwall.com/support/documentation.html>.
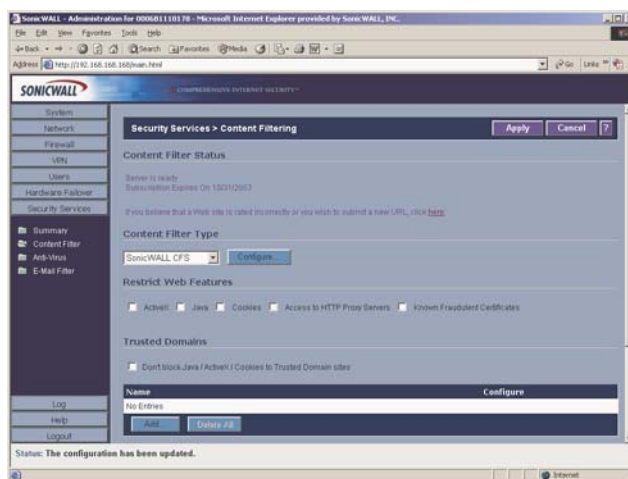
Content Filter

Content Filter Status

In this section, you can easily view 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.

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 as well as customize features such as allowed and forbidden domains as well as content filtering using keywords.
- **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>.

Restrict Web Features

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

- **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.

- **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.

- **Don't Block Java/ActiveX/Cookies to Trusted Domains**

  Select this option if you have trusted domains using Java, ActiveX, and Cookies. To add a trusted domain, enter the domain name into the **Add Trusted Domain** field. Click **Update** to add the domain to the list of trusted domains. To delete a domain, select it from the list, and then click **Delete**.

Trusted Domains

Trusted Domains can be added in the **Restrict Web Features** section of the **Configure** tab. If you trust content on specific domains, you can select **Don't block Java/ActiveX/Cookies to Trusted Domains** and then add the **Trusted Domains** to the SonicWALL using the **Add Trusted Domain** field. Java scripts, ActiveX, and cookies are not blocked from **Trusted Domains** if the checkbox is selected.

Message to Display when Blocking

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 CFS

Log into the SonicWALL using your administrator name and password. Click **Security Services** and then **Content Filter**. Select **SonicWALL CFS** from the **Content Filter Type** menu, and click **Configure**. The **SonicWALL Filter Properties** window is displayed.
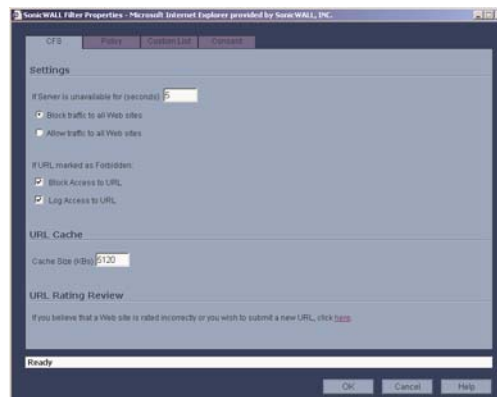
CFS

Settings

- **If Server is unavailable for (seconds)** - Sets the amount of time after the content filter server is unavailable before the SonicWALL takes action to either block access to all Web sites or allow traffic to continue to all Web sites.

    Block traffic to all Web sites - Select this feature if you want the SonicWALL to block all Web site access until the content filter server is available.

    Allow traffic to all Web sites - Select this feature if you want to allow access to all web sites when the content filter server is unavailable. However, Forbidden Domains and Keywords, if enabled, are still blocked.

- **If URL marked as blocked** - If you have enabled blocking by Categories and the URL is blocked by the server, there are two options available.

- **Block Access to URL** - Selecting this option prevents the browser from displaying the requested URL to the user.

- **Log Access to URL** - Selecting this option records the requested URL in the log file.

URL Cache

Configures the URL Cache size on the SonicWALL. The default **Cache Size (KBs)** is 3072.

Tip! A larger URL Cache size can provide noticeable improvements in Internet browsing response times.

URL Rating Review

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, you can click the here link to display the **SonicWALL CFS URL Rating Review Request** form for submitting the request.

Policy

The **Policy** tab allows you to create unique CFS policies.

- To create new policy, click **Add** to display the **Add CFS Policy** window.
- To edit an existing policy, click the **NotePad** icon in the **Policies** table for the entry.
- To delete a policy, click the **Trashcan** icon in the **Policies** table for the entry.
- To delete all policies in the **Policies** table, click the **Delete All** button.
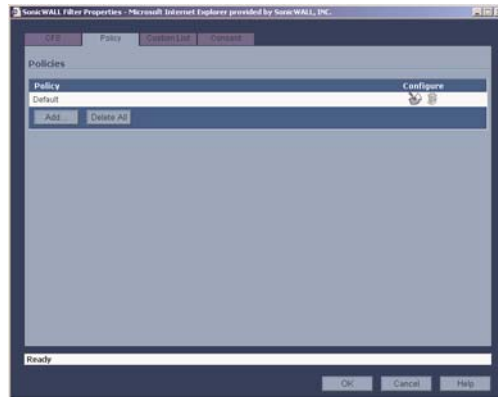
Adding a Policy

1. Click **Add** to display the **Add CFS Policy** window.
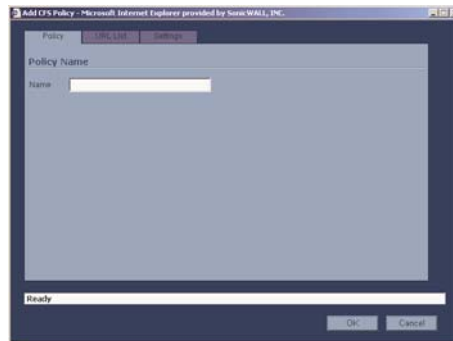
2. In the **Policy** tab, enter a name for the policy in the **Name** field.

3. Click the **URL List** tab.

4. Uncheck any category you want to pass through SonicWALL Content Filtering Service in the **Select Forbidden Categories** list. Move your mouse point over the **Down** or **Up** button to automatically scroll through the list of CFS categories. Select the **Select all categories** check box if you want to block all of these categories.

5. Click the **Settings** tab.
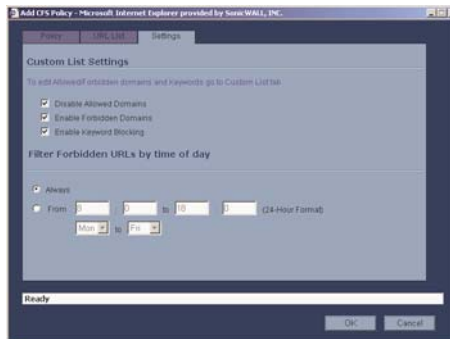
6. In **Custom List Settings** section, select any of the following settings:

   Disable Allowed Domains - select this setting to disable **Allowed Domains** from the **Custom List** tab in the **SonicWALL Filter Properties** window.
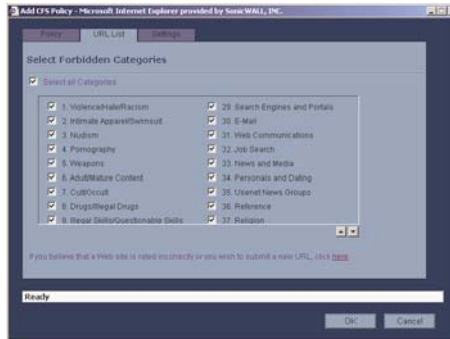   **Enable Forbidden Domains** - select this setting to enable **Forbidden Domains** from the **Custom List** tab in the **SonicWALL Filter Properties** window.
   Enable Keyword Blocking - select this setting to enable **Keyword Blocking** from the **Custom List** tab in the **SonicWALL Filter Properties** window.

7. To define specific times when **Content Filtering** is enforced, select

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

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

From/To - 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.

8. Click **OK**.

Note: *Content filtering policies are applied to user groups in the **User>Local Groups** page.*

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 allowed (accessed), forbidden (blocked), and include specific keywords to be used to block sites. Select the checkbox **Enable Allowed/Forbidden Domains** to activate this feature.
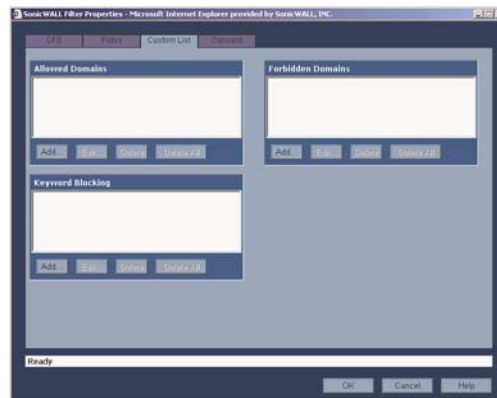
To allow access to a Web site that is blocked by the Content Filtering Service, click **Add**, and enter the host name, such as "www.ok-site.com", into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the Content Filtering 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 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 Domain**. Once the domain has been deleted, the **Status** bar displays **Ready**.

To enable blocking using keywords, click **Add** to display the **Add Keyword Entry** window. Enter the keyword to block in the **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**.

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.
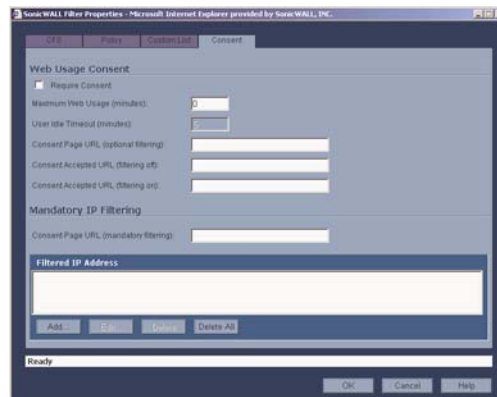
Web Usage Consent

- **Maximum Web usage** - 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 is 5 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. You must create this Web (HTML) page. 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 LAN.

- **"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 LAN.

Mandatory IP Filtering

- **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".

  Type 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** and enter the IP address of the computer in the **IP Address** field and click **OK** 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 Address.**

Security Services>Anti-Vius

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. Log into your mySonicWALL.com account for more information or contact your reseller.*

System Requirements for SonicWALL Anti-Virus on Clients

Microsoft Windows Version Supported

Windows 95, Windows 98, Windows 98 SE, Windows ME, Window NT 4.0 Workstation (SP 6 or later), Windows 2000 Professional (SP2 or later), Windows XP Home or Professional.

Supported Browsers

Microsoft Internet Explorer 5.5 with Service Pack 2 or later. Netscape Communicator 4.6 or later. Other browsers can be used on your computer but Internet Explorer is required for installation.

Hard Disk Space

VirusScan ASaP requires 7 MB of hard disk space over the requirements of Windows for a swap file. Windows generally needs twice as much free space as the amount of RAM for the swap file. A Windows 9x operating system with 32 MB of system RAM requires 64 MB free to operate properly and 7 additional MB for VirusScan ASaP.

System RAM

Minimum 32 MB for Windows 9x and Windows NT 4.x

64 MB or higher is recommended.

Minimum 64 MB for Windows 2000

128 MB or higher is recommended.

Network

SonicWALL Network Anti-Virus is designed to be a Web-based application and requires an Internet connection to install and update the software. Even though Rumor Technology shares updates, every computer using VirusScan ASaP must be able to connect to the Internet and access McAfee.com Web site to start the update process.

VirusScan ASaP only supports anonymous or Windows NT authentication proxies. Port 80 on your firewall must be open for outbound traffic to allow VirusScan ASaP updates.

Rumor technology functions entirely on the local area network (LAN). Port 6515 must be open on the proxy but can be closed on the firewall. Any network applications operating on the client computer that open port 6515 causes that node to malfunction as a Rumor server and also prevent other nodes from updating using Rumor. Also, any network applications running on the client server that open port 1967 causes the node to malfunction as a Rumor server or client.

Configuring SonicWALL Anti-Virus

This section contains detailed information on the activation, installation and configuration of the SonicWALL Network Anti-Virus subscription. Network Anti-Virus is configured from the SonicWALL Management Interface.

This section describes:

• **Activating the Network Anti-Virus Subscription**

• **Configuring Network Anti-Virus**

• **Managing Network Anti-Virus Subscriptions and Reports**

• **Configuring the Network Anti-Virus E-mail Filter**

To access the Anti-Virus status on the SonicWALL, click **System** on the left side of the browser window, and then click **Status.**
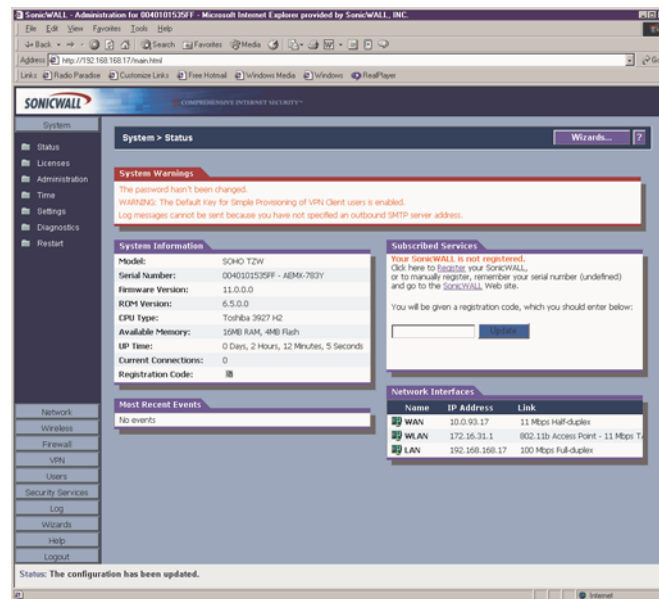

This page displays the current status of the SonicWALL. It contains an overview of the SonicWALL configuration as well as any other important messages. If a message stating, "This SonicWALL is not yet registered" is displayed, then it is necessary to complete the online registration before activating the Network Anti-Virus subscription. Click the link to <http://www.mySonicWALL.com> and complete the online registration process. Your SonicWALL must be registered before activating Network Anti-Virus.

Activating Your Subscription

To activate your Anti-Virus subscription, click **System**>**Licenses**, use the **click here** link, and then use the **click here** link on the **mySonicWALL.com Login** page to log into your mySonicWALL.com account. Or click **Security Services**>**Summary**, use the **click here** link, and then use the **click here** link on the **mySonicWALL.com Login** page to log into your mySonicWALL.com account.

Settings
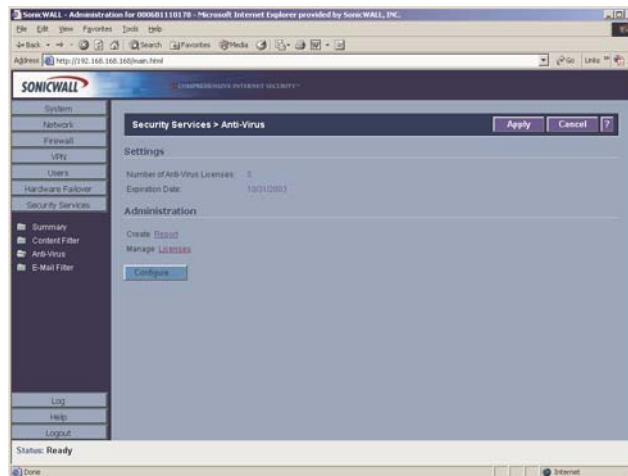
The **Security Services**>**Anti-Virus** page displays the following information:

- **Number of Anti-Virus Licenses** - Displays the number of anti-virus licenses that have been registered to the SonicWALL.
- **Expiration Date** - Displays the expiration date of the current subscription.

Tip!   *Each anti-virus license allows the use of SonicWALL Network Anti-Virus on one computer. period.*

Anti-Virus Administration

The **Anti-Virus Administration** section provides links to reports summarizing Anti-Virus activity on the network. Administrative activities such as changing passwords and renewing or adding licenses are also accessed here.

Reports

To view Network Anti-Virus statistics and reports, click the link labeled **Create Report**.
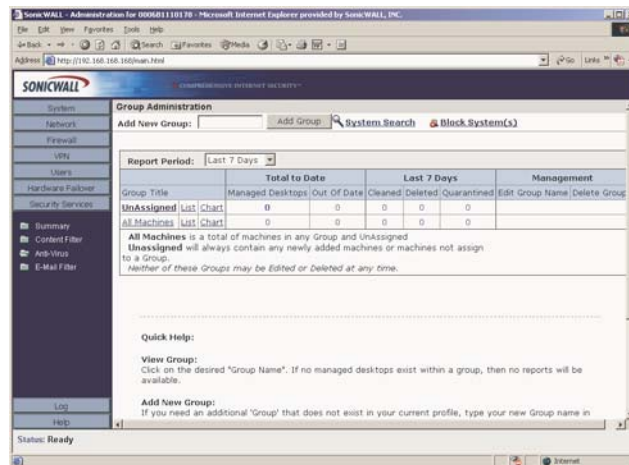
This page provides access to Anti-Virus reports. Information about the number of managed desktops, the number of outdated desktops, and the status of viruses cleaned, deleted or quarantined.

The default **Unassigned** and **All Machines** groups listed in the table cannot be edited or deleted. **All Machines** is the total of machines in any group and the **Unassigned** group. The **Unassigned** group contains any newly added machines or machine not added to a group.

You add additional groups that don't exist in your current profile by entering a group name in the **Add New Group** field and clicking **Add Group**. To delete a group, click **Delete** in the **Delete Group** column. To edit the group name, click **Edit Name** in the **Edit Group Name** column.

The **Block Systems** links displays the System Block Search page to locate and block unidentified desktops from your managed service. Using the Search function, enter one character or more and query via **System Name** or **E-Mail Address**. Alternatively, you can scroll through your **All Machines Summary** list and check the unidentified desktops to block.

Add or Renew Licenses

To manage Anti-Virus licenses, click the link labeled **Manage Licenses** on the **Anti-Virus> Settings** page, and type your mySonicWALL User Name and Password. Click **Submit**.

Add/Renew Anti-Virus Subscription

The standard SonicWALL Network Anti-Virus subscription package can be used to activate Network Anti-Virus, to increase the number of Anti-Virus licenses or to renew the current subscription. Since a Network Anti-Virus Activation Key may not be reused, additional subscription packages are required to add or renew Anti-Virus licenses.

1. Click **Renew** in the **Anti-Virus** line of the **Licenses>Summary** table.

2. Type the **New License Key** displayed on the back of the Network Anti-Virus Administrator's Guide or obtained from mysonicwall.com in the **New License Key** field. Multiple keys may be required. For example, if you have 30 computers on your network, you have purchased three 10-user subscriptions. Then, three Activation Keys are used for activation on the SonicWALL.

3. Click **Submit**. The operation takes a few seconds to complete. Once completed, the new number of Anti-Virus licenses appears in the **Licenses>Summary** table.

⚠

Alert! *When adding licenses, a new subscription is granted with a single new number of licenses and a single expiration date. Multiple grants are not tracked. The time remaining on the previous subscription is combined with the new 12-month period of the additional grant to create a single subscription.*

Renewing the Current Subscription

A **Subscription Renewal** is the process of renewing the existing Anti-Virus subscriptions and the number of Anti-Virus licenses does not increase. If the current subscription has 10 users, a 10-user renewal extends the subscription period by one year, but the total number of users remains the same.The purchase of a standard Anti-Virus subscription is necessary to renew a current license.

> *Tip!*   *When renewing a Network Anti-Virus subscription, the number of licenses for subscription renewal must be equal to the number of licenses in the current subscription.*

To renew the current subscription, complete the following steps:

1. Click **Renew** in the **Anti-Virus** line of the **Summary** table.

2. Type the Activation Key displayed on the back of the Complete Anti-Virus User's Guide in the **New License Key** field. Multiple keys can be required for activation. The number of licenses for renewal must equal the number of existing licenses to renew your subscription.

3. Click **Submit**. The operation takes a few seconds to complete. Once completed, the new expiration date appears in the Anti-Virus **Summary** window.

Anti-Virus License Sharing

Anti-Virus License Sharing allows you to distribute Anti-Virus licenses among multiple firewalls. License sharing assigns a License Sharing Group (LSG) to a firewall from which this feature is activated. You may then add other firewalls to the LSG, by their serial numbers and assign them Anti-Virus licenses from the pool of remaining available licenses in the LSG. To set up a License Sharing Group, follow the directions below:

1. Log into the Management station and click **Security Services**.

2. Click **Anti-Virus**.

3. Click **Manage Licenses,** and then click **Share** in the **Anti-Virus** line of the **Summary** table.

4. Type each SonicWALL appliance serial number in the **Add a new SonicWALL to the License Sharing Group**, and click **Add**.

5. The SonicWALL is added to the list for license sharing.

> *Tip!*   *You can only add SonicWALL appliances to your group that do not have active Anti-Virus subscriptions. The SonicWALL appliance must be registered at <http://www.mysonicwall.com> before it can be added to the group.*

6. To distribute licenses between the SonicWALL appliance, type the number of licenses for the first SonicWALL appliance into the **Licenses** field, and click **Update**. Repeat for each SonicWALL appliance.

You can also remove a SonicWALL appliance or redistribute the number of licenses between the SonicWALL appliances. To remove a SonicWALL appliance, click **Remove** next to the SonicWALL serial number. To redistribute licenses, type the new number of licenses into the **License** field and click **Update**. Repeat for each SonicWALL appliance.

The **License Availability** information changes as you change the license distribution or add more SonicWALLs.

Configuring Anti-Virus Policies

To configure Anti-Virus Policies, click **Configure** in the **Anti-Virus** page.
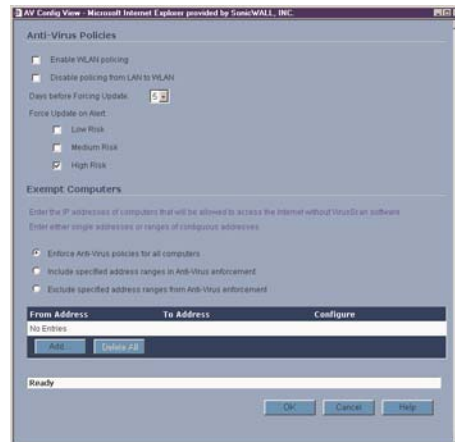
The following features are available in the **Anti-Virus Policies** section:

- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted Zones. Choosing this option allows computers on the LAN to access computers on the DMZ, even if anti-virus software is not installed on the LAN computers.

- **Days before forcing update** - This feature defines the maximum number of days may access the Internet before the SonicWALL requires the latest virus date files to be down-loaded.

- **Force Update on alert** - SonicWALL, Inc. broadcasts virus alerts to all SonicWALL appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the **Days before forcing update** selection.

  In addition, every virus alert is logged, and an alert message is sent to the administrator. Please refer to the **Logging and Alerts** section of the SonicWALL Administrator's Guide for instructions on configuring log and E-mail alerts.

- **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.

- **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.

- **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

Anti-Virus Enforcement

SonicWALL Network Anti-Virus currently supports Windows 95, 98, NT, XP, and 2000 platforms. In order to access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement. There are three options for defining exempt computers:

- **Enforce Anti-Virus policies for all computers** - Selecting this option forces computers to install VirusScan ASaP in order to access the Internet or the DMZ. This is the default configuration.
- **Include specified address range in the Anti-Virus enforcement** - Choosing this option allows the administrator to define ranges of IP addresses to receive Anti-Virus enforcement. If you select this option, specify a range of IP addresses to be enforced. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered for enforcement.
- **Exclude specified address range in the Anti-Virus enforcement** - Selecting this option allows the administrator to define ranges of IP addresses that are exempt from Anti-Virus enforcement. If you select this option, specify the range of IP addresses are exempt. Any computer requiring unrestricted Internet access needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered.

Network Anti-Virus E-Mail Filter

The **Network Anti-Virus 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. This feature is available only with the purchase of an E-mail Filter subscription.

Click **Anti-Virus** on the left side of the browser window, and then click **E-Mail Filter**.
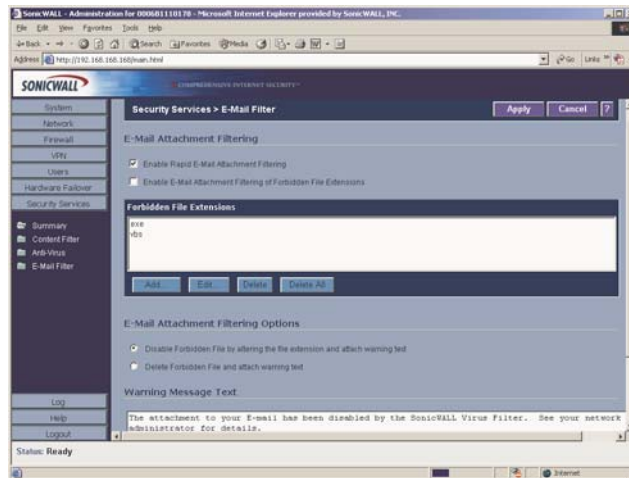
E-Mail Attachment Filtering

The **E-mail Attachment Filtering** section configures the file extensions that are filtered by the SonicWALL.

- **Enable Rapid E-Mail Attachment Filtering** - Select this feature to automatically block the most prevalent e-mail viruses on the current Rapid E-mail Attachment Block List.
- **Enable E-Mail Attachment Filtering of Forbidden File Extensions** - Select this check box to filter E-mail attachments. Click **Add**. In the **Add Forbidden File Extension**, type the file extensions to be filtered in the **File Extension** field. Hackers commonly spread viruses through Visual Basic and Windows Executable files, therefore "vbs" and "exe" are provided as default extensions for this feature. To add a file extension to the list, type the file extension in the **File Extension** field and click **OK**. To delete a file extension, select the file extension from the list, and click **Delete**.

E-Mail Attachment Filtering Options

In this section, the administrator chooses the action that the SonicWALL performs when filtering E-mail attachments. The attached file can either be deleted or it can be disabled by altering the file extension. In either case, the original E-mail text is still sent to the intended recipient.

- **Disable Forbidden File by altering the file extension and attach warning text** - Select this option to disable forbidden attachment files as they pass through the SonicWALL and include a warning message created in the **Warning Message Text** field. The SonicWALL replaces the third character of file extensions with "_". If the E-mail attachment is a valid

file, the E-mail recipient may return the attachment to its original file extension without damaging the file.

- **Delete Forbidden File and attach warning text** - Select this option to delete forbidden attachment files as they pass through the SonicWALL and include a warning message created in the **Warning Message Text** field.

Warning Message Text

This is a warning message that can be customized and added to E-mails filtered by the **Network Anti-Virus E-mail Filter**. Type the desired warning message in the **Warning Message Text** box. Up to 256 alphanumeric characters may be entered.

When you have configured the **E-mail Filter** settings, click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

E-Mail Blocking

Select **Block SMTP E-Mail Fragments (Content-Type: message\partial)** to enable blocking of partial e-mail messages. E-mail fragments are e-mail messages with the MIME Content-Type: message/partial in the header. Partial e-mails can be a security threat by allowing viruses to escape undetected by virus scanners because they are fragmented. The virus becomes fully functional once reassembled on the client.

10 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**.
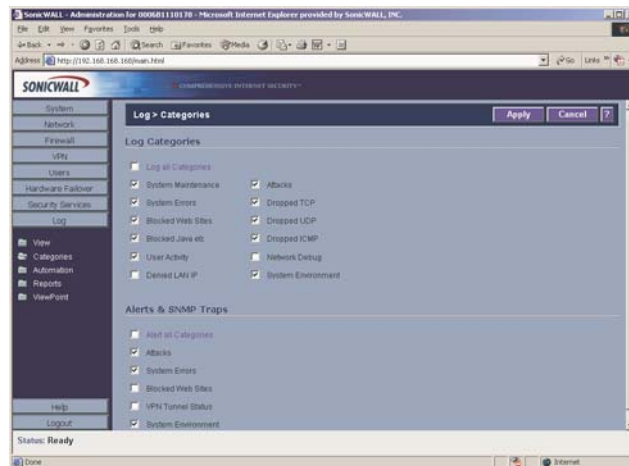
SonicWALL Log Messages

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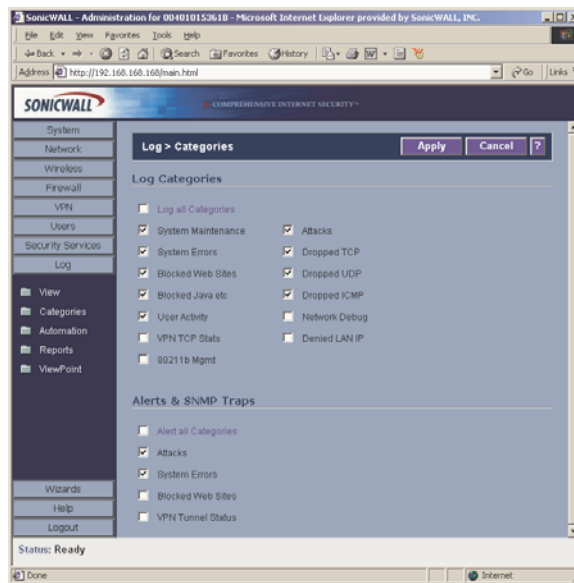
- **Log all Categories**

  Select **Log all Categories** to begin logging all event categories.

- **System Maintenance**

  Logs general system activity, such as administrator log ins, and 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.

- **Denied LAN IP**

  Logs all LAN IP addresses denied by the SonicWALL.

- **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.

- **System Environment**

  Logs physical unit events such as fan failure or power disruption.

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**

  Log entries categorized as **System Environment** generate alert messages.

Once you have configured the **Log Settings** 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.
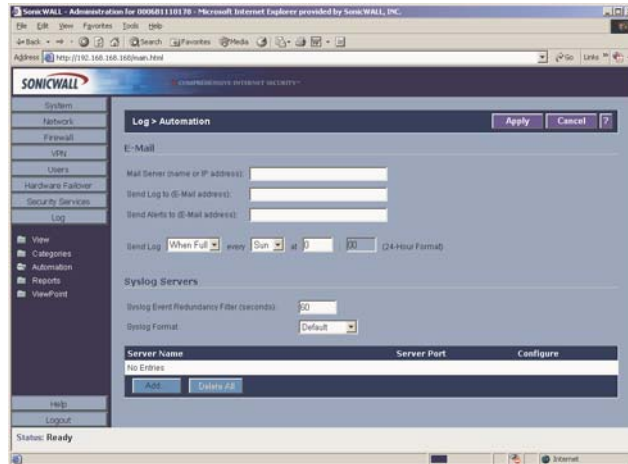
E-mail

1. **Mail Server** - to e-mail log or alert messages, type 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** - type 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** - type 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. Type 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, type 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 Analyzers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the **Syslog** data.

To add syslog servers to the SonicWALL, click **Add**. The **Add Syslog Server** window is displayed.
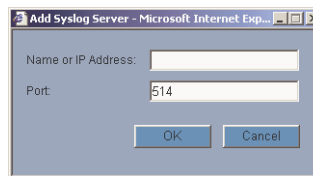
1. Type the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL are then sent to the servers. Up to three Syslog Server IP addresses can be added.

2. If your syslog is not using the default port of 514, type 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 (seconds) - This 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** 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**.
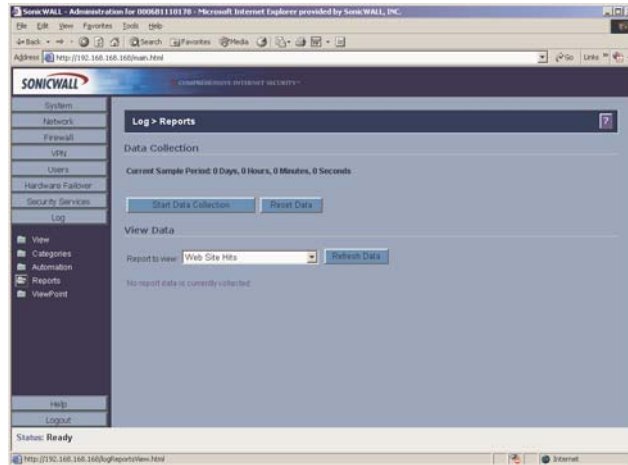
Data Collection

The **Reports** window 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 analyzed 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.

SonicWALL ViewPoint

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

11 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.

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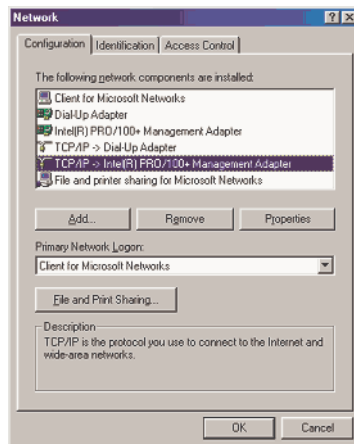
1. From the **Start** list, highlight **Settings** and then select **Control Panel**.Double-click the **Network** icon in the **Control Panel** window.

2. Double-click **TCP/IP** in the **TCP/IP Properties** window.
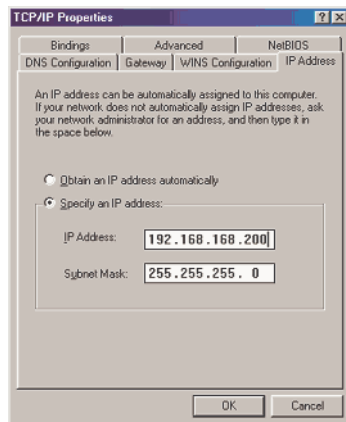
3. Select **Specify an IP Address**.

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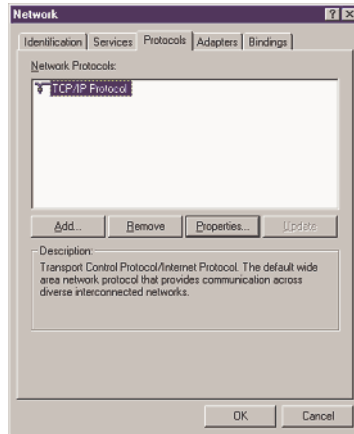
1. From the **Start** list, highlight **Settings** and then select **Control Panel**.

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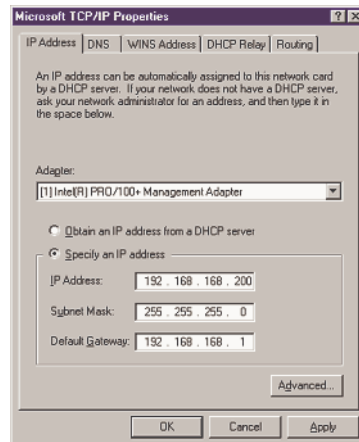
5. Type "192.168.168.200" in the **IP Address** field.

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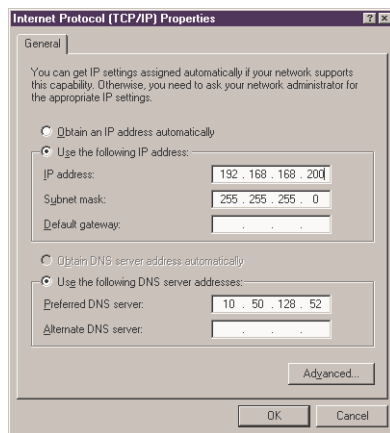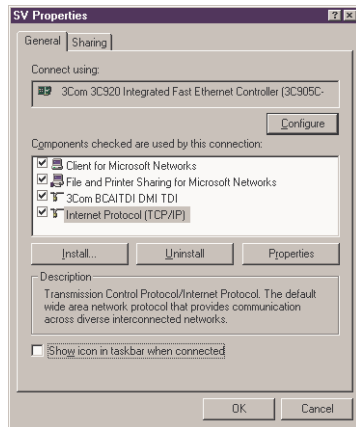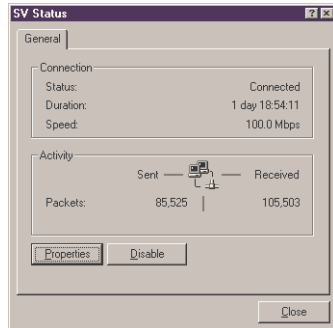
1. In Windows 2000, click **Start**, then **Settings**.

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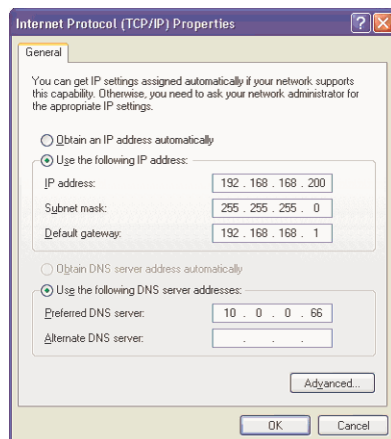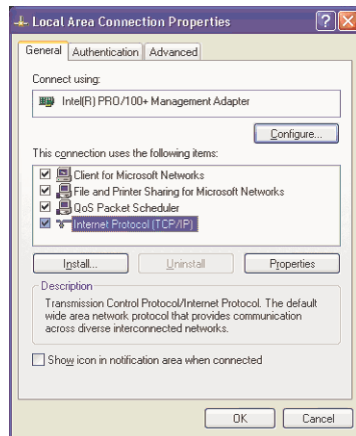
1. Open the **Local Area Connection Properties** window.

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**.

Appendix C- Configuring RADIUS and ACE Servers

Individual users must have their privileges defined on the RADIUS server used for authenticating the users. Global user privileges can be configured on the RADIUS tab of the SonicWALL management interface, but SonicWALL-specific privileges must be configured on the RADIUS server.

Different vendors also have different methods of configuring the privileges on their servers. In some cases, it can be complex, but most allow for the configuration of group profiles or policies which means you can configure the attributes once per group.

This Appendix describes the configuration of user privileges on various vendors of RADIUS servers, and also notes the particular RADIUS servers which support CHAP (Challenge Handshake Authentication Protocol) mode. CHAP support is required if HTTPS is not available for logging into the SonicWALL.

Steel Belted RADIUS (Funk Software)

Steel Belted RADIUS server version 3.0 from Funk Software supports pre-configuration of vendor-specific attributes in a vendor-specific dictionary file. SonicWALL.dct is the new dictionary file for the SonicWALL.

To configure the Steel Belted RADIUS server to include the SonicWALL.dct file, use the following instructions:

1. Locate the directory that Steel Belted RADIUS is installed, **C:\RADIUS** by default, and copy the SonicWALL.dct file into **C:\RADIUS\Service** folder.

2. Edit the vendor.ini file located in the Service folder using Notepad. Add the following lines so that they are in alphabetical order with the other vendor products in the file:

vendor-product	= SonicWALL Firewall
dictionary	= SonicWALL
ignore-ports	= no
port-number-usage	= per-port-type
help-id	= 2000

3. Edit the dictiona.dcm file using Notepad, and add the entry **@sonicwall.dct** to it, keeping the entry in alphabetical order with the existing entries.

4. Restart the Windows service called **Steel Belted RADIUS Service**.

5. Run the **Steel Belted RADIUS Administrator**.

6. Click **RAS Clients**, and select **SonicWALL Firewall** from the **Make/Model** list. Click **Save**.

If there is no entry for SonicWALL Firewall, be sure that steps 2 and 3 were performed correctly.

Configuring User Privileges

To configure user privileges, follow these steps:

1. With **Steel Belted RADIUS Administrator** open, click **Users** and select the User to configure. Or select a profile to be configured from the **Profile Name** menu.

2. Click **Ins** and select **SonicWALL-User-Privilege** from the **Available Attributes** list.

3. Select the privilege to be set, and click **Add**. Repeat until all of the privileges are added for the user.

Steel Belted RADIUS does support CHAP, so authentication takes place even if HTTPS is not available when logging into the SonicWALL management interface. Select **Allow PAP or CHAP** when setting user passwords.

ACE Server (RSA)

The ACE Server, version 4.1, from RSA, configures RADIUS attributes into the profiles. It does not support pre-configuration of vendor-specific attributes on the server. It also only allows one vendor-specific attribute to be set per profile, and only support vendor-specific attributes containing ASCII text. User privileges are added manually using the following instructions:

1. Open the **ACE Server Database Administrator** program.

2. Select **Edit Profiles** from the menu, and select the profile to be configured with user privileges. Click **OK**.

3. From the **Available Attributes** menu, select **Vendor-Specific**, and then click **Add Attribute... .**

4. Set the value to 8741 2 "***privileges-list***" where privileges list is a comma-separated list of 2-letter privileges, as follows:

   RA - Remote Access

   BF - Bypass Filters

   VC - Access from VPN Client

   VA - Access to VPNs

   LM - Limited Management

For example, to configure a profile with Access to VPN privileges and allow Access from VPN Client, the value is set as follows:

   8714 2 "VA, VC"

The ACE Server from RSA does not support CHAP with RADIUS, therefore it is necessary to configure the SonicWALL to use HTTPS when logging into the SonicWALL management interface.

ACS Server (Cisco)

The ACS server, version 2.6, from Cisco does not support the configuration of vendor-specific privileges. Therefore, if a ACS Server is deployed, user privileges cannot be configured on the server.

The ACS server can still be used for authentication if the RADIUS users are configured globally on the SonicWALL to have the same privileges. Also, the ACS server supports CHAP, so it can be used if HTTPS is not available when logging into the SonicWALL management interface.

Internet Authentication Service (Windows NT/2000 Server)

The RADIUS server used on Microsoft Windows NT and Windows 2000 servers is known as the Internet Authentication Service (IAS). The RADIUS attributes are configured using policies, and does not support pre-configuration of vendor-specific attributes. The RADIUS attributes are entered manually into the service by using the following instructions:

1. Open **IAS**, and select **Remote Access Policies**.

2. Select the policy to be configured for user privileges, and right click. Select **Properties** from the list.

3. Click **Edit Profile**, and then click **Advanced**. Click **Add**.

4. Select **Vendor-Specific** from the list, and click **Add**. The **Multivalued Attribute Information** box appears.

5. Click **Add**. The **Vendor-Specific Attribute Information** box appears.

6. Click **Enter Vendor Code**, and enter **8741** as the vendor code.

7. Click **Yes, It conforms**, and then click **Configure Attribute**. The **Configure VSA (RFC compliant)** window appears.

8. Enter 1 as the **Vendor-assigned attribute number**.

9. Select **Decimal** as the **Attribute format**.

10. Enter one of the following values as the **Attribute** value. Each value defines a privilege for users within the policy.

    1 - Remote Access

    2 - Bypass Filters

    3 - Access from VPN Client

    4 - Access to VPNs

11. Click **OK**, and then **OK** again to return to the **Multivalued Attribute Information** window.

Repeat Steps 5 through 11 for each privilege configured for a policy.

For further information, refer to "To configure vendor-specific attributes for a remote access policy" in the IAS help file.

With IAS, the user database is located on the domain controller. Therefore, IAS only supports CHAP with RADIUS if the domain controller is configured to store passwords using reversible

encryption for all users. If the domain controller is not configured in this manner, it is necessary to use HTTPS to log into the SonicWALL management interface.