SONICWALL

Internet Security Appliances

SONICWALL

Contents

Copyright Notice

Specifications and descriptions subject to change without notice.

LIMITED WARRANTY

SonicWALL, Inc. warrants the SonicWALL Internet Security Appliance (the Product) for one (1) year from the date of purchase against defects in materials and workmanship. If there is a defect in the hardware, SonicWALL will replace the product at no charge, provided that it is returned to SonicWALL with transportation charges prepaid. A Return Materials Authorization (RMA) number must be displayed on the outside of the package for the product being returned for replacement or the product will be refused. The RMA number can be obtained by calling SonicWALL Customer Service between the hours of 8:30 AM and 5:30 PM Pacific Standard Time, Monday through Friday.

Phone:(408) 752-7819

Fax:(408) 745-9300

Web: <http://www.sonicwall.com/support>

This warranty does not apply if the Product has been damaged by accident, abuse, misuse, or misapplication or has been modified without the written permission of SonicWALL.

In no event shall SonicWALL, Inc. or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or other pecuniary loss) arising out of the use of or inability to use the Product.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion can not apply to you. Where liability can not be limited under applicable law, the SonicWALL liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you can have other rights which vary from state to state.

By using this Product, you agree to these limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

No dealer, agent, or employee of SonicWALL is authorized to make any extension or addition to this warranty.

About this Guide

Thank you for purchasing the SonicWALL 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 Internet Security appliance features. For complete installation information, refer to the SonicWALL Internet Security Appliance *Installation Guide*.

Organization of This Guide

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

Chapter 2, **Managing Your SonicWALL**, provides a brief overview of the SonicWALL Web Management Interface.

Chapter 3, **Network Settings**, describes the configuration of the SonicWALL IP settings, time, and password.

Chapter 4, **Logging and Alerting**, illustrates the SonicWALL logging, alerting, and reporting features.

Chapter 5, **Content Filtering and Blocking**, describes SonicWALL Web content filtering, including subscription updates and customized Web blocking.

Chapter 6, **Web Management Tools**, provides directions to restart the SonicWALL, import and export settings, upload new firmware, and perform diagnostic tests.

Chapter 7, **Network Access Rules**, explains how to permit and block traffic through the SonicWALL, set up servers, and enable remote management.

Chapter 8, **Advanced Features**, describes advanced SonicWALL settings, such as One-to-One NAT and Automatic Web Proxying.

Chapter 9, **DHCP Server**, describes the configuration and setup of the SonicWALL DHCP server.

Chapter 10, **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 11, **High Availability**, describes the configuration of two SonicWALLs (one primary and one backup) as a **High Availability** pair.

Chapter 12, **SonicWALL Options and Upgrades**, presents a brief summary of the SonicWALL's subscription services, firmware upgrades and other options.

Chapter 13, **Hardware**, provides a description of the front and back of SonicWALL Internet security appliances, including LED lights and ports.

Chapter 14,**Troubleshooting Guide**, shows solutions to commonly encountered problems.

Appendix A, **Technical Specifications**, lists the SonicWALL specifications.

Appendix B, **SonicWALL Support Solutions**, descriptions of available support packages from SonicWALL.

Appendix C, **Introduction to Networking**, provides an overview of the Internet, TCP/IP settings, IP security, and other general networking topics.

Appendix D, **IP Port Numbers**, offers information about IP port numbering.

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

Appendix F, **Erasing the Firmware**, describes the firmware erase procedure.

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

Appendix H, **Regulatory Compliance**, presents important emissions standards approvals and EMC information.

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.

1 Introduction

Your SonicWALL Internet Security Appliance

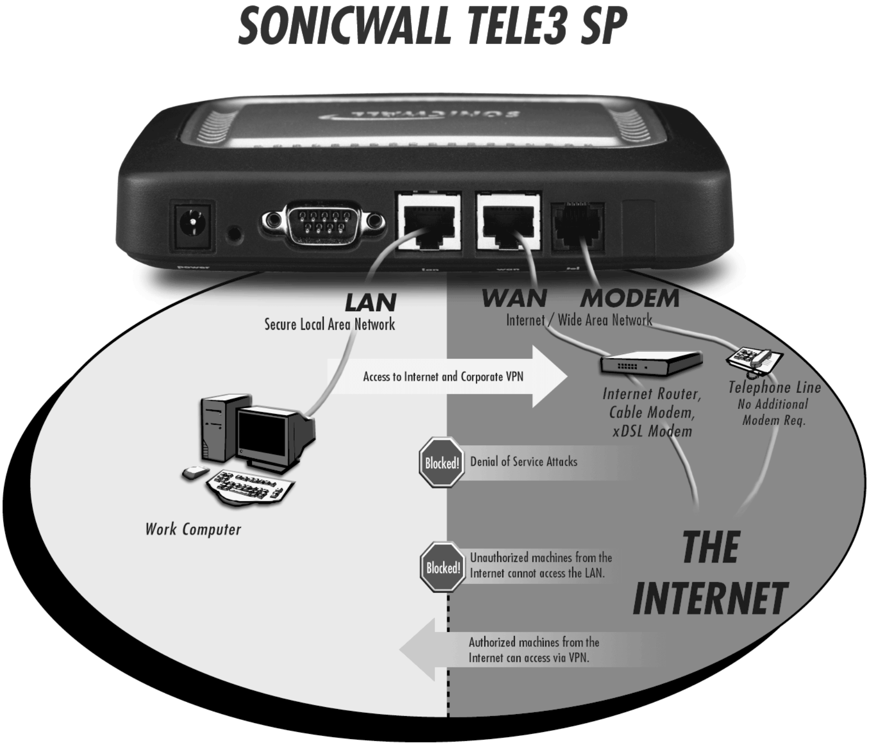
The SonicWALL SonicWALL Internet security appliance provides a complete security solution that protects your network from attacks, intrusions, and malicious tampering. In addition, the SonicWALL filters objectionable Web content and logs security threats. SonicWALL VPN provides secure, encrypted communications to business partners and branch offices.

The SonicWALL 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 encrypt 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.

For complete installation instructions, refer to the *SonicWALL Installation Guide*.

SonicWALL Internet Security Appliance Functional Diagram

The following figure illustrates the SonicWALL Internet security appliance functions.


SONICWALL TELE3 SP
LAN
Secure Local Area Network
WAN
MODEM
Internet / Wide Area Network
Access to Internet and Corporate VPN
Internet Router, Cable Modem, xDSL Modem
Telephone Line
No Additional Modem Req.
Work Computer
Blocked!
Denial of Service Attacks
Blocked!
Unauthorized machines from the Internet cannot access the LAN.
THE INTERNET
Authorized machines from the Internet can access via VPN.

By default, the SonicWALL SonicWALL Internet security appliance allows outbound access from the LAN to the Internet and blocks inbound access from the Internet to the LAN. Users on the Internet are restricted from accessing resources on the LAN unless they are authorized remote users or Network Access Rules were created to allow inbound access.

If the SonicWALL includes a DMZ port, users on the LAN and the Internet have access to the devices on the DMZ.

SonicWALL 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.

- **Hacker Attack Prevention**

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

- **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.

- **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 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. The SonicWALL also sends an e-mail with firmware release notes.

- **DMZ Port**

  The SonicWALL PRO 100, SonicWALL PRO 200, and the SonicWALL PRO 300 include a DMZ port allowing users to access public servers, such as Web and FTP servers. While Internet users have unlimited access to the DMZ, the servers on the DMZ are still protected against DoS attacks.

- **SNMP Support**

  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 Internet Security appliances and receive notification of any critical events as they occur on the network.Content Filtering

- **SonicWALL Content Filtering Overview**

  You can use the SonicWALL Web content filtering to enforce your company's Internet access policies. The SonicWALL blocks specified categories, such as violence or nudity, using an optional Content Filter List. Users on your network can bypass the Content Filter List by authenticating with a unique user name and password.

- **Content Filter List Updates (optional)**

  Since content on the Internet is constantly changing, the SonicWALL automatically updates the optional Content Filter List every week to ensure that access restrictions to new and relocated Websites and newsgroups are properly enforced.

- **Log and Block or Log Only**

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

- **Filter Protocols**

  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 compliments 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 DHCP Server offers centralized management of TCP/IP client configurations, including IP addresses, gateway addresses, and DNS addresses. Upon startup, each network client receives its TCP/IP settings automatically from the SonicWALL DHCP Server.

- **DHCP Client**

  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.

Installation and Configuration

- **Installation Wizard**

  The SonicWALL Installation Wizard helps quickly install and configure the SonicWALL.

- **Online help**

  SonicWALL help documentation is built into the SonicWALL Web Management Interface for easy access during installation and management.

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.

- **VPN Client Software for Windows**

  Mobile users with dial-up Internet accounts can securely access remote network resources with the SonicWALL VPN Client. The SonicWALL 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 the **Content Filter List, 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 Managing Your SonicWALL Internet Security Appliance

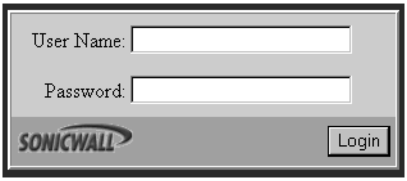
This chapter contains a brief overview of SonicWALL management commands and functions. The commands and functions are accessed through the SonicWALL Web Management Interface.

1. Log into the SonicWALL using a Web Browser

You can manage the SonicWALL from any computer connected to the LAN port of the SonicWALL using a Web browser. The computer used for management is referred to as the “Management Station".

***Note**: To manage the SonicWALL, your Web browser must have Java and Java applets enabled and support HTTP uploads.*

2. Open a Web browser and type the SonicWALL IP address, initially, "192.168.168.168", into the **Location** or **Address** field at the top of the browser. An **Authentication** window with a **Password** dialogue box is displayed.



3. Type “admin” in the **User Name** field and the password previously defined in the **Installation** Wizard in the **Password** field. Passwords are case-sensitive. Enter the password exactly as defined and click **Login**.

***Note**: All SonicWALLs are configured with the User Name “admin” and the default Password “password”. The User Name is not configurable.*

If you cannot log into the SonicWALL, a cached copy of the page is displayed instead of the correct page. Click **Reload** or **Refresh** on the Web browser and try again. Also, be sure to wait until the Java applet has finished loading before attempting to log in.

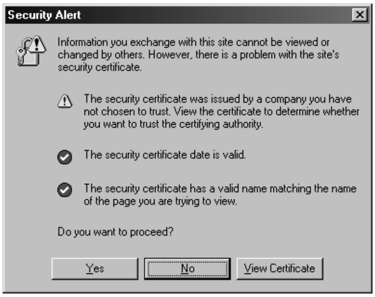
Once the password is entered, an authenticated management session is established. This session times out after 5 minutes of inactivity. The default time-out can be increased on the **Password** window in the **General** section.

HTTPS Management

To enhance the security of the SonicWALL family of Internet Security appliances, **HTTPS Management** using Secure Socket Layer (SSL) is now supported when you log into your Management interface using https://IP Address where the IP address is the SonicWALL LAN IP address. For example, if the LAN IP address of your SonicWALL appliance is 192.168.168.1, you can log into it by typing https://192.168.168.1. Access is encrypted using SSL technology for a secure connection.

HTTPS Management allows secure access to the SonicWALL without a VPN client. It is a simple and secure way to manage your SonicWALL from both the LAN and the WAN.

The first time you access the SonicWALL Management interface using HTTPS, you may see the following information message:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

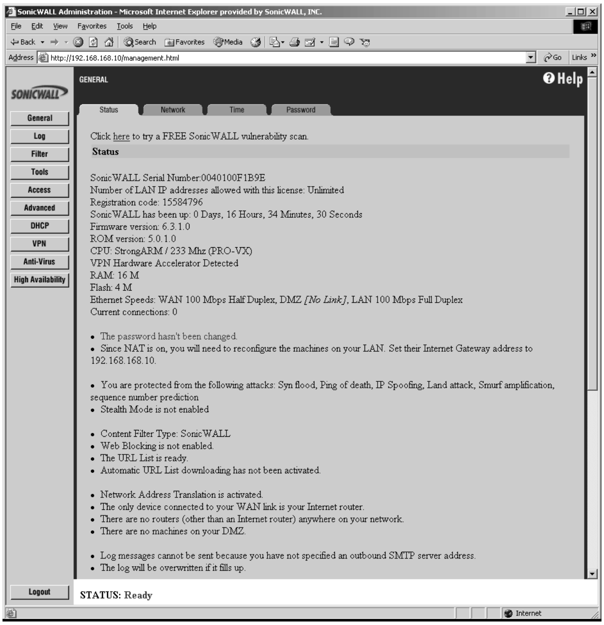
Do you want to proceed?

Click **Yes** to continue the login process. SSL is supported by Netscape 4.7 and higher, as well as Internet Explorer 5.5 and higher.

HTTPS management supports the following versions of SSL: SSLv2, SSLv3, and TLSv1. Also, the following encryption ciphers are supported: RC4-MD5, EXP-RC4-MD5, DES-CBC3-SHA, DES-CBC-SHA, RC4-SHA, EXP-RC2-CBC-MD5, NULL-SHA, and NULL-MD5. The RSA key used is 1024-bit.

Status

To view the **Status** tab, log into your SonicWALL using your Web browser. Click **General** and then click the **Status** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
GENERAL
Help
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Status
Network
Time
Password
Internet

Click here to try a FREE SonicWALL vulnerability scan.

Status

SonicWALL Serial Number:0040100F1B9E
Number of LAN IP addresses allowed with this license: Unlimited
Registration code: 15584796
SonicWALL has been up: 0 Days, 16 Hours, 34 Minutes, 30 Seconds
Firmware version: 6.3.1.0
ROM version: 5.0.1.0
CPU: StrongARM / 233 Mhz (PRO-VX)
VPN Hardware Accelerator Detected
RAM: 16 M
Flash: 4 M
Ethernet Speeds: WAN 100 Mbps Half Duplex, DMZ *[No Link]*, LAN 100 Mbps Full Duplex
Current connections: 0

- The password hasn't been changed.
- Since NAT is on, you will need to reconfigure the machines on your LAN. Set their Internet Gateway address to 192.168.168.10.

- You are protected from the following attacks: Syn flood, Ping of death, IP Spoofing, Land attack, Smurf amplification, sequence number prediction
- Stealth Mode is not enabled

- Content Filter Type: SonicWALL
- Web Blocking is not enabled.
- The URL List is ready.
- Automatic URL List downloading has not been activated.

- Network Address Translation is activated.
- The only device connected to your WAN link is your Internet router.
- There are no routers (other than an Internet router) anywhere on your network.
- There are no machines on your DMZ.

- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- The log will be overwritten if it fills up.

STATUS: Ready

***Note**: The SonicWALL Status window is displayed above. Each SonicWALL Internet Security appliance displays unique characteristics, such as the presence of VPN acceleration hardware or a different amount of memory.*

The Status tab displays the following information:

- **SonicWALL Serial Number** - the serial number of the SonicWALL unit.
- **Number of LAN IP addresses allowed with this license** - number of IP addresses that can be managed by the SonicWALL
- **Registration code** - the registration code generated when the SonicWALL is registered at <http//www.mysonicwall.com>.
- **SonicWALL Active time** - the length of time in days, hours and minutes that the SonicWALL is active.
- **Firmware version** - shows the current version number of the firmware installed on the SonicWALL.
- **ROM version** - indicates the version number of the ROM.
- **CPU** - displays the type and speed of the SonicWALL processor.
- **VPN Hardware Accelerator Detected** - indicates the presence of a VPN Hardware Accelerator in the firewall. This allows better throughput for VPN connections.

- **RAM -** shows the amount of Random Access Memory on the board.
- **Flash** - indicates the size of the flash on the board.
- **Ethernet Speeds** - displays network speeds of the network card.
- **Current Connections** - number of computers connected to the SonicWALL.

Other SonicWALL general status information is displayed in this section relating to other features in the SonicWALL such as the type of network settings in use, log settings, content filter use, and if **Stealth Mode** is enabled on the SonicWALL.

The **General**, **Log**, **Filter**, **Tools**, **Access**, **Advanced**, **DHCP**, **VPN**, **Anti-Virus**, and **High Availability** buttons appear on the left side of the window. When one of the buttons is clicked, related management functions are selected by clicking the tabs at the top of the window.

A **Logout** button at the bottom of the screen terminates the management session and redisplays the **Authentication** window. If **Logout** is clicked, you must log in again to manage the SonicWALL. **Online help** is also available. Click **Help** at the top of any browser window to view the help files stored in the SonicWALL.

The **Status** window, shown on the previous page, displays the status of your SonicWALL. It contains an overview of the SonicWALL configuration, as well as any important messages. Check the **Status** window after making changes to ensure that the SonicWALL is configured properly.

CLI Support and Remote Management

Out-of-band management is available on SonicWALL Internet security appliances using the **CLI** (**Command Line Interface**) feature. SonicWALL Internet security appliances can be managed from a console using typed commands and a modem or null-modem cable that is connected to the serial port located on the back of the SonicWALL appliance. The only modem currently supported is the US Robotics v.90/v.92 modem. CLI communication requires the following modem settings:

- **9600 bps**
- **8 bits**
- **no parity**
- **no hand-shaking**

After the modem is accessed, a terminal emulator window such as a hyper terminal window is used to manage the SonicWALL Internet security appliance. Once the SonicWALL is accessed, type in the User Name and password: admin for **User Name** and then the password used for the management interface.

The following CLI commands are available for the SonicWALL:

- **?** or **Help** - displays a listing of the top level commands available.
- **Export** - exports preferences from the SonicWALL using Z-modem file transfer protocol.
- **Import** - imports preferences from the SonicWALL using Z-modem file transfer protocol.
- **Logout** - logout of the SonicWALL appliance.

- **Ping** - pings either an IP address or domain name for a specified host.
- **Restart** - restart the SonicWALL
- **Restore** - restores the factory default settings for all saved parameters with the exception of the password, the LAN IP address, and the subnet mask.
- **Status** - displays the information typically seen on the Web management interface tab labeled **General**.
- **TSR -** retrieves a copy of the tech support report using Z-modem file transfer protocol.

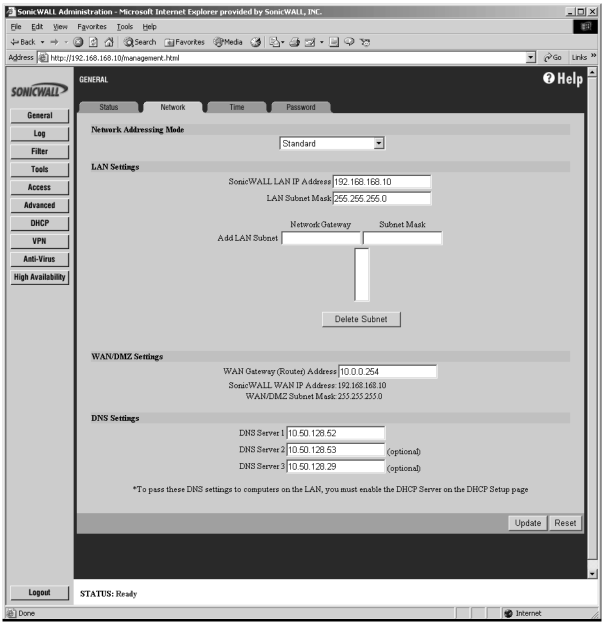
3 General and Network Settings

This chapter describes the tabs in the **General** section and the configuration of the SonicWALL SonicWALL Internet Security appliance **Network Settings**. The **Network Settings** include the SonicWALL IP settings, the administrator password, and the time and date. There are three tabs other than **Status** in the **General** section:

- **Network**
- **Time**
- **Password**

Network

To configure the SonicWALL **Network Settings**, click **General**, and then click the **Network** tab.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
GENERAL
Help
Status
Network
Time
Password
Delete Subnet
Update
Reset
Done
Internet

Network Addressing Mode

Standard

LAN Settings

SonicWALL LAN IP Address 192.168.168.10

LAN Subnet Mask 255.255.255.0

Add LAN Subnet — Network Gateway, Subnet Mask

WAN/DMZ Settings

WAN Gateway (Router) Address 10.0.0.254

SonicWALL WAN IP Address: 192.168.168.10

WAN/DMZ Subnet Mask: 255.255.255.0

DNS Settings

DNS Server 1 10.50.128.52

DNS Server 2 10.50.128.53 (optional)

DNS Server 3 10.50.128.29 (optional)

*To pass these DNS settings to computers on the LAN, you must enable the DHCP Server on the DHCP Setup page

STATUS: Ready

Network Settings

Network Addressing Mode

The **Network Addressing Mode** menu determines the network address scheme of your SonicWALL. It includes four options: **Standard**, **NAT Enabled**, **NAT with DHCP Client**, and **NAT with PPPoE**.

- **Standard** mode requires valid IP addresses for all computers on your network, but allows remote access to authenticated users.
- **NAT Enabled** mode translates the private IP addresses on the network to the single, valid IP address of the SonicWALL. Select **NAT Enabled** if your ISP assigned you only one or two valid IP addresses.
- **NAT with DHCP Client** mode configures the SonicWALL to request IP settings from a DHCP server on the Internet. **NAT with DHCP Client** is a typical network addressing mode for cable and DSL customers.
- **NAT with PPPoE** mode uses PPPoE to connect to the Internet. If desktop software and a user name and password is required by your ISP, select **NAT with PPPoE**.

LAN Settings

- **SonicWALL LAN IP Address**

  The **SonicWALL LAN IP Address** is the IP address assigned to the SonicWALL LAN port. It is used for managing the SonicWALL. This IP address should be a unique address from the LAN address range.

- **LAN Subnet Mask**

  The LAN Subnet Mask defines which IP addresses are on the LAN. The default Class C subnet mask of "255.255.255.0" supports up to 254 IP addresses on the LAN. If the Class C subnet mask is used, all local area network addresses should contain the same first three numbers as the SonicWALL LAN IP Address--for example, "192.168.168."

Multiple LAN Subnet Mask Support

***Note**: This feature does not replace or substitute configuring routes with the Routes tab in the Advanced section of the SonicWALL. If you have to define a subnet on the other side of a router, you must define a static route using the **Routes** tab in the **Advanced** section.*

Multiple LAN Subnet Mask Support facilitates the support of legacy networks incorporating the SonicWALL, and makes it easier to add additional nodes if the original subnet is full. Before you can configure multiple local LAN subnets in the SonicWALL, you must have the following information:

- **Network Gateway Address** - This is an IP address assigned to the SonicWALL in addition to the existing LAN IP address. If you have configured your SonicWALL in **Standard** mode, the IP address should be the Default Gateway IP address assigned to your Internet router on the same subnet. All users on the subnet you are configuring must use this IP address as their default router/gateway address.

- **Subnet Mask** - This value defines the size, and based upon the Network Gateway entry, the scope of the subnet. If you are configuring a subnet mask that currently exists on the LAN, enter the existing subnet mask address into the **Subnet Mask** field. If you are configuring a new subnet mask, use a subnet mask that does not overlap any previously defined subnet masks.

Note: *The SonicWALL cannot be managed from any of the additional Network Gateway addresses. You must use the IP address set as the LAN IP address of the SonicWALL. Also, you cannot mix Standard and NAT subnets behind the SonicWALL.*

WAN Settings

- **WAN Gateway (Router) Address**

  The WAN Gateway (Router) Address is the IP address of the WAN router or default gateway that connects your network to the Internet. If you use Cable or DSL, your WAN router is probably located at your ISP.

  If you select **NAT with DHCP Client** or **NAT with PPPoE** mode, the **WAN Gateway (Router) Address** is assigned automatically.

- **SonicWALL WAN IP Address**

  The SonicWALL WAN IP Address is a valid IP address assigned to the WAN port of the SonicWALL. This address should be assigned by your ISP.

  If you select **NAT Enabled** mode, this is the only address seen by users on the Internet and all activity appears to originate from this address.

  If you select **NAT with DHCP Client**, **NAT with PPPoE**, or **NAT with L2TP Client** mode, the SonicWALL WAN IP address is assigned automatically.

  If you select **Standard** mode, the SonicWALL WAN IP Address is the same as the SonicWALL LAN IP Address.

- **WAN/LAN Subnet Mask**

  The **WAN/LAN Subnet Mask** determines which IP addresses are located on the WAN. This subnet mask should be assigned by your ISP.

  If you select **NAT with DHCP Client**, **NAT with PPPoE,** or **NAT with L2TP Client** mode, the **WAN/LAN Subnet Mask** is assigned automatically.

  If you select **Standard** mode, the **WAN/LAN Subnet Mask** is the same as the LAN Subnet Mask.

DNS Settings

- **DNS Servers**

  DNS Servers, or Domain Name System Servers, are used by the SonicWALL for diagnostic tests with the **DNS Lookup Tool**, and for upgrade and registration functionality. DNS Server addresses should be assigned by your ISP.

If you select **NAT with DHCP Client** or **NAT with PPPoE** mode, the DNS Server addresses is assigned automatically.

***Note**: The SonicWALL does not relay DNS settings to the LAN; you must enable and configure the SonicWALL DHCP server or manually configure your computer DNS settings to obtain DNS name resolution.*

Standard Configuration

If your ISP provided you with enough IP addresses for all the computers and network devices on your LAN, enable **Standard** mode.

To configure **Standard** addressing mode, complete the following instructions:

1. Select **Standard** from the **Network Addressing Mode** menu. Because NAT is disabled, you must assign valid IP addresses to all computers and network devices on your LAN.
2. Enter a unique, valid IP address from your LAN address range in the **SonicWALL LAN IP Address** field. The **SonicWALL LAN IP Address** is the address assigned to the SonicWALL LAN and is used for management of the SonicWALL.
3. Enter your network subnet mask in the **LAN Subnet Mask** field. The **LAN Subnet Mask** tells your SonicWALL which IP addresses are on your LAN. The default value, "255.255.255.0", supports up to 254 IP addresses.
4. Enter your WAN router or default gateway address in the **WAN Gateway (Router) Address** field. Your router is the device that connects your network to the Internet. If you use Cable or DSL, your WAN router is located at your ISP.
5. Enter your DNS server IP address(es) in the **DNS Servers** field. The SonicWALL uses the DNS servers for diagnostic tests and for upgrade and registration functionality.
6. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Restart the SonicWALL for these changes to take effect.

NAT Enabled Configuration

Network Address Translation (NAT) connects your entire network to the Internet using a single IP address. Network Address Translation offers the following:

- Internet access to additional computers on the LAN. Multiple computers can access the Internet even if your ISP only assigned one or two valid IP addresses to your network.
- Additional security and anonymity because your LAN IP addresses are invisible to the outside world.

If your ISP hasn't provided enough IP addresses for all machines on your LAN, enable NAT and assign your network a private IP address range. You should use addresses from one of the following address ranges on your private network:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

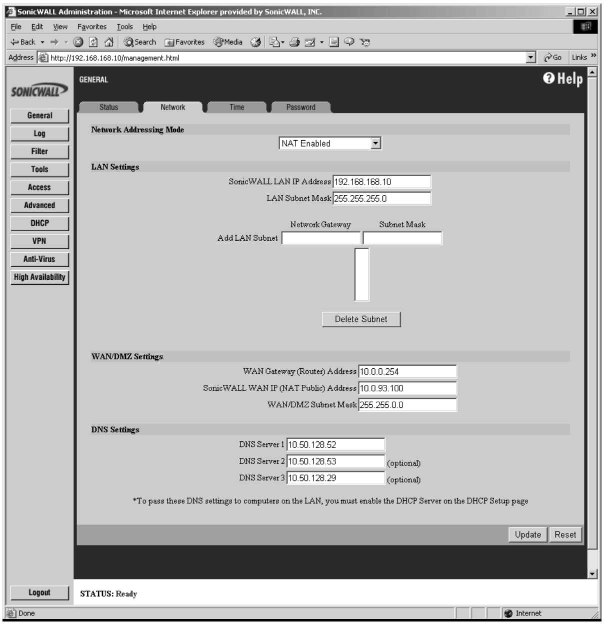
192.168.0.0 - 192.168.255.255

***Note**: If your network address range uses valid TCP/IP addresses, Internet sites within that range are not accessible from the LAN. For example, if you assign the address range 199.2.23.1 - 199.2.23.255 to your LAN, a Web server on the Internet with the address of 199.2.23.20 is not accessible.*

When NAT is enabled, users on the Internet cannot access machines on the LAN unless they have been designated as Public LAN Servers.

To enable **Network Address Translation (NAT)**, complete the following instructions.

1. Select **NAT Enabled** from the **Network Addressing Mode** menu in the **Network** window.



Address http://192.168.168.10/management.html

Network Addressing Mode: NAT Enabled

LAN Settings

SonicWALL LAN IP Address 192.168.168.10

LAN Subnet Mask 255.255.255.0

Add LAN Subnet: Network Gateway, Subnet Mask

WAN/DMZ Settings

WAN Gateway (Router) Address 10.0.0.254

SonicWALL WAN IP (NAT Public) Address 10.0.93.100

WAN/DMZ Subnet Mask 255.255.0.0

DNS Settings

DNS Server 1 10.50.128.52

DNS Server 2 10.50.128.53 (optional)

DNS Server 3 10.50.128.29 (optional)

*To pass these DNS settings to computers on the LAN, you must enable the DHCP Server on the DHCP Setup page

STATUS: Ready

2. Enter a unique IP address from your LAN address range in the **SonicWALL LAN IP Address** field. The SonicWALL LAN IP Address is the address assigned to the SonicWALL LAN and is used for management of the SonicWALL.
3. Enter your network subnet mask in the **LAN Subnet Mask** field. The **LAN Subnet Mask** tells the SonicWALL which IP addresses are on your LAN. Use the default value, "255.255.255.0", if there are less than 254 computers on your LAN.
4. Enter your WAN router or default gateway address in the **WAN Gateway (Router) Address** field. This is the device that connects your network to the Internet. If you use Cable or DSL, your WAN router is probably located at your ISP.

5. Enter a valid IP address assigned by your ISP in the **SonicWALL WAN IP (NAT Public) Address** field. Because NAT is enabled, all network activity appears to originate from this address.

6. Enter your WAN subnet mask in the **WAN/LAN Subnet Mask** field. This subnet mask should be assigned by your ISP.

7. Enter your DNS server IP address(es) in the **DNS Servers** field. The SonicWALL uses these DNS servers for diagnostic tests and for upgrade and registration functionality.

8. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Restart the SonicWALL for these changes to take effect.

If you enable Network Address Translation, designate the **SonicWALL LAN IP Address** as the gateway address for computers on your LAN. Consider the following example:

- The SonicWALL **WAN Gateway (Router) Address** is "10.1.1.1".
- The SonicWALL **WAN IP (NAT Public) Address** is "10.1.1.25".
- The private SonicWALL **LAN IP Address** is "192.168.168.1".
- Computers on the LAN have private IP addresses ranging from "192.168.168.2" to "192.168.168.255".

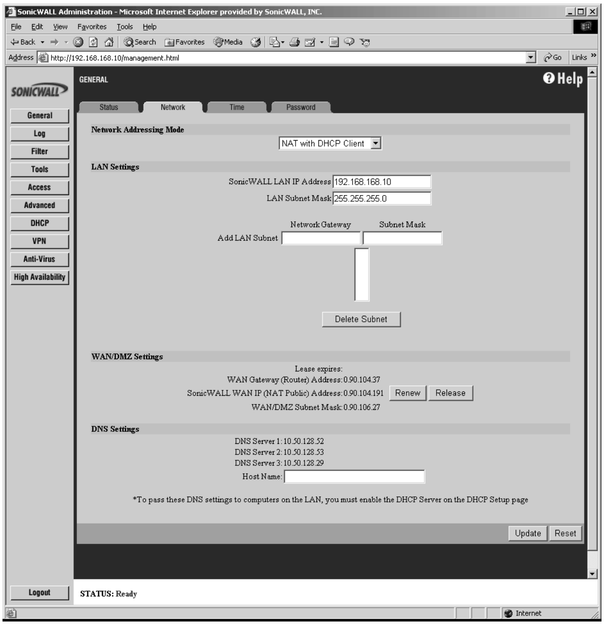
In this example, "192.168.168.1", the SonicWALL **LAN IP Address**, is used as the gateway or router address for all computers on the LAN.

NAT with DHCP Client Configuration

The SonicWALL can receive an IP address from a DHCP server on the Internet. If your ISP did not provide you with a valid IP address, and instructed you to set your network settings to obtain an IP address automatically, enable **NAT with DHCP Client**. **NAT with DHCP Client** mode is typically used with Cable and DSL connections.

To obtain IP settings dynamically, complete the following instructions.

1. Select **NAT with DHCP Client** from the **Network Addressing Mode** menu.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

GENERAL

Network Addressing Mode: NAT with DHCP Client

LAN Settings

SonicWALL LAN IP Address 192.168.168.10

LAN Subnet Mask 255.255.255.0

WAN/DMZ Settings

Lease expires:

WAN Gateway (Router) Address: 0.90.104.37

SonicWALL WAN IP (NAT Public) Address: 0.90.104.191

WAN/DMZ Subnet Mask: 0.90.106.27

DNS Settings

DNS Server 1: 10.50.128.52

DNS Server 2: 10.50.128.53

DNS Server 3: 10.50.128.29

*To pass these DNS settings to computers on the LAN, you must enable the DHCP Server on the DHCP Setup page

STATUS: Ready

2. Enter a unique IP address from your LAN address range in the **SonicWALL LAN IP Address** field. The SonicWALL LAN IP Address is the address assigned to the SonicWALL LAN and is used for management of the SonicWALL.

3. Enter your network subnet mask in the **LAN Subnet Mask** field. The LAN Subnet Mask tells your SonicWALL which IP addresses are on your LAN. The default value, "255.255.255.0", supports up to 254 IP addresses.

4. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Restart the SonicWALL for these changes to take effect.

***Note**: When NAT is enabled, designate the SonicWALL LAN IP Address as the gateway address for computers on the LAN.*

When your SonicWALL has successfully received a DHCP lease, the **Network** window displays the SonicWALL WAN IP settings.

- The **Lease Expires** value shows when your DHCP lease expires.
- The **WAN Gateway (Router) Address, SonicWALL WAN IP (NAT Public) Address**, **WAN/LAN Subnet Mask**, and **DNS Servers** are obtained from a DHCP server on the Internet.

***Note**: The SonicWALL does not relay DNS settings to the LAN; you must enable and configure the SonicWALL DHCP server or manually configure DNS settings on your computers to obtain DNS name resolution.*

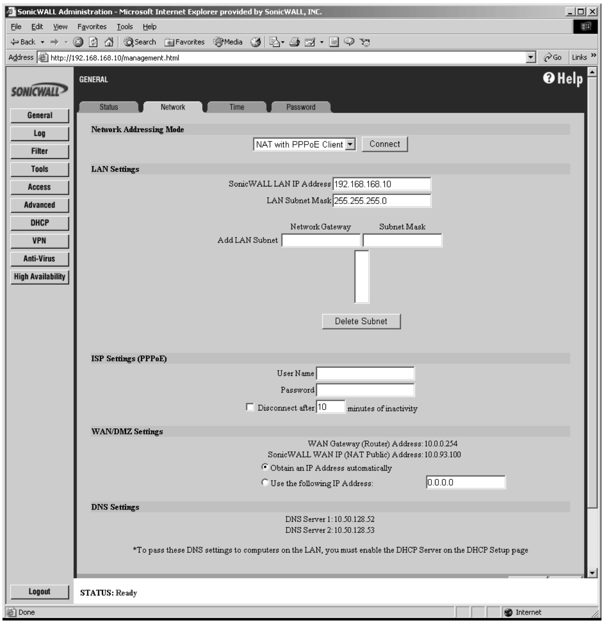
In the **WAN/LAN Settings** section of **Network**, you can **Renew** and **Release** the SonicWALL WAN IP (NAT Public) Address lease. When you click on **Renew**, the SonicWALL renews the IP address used for the WAN IP address. Click **Release**, and the lease is released with the DHCP server.

NAT with PPPoE Configuration

The SonicWALL can use Point-to-Point Protocol over Ethernet to connect to the Internet. If your ISP requires the installation of desktop software and user name and password authentication to access the Internet, enable **NAT with PPPoE**.

To configure **NAT with PPPoE**, complete the following instructions.

1. Select **NAT with PPPoE** from the **Network Addressing Mode** menu.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

Network Addressing Mode: NAT with PPPoE Client

LAN Settings
SonicWALL LAN IP Address 192.168.168.10
LAN Subnet Mask 255.255.255.0
Add LAN Subnet: Network Gateway, Subnet Mask

ISP Settings (PPPoE)
User Name
Password
□ Disconnect after 10 minutes of inactivity

WAN/DMZ Settings
WAN Gateway (Router) Address: 10.0.0.254
SonicWALL WAN IP (NAT Public) Address: 10.0.93.100
● Obtain an IP Address automatically
○ Use the following IP Address: 0.0.0.0

DNS Settings
DNS Server 1: 10.50.128.52
DNS Server 2: 10.50.128.53

*To pass these DNS settings to computers on the LAN, you must enable the DHCP Server on the DHCP Setup page

STATUS: Ready

2. Enter a unique IP address from your LAN address range in the **SonicWALL LAN IP Address** field. The SonicWALL LAN IP Address is the address assigned to the SonicWALL LAN port and is used for management of the SonicWALL.
3. Enter your network subnet mask in the **LAN Subnet Mask** field. The **LAN Subnet Mask** tells your SonicWALL which IP addresses are on your LAN. Use the default value, "255.255.255.0", if there are less than 254 computers on your LAN.
4. Enter the user name provided by your ISP in the **User Name** field. The user name identifies the PPPoE client.
5. Enter the password provided by your ISP in the **Password** field. The password authenticates the PPPoE session. This field is case sensitive.
6. Select the **Disconnect after __ Minutes of Inactivity** check box to automatically disconnect the PPPoE connection after a specified period of inactivity. Define a maximum number of minutes of inactivity in the **Minutes** field. This value can range from 1 to 99 minutes.
7. In the **WAN/LAN** section, select **Obtain an IP Address Automatically** if your ISP does not provide a static IP address. Select **Use the following IP Address** if your ISP assigns a specific IP address to you.
8. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Restart the SonicWALL for these changes to take effect.

***Note**: When NAT is enabled, the SonicWALL LAN IP Address is used as the gateway address for computers on the LAN.*

When your SonicWALL has successfully established a PPPoE connection, the **Network** page displays the SonicWALL WAN IP settings. The **WAN Gateway (Router) Address**, **SonicWALL WAN IP (NAT Public) Address**, **WAN/LAN Subnet Mask**, and **DNS Servers** are displayed.

***Note**: The SonicWALL does not relay DNS settings to the LAN; you must enable and configure the SonicWALL DHCP server or manually configure the computer DNS settings to obtain DNS name resolution.*

Restarting the SonicWALL

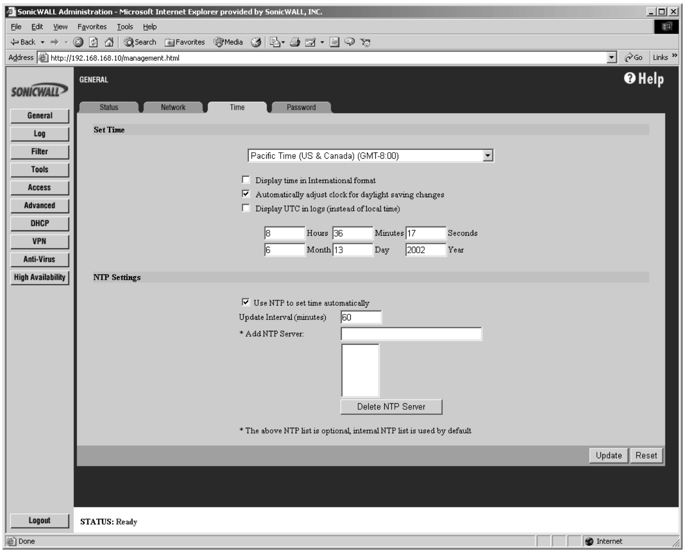
Once the network settings have been updated, the **Status** bar at the bottom of the browser window displays "Restart SonicWALL for changes to take effect." Restart the SonicWALL by clicking **Restart**. Then click **Yes** to confirm the restart and send the restart command to the SonicWALL. The restart can take up to 90 seconds, during which time the SonicWALL is inaccessible and all network traffic through the SonicWALL is halted.

***Note**: If you change the SonicWALL LAN IP Address, you must to change the Management Station IP address to be in the same subnet as the new LAN IP address.*

Setting the Time and Date

The SonicWALL uses the time and date settings to time stamp log events, to automatically update the **Content Filter List**, and for other internal purposes.

1. Click the **Time** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
GENERAL
Help
Status
Network
Time
Password
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Update
Reset
Delete NTP Server
Done
Internet

Set Time

Pacific Time (US & Canada) (GMT-8:00)

□ Display time in International format
☑ Automatically adjust clock for daylight saving changes
□ Display UTC in logs (instead of local time)

8 Hours 36 Minutes 17 Seconds
6 Month 13 Day 2002 Year

NTP Settings

☑ Use NTP to set time automatically
Update Interval (minutes) 60
* Add NTP Server:

* The above NTP list is optional, internal NTP list is used by default

STATUS: Ready

2. Select your time zone from the **Time Zone** menu.
3. Click **Update** to add the information to the SonicWALL.

You can also enable automatic adjustments for **daylight savings time**, **use universal time (UTC) rather than local time**, and **display the date in International format, with the day preceding the month**.

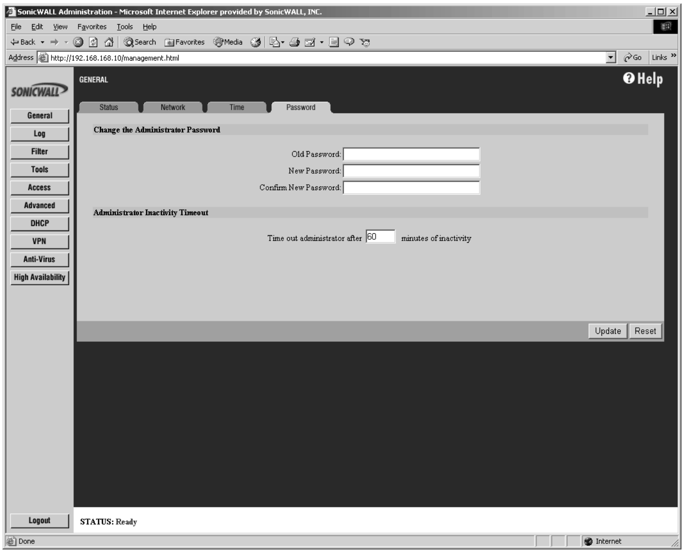
To set the time and date manually, clear the check boxes and enter the time (in 24-hour format) and the date.

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. Select **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL clock. You can also set the **Update Interval** for the NTP server to synchronize the time in the SonicWALL. The default value is 60 minutes. You can add NTP servers to the SonicWALL for time synchronization by entering in the IP address of an NTP server in the **Add NTP Server** field. If there are no NTP Servers in the list, the internal NTP list is used by default. To remove an NTP server, highlight the IP address and click **Delete NTP Server**.When you have configured the **Time** window, click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Setting the Administrator Password

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


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
GENERAL
Help
Status Network Time Password
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Update Reset
Done
Internet

Change the Administrator Password

Old Password:

New Password:

Confirm New Password:

Administrator Inactivity Timeout

Time out administrator after 60 minutes of inactivity

STATUS: Ready

***Note**: When setting the password for the first time, remember that the SonicWALL default password is "password".*

If the password is not entered exactly the same in both **New Password** fields, the password is not changed. If you mistype the password, you are not locked out of the SonicWALL.

***Warning**: The password cannot be recovered if it is lost or forgotten. If the password is lost, you must to reset the SonicWALL to its factory default state. Go to Appendix F for instructions.*

Setting the Administrator Inactivity Timeout

The **Administrator Inactivity Timeout** setting allows you to configure the length of inactivity that can elapse before you are automatically logged out of the Web Management Interface. The SonicWALL is preconfigured to log out the administrator after 5 minutes of inactivity.

***Note**: 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.*

Enter the desired number of minutes in the **Administrator Inactivity Timeout** section and click **Update**. The **Inactivity Timeout** can range from 1 to 99 minutes. Click **Update**, and a message confirming the update is displayed at the bottom of the browser window.

4 Logging and Alerts

This chapter describes the SonicWALL Internet security appliance logging, alerting, and reporting features, which can be viewed in the **Log** section of the SonicWALL Web Management Interface.There are four tabs in the **Log** section:

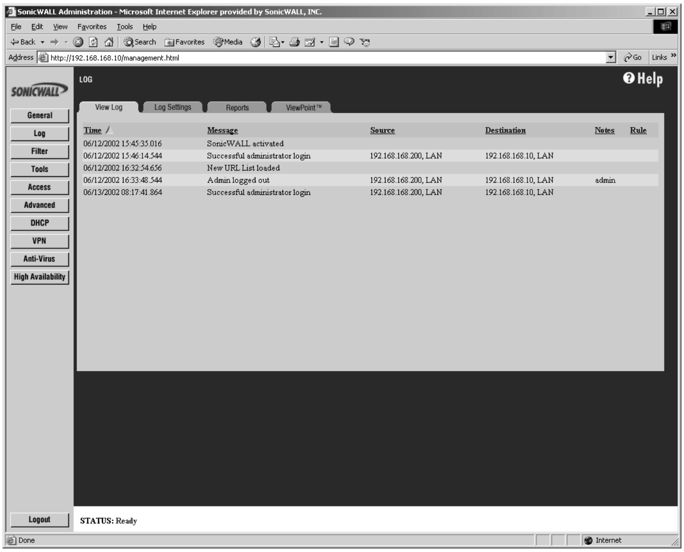
- **View Log**
- **Log Settings**
- **Reports**
- **ViewPoint** (requires a purchased upgrade)

View Log

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 is sortable 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, and then click **View Log**.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
LOG
Help
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
View Log
Log Settings
Reports
ViewPoint™
Done
Internet

Time	Message	Source	Destination	Notes	Rule
06/12/2002 15:45:35.016	SonicWALL activated				
06/12/2002 15:46:14.544	Successful administrator login	192.168.168.200, LAN	192.168.168.10, LAN		
06/12/2002 16:32:54.656	New URL List loaded				
06/12/2002 16:33:48.544	Admin logged out	192.168.168.200, LAN	192.168.168.10, LAN	admin	
06/13/2002 08:17:41.864	Successful administrator login	192.168.168.200, LAN	192.168.168.10, LAN		

STATUS: Ready

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.

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

  When IP packets are blocked by the SonicWALL, dropped TCP, UDP and ICMP messages is 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.

- **Web**, **FTP**, **Gopher**, **or Newsgroup blocked**

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

a=Violence/Profanity

b=Partial Nudity

c=Full Nudity

d=Sexual Acts

e=Gross Depictions

f=Intolerance

g=Satanic/Cult

h=Drug Culture

i=Militant/Extremist

j=Sex Education

k=Gambling/Illegal

l=Alcohol/Tobacco

Descriptions of the categories are available at <http://www.sonicwall.com/Content-Filter/categories.html>.

- **ActiveX**, **Java**, **Cookie or Code Archive blocked**

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

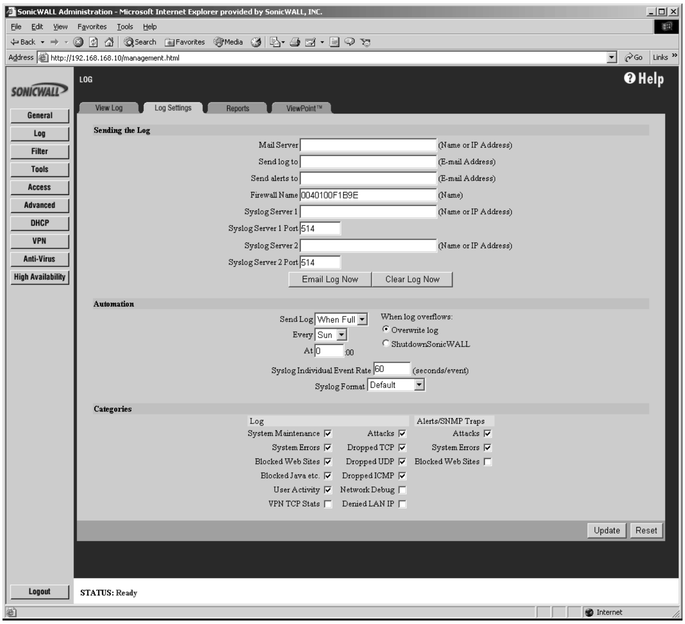
- **Ping of Death, IP Spoof, and SYN Flood Attacks**

  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.

***Note**: Some network conditions can produce network traffic that appears to be an attack, even when no one is deliberately attacking the LAN. To follow up on a possible attack, contact your ISP to determine the source of the attack. Regardless of the nature of the attack, your LAN is protected and no further steps must be taken.*

Log Settings

Click **Log** on the left side of the browser window, and then click the **Log Settings** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
LOG
Help
View Log
Log Settings
Reports
ViewPoint™
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Email Log Now
Clear Log Now
Update
Reset
Internet

Sending the Log

Mail Server ____ (Name or IP Address)
Send log to ____ (E-mail Address)
Send alerts to ____ (E-mail Address)
Firewall Name 0040100F1B9E (Name)
Syslog Server 1 ____ (Name or IP Address)
Syslog Server 1 Port 514
Syslog Server 2 ____ (Name or IP Address)
Syslog Server 2 Port 514

Automation

Send Log When Full
Every Sun
At 0 :00
When log overflows:
● Overwrite log
○ ShutdownSonicWALL
Syslog Individual Event Rate 60 (seconds/event)
Syslog Format Default

Categories

Log		Alerts/SNMP Traps
System Maintenance ☑	Attacks ☑	Attacks ☑
System Errors ☑	Dropped TCP ☑	System Errors ☑
Blocked Web Sites ☑	Dropped UDP ☑	Blocked Web Sites □
Blocked Java etc. ☑	Dropped ICMP ☑	
User Activity ☑	Network Debug □	
VPN TCP Stats □	Denied LAN IP □	

STATUS: Ready

Configure the following settings:

1. **Mail Server** - To e-mail log or alert messages, enter the name or IP address of your mail server in the Mail Server field. If this field is left blank, log and alert messages are not e-mailed.

2. **Send Log To** - Enter your full e-mail address(username@mydomain.com) in the **Send** log to field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL memory. If this field is left blank, the log is not e-mailed.

3. **Send Alerts To** - Enter your full e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Enter a standard e-mail address or an e-mail paging service. If this field is left blank, alert messages are not e-mailed.

4. **Firewall Name** - The **Firewall Name** appears in the subject of e-mails sent by the SonicWALL. The **Firewall Name** is helpful if you are managing multiple SonicWALLs because it specifies the individual SonicWALL sending a log or an alert e-mail. By default, the **Firewall Name** is set to the SonicWALL serial number.

5. **Syslog Server** - In addition to the standard event log, the SonicWALL can send a detailed log to an external Syslog server. Syslog is an industry-standard protocol used to capture information about network activity. 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 WebTrends Firewall Suite can be used to sort, analyze, and graph the **Syslog** data.

Enter the Syslog server name or IP address in the **Syslog Server 1** or **Syslog Server 2** field. Messages from the SonicWALL are then sent to the servers. If the SonicWALL is managed by SGMS, however, the **Syslog Server** fields cannot be configured by the administrator of the SonicWALL.

6. **E-mail Log Now** - Clicking **E-mail Log Now** immediately sends the log to the address in the Send Log To field and then clears the log.
7. **Clear Log Now** - Clicking **Clear Log Now** deletes the contents of the log.
8. **Send Log / Every / At** - The **Send Log** menu determines the frequency of log e-mail messages: **Daily**, **Weekly**, or **When Full**. If the **Weekly** option is selected, then enter the day of the week the e-mail is sent in the **Every** menu. If the **Weekly** or the **Daily** option is selected, enter the time of day when the e-mail is sent in the **At** field. If the **When Full** option is selected and the log fills up, it is e-mailed automatically.
9. **When log overflows** - The log buffer fills up if the SonicWALL cannot e-mail the log file. The default behavior is to overwrite the log and discard its contents. However, you can configure the SonicWALL to shut down and prevent traffic from traveling through the SonicWALL if the log is full.
10. **Syslog Individual Event Rate (seconds/event)** - The **Syslog Individual Event Rate** setting filters repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Individual Event 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 Individual Event Rate** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.
11. **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 Categories

You can define which log messages appear in the SonicWALL **Event Log**. All **Log Categories** are enabled by default except **Network Debug**.

- **System Maintenance**
  Logs general system activity, such as administrator log ins, automatic downloads of the **Content Filter Lists**, and system activations.
- **System Errors**
  Logs problems with DNS, e-mail, and automatic downloads of the Content Filter List.
- **Blocked Web Sites**
  Logs Web sites or newsgroups blocked by the Content Filter List or by customized filtering.
- **Blocked Java**, **ActiveX**, **and Cookies**
  Logs Java, ActiveX, and Cookies blocked by the SonicWALL.
- **User Activity**
  Logs successful and unsuccessful log in attempts.
- **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.

Alert Categories

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** is disabled.

- **Attacks**
  Log entries categorized as **Attacks** generate alert messages.
- **System Errors**

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

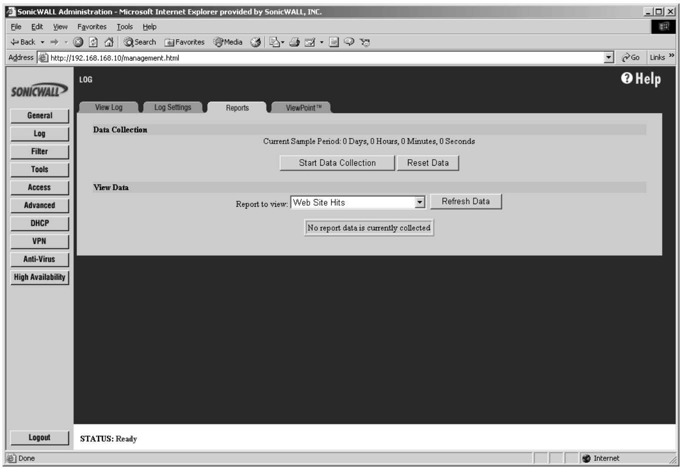
- **Blocked Web Sites**

  Log entries categorized as **Blocked Web Sites** generate alert messages.

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

Reports

The SonicWALL is able to 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** tab.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

LOG

Data Collection

Current Sample Period: 0 Days, 0 Hours, 0 Minutes, 0 Seconds

View Data

Report to view: Web Site Hits

No report data is currently collected

STATUS: Ready

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** 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 **Display Report** 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 **Display Report** 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 **Display Report** 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.

5 Content Filtering and Blocking

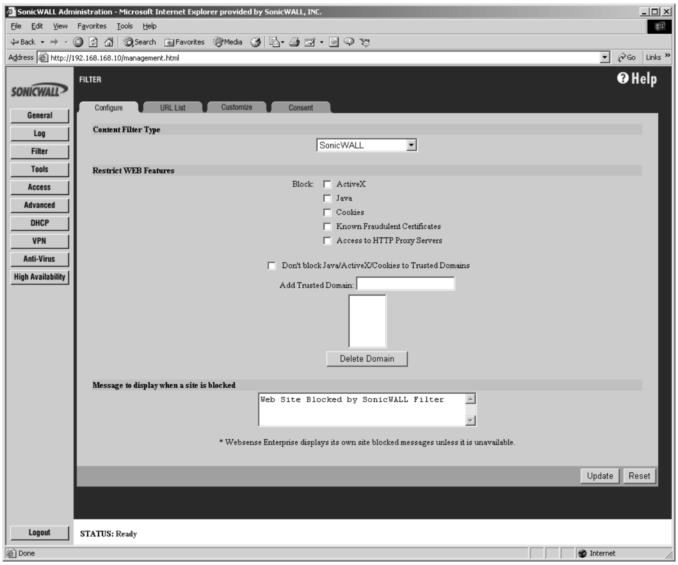
Internet content filtering allows you to create and enforce Internet access policies tailored to the needs of the organization. You can select categories to block or monitor, such as pornography or racial intolerance, from a pre-defined list.

There are now three **Content Filter Lists** available for selection:

- **SonicWALL** - Selecting **SonicWALL** for the **Content Filter List Type** allows you use the URL list and completely customize your Content Filter feature including 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>. If you select **N2H2** from the list, an **N2H2** tab is available to configure the location of the N2H2 server and other settings.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list package supported by SonicWALL. You can obtain more information on Websense Enterprise at <http://www.Websense.com>. If you select **Websense Enterprise** from the list, a **Websense** tab is available to configure the location of the Websense server and other settings.

There are four tabs in the **Filter** section if the SonicWALL Content Filter is selected:

- **Configure**
- **URL List**
- **Customize**
- **Consent**



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

FILTER

Content Filter Type

SonicWALL

Restrict WEB Features

Block: ☐ ActiveX
☐ Java
☐ Cookies
☐ Known Fraudulent Certificates
☐ Access to HTTP Proxy Servers

☐ Don't block Java/ActiveX/Cookies to Trusted Domains

Add Trusted Domain:

Message to display when a site is blocked

Web Site Blocked by SonicWALL Filter

* Websense Enterprise displays its own site blocked messages unless it is unavailable.

STATUS: Ready

Configuring SonicWALL Content Filtering

The **Configure** tab is common between the three types of Content Filtering. Click **Filter** on the left side of the browser window, and then click on the **Configure** tab.

Select the type of Content Filter from the **Content Filter Type** menu. To enforce Content Filtering on the LAN, select **Apply Content Filter**.

Restrict Web Features

Select any of the following applications to block:

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

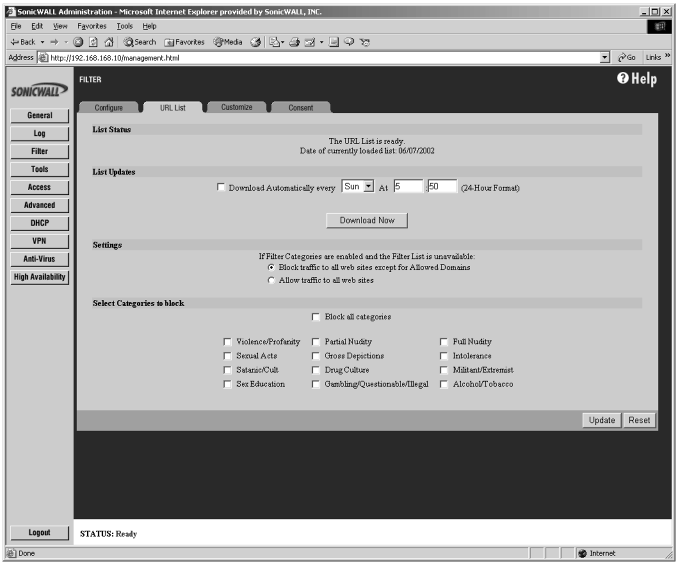
Trusted Domains can be added in the **Restrict Web Features** section of the **Configure** tab. If you trust content on specific domains, you can select **Don’t block Java/ActiveX/ Cookies to Trusted Domains** and then add the **Trusted Domains** to the SonicWALL. Java scripts, ActiveX, and cookies are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

Message to display when a site is blocked

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

URL List

The **URL List** page allows you to see the status of the Content Filter List as well as configure a specific time to download the list. You can also determine how the SonicWALL responds when a Content Filter List is unavailable. Selecting categories to block is also configured on this page.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
FILTER
Help
Configure
URL List
Customize
Consent
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Download Now
Update
Reset
Done
Internet

List Status

The URL List is ready.
Date of currently loaded list: 06/07/2002

List Updates

□ Download Automatically every Sun At 5 :50 (24-Hour Format)

Settings

If Filter Categories are enabled and the Filter List is unavailable:
● Block traffic to all web sites except for Allowed Domains
○ Allow traffic to all web sites

Select Categories to block

□ Block all categories

□ Violence/Profanity □ Partial Nudity □ Full Nudity
□ Sexual Acts □ Gross Depictions □ Intolerance
□ Satanic/Cult □ Drug Culture □ Militant/Extremist
□ Sex Education □ Gambling/Questionable/Illegal □ Alcohol/Tobacco

STATUS: Ready

***Note**: Content Filtering applies only to the SonicWALL LAN.*

List Status

This section of the **URL List** tab indicates the status of the URL list. If the Content Filter List is loaded, a status message is displayed in this section.

List Updates

It is important to note that Host names, and not TCP/IP addresses, are used for all filtering for several reasons. One reason is because many blocked sites operate server pools, where many computers service a single host name, making it impractical and difficult to add and maintain the numerical addresses of every server in the pool. Another reason is the fact that many sites which are included in the Content Filter List regularly change the IP address of the server to try to bypass Content Filter Lists. For this reason, maintaining a current list subscription is critical for effective content filtering.

Download Automatically every

Selecting **Download Automatically every** allows you to configure a specific time to download your Content Filter List. Select a day of the week and a time (24-hour format), for example, Sun. at 22:00 hours. Or, you can click **Download Now** to immediately download your Content Filter List.

It is recommended to download the URL List at a time when access to the Internet is at a minimum as downloading the URL List disrupts connectivity to the Internet.

Settings

If you have enabled blocking by **Filter Categories** and the **URL List** becomes unavailable, there are two options available:

- **Block traffic to all Web sites except for Allowed Domains**

  Selecting this option blocks traffic to all Web sites except Allowed Domains until the URL List is available.

- **Allow traffic to all Web sites**

  Selecting this option allows traffic to all Web sites without the URL List. However, **Forbidden Domains** and **Keywords**, if enabled, are still blocked.

Select Categories to Block

Block all categories

The SonicWALL uses a **Content Filter List** generated by CyberPatrol to block access to objectional Web sites. CyberPatrol classifies objectional Web sites based upon input from a wide range of social, political, and civic organizations. Select the **Block all categories** check box to block all of these categories. Alternatively, you can select categories individually by selecting the appropriate check box.

When you register your SonicWALL at <http://www.mysonicwall.com>, you can download a one month subscription to Content Filter List updates.

The following is a list of the **Content Filter List** categories:

Violence/Profanity

Partial Nudity

Full Nudity

Sexual Acts

Gross Depictions

Intolerance

Satanic/Cult

Drugs/Drug Culture

Militant/Extremist

Sex Education

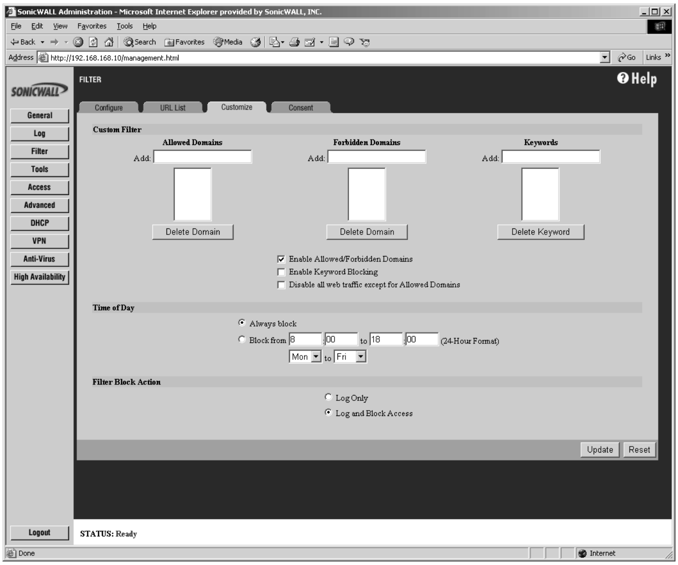
Questionable/Illegal Gambling

Alcohol & Tobacco

Visit <http://www.sonicwall.com/Content-Filter/categories.html> for a detailed description of the criteria used to define Content Filter List categories.

Customizing the Content Filtering List

The **Customize** tab allows you to customize your URL List by manually entering domain names or keywords to be blocked or allowed.



Custom Filter

Allowed Domains — Add:

Forbidden Domains — Add:

Keywords — Add:

☑ Enable Allowed/Forbidden Domains
☐ Enable Keyword Blocking
☐ Disable all web traffic except for Allowed Domains

Time of Day

● Always block
○ Block from 8 :00 to 18 :00 (24-Hour Format)
Mon to Fri

Filter Block Action

○ Log Only
● Log and Block Access

STATUS: Ready

Custom Filter

You can customize your URL list to include **Allowed Domains**, **Forbidden Domains**, and **Keywords**. 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 Filter List, enter the host name, such as “www.ok-site.com”, into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter List**, 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.

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

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete Domain**. Once the domain has been deleted, a message is displayed at the bottom of the Web browser window.

To enable blocking using **Keywords**, select the **Enable Keyword Blocking** check box.

Enter the keyword to block in the **Add Keyword** field, and click **Update**. Once the keyword has been added, a message confirming the update is displayed at the bottom of the browser window.

To remove a keyword, select it from the list and click **Delete Keyword**. Once the keyword has been removed, a message confirming the update is displayed at the bottom of the browser window.

***Note**: Customized domains do not have to be re-entered when the Content Filter List is updated each week and do not require a URL list subscription.*

- **Enable Allowed/Forbidden Domains**

  To deactivate **Custom Filter** customization, clear the **Enable Allowed/Forbidden Domains**, and click **Update**. This option allows you to enable and disable customization without removing and re-entering custom domains.

- **Enable Keyword Blocking**

  Select the **Enable Keyword Blocking** if you want to block Web traffic based on your list of customized keywords.

- **Disable all Web traffic except for Allowed Domains**

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

Time of Day

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

***Note**: 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 Block**

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

- **Block Between**

  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.

Filter Block Action

- **Log Only**

  If this check box is selected, the SonicWALL logs and then allows access to all sites on the Content Filter, custom, and keyword lists. The **Log Only** check box allows you to monitor inappropriate usage without restricting access.

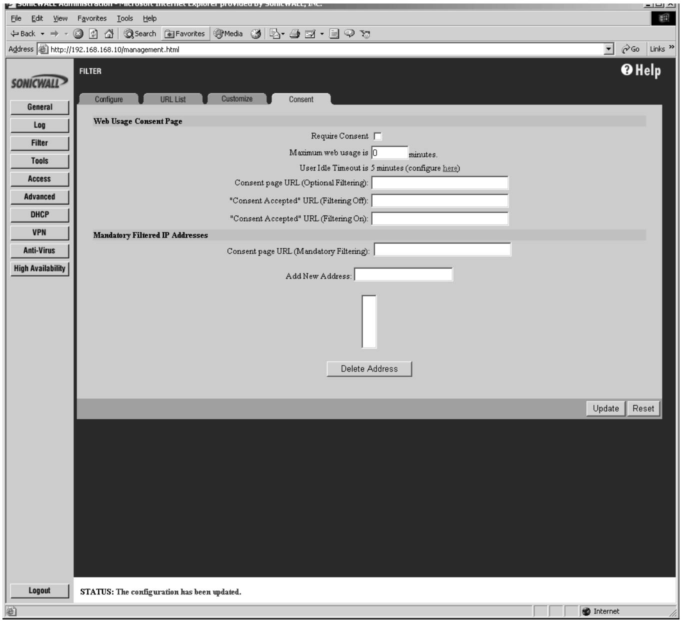
- **Log and Block Access**

  Select the check box and the SonicWALL blocks access to sites on the Content Filter, custom, and keyword lists. The SonicWALL also logs attempts to access these sites.

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.

Click **Filter** on the left side of the browser window, and then click the **Consent** tab.



Address: http://192.168.168.10/management.html

Web Usage Consent Page

Require Consent □

Maximum web usage is 0 minutes.

User Idle Timeout is 5 minutes (configure here)

Consent page URL (Optional Filtering):

"Consent Accepted" URL (Filtering Off):

"Consent Accepted" URL (Filtering On):

Mandatory Filtered IP Addresses

Consent page URL (Mandatory Filtering):

Add New Address:

STATUS: The configuration has been updated.

- **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 (configure here)**

  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 Filtered IP Addresses

- **Consent page URL (Mandatory Filtering)**

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

  This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL that tells the

SonicWALL that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of "192.168.168.168".

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

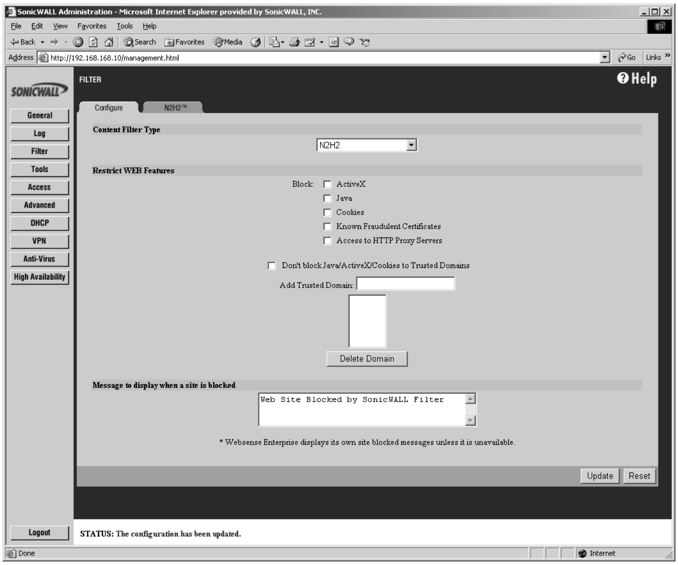
- **Add New Address**

  The SonicWALL can be configured to enforce content filtering for certain computers on the LAN. Enter the IP addresses of these computers in the **Add New Address** field and click **Submit** button. Up to 128 IP addresses can be entered.

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

Configuring N2H2 Internet Filtering

N2H2 is a third party Internet filtering package that allows you to use Internet filtering through the SonicWALL. When you select N2H2 as your Content Filter List, the **N2H2** tab is available.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
FILTER
Help
Configure
N2H2™
Delete Domain
Update
Reset
Done
Internet

Content Filter Type

N2H2

Restrict WEB Features

Block: □ ActiveX
□ Java
□ Cookies
□ Known Fraudulent Certificates
□ Access to HTTP Proxy Servers

□ Don't block Java/ActiveX/Cookies to Trusted Domains

Add Trusted Domain:

Message to display when a site is blocked

Web Site Blocked by SonicWALL Filter

* Websense Enterprise displays its own site blocked messages unless it is unavailable.

STATUS: The configuration has been updated.

Restrict Web Features

Select any of the following applications to block:

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**.

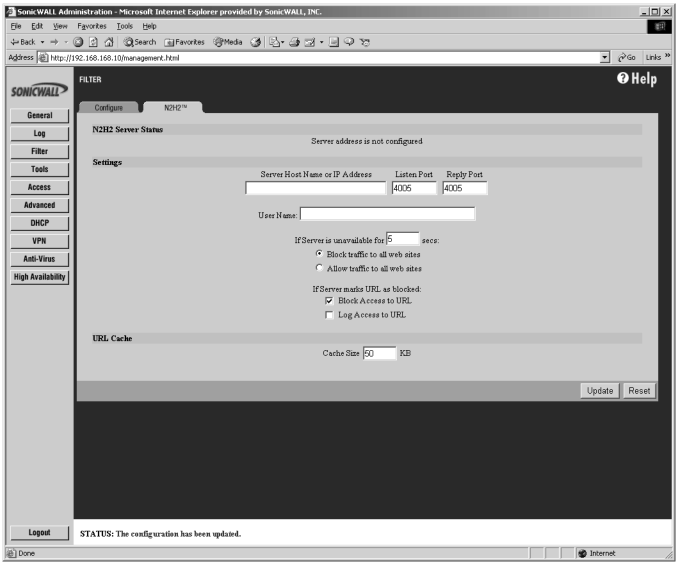
Trusted Domains

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. Java scripts, ActiveX, and cookies are not blocked from **Trusted Domains** if the checkbox is selected.

Message to display when a site is blocked

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

Customization of Content Filtering is not available if you select N2H2 as your source for your Content Filter List. Refer to your N2H2 documentation for details on configuring N2H2 Internet Filtering for your network.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
FILTER
Help
Configure
N2H2™
Update
Reset
Done
Internet

N2H2 Server Status

Server address is not configured

Settings

Server Host Name or IP Address:
Listen Port: 4005
Reply Port: 4005

User Name:

If Server is unavailable for 5 secs:

● Block traffic to all web sites

○ Allow traffic to all web sites

If Server marks URL as blocked:

☑ Block Access to URL

□ Log Access to URL

URL Cache

Cache Size 50 KB

STATUS: The configuration has been updated.

N2H2 Server Status

This section displays the status of the N2H2 Internet Filtering Protocol (IFP) server you are using for Internet filtering.

Settings

Server Host Name or IP Address

Enter the Server Host Name or the IP address of the N2H2 Internet Filtering Protocol (IFP) server used to receive IFP requests.

Listen Port

Enter the UDP port number for the N2H2 Internet Filtering Protocol (IFP) server to “listen” for the N2H2 traffic. The default port is 4005.

Reply Port

Enter the UCP port number for the N2H2 server to send packets from the N2H2 client to the SonicWALL. The default port is 4005.

User Name

The **User Name** refers to a configuration of users, a group of users, or network defined within the N2H2 software

If Server is unavailable for 5 secs:

The default value for timeout of the server is 5 seconds, but you can enter a value between 1 and 10 seconds.

If the N2H2 server becomes unavailable, select from the following two options:

- **Block traffic to all Web sites**
- **Allow traffic to all Web sites**

URL Cache

Configure the size of the **URL Cache** in KB.

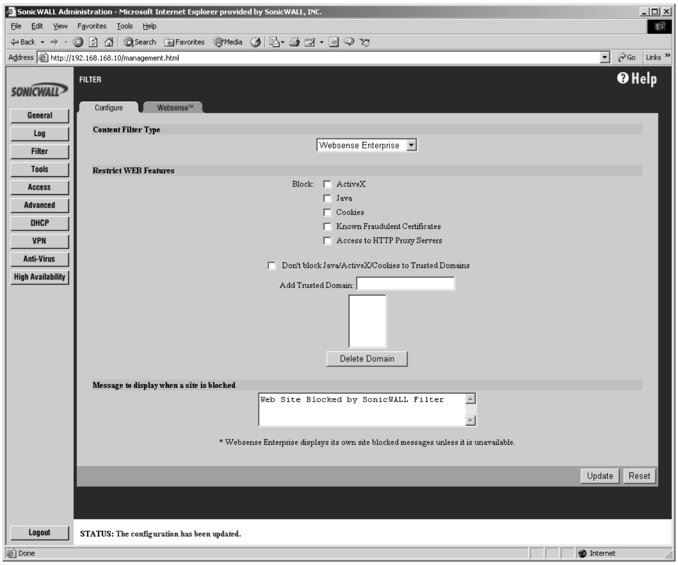
Model	Cache Size
XPRS, PRO, SOHO2, TELE2, SOHO3, TELE3, and PRO-Vx	128
PRO 100, PRO 200, PRO 300, PRO2, PRO-VX2	256
GX250, GX 2500, GX650, GX 6500	1024

***Note**: A larger URL Cache size can increase in noticeable improvements in Internet browsing response times.*

Configuring Websense Enterprise Content Filter

Websense is a third party software package that allows you to use content filtering through the SonicWALL. Select **Websense Enterprise** from the **Content Filter Type** menu.

Customization of the Content Filter List is not available if you select Websense as your source for content filtering.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
FILTER
Help
Configure
Websense™
Delete Domain
Update
Reset
Done
Internet

Content Filter Type

Websense Enterprise

Restrict WEB Features

Block: □ ActiveX

□ Java

□ Cookies

□ Known Fraudulent Certificates

□ Access to HTTP Proxy Servers

□ Don't block Java/ActiveX/Cookies to Trusted Domains

Add Trusted Domain:

Message to display when a site is blocked

Web Site Blocked by SonicWALL Filter

* Websense Enterprise displays its own site blocked messages unless it is unavailable.

STATUS: The configuration has been updated.

Restrict Web Features

Select any of the following applications to block:

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

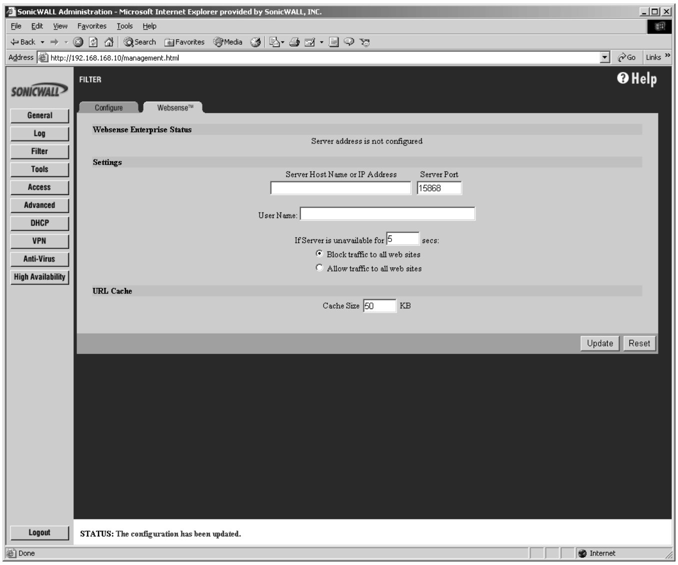
Trusted Domains can be added in the **Restrict Web Features** section of the **Configure** tab. If you trust content on specific domains, you can select **Don't block Java/ActiveX/Cookies to Trusted Domains** and then add the **Trusted Domains** to the SonicWALL. Java scripts, ActiveX, and cookies are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

Message to display when a site is blocked

When a user attempts to access a site blocked by the Websense Enterprise Content Filter List, only Websense Enterprise messages are displayed in the browser. If the Websense Enterprise Content Filter List server is unavailable, the default SonicWALL message is displayed.

Configuring Websense Content Filter List

Configure the Websense Enterprise settings on this page.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
FILTER
Help
Configure
Websense™
Update
Reset
Done
Internet

Websense Enterprise Status

Server address is not configured

Settings

Server Host Name or IP Address:

Server Port: 15868

User Name:

If Server is unavailable for 5 secs:

● Block traffic to all web sites

○ Allow traffic to all web sites

URL Cache

Cache Size 50 KB

STATUS: The configuration has been updated.

Websense Server Status

This section displays the status of the Websense Enterprise server used for content filtering.

Settings

Server Host Name or IP Address

Enter the Server Host Name or the IP address of the Websense Enterprise server used for the Content Filter List.

Server Port

Enter the UDP port number for the SonicWALL to “listen” for the Websense Enterprise traffic. The default port number is 15686.

User Name

To enable reporting of users and groups defined on the Webense Enterprise server, leave this field blank. To enable reporting by a specific user or group behind the SonicWALL, enter the **User Name** configured on the Websense Enterprise Server for the user or group. If using NT-based directories on the Websense Enterprise Server, the **User Name** is in this format, for example: NTLM:\\domainname\username. If using LDAP-based directories on the Websense

Enterprise server, the **User Name** is in this format, for example: LDAP://o-domain/ou=sales/username.

If you are not sure about the entering a user name in this section, leave the field blank and consult your Websense documentation for more information.

If Server is unavailable for 5 secs:

If the Websense Enterprise server becomes unavailable, select from the following two options:

- **Block traffic to all Web sites**
- **Allow traffic to all Web sites**

URL Cache

Configure the size of the URL Cache in KB.

Model	Cache Size
XPRS, PRO, SOHO2, TELE2, SOHO3, TELE3, and PRO-Vx	128
PRO 100, PRO 200, PRO 300, PRO2, PRO-VX2	256
GX250, GX 2500, GX650, GX 6500	1024

***Note**: A larger URL Cache size can result in noticeable improvements in Internet browsing response times.*

6 Web Management Tools

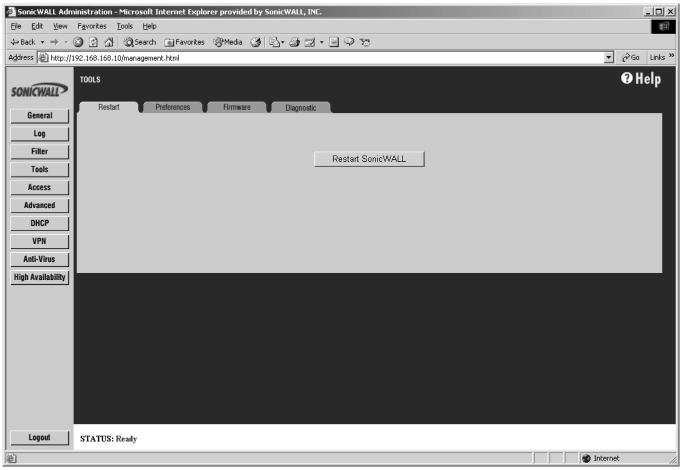
This chapter describes the SonicWALL **Management Tools**, available in the **Tools** section of the SonicWALL **Web Management Interface**. The **Web Management Tools** section allows you to restart the SonicWALL, import and export configuration settings, update the SonicWALL firmware, and perform several diagnostic tests.

There are four tabs in the **Tools** section:

- **Restart**
- **Preferences**
- **Firmware**
- **Diagnostic**

Restarting the SonicWALL

Click **Tools** on the left side of the browser window, and then click the **Restart** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
TOOLS
Help
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Restart
Preferences
Firmware
Diagnostic
Restart SonicWALL
Internet

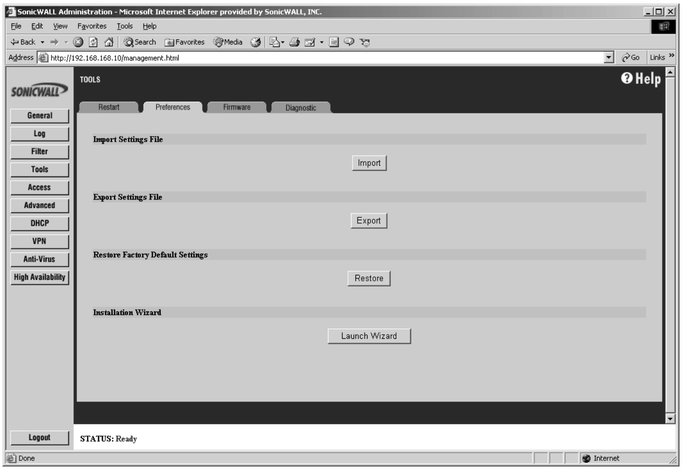
STATUS: Ready

The SonicWALL can be restarted from the Web Management Interface. Click **Restart SonicWALL**, and then click **Yes** to confirm the restart.

The SonicWALL takes up to 90 seconds to restart, and the yellow Test LED is lit. During the restart time, Internet access for all users on the LAN is momentarily interrupted.

Preferences

Click **Tools** on the left side of the browser window, and then click the **Preferences** tab.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

TOOLS

Import Settings File

Export Settings File

Restore Factory Default Settings

Installation Wizard

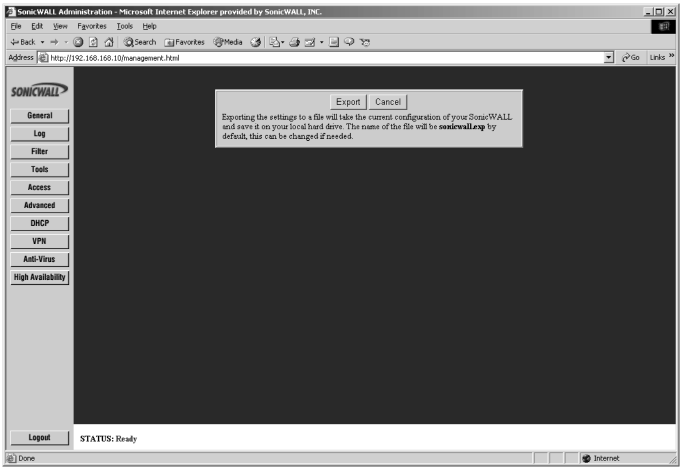
STATUS: Ready

You can save the SonicWALL settings, and then retrieve them later for backup purposes. SonicWALL recommends saving the SonicWALL settings when upgrading the firmware.

The **Preferences** window also provides options to restore the SonicWALL factory default settings and launch the SonicWALL Installation Wizard. These functions are described in detail in the following pages.

Exporting the Settings File

It is possible to save the SonicWALL configuration information as a file on your computer, and retrieve it for later use. Click **Export** in the **Preferences** tab.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

Exporting the settings to a file will take the current configuration of your SonicWALL and save it on your local hard drive. The name of the file will be **sonicwall.exp** by default, this can be changed if needed.

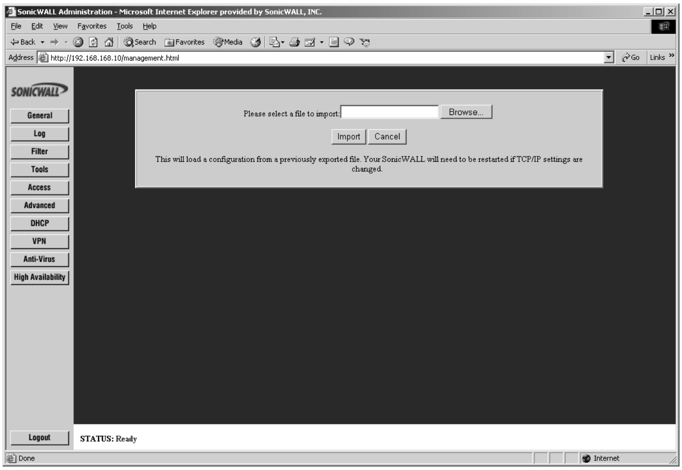
STATUS: Ready

1. Click **Export** again to download the settings file. Then choose the location to save the settings file. The file is named “sonicwall.exp” by default, but it can be renamed.
2. Click **Save** to save the file. This process can take up to a minute.

Importing the Settings File

After exporting a settings file, you can import it back to the SonicWALL.

1. Click **Import** in the **Preferences** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Browse...
Import
Cancel
Done
Internet

Please select a file to import:

This will load a configuration from a previously exported file. Your SonicWALL will need to be restarted if TCP/IP settings are changed.

STATUS: Ready

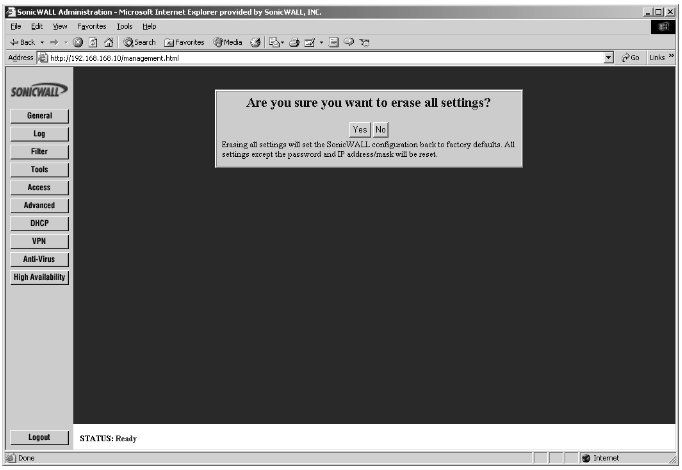
2. Click **Browse** to locate a settings file which was saved using **Export**.
3. Select the file, and click **Import**.
4. Restart the SonicWALL for the settings to take effect.

***Note**: The Web browser used to Import Settings must support HTTP uploads. Microsoft Internet Explorer 5.0 and higher as well as Netscape Navigator 4.0 and higher are recommended.*

Restoring Factory Default Settings

You can erase the SonicWALL configuration settings and restore the SonicWALL to its factory default state.

1. Click **Restore** on the **Preferences** tab to restore factory default settings.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Done
Internet

Are you sure you want to erase all settings?

Yes No

Erasing all settings will set the SonicWALL configuration back to factory defaults. All settings except the password and IP address/mask will be reset.

STATUS: Ready

2. Click **Yes**, and then restart the SonicWALL for the change to take effect.

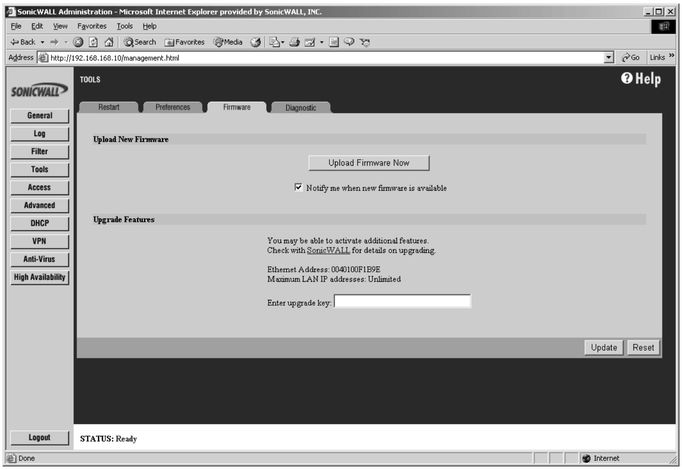
Note*: The SonicWALL LAN IP Address, LAN Subnet Mask, and the Administrator Password are not reset.*

Updating Firmware

The SonicWALL has flash memory and can be easily upgraded with new firmware. Current firmware can be downloaded from SonicWALL, Inc. Web site directly into the SonicWALL.

Note*: Firmware updates are only available to registered users. You can register your SonicWALL online at <http://www.mysonicwall.com>*.

1. Click **Tools** on the left side of the browser window, and then click the **Firmware** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
TOOLS
Help
Restart
Preferences
Firmware
Diagnostic
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Upload Firmware Now
Update
Reset
Done
Internet

Upload New Firmware

☑ Notify me when new firmware is available

Upgrade Features

You may be able to activate additional features.
Check with SonicWALL for details on upgrading.

Ethernet Address: 0040100F1B9E
Maximum LAN IP addresses: Unlimited

Enter upgrade key:

STATUS: Ready

To be automatically notified when new firmware is available, select the **Notify me when new firmware is available** check box. Then click **Update**. If you enable firmware notification, your SonicWALL sends a status message to SonicWALL, Inc. Firmware Server on a daily basis. The status message includes the following information:

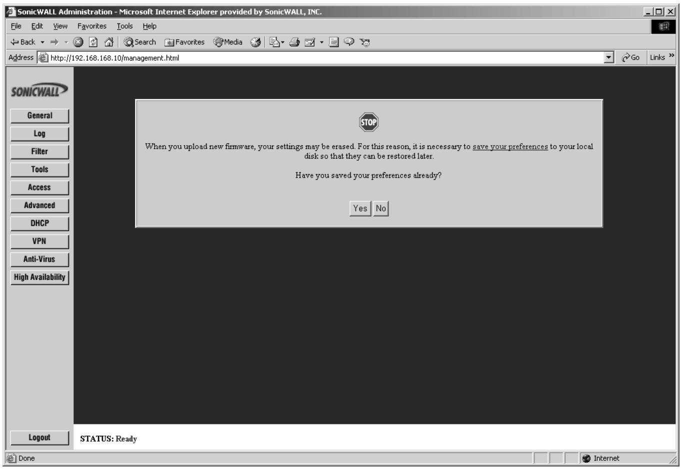
- **SonicWALL Serial Number**
- **Unit Type**
- **Current Firmware Version**
- **Language**
- **Current Available memory**
- **ROM version**
- **Options and Upgrades (SonicWALL VPN, Network Anti-Virus)**

***Note**: The SonicWALL Privacy Policy is available at <http://www.sonicwall.com/corporate_info/privacy.html> for additional information about privacy.*

When new firmware is available, a message is e-mailed to the address specified in the **Log Settings** window. In addition, the **Status** window includes notification of new firmware availability. This notification provides links to firmware release notes and to a **Firmware Update Wizard.** The **Firmware Update Wizard** simplifies and automates the upgrade process. Follow the instructions in the **Firmware Update Wizard** to update the firmware.

Updating Firmware Manually

You can also upload firmware from the local hard drive. Click **Upload Firmware**.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Done
Internet

STOP

When you upload new firmware, your settings may be erased. For this reason, it is necessary to save your preferences to your local disk so that they can be restored later.

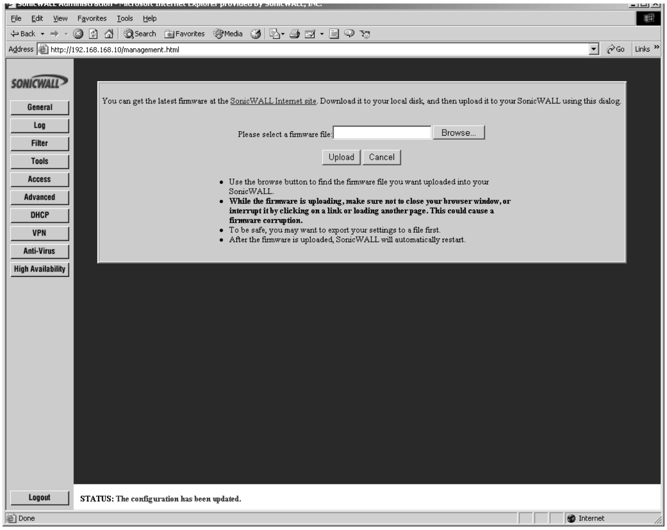
Have you saved your preferences already?

Yes No

STATUS: Ready

***Note**: The Web browser used to Import Settings must support HTTP uploads. Microsoft Internet Explorer 5.0 and higher as well as Netscape Navigator 4.0 and higher are recommended.*

When firmware is uploaded, the SonicWALL settings can be erased. Before uploading new firmware, export and save the SonicWALL settings so that they can be restored later. Once the settings have been saved, click **Yes**.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Browse...
Upload
Cancel
Done
Internet

You can get the latest firmware at the SonicWALL Internet site. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Please select a firmware file:

- Use the browse button to find the firmware file you want uploaded into your SonicWALL.
- **While the firmware is uploading, make sure not to close your browser window, or interrupt it by clicking on a link or loading another page. This could cause a firmware corruption.**
- To be safe, you may want to export your settings to a file first.
- After the firmware is uploaded, SonicWALL will automatically restart.

STATUS: The configuration has been updated.

Click **Browse** and select the firmware file from your local hard drive or from the SonicWALL Companion CD. Click **Upload**, and then restart the SonicWALL.

Note*: When uploading firmware to the SonicWALL, you must not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it can corrupt the SonicWALL firmware.*

Upgrade Features

The SonicWALL can be upgraded to support new or optional features.

Chapter 12, **SonicWALL Options and Upgrades**, provides a summary of the SonicWALL firmware upgrades, subscription services, and support offerings. You can contact SonicWALL or your local reseller for more information about SonicWALL options and upgrades.

Web:http://www.sonicwall.com

E-mail:sales@sonicwall.com

Phone:(408) 745-9600

Fax:(408) 745-9300

When an upgrade is purchased, an **Activation Key** and instructions for registering the upgrade are included. Once you have registered the upgrade, an **Upgrade Key** is issued. Enter this key in the **Enter upgrade key** field and click **Update**. Follow the instructions included with the upgrade for configuration.

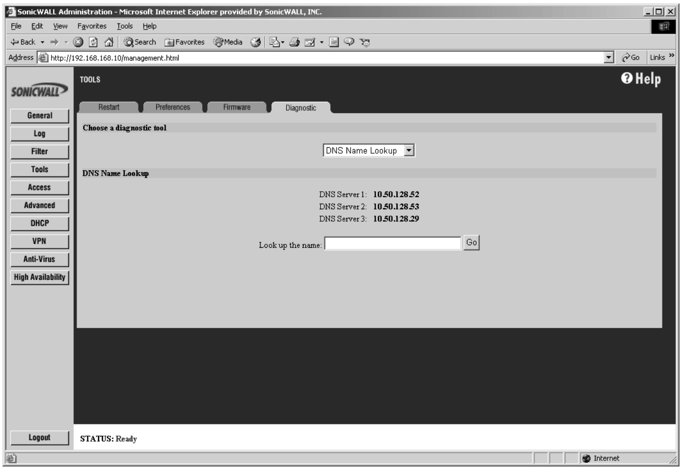
Diagnostic Tools

The SonicWALL has several built-in tools which help troubleshoot network problems. Click **Tools** on the left side of the browser window and then click the **Diagnostic** tab.

DNS Name Lookup

The SonicWALL has a DNS lookup tool that returns the numerical IP address of a domain name or if you enter an IP address, it returns the domain name.

1. Select **DNS Name Lookup** from the **Choose a diagnostic tool** menu.



Address: http://192.168.168.10/management.html

Choose a diagnostic tool: DNS Name Lookup

DNS Name Lookup

DNS Server 1: 10.50.128.52
DNS Server 2: 10.50.128.53
DNS Server 3: 10.50.128.29

Look up the name:

STATUS: Ready

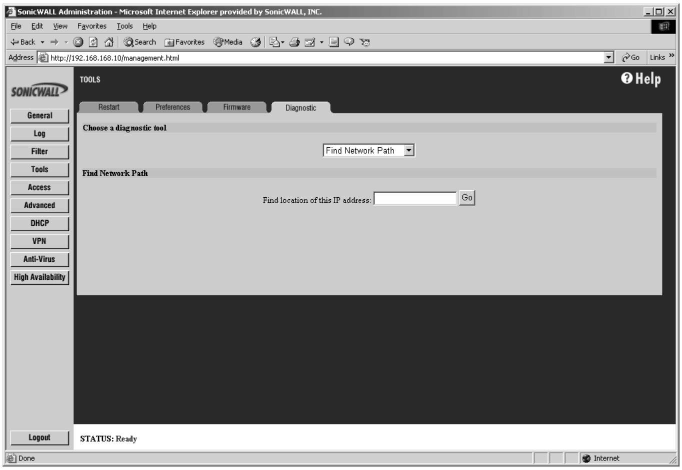
2. Enter the host name to lookup in the **Look up the name** field and click **Go**. Do not add the prefix "http://". The SonicWALL then queries the DNS server and displays the result at the bottom of the screen.

***Note**: You must define a DNS server IP address in the **Network** tab of the **General** section to perform a DNS Name Lookup.*

Find Network Path

The **Find Network Path** tool shows whether an IP host is located on the LAN or the WAN. This is helpful to determine if the SonicWALL is properly configured. For example, if the SonicWALL “thinks” that a computer on the Internet is located on the LAN, then the SonicWALL Network or Intranet settings can be misconfigured. **Find Network Path** shows if the target device is behind a router, and the Ethernet address of the target device. **Find Network Path** also shows the gateway the device is using and helps isolate configuration problems.

1. Select **Find Network Path** from the **Choose a diagnostic tool** menu.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

TOOLS

Choose a diagnostic tool

Find Network Path

Find Network Path

Find location of this IP address:

STATUS: Ready

2. Enter the IP address of the device and click **Go**. The test takes a few seconds to complete. Once completed, a message showing the results is displayed in the browser window.

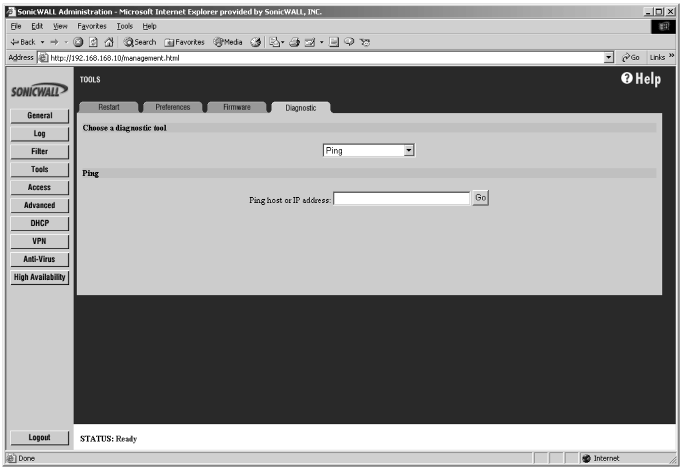
If the network path is incorrect, select the SonicWALL Intranet and Static Routes settings.

***Note**: **Find Network Path** requires an IP address. The SonicWALL **DNS Name Lookup** tool can be used to find the IP address of a host.*

Ping

The **Ping** test bounces a packet off a machine on the Internet back 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 this test is successful, try pinging devices outside the ISP. This shows if the problem lies with the ISP connection.

1. Select **Ping** from the **Choose a diagnostic tool** menu.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
TOOLS
Help
Restart
Preferences
Firmware
Diagnostic
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Done
Internet

Choose a diagnostic tool

Ping

Ping

Ping host or IP address: Go

STATUS: Ready

2. Enter the IP address of the target device to ping and click **Go**. The test takes a few seconds to complete. Once completed, a message showing the results is displayed in the browser window.

***Note**: **Ping** requires an IP address. The SonicWALL **DNS Name Lookup** tool can be used to find the IP address of a host.*

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]

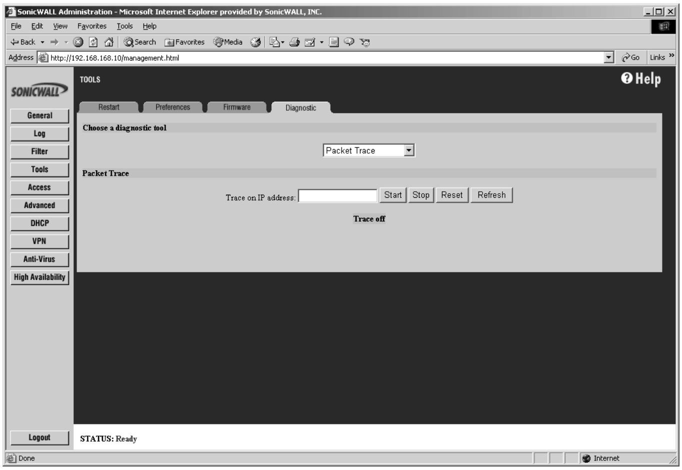
   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e

   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.

1. Select **Packet Trace** from the **Choose a diagnostic tool** menu.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

TOOLS

Choose a diagnostic tool

Packet Trace

Packet Trace

Trace on IP address:

Trace off

STATUS: Ready

__Note__: __Packet Trace__ requires an IP address. The SonicWALL __DNS Name Lookup__ tool can be used to find the IP address of a host.

2. Enter the IP address of the remote host in the **Trace on IP address** field, and click **Start**. You must enter an IP address in the **Trace on IP address** field; do not enter a host name, such as “www.yahoo.com”.
3. Contact the remote host using an IP application such as Web, FTP, or Telnet.
4. Click **Refresh** and the packet trace information is displayed.
5. Click **Stop** to terminate the packet trace, and **Reset** to clear the results.

Tech Support Report

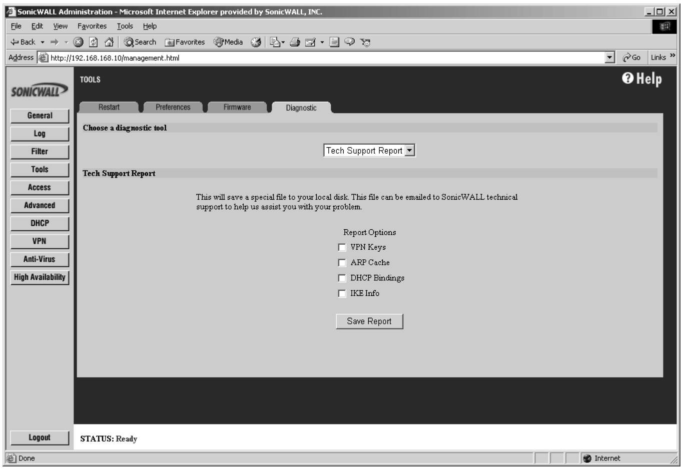
The **Tech Support Report** generates a detailed report of the SonicWALL configuration and status, and saves it to the local hard disk. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.

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

In the **Tools** section, click the **Diagnostic** tab, and then select **Tech Support Report** from the **Choose 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.

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


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
TOOLS
Help
Restart
Preferences
Firmware
Diagnostic
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Save Report
Done
Internet

Choose a diagnostic tool

Tech Support Report ▾

Tech Support Report

This will save a special file to your local disk. This file can be emailed to SonicWALL technical support to help us assist you with your problem.

Report Options

☐ VPN Keys

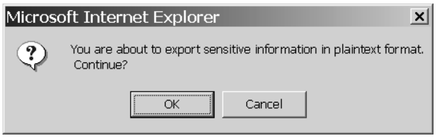
☐ ARP Cache

☐ DHCP Bindings

☐ IKE Info

STATUS: Ready

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.

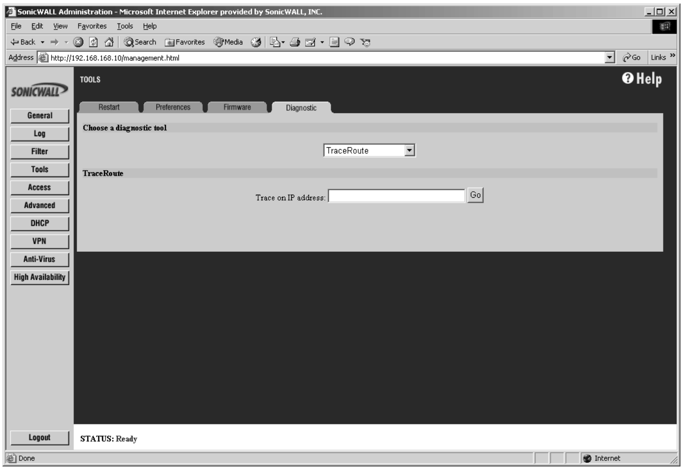


You are about to export sensitive information in plaintext format. Continue?

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.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
TOOLS
Help
Restart
Preferences
Firmware
Diagnostic
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Go
Done
Internet

Choose a diagnostic tool

TraceRoute

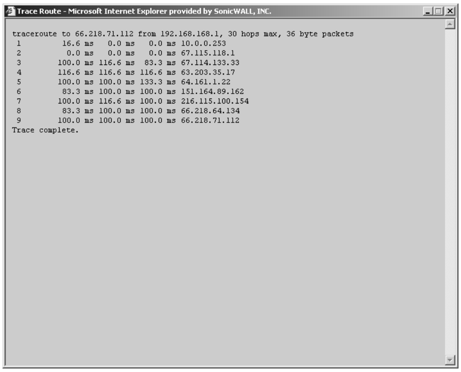
TraceRoute

Trace on IP address:

STATUS: Ready

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

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


Trace Route - Microsoft Internet Explorer provided by SonicWALL, INC.

```
traceroute to 66.218.71.112 from 192.168.168.1, 30 hops max, 36 byte packets
 1         16.6 ms   0.0 ms   0.0 ms 10.0.0.253
 2          0.0 ms   0.0 ms   0.0 ms 67.115.118.1
 3        100.0 ms 116.6 ms  83.3 ms 67.114.133.33
 4        116.6 ms 116.6 ms 116.6 ms 63.203.35.17
 5        100.0 ms 100.0 ms 133.3 ms 64.161.1.22
 6         83.3 ms 100.0 ms 100.0 ms 151.164.89.162
 7        100.0 ms 116.6 ms 100.0 ms 216.115.100.154
 8         83.3 ms 100.0 ms 100.0 ms 66.218.64.134
 9        100.0 ms 100.0 ms 100.0 ms 66.218.71.112
Trace complete.
```

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

7 Network Access Rules

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. This behavior is 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.
- Allow 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.

The custom rules evaluate network traffic source IP address, destination IP address, IP protocol type, 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.

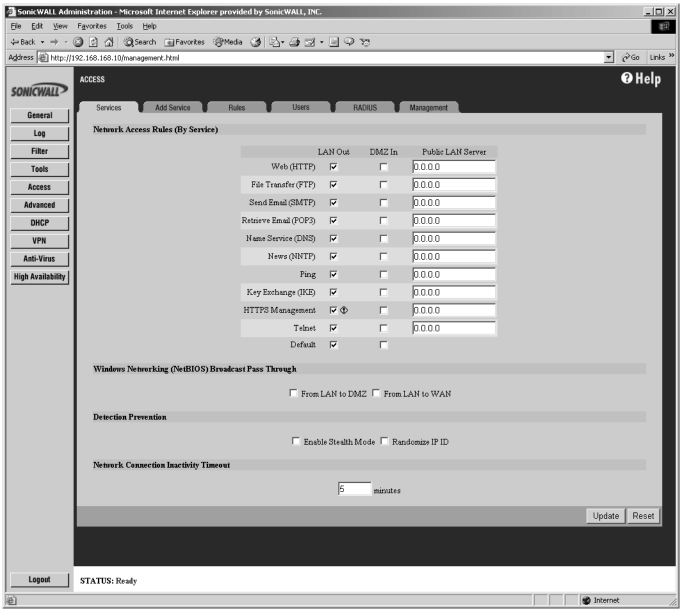
***Note**: The ability to define Network Access Rules is a very powerful tool. Using custom rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting Network Access Rules.*

Viewing Network Access Rules

The **Services** window displays a table of defined Network Access Rules. Rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Default** rule. The Default rule is all IP services except those listed in the Services window. 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. However, LAN access to NNTP can be unblocked by deselecting **LAN Out** corresponding to the NNTP News service.

Services

Click **Access** on the left side of the browser window, and then click the **Services** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
ACCESS
Help
Services
Add Service
Rules
Users
RADIUS
Management
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Update
Reset
Internet

Network Access Rules (By Service)

	LAN Out	DMZ In	Public LAN Server
Web (HTTP)	☑	□	0.0.0.0
File Transfer (FTP)	☑	□	0.0.0.0
Send Email (SMTP)	☑	□	0.0.0.0
Retrieve Email (POP3)	☑	□	0.0.0.0
Name Service (DNS)	☑	□	0.0.0.0
News (NNTP)	☑	□	0.0.0.0
Ping	☑	□	0.0.0.0
Key Exchange (IKE)	☑	□	0.0.0.0
HTTPS Management	☑ ⚠	□	0.0.0.0
Telnet	☑	□	0.0.0.0
Default	☑	□	

Windows Networking (NetBIOS) Broadcast Pass Through

□ From LAN to DMZ □ From LAN to WAN

Detection Prevention

□ Enable Stealth Mode □ Randomize IP ID

Network Connection Inactivity Timeout

5 minutes

STATUS: Ready

***Note**: The LAN In column is not displayed if NAT is enabled.*

The **Services** window allows you to customize **Network Access Rules** by service. Services displayed in the **Services** window relate to the rules in the **Rules** window, so any changes on the **Services** window appear in the **Rules** window. The **Default** rule, at the bottom of the table, encompasses all Services.

LAN Out

If the **LAN Out** check box is selected, you can access that service from your LAN on the Internet. Otherwise, you are blocked from accessing that service. By default, the **LAN Out** check boxes are selected.

DMZ In (Optional)

If the **DMZ In** is selected, users on the Internet can access that service on the DMZ. Otherwise, they are blocked from accessing that service on the DMZ. By default, **DMZ In** is selected. The **DMZ In** column does not appear in the Web Management Interface for the SonicWALL SOHO3 and TELE3 which do not have a separate DMZ port.

***Note**: If an **Alert** Icon appears next to a **LAN Out**, **LAN In,** or **DMZ In** check box, a rule in the **Rules** window modifies that service.*

Public LAN Server

A **Public LAN Server** is a LAN server designated to receive inbound traffic for a specific service, such as Web or e-mail. You can define a **Public LAN Server** by entering the server's

IP address in the **Public LAN Server** field for the appropriate service. If you do not have a Public LAN Server for a service, enter "0.0.0.0" in the field.

Windows Networking (NetBIOS) Broadcast Pass Through

Computers running Microsoft Windows communicate with one another through NetBIOS broadcast packets. By default, the SonicWALL blocks these broadcasts. If you select **From LAN to WAN**, your SonicWALL allows NetBIOS broadcasts from LAN to DMZ or from LAN to WAN. Then, LAN users are able to view machines on the DMZ and the WAN in their Windows Network Neighborhood.

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

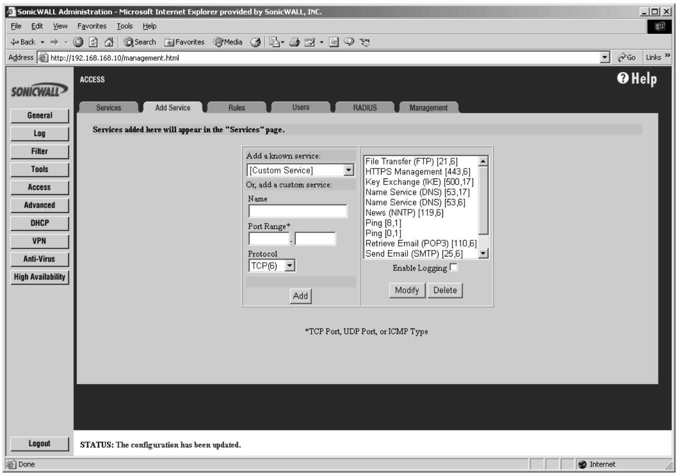
A **Randomize IP ID** check box is available to prevent hackers using various detection tools from detecting the presence of a SonicWALL appliance. IP packets are given random IP IDs which makes it more difficult for hackers to “fingerprint” the SonicWALL appliance. Use this check box for additional security from hackers.

Network 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.

Add Service

To add a service not listed in the **Services** window, click **Access** on the left side of the browser window, and then click the **Add Service** tab.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

Services added here will appear in the "Services" page.

Add a known service: [Custom Service]

Or, add a custom service:

Name

Port Range* -

Protocol TCP(6)

File Transfer (FTP) [21,6]
HTTPS Management [443,6]
Key Exchange (IKE) [500,17]
Name Service (DNS) [53,17]
Name Service (DNS) [53,6]
News (NNTP) [119,6]
Ping [8,1]
Ping [0,1]
Retrieve Email (POP3) [110,6]
Send Email (SMTP) [25,6]

Enable Logging □

*TCP Port, UDP Port, or ICMP Type

STATUS: The configuration has been updated.

The list on the right side of the window displays the services that are currently defined. These services also appear in the **Services** window.

Two numbers appear in brackets next to each service. The first number indicates the service's IP port number. The second number indicates the IP protocol type (6 for TCP, 17 for UDP, or 1 for ICMP).

Note: There can be multiple entries with the same name. For example, the default configuration has two entries labeled “Name Service (DNS)” for UDP port 53 and TCP port 53. Multiple entries with the same name are grouped together, and are treated as a single service. Up to 128 entries are supported.

Add a Known Service

1. Select the name of the service you want to add from the **Add a known service** list.
2. Click **Add**. The new service appears in the list box on the right side of the browser window. Note that some services add more than one entry to the list.

   ***Note**: Session Initiation Protocol (SIP) and HTTPS are also available **Services**.*

Add a Custom Service

1. Select **[Custom Service]** from the **Add** a known service list.
2. Type a unique name, such as "CC:mail" or "Quake" in the **Name** field.
3. Enter the beginning number of the IP port range and ending number of the IP port range in the **Port Range** fields. If the service only requires one IP port, enter the single port number in both **Port Range** fields.

Note: *Visit <http://www.ietf.org/rfc/rfc1700.txt> for a list of IP port numbers.*

4. Select the IP protocol type, **TCP**, **UDP** or **ICMP**, from the **Protocol** list.
5. Click **Add**. The new service appears in the list on the right side of the browser window.

Note: If multiple entries with the same name are created, they are grouped together as a single service and can not function as expected.

Enable Logging

You can enable and disable logging of events in the SonicWALL **Event Log**. For example, if Linux authentication messages are filling up your log, you can disable logging of Linux authentication.

1. Highlight the name of the desired service in the list.
2. Clear the **Enable Logging** check box.
3. Click **Modify**.

Delete a Service

To delete a service, highlight the name in the list, and click **Delete Service**. If multiple entries with the same name exist, delete all entries to remove the service.

Rules

The SonicWALL evaluates the source IP address, the destination IP address, and the service type when determining whether to allow or deny traffic. Custom rules take precedence and override the SonicWALL default rules.

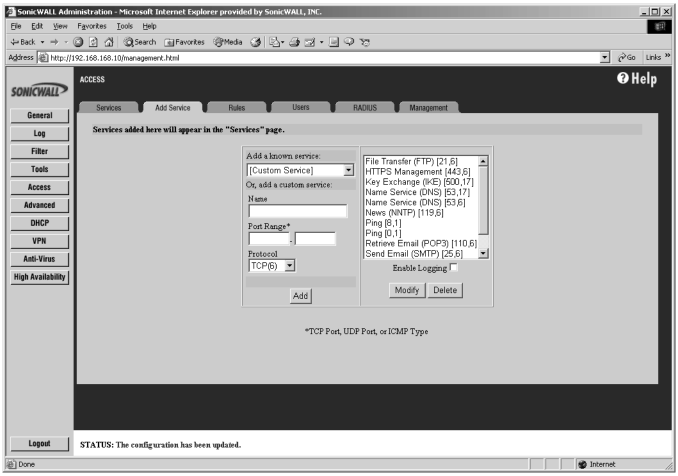
By default, the SonicWALL blocks all traffic from the Internet to the LAN and allows all traffic from the LAN to the Internet. Custom rules can be created to modify the default rules. For example, rules can be created for the following purposes:

- Allow traffic from the Internet to a mail server on the LAN.
- Restrict users on the LAN from using a specified service, such as QuickTime.
- Allow specified IP addresses on the Internet to access a sensitive server on the LAN.
- Configure bandwidth management for individual services.

Maximum Number of Rules by Product

Product	**Maximum Rules**	**Rules Available for Bandwidth Management**
GX Series	300	100
PRO 300	200	100
PRO 100, PRO 200	100	50
TELE3, SOHO3	100	50
TELE2, SOHO2, XPRS2, XPRS, PRO, PRO-Vx	100	20

To create custom **Network Access Rules**, click **Access** on the left side of the browser window, and then click the **Rules** tab.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
ACCESS
Help
Services
Add Service
Rules
Users
RADIUS
Management
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Add
Modify
Delete
Done
Internet

Services added here will appear in the "Services" page.

Add a known service: [Custom Service]

Or, add a custom service:

Name

Port Range* -

Protocol TCP(6)

File Transfer (FTP) [21,6]
HTTPS Management [443,6]
Key Exchange (IKE) [500,17]
Name Service (DNS) [53,17]
Name Service (DNS) [53,6]
News (NNTP) [119,6]
Ping [8,1]
Ping [0,1]
Retrieve Email (POP3) [110,6]
Send Email (SMTP) [25,6]

Enable Logging □

*TCP Port, UDP Port, or ICMP Type

STATUS: The configuration has been updated.

***Note**: Use extreme caution when creating or deleting Network Access Rules, because you can disable firewall protection or block access to the Internet.*

Network Access Rule Logic List

It is important to fully consider the logic behind the new rule before it is added to the list. The following list of statements/questions can help you determine how to add rules to the list:

1. State the intent of the rule. For example, “This rule restricts all IRC access from the LAN to the Internet.”
2. Is the intent of the rule to allow or deny traffic?
3. What is the direction of the traffic? From the LAN to the WAN, or from the WAN to the LAN?
4. List IP services affected by the rules.
5. List the computers on the LAN affected by the rule.
6. List the computers on the WAN affected by the rule. If allowing traffic from the WAN to the LAN, it is better to allow WAN traffic only to certain computers on the LAN.
7. Does the rule prevent users from accessing critical resources on the Internet?
8. Does the rule create any security vulnerabilities?
9. Does the rule conflict with any existing rules?

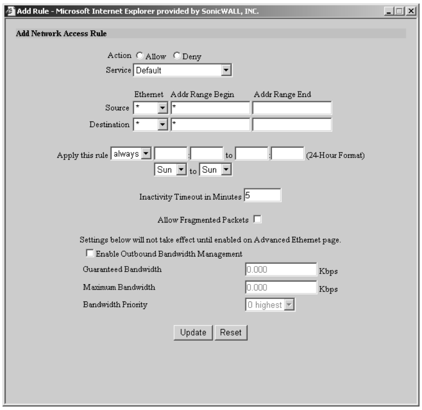
Bandwidth Management

The SonicWALL can now be configured for bandwidth management of outbound (WAN) network traffic via bandwidth management. Each **Service** add via a **Rule** has a checkbox to enable bandwidth management for the **Service**. Select **Enable Bandwidth Management**, then enter the **Guaranteed Bandwidth** in Kpbs for the **Service**, and enter the **Maximum Bandwidth** in number of Kpbs for the **Service**. Before you can enable and configure bandwidth management for **Rules**, you must enable it on the **Ethernet** page in the **Advanced** section.

***Note**: Bandwidth management is very complex and requires extensive knowledge of networks and networking protocols. Incorrect bandwidth management may cause network problems or degradation of network performance. See Bandwidth Management in Chapter 10, Advanced, of this manual.*

Add A New Rule

1. Click **Add New Rule...** to open the **Add Rule** window.


Add Rule - Microsoft Internet Explorer provided by SonicWALL, INC.

Add Network Access Rule

Action ○ Allow ○ Deny

Service Default

	Ethernet	Addr Range Begin	Addr Range End
Source	*	*	
Destination	*	*	

Apply this rule always : to : (24-Hour Format)
Sun to Sun

Inactivity Timeout in Minutes 5

Allow Fragmented Packets □

Settings below will not take effect until enabled on Advanced Ethernet page.

□ Enable Outbound Bandwidth Management

Guaranteed Bandwidth 0.000 Kbps

Maximum Bandwidth 0.000 Kbps

Bandwidth Priority 0 highest

2. Select **Allow or Deny** in the **Action** list depending upon whether the rule is intended to permit or block IP traffic.

3. Select the name of the service affected by the **Rule from the Service** list. If the service is not listed, you must define the service in the **Add Service** window. The **Default** service encompasses all IP services.

4. Select the source of the traffic affected by the rule, either LAN or WAN, *(both), from the **Source Ethernet** menu.

   If you want to define the source IP addresses that are affected by the rule, such as restricting certain users from accessing the Internet, enter the starting IP addresses of the address range in the **Addr Range Begin** field and the ending IP address in the **Addr Range End** field. To include all IP addresses, enter * in the **Addr Range Begin** field.

5. Select the destination of the traffic affected by the rule, either **LAN** or **WAN** or *, from the **Destination Ethernet** menu.

If you want to define the destination IP addresses that are affected by the rule, for example, to allow inbound Web access to several Web servers on your LAN, enter the starting IP addresses of the address range in the **Addr Range Begin** field and the ending IP address in the **Addr Range End** field. To include all IP addresses, enter * in the **Addr Range Begin** field.

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

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

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

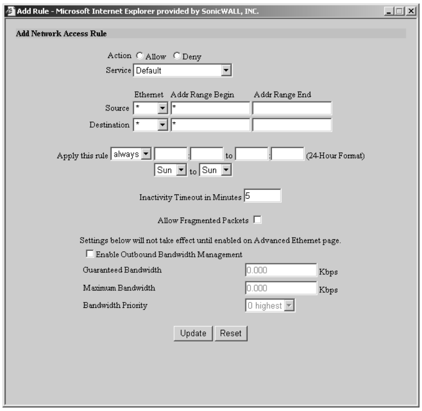
7. If you would like for the rule to timeout after a period of inactivity, set the amount of time, in minutes, in the **Inactivity Timeout in Minutes** field. The default value is 5 minutes.
8. Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments 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.
9. Enable **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in **Kpbs**.
10. Enter the maximum amount of bandwidth available to the **Rule** at any time in the **Maximum Bandwidth** field. Assign a priority from 0 (highest) to 7 (lowest).
11. Click **Update**. Once the SonicWALL has been updated, the new rule appears in the list of **Current Network Access Rules**.

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

For example, to configure the SonicWALL to allow Internet traffic to your Web server with an IP address of 208.5.5.5 (**Standard** mode), create the following rule:

1. Verify that **HTTP** has been added as a **Service** as outlined previously.

2. Click the **Rules** tab, and click **Add New Rule....**



Add Rule - Microsoft Internet Explorer provided by SonicWALL, INC.

Add Network Access Rule

Action ○ Allow ○ Deny

Service: Default

	Ethernet	Addr Range Begin	Addr Range End
Source	*	*	
Destination	*	*	

Apply this rule: always ___ : ___ to ___ : ___ (24-Hour Format)
Sun to Sun

Inactivity Timeout in Minutes: 5

Allow Fragmented Packets □

Settings below will not take effect until enabled on Advanced Ethernet page.

□ Enable Outbound Bandwidth Management

Guaranteed Bandwidth	0.000	Kbps
Maximum Bandwidth	0.000	Kbps
Bandwidth Priority	0 highest	

3. Select **Allow**, then **Web (HTTP)** from the **Service** menu.

4. Select **WAN** from the **Ethernet Source** menu, and leave the **Addr Range Begin** and **Addr Range End** as they appear.

5. Select **LAN** from the **Ethernet Destination** menu, and type in the IP address of the Web server, 208.5.5.5 in the **Addr Range Begin** field. No IP address is added in the **Addr Range End** since the destination is not a range of IP addresses.

6. Select **always** from the **Apply this rule** menu.

7. Enter a value (in minutes) in the **Activity Timeout in Minutes** field.

8. Do not select the **Allow Fragmented Packets** check box.

9. If you want the Rule to have guaranteed bandwidth, select **Enable Outbound Bandwidth Management**, and enter values for **Guaranteed Bandwidth**, **Maximum Bandwidth**, and **Bandwidth Priority**.

10. Click **Update** to add the rule to the SonicWALL.

***Note**: The source part (WAN or LAN) can be limited to certain parts of the Internet using a range of IP addresses on the WAN or LAN. For example, the following rule can be used to configure the same Web server to be only visible from a single C class subnet on the Internet: Allow HTTP, Source WAN 216.77.88.1 - 216.77.88.254, Destination LAN 208.5.5.5.*

Current Network Access Rules List

All **Network Access Rules** are listed in the **Current Network Access Rules** table. The rules are listed from most to least specific. The rules at the top of **Current Network Access Rules** list take precedence over rules at the bottom of the list.

Edit a Rule

To edit a rule, click the **Note Pad** icon on the right side of the browser window. A new Web browser window appears, displaying the current configuration of the rule. Make the desired changes and click **Update** to update the rule. The modified rule is displayed in the list of **Current Network Access Rules**.

Delete a Rule

To delete a rule, click the **Trash Can** icon at the right side of the browser window. A dialog box appears with the message "Do you want to remove this rule?". Click **OK**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Enable/Disable a Rule

To disable a rule without permanently removing it, clear the **Enable** check box to the right of the rule. To enable a disabled rule, select the **Enable** check box. The configuration is updated automatically, and a message confirming the update is displayed at the bottom of the browser window.

Restore the Default Network Access Rules

If the SonicWALL **Network Access Rules** have been modified or deleted, you can restore the **Default Rules.** The **Default Rules** prevent malicious intrusions and attacks, block all inbound IP traffic and allow all outbound IP traffic. Click **Restore Rules to Defaults** to reset the **Network Access Rules**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Understanding the Access Rule Hierarchy

The rule hierarchy has two basic concepts:

1. Specific rules override general rules:

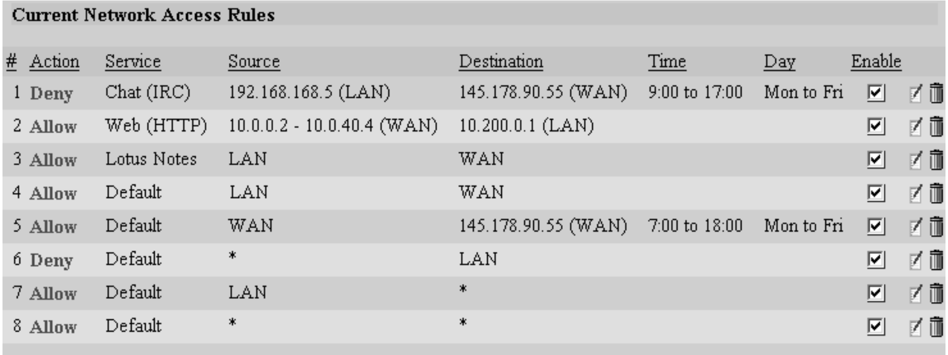
   An individual service is more specific than the **Default** service.

   A single Ethernet link, such as LAN or WAN, is more specific than * (all).

   A single IP address is more specific than an IP address range.

2. Equally specific **Deny** rules override **Allow** rules.

Rules are displayed in the **Current Network Access Rules** list from the most specific to the least specific, and rules at the top override rules listed below. For example, consider the section of the **Rules** window shown below.



Current Network Access Rules

#	Action	Service	Source	Destination	Time	Day	Enable
1	Deny	Chat (IRC)	192.168.168.5 (LAN)	145.178.90.55 (WAN)	9:00 to 17:00	Mon to Fri	☑
2	Allow	Web (HTTP)	10.0.0.2 - 10.0.40.4 (WAN)	10.200.0.1 (LAN)			☑
3	Allow	Lotus Notes	LAN	WAN			☑
4	Allow	Default	LAN	WAN			☑
5	Allow	Default	WAN	145.178.90.55 (WAN)	7:00 to 18:00	Mon to Fri	☑
6	Deny	Default	*	LAN			☑
7	Allow	Default	LAN	*			☑
8	Allow	Default	*	*			☑

The **Default Allow Rule** (#7) at the bottom of the page allows all traffic from the LAN to the WAN. However, Rule #1 blocks IRC (Chat) traffic from a computer on the LAN to a server on the WAN.

The **Default Deny Rule** (#6) blocks all traffic from the WAN to the LAN, however, Rule #2 overrides this rule by allowing Web traffic from the WAN to the LAN.

Examples

The following examples illustrate methods for creating **Network Access Rules**.

Blocking LAN access for specific services

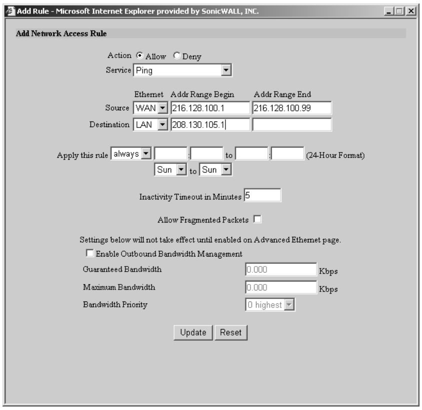
This example shows how to block LAN access to NNTP servers on the Internet during business hours.

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

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 New Rule** in the **Rules** window to launch the **"Add Network Access Rule"** window.
2. Select **Allow** from the **Action** menu.
3. Select **Ping** from the **Service** menu.
4. Select **WAN** from the **Source Ethernet** menu.
5. Enter the starting IP address of the ISP network in the **Source Addr Range Begin** field and the ending IP address of the ISP network in the **Source Addr Range End** field.
6. Select **LAN** from the **Destination Ethernet** menu.
7. Since the intent is to allow a ping only to the SonicWALL, enter the SonicWALL LAN IP Address in the **Destination Addr Range Begin** field.
8. Select **Always** from the **Apply this rule** menu to ensure continuous enforcement.
9. Click **Update** to add your new Rule.



Add Rule - Microsoft Internet Explorer provided by SonicWALL, INC.

Add Network Access Rule

Action ● Allow ○ Deny

Service: Ping

	Ethernet	Addr Range Begin	Addr Range End
Source	WAN	216.128.100.1	216.128.100.99
Destination	LAN	208.130.105.1	

Apply this rule: always : to : (24-Hour Format)

Sun to Sun

Inactivity Timeout in Minutes: 5

Allow Fragmented Packets □

Settings below will not take effect until enabled on Advanced Ethernet page.

□ Enable Outbound Bandwidth Management

Guaranteed Bandwidth: 0.000 Kbps

Maximum Bandwidth: 0.000 Kbps

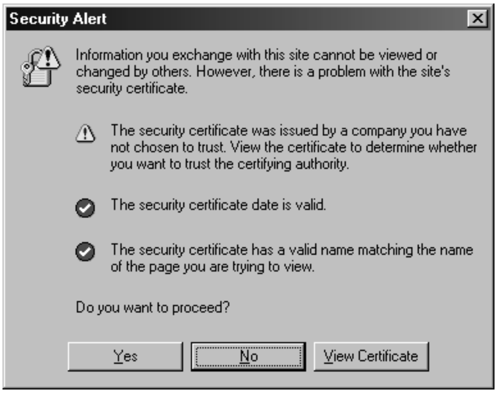
Bandwidth Priority: 0 highest

HTTPS Management of the SonicWALL

To enhance the security of the TELE3 SP, **HTTPS Management** using Secure Socket Layer (SSL) is supported when you log into the SonicWALL using https://IP Address where the IP address is the SonicWALL LAN IP address. For example, if the LAN IP address of your SonicWALL appliance is 192.168.168.1, you can log in using HTTPS by entering <https://192.168.168.1>. Access is encrypted using SSL technology for a secure connection.

HTTPS Management allows secure access to the SonicWALL without a VPN client. It is a simple and secure way to manage your SonicWALL from both the LAN and the WAN.

The first time you log into the SonicWALL using HTTPS, you may see the following information message:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Click **Yes** to continue the login process. SSL is supported by Netscape 4.7 and higher, as well as Internet Explorer 5.5 and higher.

HTTPS Management supports the following versions of SSL: SSLv2, SSLv3, and TLSv1. Also, the following encryption ciphers are supported: RC4-MD5, EXP-RC4-MD5, DES-CBC3-SHA, RC4-SHA, EXP-RC2-CBC-MD5, NULL-SHA, and NULL-MD-5. An 1024-bit RSA key is used.

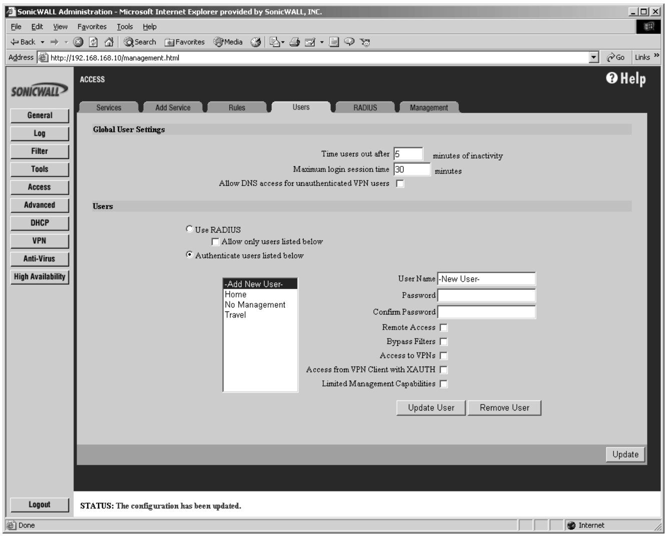
To use this feature, you must add **HTPP Management** as a **Service** to the firewall. See “Add Service” on page 69 for instructions on adding Services to the SonicWALL.

Users

Extensive modifications and additional features are available on the **Users** tab in the **Access** section of the Management interface. User level access can now be configured for authentication and access to the network. Authentication can be performed using a local user database, RADIUS, or a combination of the two applications.

For instructions on configuring individual users on RADIUS servers, see Appendix G at the end of this Guide.

Currently, when a VPN tunnel is established between two SonicWALL appliances, any users residing on the local LAN of each SonicWALL can send data across the VPN. In some cases, complete user access could be a security risk, and only authenticated users access the VPN tunnel and send data across the network.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
ACCESS
Help
Services Add Service Rules Users RADIUS Management
General Log Filter Tools Access Advanced DHCP VPN Anti-Virus High Availability
Logout
Update User Remove User
Update
Done
Internet

Global User Settings

Time users out after 5 minutes of inactivity

Maximum login session time 30 minutes

Allow DNS access for unauthenticated VPN users □

Users

○ Use RADIUS

□ Allow only users listed below

● Authenticate users listed below

-Add New User-
Home
No Management
Travel

User Name -New User-

Password

Confirm Password

Remote Access □

Bypass Filters □

Access to VPNs □

Access from VPN Client with XAUTH □

Limited Management Capabilities □

STATUS: The configuration has been updated.

Global User Settings

- **Time users out after 5 minutes of inactivity** - Enter the number of allowable inactivity minutes before a user is automatically logged out of the network via the SonicWALL.
- **Maximum login session time** - Configure the length of time, in minutes, that a user is allowed to be logged into the network via the SonicWALL. When a user logs into the SonicWALL using his username and password, the user can also set the maximum login session time, but LAN it cannot be longer than the time configured by the administrator. You may set the login session time to 0 (zero) for unlimited login session time.
- **Allow DNS access for unauthenticated VPN users** - Enabling this check box allows unauthenticated DNS traffic to access the DNS server over a VPN tunnel with authentication enforcement. Use this checkbox if you allow unauthenticated users to access the DNS server on your LAN.

Users

- **Use RADIUS** - Select this radio button if you have configured RADIUS to authenticate users accessing the network through the SonicWALL. If you have more than 100 users that require authentication, you must use RADIUS. If you select **Use RADIUS**, 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.
- **Allow only users listed below** - Enable this setting if you have a subset of RADIUS users accessing the SonicWALL. The user names must be added to the internal SonicWALL user database before they can be authenticated using RADIUS.

- **Authenticate users listed below** - Electing this option allows you to configure users in the local database. To add new users, fill out the **User Name**, **Password**, and **Confirm Password** fields, then select from the list of privileges allowed for the user:

  - Remote Access - Enable this check box if the user accesses LAN resources through the firewall from a remote location on the Internet.

  Note: By enabling Remote Access, you allow unencrypted traffic over the Internet.

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

  - Access to VPNs - Enable the check box if the user can send information over the VPN Security Associations with authentication enforcement.

  - **Access from the VPN Client with XAUTH** - Enable the check box if the user requires XAUTH for authentication and accesses the firewall via a VPN client.

  - 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

***Note**: The SonicWALL supports 100 users in the local database.*

Adding a User to the Local Database

***Note**: You must add a user to the Local Database to enforce access privileges.*

To add a new user, complete the following steps.

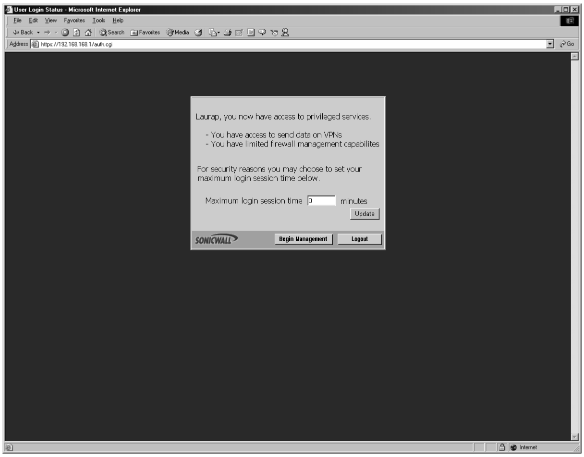
1. Log into the Management interface, click **Access**, then **Users**.
2. Highlight **-Add New User-** in the **Current User** list box.
3. Enter the name of a user into the **User Name** field.
4. Enter the user password in the **Password** and **Confirm Password** field. It is important to select a password not easily guessed by someone. Using a random mixture of alphanumeric characters and symbols is recommended. The password is case-sensitive.
5. Choose the privileges to be enabled for the user by selecting the appropriate check boxes.
6. Click **Update** to add the user to the SonicWALL database.
7. To remove a user, highlight the **User Name**, and click **Remove User**.

User Login Changes

When a user other than the administrator logs into the SonicWALL Management interface, a page is displayed with the user's privileges listed. The user can set the maximum time for a login session, but it cannot be longer than the session time set by the administrator.The connection closes when the user exceeds the inactivity time-out period or the maximum session time is exceeded. If the connection is closed, the user must re-authenticate to regain their access through the SonicWALL.

Logging into the SonicWALL as the administrator automatically gives the user access to all VPN tunnels requiring authentication.

***Note**: Authentication sessions create a log entry in the SonicWALL, but user activity is not logged*.



User Login Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.168.1/auth.cgi
Go

Laurap, you now have access to privileged services.

- You have access to send data on VPNs
- You have limited firewall management capabilites

For security reasons you may choose to set your maximum login session time below.

Maximum login session time 0 minutes

Update
SONICWALL
Begin Management
Logout
Internet

RADIUS

RADIUS has moved from **VPN** to **Access** because RADIUS can now provide control over user access and not just VPN access in this firmware release.

To configure RADIUS settings, complete the following instructions.

Click the **RADIUS** tab.

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

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. Enter the IP address of the RADIUS server in the **IP Address** field.
5. Enter the **Port Number** for the RADIUS server.
6. If there is a secondary RADIUS server, enter the appropriate information in the **Secondary Server** section.
7. Enter 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 is case sensitive.

RADIUS Users

You can select the default privileges for all RADIUS users in this section.

- **Remote Access** - Enable this check box if the user accesses the SonicWALL from a remote computer. This option is only available in Standard mode.
- **Bypass Filters** - Enable **Bypass Filters** if the user can bypass Content Filter settings.
- **Access to VPNs** - Enable the check box if the user can send information over VPN Security Associations.
- **Access from the VPN Client with XAUTH** - Enable the check box if a VPN client is using XAUTH for authentication.
- **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

RADIUS Client Test

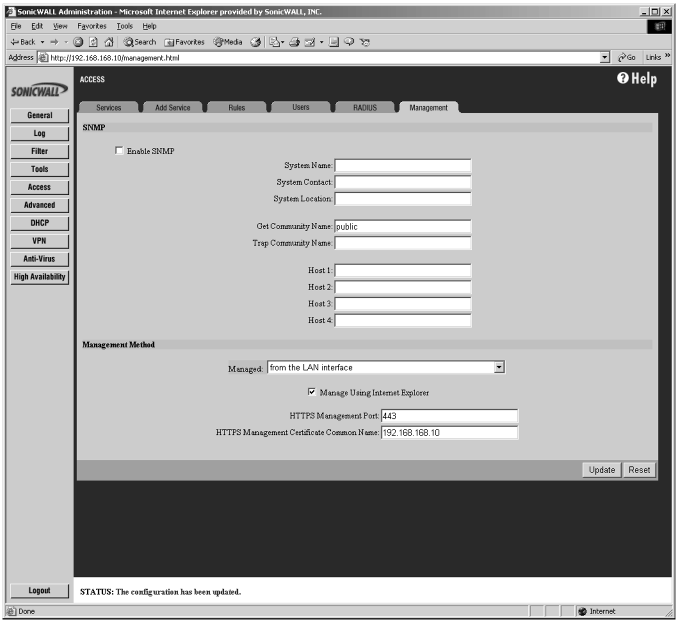
You can test your RADIUS Client user name and password by typing in a valid User name in the **User** field, and the Password in the **Password** field. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**. Once the SonicWALL has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to enter a User Name and Password into a dialogue box.

SonicWALL Management

SonicWALL SNMP Support

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 Internet Security appliances and receive notification of any critical events as they occur on the network. SonicWALL Internet security appliances support SNMP v1/v2c and all relevant Management Information Base II (MIBII) 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 Website and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

To configure **SNMP** in the SonicWALL Internet Security appliance, log into the SonicWALL Management interface. Click **Access**, then **Management**. The **SNMP** configuration panel is displayed.



Address http://192.168.168.10/management.html

SNMP

□ Enable SNMP

System Name:

System Contact:

System Location:

Get Community Name: public

Trap Community Name:

Host 1:

Host 2:

Host 3:

Host 4:

Management Method

Managed: from the LAN interface

☑ Manage Using Internet Explorer

HTTPS Management Port: 443

HTTPS Management Certificate Common Name: 192.168.168.10

STATUS: The configuration has been updated.

The SonicWALL SNMP agent generates two traps: **Cold Start Trap** and **Alert Traps**. **Cold Start Traps** indicates that the SonicWALL appliance is re-initializing itself so that the agent configuration or the appliance can be altered. **Alert Traps** are based on the existing SonicWALL alert messages which allows the trap messages to share a common message string with the alerts. Accordingly, no trap message can exist without a corresponding alert message.

To configure **SNMP**, enter the necessary information in the following fields:

1. To enable the SNMP agent, select **Enable SNMP**.
2. Enter the **System Name.** This is the hostname of the SonicWALL appliance.
3. In the **System Contact** field**,** type in the name of the network administrator for the SonicWALL appliance.
4. Enter an e-mail address, telephone number, or pager number in the **System Location** field.
5. Create a name for a group or community of administrators who can view SNMP data, and enter it in the **Get Community Name** field.
6. Create a name for a group or community of administrators who can view SNMP traps, and enter it in the **Trap Community Name** field.
7. Enter the IP address or hostname of the SNMP management system receiving the SNMP traps in the **Host 1 through 4** fields. Up to 4 addresses or hostnames can be specified.

Configuration of the Log/Log Settings for SNMP

Trap messages are generated only for the categories that alert messages are normally sent, i.e. attacks, system errors, blocked Web sites. If none of the categories are selected on the **Log Settings** page, then none of the trap messages are sent out.

Configuration of the Service and Rules Pages

By default, the SonicWALL appliance responds only to **SNMP Get** messages received on its LAN interface. Appropriate rules must be set up in the SonicWALL to allow SNMP traffic to and from the WAN. SNMP trap messages can be sent via the LAN, WAN, or LAN interface.

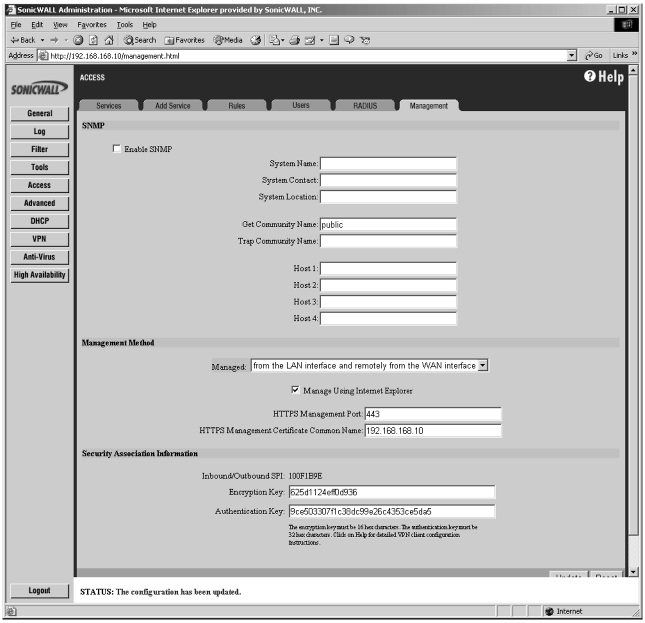
If your SNMP management system supports discovery, the SNMP agent should automatically discover the SonicWALL appliance on the network. Otherwise, you must add the SonicWALL appliance to the list of SNMP manageable devices on the SNMP management system.

SonicWALL Remote Management

All SonicWALLs include a **Management Security Association** (SA) for secure remote management. The **Management SA** does not permit access to remote network resources.

***Note**: If you have enabled VPN on your SonicWALL, the SonicWALL can be managed remotely using a **Management SA** or with a **VPN SA**. See Chapter 10 for VPN configuration instructions and basic VPN terms and concepts.*

To enable secure remote management, click **Access** on the left side of the browser window, and click the **Management** tab. Then select **Managed: "from the LAN interface and remotely from the WAN interface"** to enable secure remote management.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
ACCESS
Help
Services
Add Service
Rules
Users
RADIUS
Management
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Internet

SNMP

☐ Enable SNMP

System Name:

System Contact:

System Location:

Get Community Name: public

Trap Community Name:

Host 1:

Host 2:

Host 3:

Host 4:

Management Method

Managed: from the LAN interface and remotely from the WAN interface

☑ Manage Using Internet Explorer

HTTPS Management Port: 443

HTTPS Management Certificate Common Name: 192.168.168.10

Security Association Information

Inbound/Outbound SPI: 100F1B9E

Encryption Key: 625d1124eff0d936

Authentication Key: 9ce503307f1c38dc99e26c4353ce5da5

The encryption key must be 16 hex characters. The authentication key must be 32 hex characters. Click on Help for detailed VPN client configuration instructions.

STATUS: The configuration has been updated.

When remote management is enabled, a **Management SA** is automatically generated. The **Management SA** uses Manual Keying to set up a VPN tunnel between the SonicWALL and the VPN client. The **Management SA** also defines **Inbound** and **Outbound Security Parameter Indices (SPIs)** which match the last eight digits of the SonicWALL serial number. The preset SPIs are displayed in the **Security Association Information** section. It is not necessary to configure a VPN connection for **Remote Management** as the **Management SA** is automatically configured in this section.

1. Enter a 16-character hexadecimal encryption key in the **Encryption Key** field. Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F. An example of a valid encryption key is 1234567890A-BCDEF. Or you can use the randomly generated key that appears in the **Encryption Key** field.
2. Enter a 32-character hexadecimal authentication key in the **Authentication Key** field. An example of a valid authentication key is 1234567- 890ABCDEF1234567890ABCDEF. Or you can use the randomly generated key that appears in the **Authentication Key** field.
3. Click **Update**. Restart the SonicWALL for the change to take effect.

***Note**: When a **Management SA** is created, the remote SonicWALL is managed at the SonicWALL WAN IP Address.*

4. Click **Help** in the upper right corner of the SonicWALL Management Interface to access detailed instructions for configuring the VPN client. Additional instructions are available at <http://www.sonicwall.com/products/documentation/VPN_documentation.html>.

***Note**: The **Management Method** list also includes the option for management by **SonicWALL Global Management System (SonicWALL GMS)**. Select this option if the SonicWALL is managed remotely by **SonicWALL GMS**.*

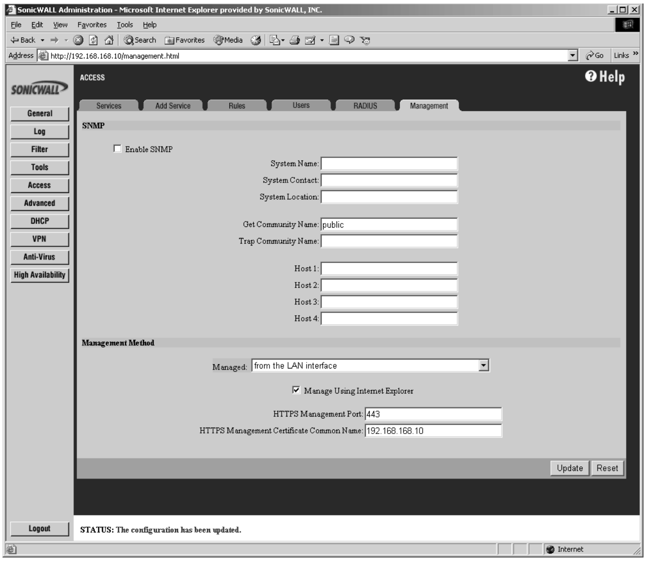
Manage Using Internet Explorer check box

The check box labeled **Manage Using Internet Explorer** is selected by default. It enables the Microsoft Internet Explorer Web browser to quickly load the SonicWALL Web Management Authentication Web page. With the IE check box enabled, the SonicWALL Internet security appliance LAN responds to NetBIOS name request on port 137.

Users can disable the LAN port response to port 137 by clearing the IE check box, but the log in process into the SonicWALL Management interface slows down.

HTTPS Port Management

A new feature allows you to configure the port used HTTPS authentication. By configuring an alternate port to 443, the standard port, you may be adding another layer of security of logging into the SonicWALL. To configure another port for HTTPS management, enter the preferred port number into the **HTTPS Management 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..



Address: http://192.168.168.10/management.html

SNMP

□ Enable SNMP

System Name:

System Contact:

System Location:

Get Community Name: public

Trap Community Name:

Host 1:

Host 2:

Host 3:

Host 4:

Management Method

Managed: from the LAN interface

☑ Manage Using Internet Explorer

HTTPS Management Port: 443

HTTPS Management Certificate Common Name: 192.168.168.10

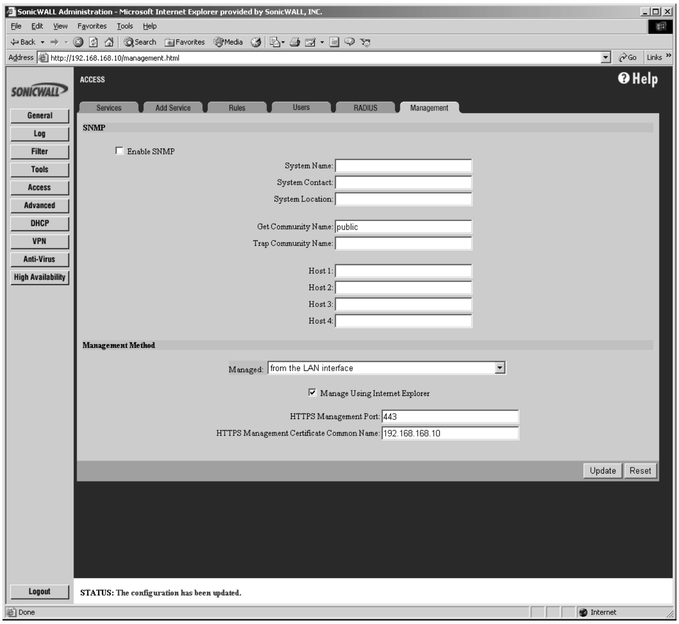
STATUS: The configuration has been updated.

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.

8 Advanced Features

This chapter describes the SonicWALL **Advanced Features**, such as **Web Proxy Forwarding**, **DMZ Address** settings, and **One-to-One NAT**. The **Advanced Features** can be accessed in the **Advanced** section of the SonicWALL Web Management Interface.There are six tabs in the **Advanced** section:

- **Proxy Relay**
- **Intranet**
- **Routes**
- **DMZ Addresses**
- **One-to-One NAT**
- **Ethernet**



Address: http://192.168.168.10/management.html

SNMP

☐ Enable SNMP

System Name:
System Contact:
System Location:

Get Community Name: public
Trap Community Name:

Host 1:
Host 2:
Host 3:
Host 4:

Management Method

Managed: from the LAN interface

☑ Manage Using Internet Explorer

HTTPS Management Port: 443
HTTPS Management Certificate Common Name: 192.168.168.10

STATUS: The configuration has been updated.

Proxy Relay

Web Proxy Forwarding

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 to point to the proxy server, you can move the server to the WAN and enable **Web ProxyForwarding**. The SonicWALL automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.

Configuring Web Proxy Relay

1. Connect your Web proxy server to a hub, and connect the hub to the SonicWALL WAN port.

   ***Note**: The proxy server must be located on the WAN or the DMZ; it can not be located on the LAN.*

2. Log into the SonicWALL Web Management Interface. Click **Advanced** at the left side of the browser window, and then click the **Proxy Relay** tab at the top of the window.
3. Enter the name or IP address of the proxy server in the **Proxy Web Server** field, and the proxy IP port in the **Proxy Web Server Port** field. Click **Update**.
4. If the Web proxy server is located on the WAN between the SonicWALL and the Internet router, add the Web proxy server address in the SonicWALL **Intranet** tab. Click the **Intranet** tab at the top of the window.
5. To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.

   ***Note**: The **Intranet** settings tab is displayed on page 98.*

6. In the **Intranet** tab, enter the proxy server's IP address in the **Add Range** field.
7. Select **Specified address ranges are attached to the WAN link** and click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

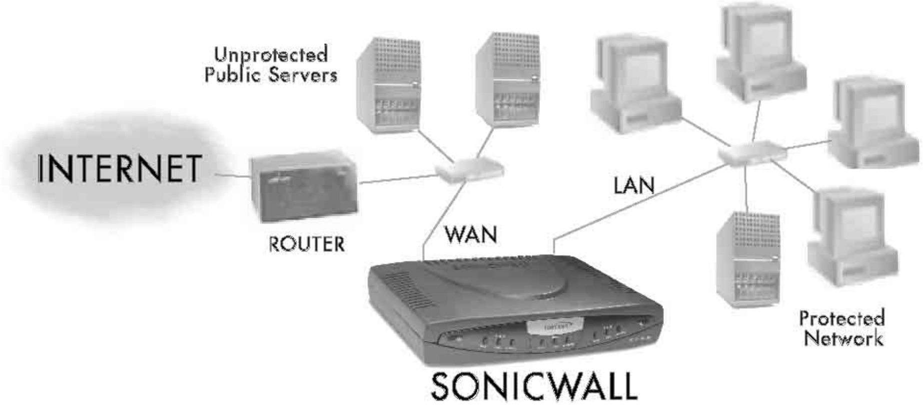
Bypass Proxy Servers Upon Proxy Failure

If a web proxy server is specified in the **Proxy Relay** tab of the **Advanced** section, 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.

Intranet

The SonicWALL can be configured as an Intranet firewall to prevent network users from accessing sensitive servers. By default, users on your LAN can access the Internet router, but not devices connected to the WAN port of the SonicWALL. To enable access to the area between the SonicWALL WAN port and the Internet, you must configure the **Intranet** settings on the SonicWALL.

Intranet firewalling is achieved by connecting the SonicWALL between an unprotected and a protected segment, as shown below.



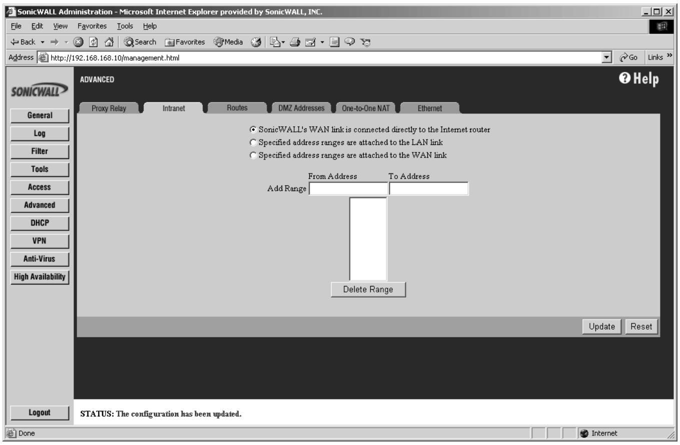
Installation

1. Connect the LAN Ethernet port on the back of the SonicWALL to the network segment to be protected against unauthorized access.
2. Connect the WAN Ethernet port on the back of the SonicWALL to the rest of the network.

   ***Note**: Devices connected to the WAN port do not have firewall protection. It is recommended that you use another SonicWALL Internet security appliance to protect computers on the WAN.*
3. Connect the SonicWALL to a power outlet. For SonicWALL PRO 200 and SonicWALL PRO 300, press the Power Switch to the **ON** position.

Intranet Configuration

Click **Advanced** on the left side of the browser window, and then click the **Intranet** tab.



● SonicWALL's WAN link is connected directly to the Internet router
○ Specified address ranges are attached to the LAN link
○ Specified address ranges are attached to the WAN link

Add Range — From Address: ______ To Address: ______

STATUS: The configuration has been updated.

To enable an Intranet firewall, you must specify which machines are located on the LAN, or you must specify which machines are located on the WAN.

It is best to select the network area with the least number of machines. For example, if only one or two machines are connected to the WAN, select **Specified address ranges are attached to the WAN link**. That way, you only have to enter one or two IP addresses in the **Add Range** section. Specify the IP addresses individually or as a range.

Intranet Settings

Select one of the following four options:

- **SonicWALL WAN link is connected directly to the Internet router**

  Select this option if the SonicWALL is protecting your entire network. This is the default setting.

- **Specified address ranges are attached to the LAN link**

  Select this option if it is easier to specify the devices on your LAN. Then enter your LAN IP address range(s). If you do not include all computers on your LAN, the computers not included will be unable to send or receive data through the SonicWALL.

- **Specified address ranges are attached to the WAN link**

  Select this option if it is easier to specify the devices on your WAN. Then enter your WAN IP address range(s). Computers connected to the WAN port that are not included are inaccessible to users on your LAN.

- **Add Range**

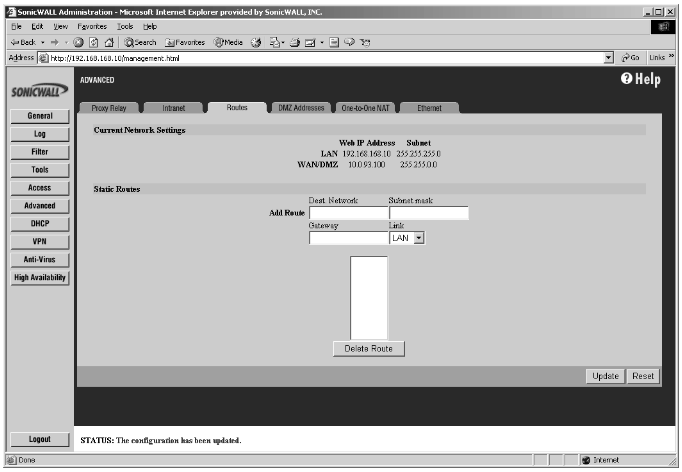
  To add a range of addresses, such as "199.2.23.50" to "199.2.23.54", enter the starting address in the **From Address** field and the ending address in the **To Address** field. An individual IP address should be entered in the **From Address** field only.

  Note*: Up to 64 address ranges can be entered.*

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

Routes

If you have routers on your Local Area Network (LAN), Demilitarized Zone (DMZ), or Wide Area Network (WAN), you can configure **Static Routes** on the SonicWALL.



Current Network Settings

	Web IP Address	Subnet
LAN	192.168.168.10	255.255.255.0
WAN/DMZ	10.0.93.100	255.255.0.0

Static Routes

Add Route Dest. Network: Subnet mask:

Gateway: Link: LAN

STATUS: The configuration has been updated.

Click **Advanced** on the left side of the browser window, and then click the **Routes** tab.

Static routes must be defined if the LAN, DMZ, or WAN are 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 traffic on the rest of the LAN, DMZ, or WAN.

The **SonicWALL LAN IP Address**, **LAN Subnet**, **WAN IP Address,** and **WAN/DMZ Subnet** are displayed in the **Current Network Settings** section. Refer to these settings when configuring your **Static Routes**.The SonicWALL LAN IP Address, LAN Subnet Mask, WAN IP Address and WAN/DMZ Subnet Mask are displayed in the **Current Network Settings** section. Refer to these settings when configuring your Static Routes.

To add Static Route entries, complete the following instructions:

1. Enter the destination network of the static route in the **Dest. Network** field. The destination network is the IP address subnet of the remote network segment.

*Note: If the destination network uses IP addresses ranging from "192.168.1.1" to "192.168.1.255", enter "192.168.1.0" in the **Dest. Network** field.*

2. Enter the subnet mask of the remote network segment in the **Subnet mask** field.
3. Enter the IP address of your router in the **Gateway** field. This IP address should be in the same subnet as the SonicWALL. If your router is located on the SonicWALL LAN, the Gateway address should be in the same subnet as the SonicWALL LAN IP Address.
4. Select the port on the SonicWALL that the router is connected to either the LAN, the WAN, or the DMZ, from the **Link** list.
5. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the Web browser window. Restart the SonicWALL for the change to take effect.

   ***Note**: The SonicWALL can support up to 128 static route entries.*

DMZ Addresses

(SonicWALL PRO 100, PRO 200, and PRO 300 Only)

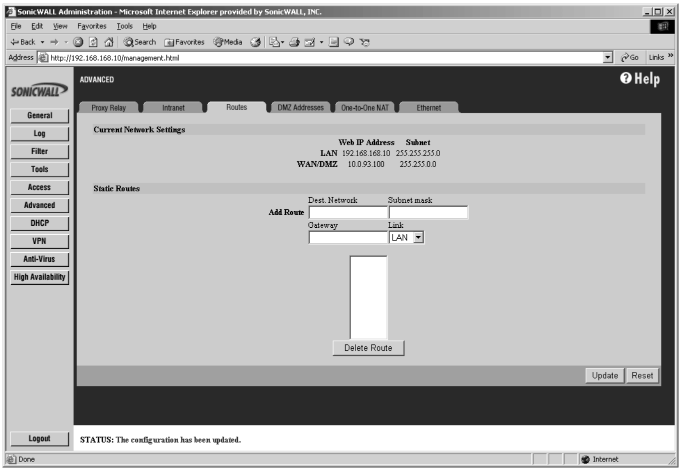
The SonicWALL provides security by preventing Internet users from accessing machines on the LAN. This security, however, also prevents users from reaching public servers, such as Web or e-mail servers.

The SonicWALL offers a special **DMZ** ("Demilitarized Zone") port that provides Internet access to network servers. The DMZ sits between the local network and the Internet. Servers on the DMZ are publicly accessible, but they are protected from attacks such as SYN Flood and Ping of Death. Use of the **DMZ** port is optional.

If you are configuring the SonicWALL SOHO3 or the SonicWALL TELE3, please go to Chapter 8, **Network Access Rules**, for information about setting up publicly accessible servers.

Using the DMZ is a strongly recommended alternative to placing servers on the WAN port where they are not protected or established Public LAN servers.

Click **Advanced** on the left side of the browser window, and then click **DMZ Addresses**.



Address http://192.168.168.10/management.html

Current Network Settings

	Web IP Address	Subnet
LAN	192.168.168.10	255.255.255.0
WAN/DMZ	10.0.93.100	255.255.0.0

Static Routes

Add Route: Dest. Network ______ Subnet mask ______ Gateway ______ Link LAN

STATUS: The configuration has been updated.

Servers on the **DMZ** must have unique, valid IP addresses in the same subnet as the SonicWALL WAN IP Address. Your ISP should be able to provide these IP addresses, as well as information on setting up public servers.

DMZ in Standard Mode

To configure **DMZ Addresses**, complete the following instructions.

1. Enter the starting IP address of your valid IP address range in the **From Address** field.
2. Enter the ending IP address of your valid IP address range in the **To Address** field.

   Note*: You can enter an individual IP address in the* ***From Address*** *field only.*

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

If you receive an error when you click **Update**, confirm that the **DMZ Address Range** does not include the SonicWALL WAN IP Address, the WAN Gateway (Router) Address, or any IP addresses assigned on the One-to-One NAT or Intranet windows.

Note*: The SonicWALL supports up to 64 DMZ address ranges.*

DMZ in NAT Mode

The SonicWALL **DMZ** now has the ability to use private internal IP addresses rather than public IP addresses on the network. Since NAT hides the true IP addresses in use on the network, NAT on the DMZ is an additional security feature for the SonicWALL. The outside world only sees the outside public IP address of the DMZ and not the internal private addresses.

To configure the **DMZ in NAT Mode**, use the following instructions:

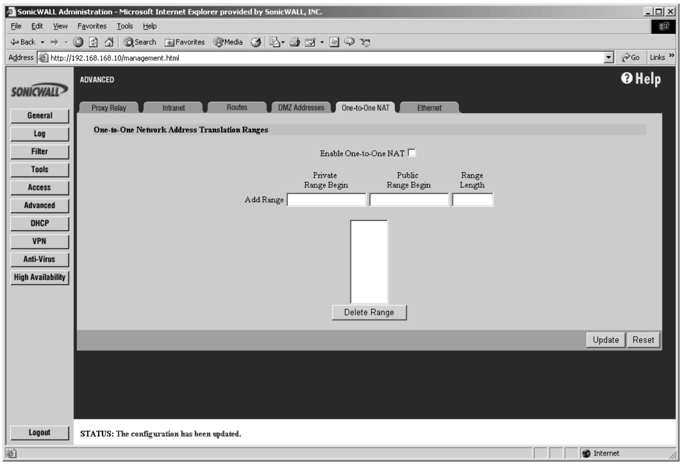
1. In the **DMZ Private Address** field, enter the private internal IP address assigned to the DMZ interface.
2. Assign a subnet mask in the **DMZ Subnet Mask** field. The LAN and DMZ can have the same subnet mask, but the subnets must be different. For instance, the LAN subnet can be 192.168.0.1 with a subnet mask of 255.255.255.0, and the DMZ subnet can be 172.16.18.1 with a subnet mask of 255.255.255.0.
3. If you choose to use **DMZ NAT Many to One Public Address (Optional)**, enter the DMZ public IP address which is on the same subnet as the WAN for access to devices on the DMZ interface. **DMZ NAT Many to One Public Address** is only available if your SonicWALL is configured in **NAT Enabled** networking mode.

Delete a DMZ Address Range

To delete an address or range, select it in the **Address Range** list and click **Delete**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

One-to-One NAT

One-to-One NAT maps valid, external addresses to private addresses hidden by NAT. Computers on your private LAN are accessed on the Internet at the corresponding public IP addresses.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

ADVANCED

One-to-One Network Address Translation Ranges

Enable One-to-One NAT □

	Private Range Begin	Public Range Begin	Range Length
Add Range			

STATUS: The configuration has been updated.

You can create a relationship between internal and external addresses by defining internal and external address ranges of equal length. Once the relationship is defined, the computer with the first IP address of the private address range is accessible at the first IP address of the external address range, the second computer at the second external IP address, etc.

To configure **One-to-One NAT**, complete the following instructions.

1. Select the **Enable One-to-One NAT** check box.
2. Enter the beginning IP address of the private address range being mapped in the **Private Range Begin** field. This is the IP address of the first machine that is accessible from the Internet.
3. Enter the beginning IP address of the valid address range being mapped in the **Public Range Begin** field. This address should be assigned by your ISP.

   ***Note**: Do not include the SonicWALL **WAN IP (NAT Public) Address** or the **WAN Gateway (Router) Address** in this range.*

4. Enter the number of public IP addresses that should be mapped to private addresses in the **Range Length** field. The range length can not exceed the number of valid IP addresses. Up to 64 ranges can be added. To map a single address, enter a **Range Length** of 1.
5. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Restart the SonicWALL for changes to take effect.

   ***Note**: The **One-to-One NAT** window maps valid, public IP addresses to private LAN IP addresses. It does not allow traffic from the Internet to the private LAN.*

   *A rule must be created in the **Rules** section to allow access to LAN servers. After **One-to-One NAT** is configured, create an **Allow** rule to permit traffic from the Internet to the private IP address(es) on the LAN.*

One-to-One NAT Configuration Example

This example assumes that you have a SonicWALL running in the NAT-enabled mode, with IP addresses on the LAN in the range 192.168.1.1 - 192.168.1.254, and a WAN IP address of 208.1.2.2. Also, you own the IP addresses in the range 208.1.2.1 - 208.1.2.6.

***Note**: If you have only one IP address from your ISP, you cannot use **One-to-One NAT**.*

You have three web servers on the LAN with the IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.12. Each of the servers must have a default gateway pointing to 192.168.1.1, the SonicWALL LAN IP address.

You also have three additional IP addresses from your ISP, 208.1.2.4, 208.1.2.5, and 208.1.2.6, that you want to use for three additional web servers. Use the following steps to configure One-to-One NAT:

1. Log into the Management Interface, and click **Advanced**. Then click the **One-to-One NAT** tab.

2. Select **Enable One-to-One NAT** and click **Update**.
3. Type in the IP address, 192.168.1.10, in the **Private Range Begin** field.
4. Type in the IP address, 208.1.2.4, in the **Public Range Begin** field
5. Type in 3 in the **Range length** field,.

   ***Note**: You can configure the IP addresses individually, but it is easier to configure them in a range. However, the IP addresses on both the private and public sides must be consecutive to configure a range of addresses.*

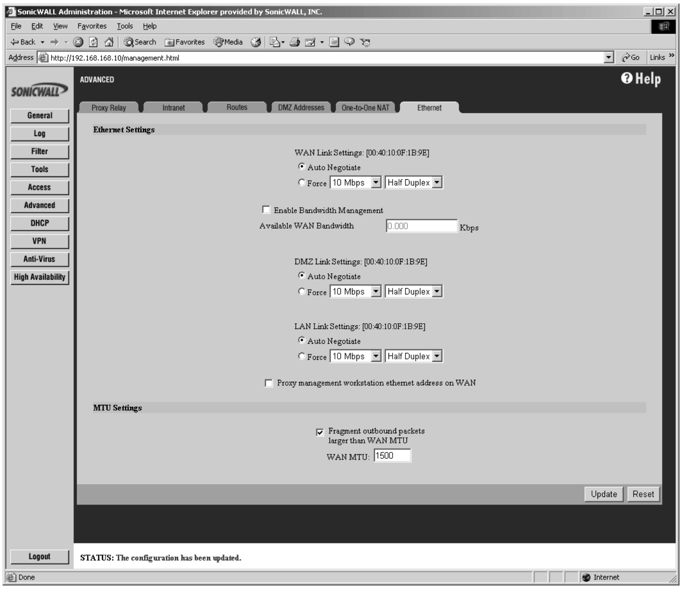
6. Click **Update**.
7. Click **Access**, then the **Rules** tab.
8. Click **Add New Rule** and configure the following settings:
   - **Allow**
   - **Service** - **HTTP**
   - **Source - WAN**
   - **Destination** - **LAN 192.168.1.10 - 192.168.1.12**
   - **Apply this rule** - **always**
9. Click **Update** and restart the SonicWALL.

The server configurations take effect after the SonicWALL restarts and the configuration is updated. Requests for http://208.1.2.4 are answered by the server at 192.168.1.10. Requests for http://208.1.2.5 are answered by the server at 192.168.1.11, and requests for for http://208.1.2.6 are answered by the server at 192.168.1.12. From the LAN, the servers can only be accessed using the private IP addresses (192.168.1.x), not the public IP addresses or domain names. For example, from the LAN, you must use URLs like http://1921.168.1.10 to reach the web servers. An IP address, such as 192.168.1.10, on the LAN cannot be used in both public LAN server configurations and in public LAN server One-to-One NAT configurations.

The Ethernet Tab

The **Ethernet** tab allows the management of Ethernet settings using the SonicWALL Management interface. The tab has the following settings:

- **WAN Link Settings**
- **DMZ Link Settings**
- **LAN Link Settings**


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
ADVANCED
Help
Proxy Relay
Intranet
Routes
DMZ Addresses
One-to-One NAT
Ethernet
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Update
Reset
Done
Internet

Ethernet Settings

WAN Link Settings: [00:40:10:0F:1B:9E]

● Auto Negotiate

○ Force 10 Mbps Half Duplex

□ Enable Bandwidth Management

Available WAN Bandwidth 0.000 Kbps

DMZ Link Settings: [00:40:10:0F:1B:9E]

● Auto Negotiate

○ Force 10 Mbps Half Duplex

LAN Link Settings: [00:40:10:0F:1B:9E]

● Auto Negotiate

○ Force 10 Mbps Half Duplex

□ Proxy management workstation ethernet address on WAN

MTU Settings

☑ Fragment outbound packets larger than WAN MTU

WAN MTU: 1500

STATUS: The configuration has been updated.

The default selection for all of the link settings is **Auto Negotiate** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. The other choice, **Force**, with lists for **speed** and **duplex**, should be used only if your Ethernet card also forces these settings. You must force from both sides of your connection to enable this setting.

Proxy Management workstation Ethernet address on WAN

If you are managing the Ethernet connection from the LAN side of your network, this check box can be selected. The SonicWALL appliance takes the Ethernet address of the computer managing the SonicWALL appliance and proxies that address onto the WAN port of the SonicWALL. If you are not managing the SonicWALL appliance from the LAN side, the firmware looks for a random computer on the LAN creating a lengthy search process.

MTU Settings

A network administrator may set the **MTU** (Maximum Transmission Unit) allowed over a packet or frame-based network such as TCP/IP. If the MTU size is too large, it may require more transmissions if the packet encounters a router unable to handle a larger packet. If the packet size is too small, this could result in more packet header overhead and more acknowledgements that have to sent and processed.

The default value is 1500 octets based on the Ethernet standard MTU. The minimum value that can be set is 68. Decreasing the packet size may improve the performance of the network.

Ethernet

Enable Bandwidth Management

Definition of Bandwidth

Bandwidth is the capacity of a communication channel (cable, DSL, T1 lines, etc.) to carry signals. A larger bandwidth can transfer more data over a communication channel in a given time. Sometimes referred to as “throughput”, and in digital communications, it is usually measured in bits per second (bps) or a multiple of bps such as Kbps, Mbps, or Gbps.

Introduction to Bandwidth Management

Bandwidth management is a means of allocating bandwidth resources to critical applications on a network. Without bandwidth management, an application or a user can take control of all available bandwidth and prevent other applications or users from using the network. Because it is impossible to differentiate between types of network traffic, it is also impossible to control which users or applications have priority on the network.

Applications can also require a specific quantity and quality of service which cannot be predicted in terms of available bandwidth. This can make some applications run poorly if bandwidth is not properly allocated to the application when necessary.

Bandwidth management works by sorting outbound network traffic into classes by application and service type. Traffic is then scheduled according to minimum and maximum bandwidth configured for each traffic type.

Why Use Bandwidth Management?

Corporate networks using intranets for information sharing and Web navigation have an increased demand for bandwidth, but simply adding on more connections or larger connections (T1 lines or larger) doesn't address the bandwidth issue because network availability is not guaranteed.

Nearly all network links are shared by more than one user or application which means available bandwidth is shared between all users and all applications. Using bandwidth management to allocate bandwidth to applications or users during peak times can prevent traffic congestion on the network. Temporary network congestion can be improved by using bandwidth management.

SonicWALL Bandwidth Management

Bandwidth Management is controlled by the SonicWALL Internet Security Appliance on outbound traffic only. It allows network administrators to guarantee minimum bandwidth and prioritize traffic based on **Rules** created in the **Access** section of the SonicWALL Management interface. By controlling the amount of bandwidth to an application or user, the network administrator can prevent a small number of applications or users to consume all available bandwidth.

Key Features of SonicWALL Bandwidth Management

- Outgoing traffic is managed according to traffic type: Telnet, FTP, HTTP, etc.
- Network Access Rules can be configured to allocate bandwidth based on IP addresses.
- VPN traffic can also be managed by enabling bandwidth management on the VPN Configure tab, and then specifying the Guaranteed, Maximum, and priority of all VPN traffic through the SonicWALL.

***Note**: Bandwidth management cannot be configured for individual VPN Security Associations. It can only be configured for all VPN traffic.*

Key Benefits of SonicWALL Bandwidth Management

- The network administrator has full control of outbound network traffic and can prevent traffic congestion on the network.
- Prevent a small number of applications and users from consuming all available bandwidth.
- Quality of Service policies can be implemented across the network allowing priority applications to run smoothly.

How does SonicWALL Bandwidth Management Work?

Bandwidth management works by allocating traffic to a class based upon application type, source or destination addresses, or a combination of both. It then assigns individual limits for each class of network traffic. By assigning priorities to network traffic, applications requiring a quick response time, such as telnet, can take precedence over traffic requiring less response time, such as FTP.

Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic can improve network performance.

Traffic is classified in the following manner:

- TCP/IP or UDP ports
- Services such as FTP, HTTP, E-mail, SIP
- Source or destination IP address

SonicWALL Bandwidth Management can assign a portion of the available bandwidth and a priority to each class of network traffic. Priorities rank from 0 (zero), highest, to 7, lowest.

The packet classifier analyzes a packet when it arrives for its packet protocol, source information, and destination information. It then allocates the packet to a class queue where it waits to be processed. If the queue is full, the packet is dropped. Normal retransmission of data ensures that the packet is sent again.

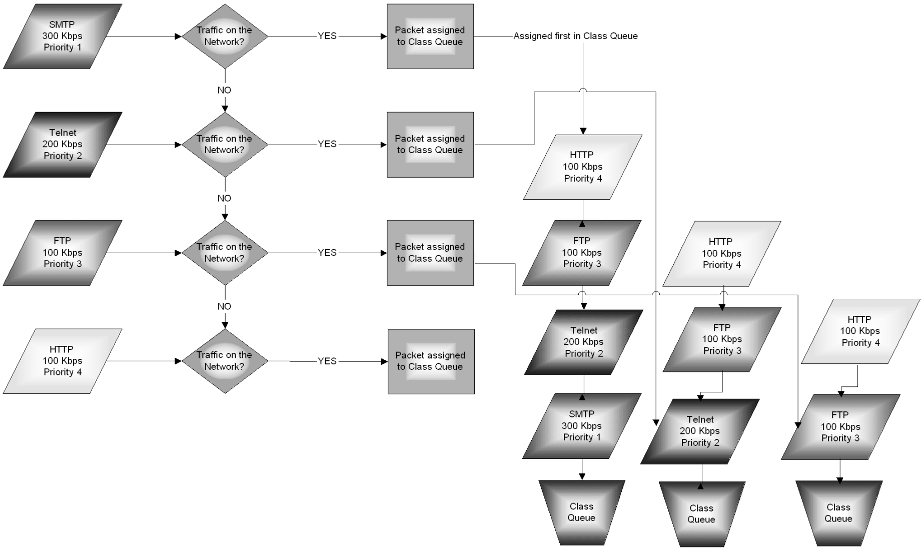
Class queues are processed based on the amount of bandwidth allocated (guaranteed and maximum), and the priority assigned to the class queue. Within the class queue, packets are processed on a first-in, first-out basis. When network traffic reaches the maximum allocated to the class, packets from the next class in priority order are processed.

Typically, each class is allocated a portion of the available bandwidth, and when that limit is reached, no more traffic for that particular class is forwarded. But if there is available bandwidth on the network that is not in use by a particular class, a class can temporarily borrow bandwidth and send traffic until the maximum bandwidth allocated to the class is reached.

Spare bandwidth is allocated among the highest priority classes until no more bandwidth is available or until all of those classes have reached their maximum bandwidth. If this happens, the remainder of the bandwidth is divided among the next priority classes. This process is repeated until all of the available bandwidth is consumed.

Defining a class of traffic that has 0 bandwidth allocated to it effectively blocks the traffic unless there is no other traffic with higher priority on the network

.



Bandwidth Management Schema

Examples of Bandwidth Management Rules

Rule	Service	Priority	Guaranteed	Maximum
Allow	SMTP	0	300 Kbps	1000 Kbps
Allow	FTP	1	100 Kbps	200 Kbps
Allow	HTTP	2	100 Kbps	200 Kbps

Enabling Bandwidth Management on the SonicWALL

To enable **Bandwidth Management** on the SonicWALL, you must know the current bandwidth of your connection. Once you have this figure, you can select **Enable Bandwidth Management** on the **Advanced/Ethernet** page, and then enter the amount of available WAN bandwidth in Kbps. Now that you have enabled **Bandwidth Management**, you can begin configuring **Rules** to use bandwidth management.

***Note**: Traffic inbound from the WAN to the LAN/DMZ based on a Rule using bandwidth management is allowed as if there is no bandwidth management in place. However, outbound traffic (reply packets) for traffic associated with an inbound Rule is managed based on the configuration for that Rule.*

9 DHCP Server

This chapter describes the configuration of the SonicWALL **DHCP Server**.

DHCP, Dynamic Host Configuration Protocol, is a method to distribute TCP/IP settings from a centralized server to computers on a network.

The SonicWALL **DHCP Server** distributes IP addresses, gateway addresses and DNS server addresses to the computers on your LAN. To access the SonicWALL **DHCP Setup** window, click **DHCP** on the left side of the browser window. There are three tabs in the **DHCP** section:

- **Setup**
- **DHCP over VPN**
- **Status**

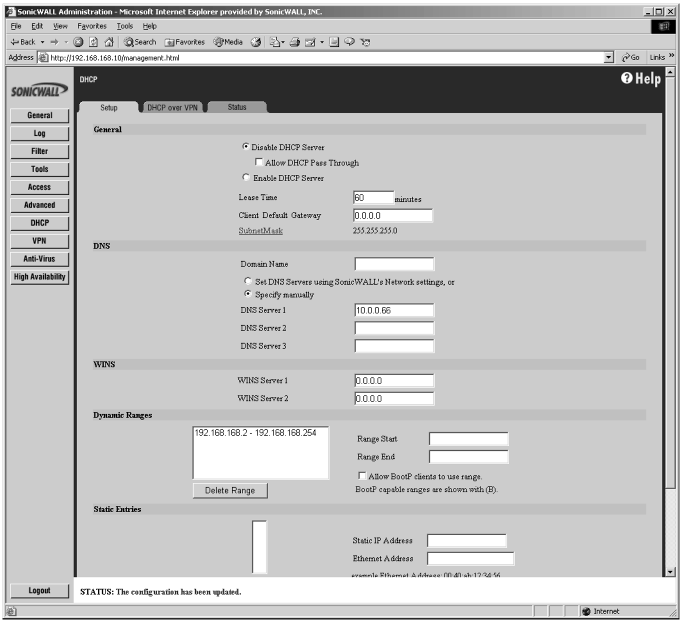
Setup

Disable DHCP Server is the default setting in the SonicWALL.

Allow DHCP Pass Through in Standard Mode

Network administrators can have a DHCP server located outside the SonicWALL Internet Security appliance. To enable this feature in the SonicWALL appliance, follow these steps:

1. Click **DHCP** on the management interface. On the **Setup** tab, select **Disable DHCP Server.**
2. Select the **Allow DHCP Pass Through** check box.



http://192.168.168.10/management.html

General

● Disable DHCP Server

□ Allow DHCP Pass Through

○ Enable DHCP Server

Lease Time 60 minutes

Client Default Gateway 0.0.0.0

SubnetMask 255.255.255.0

DNS

Domain Name

○ Set DNS Servers using SonicWALL's Network settings, or

● Specify manually

DNS Server 1 10.0.0.66

DNS Server 2

DNS Server 3

WINS

WINS Server 1 0.0.0.0

WINS Server 2 0.0.0.0

Dynamic Ranges

192.168.168.2 - 192.168.168.254

Range Start

Range End

□ Allow BootP clients to use range.

BootP capable ranges are shown with (B).

Static Entries

Static IP Address

Ethernet Address

example Ethernet Address: 00:40:ab:12:34:56

STATUS: The configuration has been updated.

Enable DHCP Server

To configure the SonicWALL DHCP server for the LAN, complete the following instructions.

1. Select the **Enable DHCP Server**.

   Note*: Make sure there are no other DHCP servers on the LAN before you enable the DHCP server.*

2. Enter the maximum length of the DHCP lease in the **Lease Time** field. The **Lease Time** determines how often the DHCP Server renews IP leases. The default Lease Time is 60 minutes. The length of time can range from 1 to 9999 minutes.
3. If configuring DHCP server for the LAN, enter the gateway address used by LAN computers to access the Internet in the **LAN Default Gateway** field. Enter the SonicWALL LAN IP Address if NAT is enabled.
4. If configuring DHCP server for the LAN, enter the gateway address used by LAN computers to access the Internet in the **LAN Default Gateway** field. Enter the SonicWALL LAN IP Address if NAT is enabled.
5. Enter the domain name registered for your network in the **Domain Name** field. An example of a domain name is "your-domain.com". If you do not have a domain name, leave this field blank.
6. Select **Set DNS Servers using the SonicWALL Network settings** to use the DNS servers that you specified in the SonicWALL **Network** section.

If you wish to use different DNS servers than the ones specified in the SonicWALL **Network** section, then select **Specify Manually**. Enter your **DNS Server** addresses in the **DNS Server 1**, **DNS Server 2**, and **DNS Server 3** fields. The DNS servers are used by computers on your LAN to resolve domain names to IP addresses. You only enter one DNS Server address, but multiple DNS entries improve performance and reliability.

7. Enter your **WINS Server** address(es) in the **WINS Server 1** and **WINS Server 2** fields. **WINS Servers** resolve Windows-based computer names to IP addresses. If you do not have a WINS server, leave these fields blank.
8. **Dynamic Ranges** are the ranges of IP addresses dynamically assigned by the DHCP server. The **Dynamic Ranges** should be in the same subnet as the SonicWALL LAN IP Address.
9. Enter the beginning IP address of your **LAN IP address** range in the **Range Start** field. Enter the ending IP address in the **Range End** field. Select the **Allow BootP clients to use range** check box if you want BootP clients to receive IP leases. Then click **Update**. When the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Continue this process until you have added all the desired dynamic ranges.
10. Enter the beginning IP address of your **LAN IP address** range in the **Range Start** field. Enter the ending IP address in the **Range End** field. Select the **Allow BootP clients to use range** check box if you want BootP clients to receive IP leases. Then click **Update**.

When the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window. Continue this process until you have added all the desired dynamic ranges.

***Note**: The **DHCP Server** does not assign an IP address from the dynamic range if the address is already being used by a computer on your LAN.*

11. The **DHCP Server** can also assign **Static Entries**, or static IP addresses, to computers on the LAN. Static IP addresses should be assigned to servers that require permanent IP settings. Enter the IP address assigned to your computer or server in the **Static IP Address** field.
12. Enter the Ethernet (MAC) address of your computer or server in the **Ethernet Address** field. Then click **Update**. When the SonicWALL has been updated, a message confirming the update is displayed at the bottom of your Web browser window.Continue this process until you have added all the desired static entries.

***Note**: The SonicWALL DHCP server can assign a total of 254 dynamic and static IP addresses.*

Deleting Dynamic Ranges and Static Entries

- To remove a range of addresses from the dynamic pool, select it from the list of dynamic ranges, and click **Delete Range**. When the range has been deleted, a message confirming the update is displayed at the bottom of the browser window.
- To remove a static address, select it from the list of static entries and click **Delete Static**. When the static entry has been deleted, a message confirming the update is displayed at the bottom of the browser window.

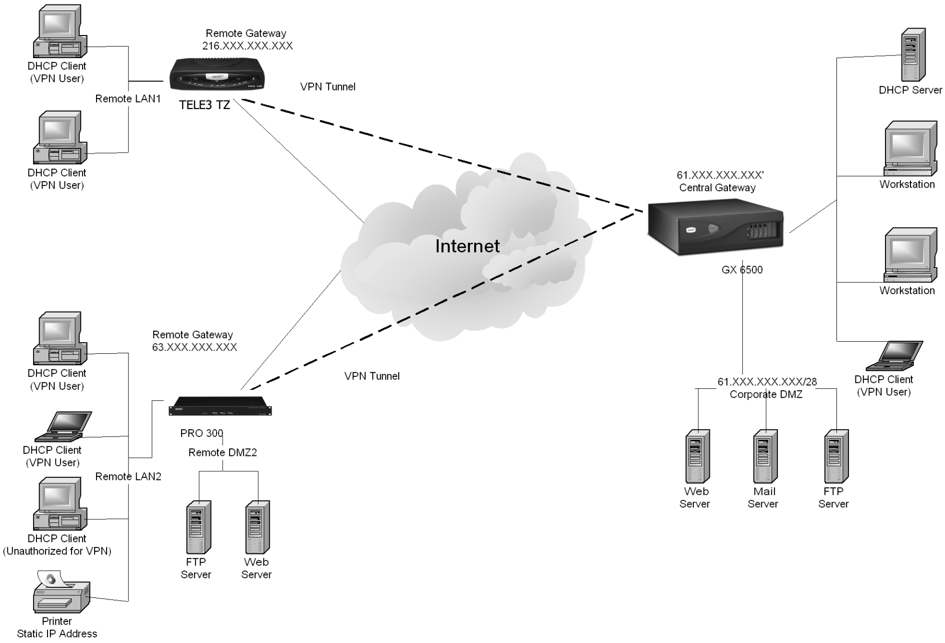
DHCP over VPN

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

DHCP Relay Mode

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

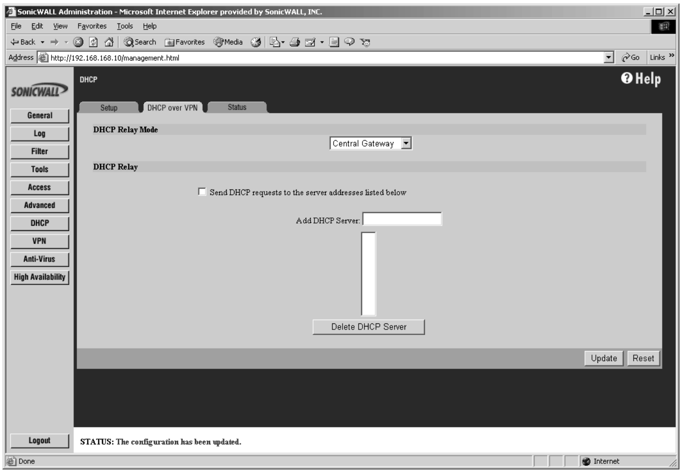
DHCP over a VPN Tunnel



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. If you want to send DHCP requests to specific servers, enable the **Send DHCP requests to the server addresses listed below** check box. Enter the IP addresses of DHCP

servers in the **Add DHCP Server** field, and click **Update**. The SonicWALL now directs DHCP requests to the specified servers.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
DHCP
Help
Setup
DHCP over VPN
Status
Done
Internet

DHCP Relay Mode

Central Gateway

DHCP Relay

☐ Send DHCP requests to the server addresses listed below

Add DHCP Server:

Delete DHCP Server

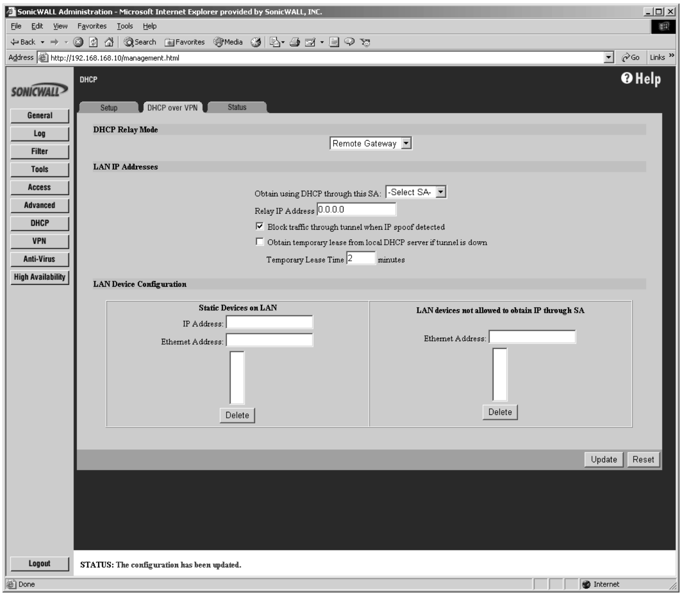
Update Reset

STATUS: The configuration has been updated.

4. To delete DHCP servers, click on the IP address of the DHCP server, and click **Delete DHCP Server**. The server is removed from the list of DHCP servers.
5. To complete the configuration, go to **VPN** and click **Configure**.
6. Select **Destination network obtains IP addresses using DHCP through this SA** in the **Destination Networks** section. Click **Update**.

To configure the SonicWALL as a **Remote Gateway**, use the following steps:

1. Log into the Management interface, click **DHCP**, and then **DHCP over VPN**.
2. Select **Remote Gateway** from the **DHCP Relay Mode** menu.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.10/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
DHCP
Help
Setup
DHCP over VPN
Status
Delete
Delete
Update
Reset
Done
Internet

DHCP Relay Mode

Remote Gateway

LAN IP Addresses

Obtain using DHCP through this SA: -Select SA-

Relay IP Address 0.0.0.0

☑ Block traffic through tunnel when IP spoof detected

☐ Obtain temporary lease from local DHCP server if tunnel is down

Temporary Lease Time 2 minutes

LAN Device Configuration

Static Devices on LAN

IP Address:

Ethernet Address:

LAN devices not allowed to obtain IP through SA

Ethernet Address:

STATUS: The configuration has been updated.

LAN IP Addresses

3. Select the VPN Security Association to be used for the VPN tunnel from the **Obtain using DHCP through this SA** menu.

   ***Note**: 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 entered for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL to respond to IP spoofs.
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, enter the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is two (2) minutes.

LAN Device Configuration

7. To configure **Static Devices on the LAN**, enter the IP address of the device in the **IP Address** field. Then enter the Ethernet Address of the device in the **Ethernet Address** field. An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to enter the Ethernet address of a device.

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.

9. Select **LAN Devices not allowed to obtain IP through SA** if there are devices on the LAN that you do not want to obtain IP addresses through the VPN tunnel, such as children's computers. You must know the Ethernet address of the device to configure this setting. The Ethernet address of a device can be determined by typing ***ipconfig/all*** into a **Command Prompt** window.

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

Note*: 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 PC.*

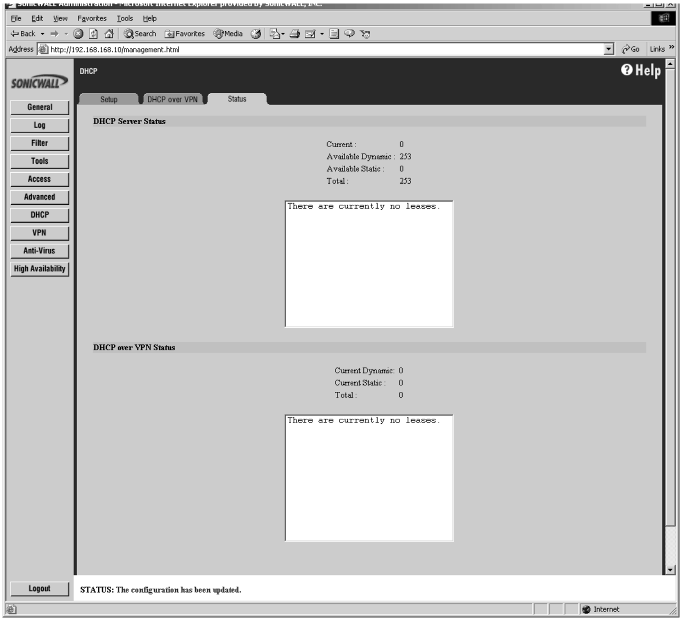
Note*: If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.*

DHCP Status

A **Status** page is now available to review **DHCP Server Status** and **DHCP over VPN Status**. The **DHCP Server Status** section reports the number of **Current**, **Available Dynamic**, **Available Static** leases as well as the **Total** leases. The **DHCP over VPN Status** section reports the number of **Current Dynamic**, **Current Static**, and the **Total** leases.

DHCP Status

Click the **Status** tab.



http://192.168.168.10/management.html

DHCP Server Status

Current :	0
Available Dynamic :	253
Available Static :	0
Total :	253

```
There are currently no leases.
```

DHCP over VPN Status

Current Dynamic:	0
Current Static :	0
Total :	0

```
There are currently no leases.
```

STATUS: The configuration has been updated.

The scrolling window shows the details on the current bindings: IP and MAC address of the bindings, along with the type of binding (Dynamic, Dynamic BootP, or Static BootP).

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click **Delete Binding**. 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 **Refresh** to reload the list of bindings. This can be necessary because Web pages are not automatically refreshed, and new bindings can have been issued since the page was first loaded.

10 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.

This chapter is organized into the following sections:

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

NAT Traversal Support

VPN **NAT Traversal** is an Internet Draft proposed to IETF (Internet Engineering Task Force) to overcome problems faced when IPSec traffic is intended to pass through a NAT device. **NAT Traversal** addresses the issue of UDP (User Datagram Protocol) encapsulation and addresses the traffic problem by wrapping an IPSec packet inside a UDP packet when a NAT or NAPT (Network Address Port Translator) device is detected between peers.

Encapsulation of the IPSec packet requires decapsulation of the IPSec packet. Since ESP-protected packets are exchanged between IKE peers using one of three methods, gateway to gateway, client to gateway, and client to client, the IKE peers must support the same method of UDP encapsulation. IKE peers exchange a known value to determine if they both support **NAT Traversal**. If the IKE peers agree, IKE probes or discovery payloads are used to determine if a NAT or NAPT device is present. Only if a NAT or NAPT device is detected is UDP encapsulation is used for IPSec packets.

NAT/NAT Traversal devices use dynamic mappings where a private IP address and source port (192.168.168.168:X) are temporarily bound to a shared public IP address and an unused port (207.126.101.100:Y). This binding is dissolved after a period of inactivity (minutes or seconds), enabling pool reuse.

IPSec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPSec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPSec peer.

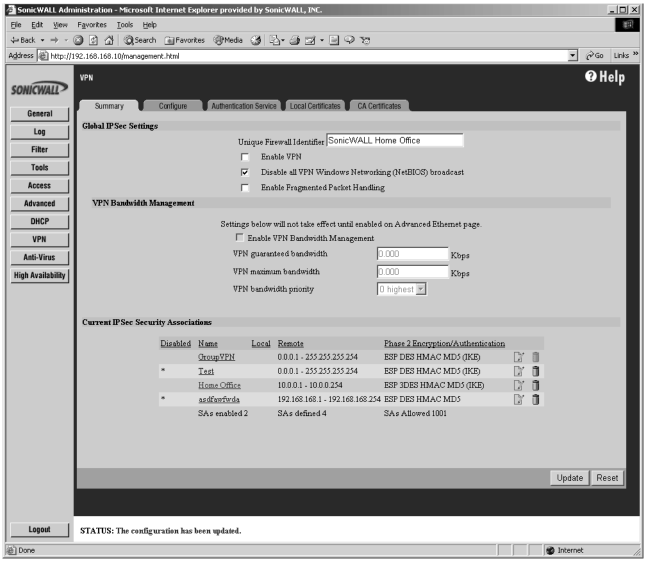
NAT Traversal support is transparent, but log messages are generated by the SonicWALL when a IPSec Security Gateway is detected behind a NAT/NAPT device. The following log messages are found on the **View Log** tab:

- **Peer IPSec Gateway behind a NAT/NAPT device**
- **Local IPSec Security Gateway behind a NAT/NAPT device**
- **No NAT/NAPT device detected between IPSec Security**
- **Peer IPSec Security Gateway doesn’t support VPN NAT Traversal**

The VPN Interface

Click **VPN** on the SonicWALL management station interface. There are five tabs in the VPN interface:

- **Summary**
- **Configure**
- **Authentication Service**
- **Local Certificates**
- **CA Certificates**



Global IPSec Settings

Unique Firewall Identifier: SonicWALL Home Office

□ Enable VPN

☑ Disable all VPN Windows Networking (NetBIOS) broadcast

□ Enable Fragmented Packet Handling

VPN Bandwidth Management

Settings below will not take effect until enabled on Advanced Ethernet page.

□ Enable VPN Bandwidth Management

VPN guaranteed bandwidth: 0.000 Kbps

VPN maximum bandwidth: 0.000 Kbps

VPN bandwidth priority: 0 highest

Current IPSec Security Associations

Disabled	Name	Local	Remote	Phase 2 Encryption/Authentication
	GroupVPN		0.0.0.1 - 255.255.255.254	ESP DES HMAC MD5 (IKE)
*	Test		0.0.0.1 - 255.255.255.254	ESP DES HMAC MD5 (IKE)
	Home Office		10.0.0.1 - 10.0.0.254	ESP 3DES HMAC MD5 (IKE)
*	asdfawfwda		192.168.168.1 - 192.168.168.254	ESP DES HMAC MD5
	SAs enabled 2		SAs defined 4	SAs Allowed 1001

STATUS: The configuration has been updated.

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

Global IPSec Settings

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

VPN Bandwidth Management

You can allocate bandwidth to all outbound VPN traffic. To enable VPN Bandwidth Management, select Enable VPN Bandwidth Management, and enter the amount of bandwidth in **Kbps** for **VPN guaranteed bandwidth** and **VPN maximum bandwidth**. Select VPN bandwidth priority from the **VPN bandwidth priority** menu, 0 (highest) to 7 (lowest).

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

Current IPSec Security Associations

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

SonicWALL VPN Client for Remote Access and Management

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

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

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

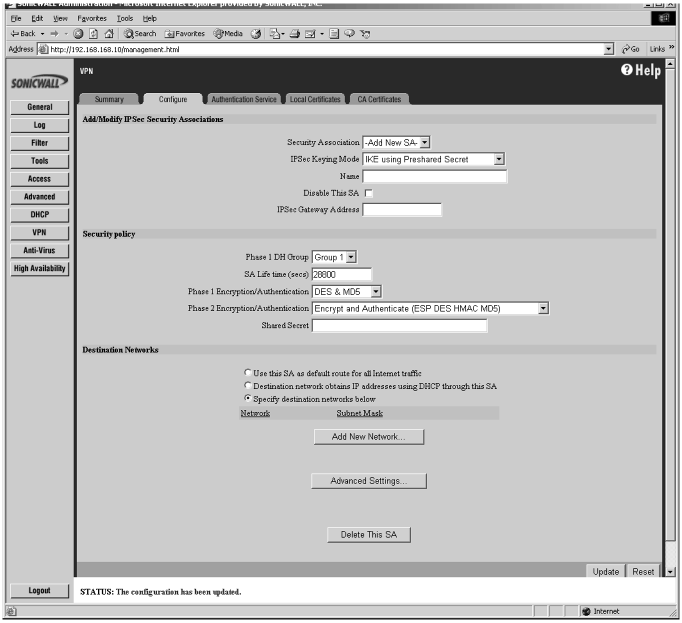
Simple Configuration Using Pre-shared Secret is a VPN client configuration that is appropriate only for firmware versions 5.1.1 or below.

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

The Configure Tab

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

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



Address http://192.168.168.10/management.html

Add/Modify IPSec Security Associations

Security Association: -Add New SA-
IPSec Keying Mode: IKE using Preshared Secret
Name:
Disable This SA ☐
IPSec Gateway Address:

Security policy

Phase 1 DH Group: Group 1
SA Life time (secs): 28800
Phase 1 Encryption/Authentication: DES & MD5
Phase 2 Encryption/Authentication: Encrypt and Authenticate (ESP DES HMAC MD5)
Shared Secret:

Destination Networks

○ Use this SA as default route for all Internet traffic
○ Destination network obtains IP addresses using DHCP through this SA
● Specify destination networks below

Network	Subnet Mask

STATUS: The configuration has been updated.

Add/Modify IPSec Security Associations

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

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

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

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

Security policy Settings for IKE using Pre-shared Secret

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

  - Group 1

  - **Group 2**

  - **Group 5**

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

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

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

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

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

  - **DES & MD5**

  - DES & SHA1

  - 3DES & MD5

  - 3DES & SHA1

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

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

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

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

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

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

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

Security Policy Settings using Manual Key

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

- **Incoming SPI** - Enter the Security Parameter Index (SPI) that the remote location transmits to identify the Security Association used for the VPN Tunnel. The SPI may be up to eight characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). The hexadecimal characters "0" to "ff" inclusive are reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. These numbers are not accepted by the SonicWALL when entered as an SPI; an error message is displayed at the bottom of the Web browser window when **Update** is pressed. For example, a valid SPI would be 1234abcd.

- **Outgoing SPI** - Enter the Security Parameter Index (SPI) that the local SonicWALL transmits to identify the Security Association used for the VPN Tunnel. The SPI may be up to eight characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). The hexadecimal characters "0" to "ff" inclusive are reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. These numbers are not accepted by the SonicWALL when entered as an SPI; an error message is displayed at the bottom of the Web browser window when **Update** is pressed. For example, a valid SPI would be 1234abcd.

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

Destination Networks

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

- **Use this SA as the default route for all Internet traffic** (Security Associations using IKE with Pre-shared Secret and Manual Key) - 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.
- **Destination network obtains IP addresses using DHCP through this SA** (Security Associations using IKE and Pre-shared Secret but not Group VPN) - Enable this check box if you are managing your IP address allocation from a central location.
- **Specify destination networks below** - Configure the destination networks for your VPN Security Association. Click **Destination Networks** to enter the IP address and subnet mask.

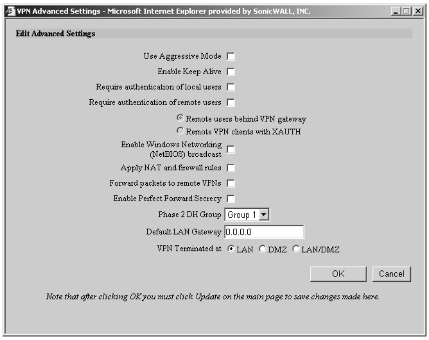
VPN Advanced Settings

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

- **Use Aggressive Mode**
- **Enable Keep Alive**
- **Require authentication of local users**
- **Require authentication of remote users**

  - Remote users behind VPN gateway

  - Remote VPN clients with XAUTH
- **Enable Windows Networking (NetBIOS) broadcast**
- **Apply NAT and firewall rules**
- **Forward packets to remote VPNs**
- **Enable Perfect Forward Secrecy**
- **Phase 2 DH Group**
- **Default LAN Gateway**



VPN Advanced Settings - Microsoft Internet Explorer provided by SonicWALL, INC.

Edit Advanced Settings

Use Aggressive Mode □

Enable Keep Alive □

Require authentication of local users □

Require authentication of remote users □

● Remote users behind VPN gateway

○ Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast □

Apply NAT and firewall rules □

Forward packets to remote VPNs □

Enable Perfect Forward Secrecy □

Phase 2 DH Group: Group 1

Default LAN Gateway: 0.0.0.0

VPN Terminated at ● LAN ○ DMZ ○ LAN/DMZ

Note that after clicking OK you must click Update on the main page to save changes made here.

Use Aggressive Mode

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

***Note**: If a WAN Failover to the modem occurs on the SP, the Security Association uses **Aggressive Mode** even if it is not configured for the SA.*

Enable Keep Alive

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

Require authentication of local users

Selecting this check box requires that all outbound VPN traffic on this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

Require authentication of remote users

Enabling this feature requires that all inbound traffic on this SA is from an authenticated user. Unauthenticated traffuc is not allowed on the VPN tunnel. Select **Remote users behind VPN gateway** if remote users have a VPN tunnel terminating on the VPN gateway. Select **Remote VPN clients behind VPN gateway** if remote users require authentication using XAUTH and are accessing the SonicWALL via a VPN client.

Enable Windows Networking (NetBIOS) broadcast

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

Apply NAT and firewall rules

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

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

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

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

Forward Packets to Remote VPNs

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

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

Route all internet traffic through this SA

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

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

Enable Perfect Forward Secrecy

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

Phase 2 DH Group

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

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

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

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

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

Default LAN Gateway

A **Default LAN Gateway** is used at a central site in conjunction with a remote site using the **Route all internet traffic through this SA** check box. The **Default LAN Gateway** field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a **Default LAN Gateway.** If a **Default LAN Gateway** is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

Advanced Settings for VPN Configurations

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

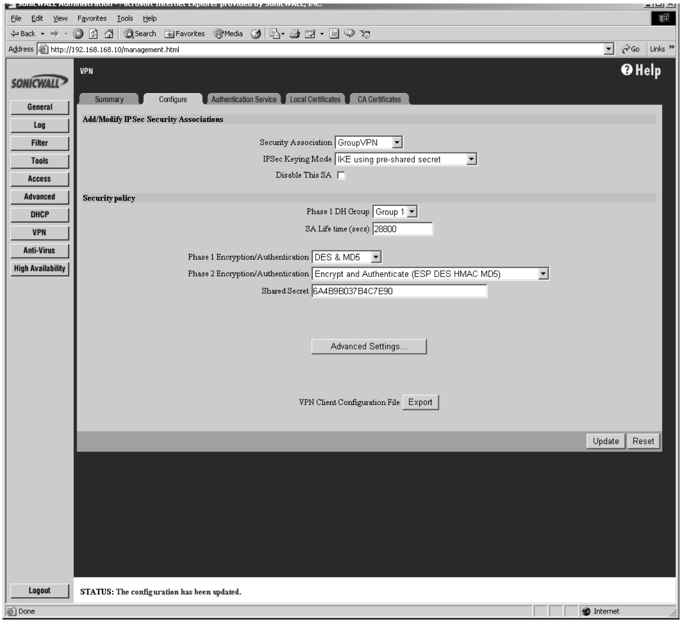
	Group VPN using IKE / Pre-shared Secret	Group VPN using IKE / Certificates	Manual Key*	IKE using Pre-shared Secret	IKE using Certificates[1]
Use Aggressive Mode				✓	✓
Enable Keep Alive				✓	✓
Require authentication of VPN clients using XAUTH	✓			✓	
Require authentication of local users			✓	✓	✓
Require authentication of remote users			✓	✓	✓
Enable Windows Networking (NetBIOS) broadcast	✓	✓	✓	✓	✓
Apply NAT and Firewall Settings	✓	✓	✓	✓	✓
Forward Packets to Remote VPNs	✓	✓	✓	✓	✓
Enable Perfect Forward Secrecy	✓	✓		✓	✓
Phase 2 DH Group	✓	✓		✓	✓
Default LAN Gateway	✓	✓	✓	✓	✓

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

[1] These parameters apply to both SonicWALL Certificates and Third Party Certificates.

Enabling Group VPN on the SonicWALL

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



Add/Modify IPSec Security Associations

Security Association: GroupVPN

IPSec Keying Mode: IKE using pre-shared secret

Disable This SA ☐

Security policy

Phase 1 DH Group: Group 1

SA Life time (secs): 28800

Phase 1 Encryption/Authentication: DES & MD5

Phase 2 Encryption/Authentication: Encrypt and Authenticate (ESP DES HMAC MD5)

Shared Secret: 6A4B9B037B4C7E90

VPN Client Configuration File

STATUS: The configuration has been updated.

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

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

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

7. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** from the **Phase 2 Encryption/Authentication** menu.

8. Create and enter a **Shared Secret** in the **Shared Secret** field or use the **Shared Secret** automatically generated by the SonicWALL. The **Shared Secret** should consist of a combination of letters and numbers rather than the name of a family member, pet, etc. It is also case-sensitive.

9. Click **Advanced Settings** to open the window. Select any of the following boxes that apply to your SA:

- **Require authentication of VPN clients via XAUTH** - requires VPN client authentication via a RADIUS server.
- **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Forward packets to remote VPNs** - if creating a “hub and spoke” network.
- **Enable Perfect Forward Secrecy** - if adding an additional layer of security using a second Diffie_Hellman key exchange.
- **Phase 2 DH Group** - generates a additional key exchange.
- **Default LAN Gateway** - The **Default LAN Gateway** field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

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

10. Click **Update** to enable the changes.

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

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

Installing the VPN Client Software

1. When you register your SonicWALL or SonicWALL VPN Upgrade, a unique VPN client serial number and link to download the SonicWALL VPN Client zip file is displayed.

2. Unzip the SonicWALL VPN Client zip file.

3. Double-click **setup.exe** and follow the VPN client setup program step-by-step instructions. Enter the VPN client serial number when prompted.

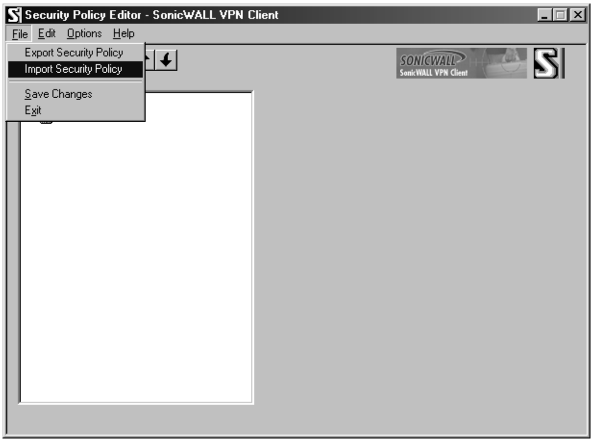
4. Restart your computer after you have installed the VPN client software.

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

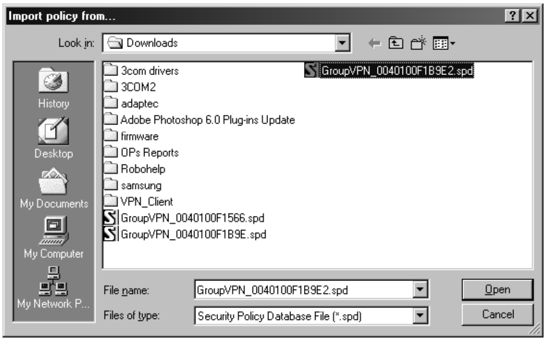
Group VPN Client Configuration

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

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



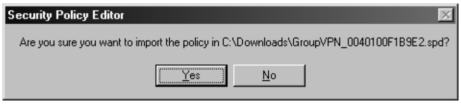
2. A file location box appears which allows you to search for the location of the saved security file. Select the file, and click **Open**.



File name: GroupVPN_0040100F1B9E2.spd

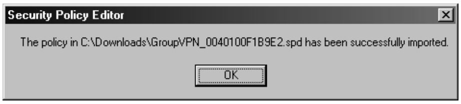
Files of type: Security Policy Database File (*.spd)

3. A dialogue box confirming the request to import the security file appears.



Are you sure you want to import the policy in C:\Downloads\GroupVPN_0040100F1B9E2.spd?

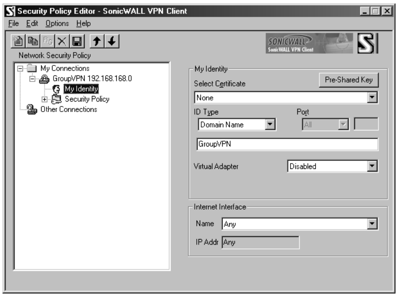
Click **Yes**, and another box appears confirming the file is successfully imported into the client. The client application now has an imported **Group VPN** policy.



Security Policy Editor

The policy in C:\Downloads\GroupVPN_0040100F1B9E2.spd has been successfully imported.

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



Security Policy Editor - SonicWALL VPN Client

My Identity

Select Certificate: None

ID Type: Domain Name

Port: All

GroupVPN

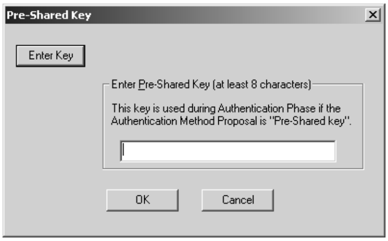
Virtual Adapter: Disabled

Internet Interface

Name: Any

IP Addr: Any

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

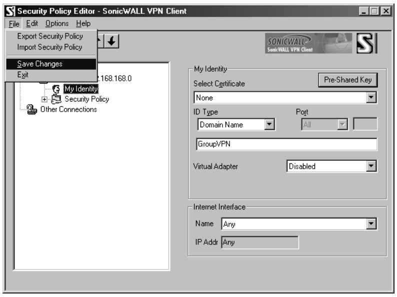


Pre-Shared Key

Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

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



Security Policy Editor - SonicWALL VPN Client

My Identity

Select Certificate: None

ID Type: Domain Name

Port: All

GroupVPN

Virtual Adapter: Disabled

Internet Interface

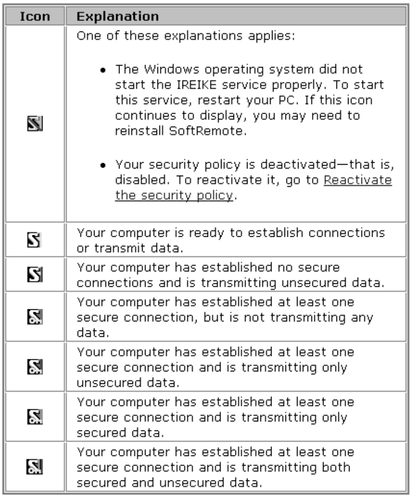
Name: Any

IP Addr: Any

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

Verifying the VPN Tunnel as Active

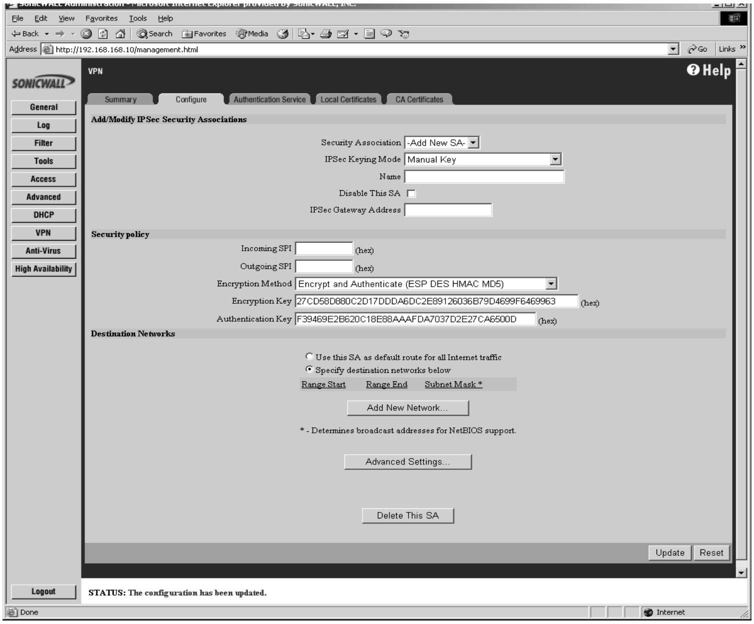
After the Group VPN Policy is active on the VPN Client, you can verify that a secure tunnel is active and sending data securely across the connection. You can verify the connection by verifying the type of icon displayed in the system tray near the system clock. The SonicWALL VPN Client icon is displayed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



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

Manual Key Configuration for a SonicWALL and VPN Client

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



Add/Modify IPSec Security Associations

Security Association: -Add New SA-

IPSec Keying Mode: Manual Key

Name:

Disable This SA ☐

IPSec Gateway Address:

Security policy

Incoming SPI: (hex)

Outgoing SPI: (hex)

Encryption Method: Encrypt and Authenticate (ESP DES HMAC MD5)

Encryption Key: 27CD58D880C2D17DDDA6DC2E89126036B79D4699F6469963 (hex)

Authentication Key: F39469E2B620C18E88AAAFDA7037D2E27CA6500D (hex)

Destination Networks

○ Use this SA as default route for all Internet traffic

● Specify destination networks below

Range Start | Range End | Subnet Mask *

* - Determines broadcast addresses for NetBIOS support.

STATUS: The configuration has been updated.

1. Select **Disable VPN Windows Networking (NetBIOS) broadcast.** Leave the **Enable Fragmented Packet Handling** unselected until the SonicWALL logs show many fragmented packets transmitted.

2. Click the **Configure** tab and select **Add New SA** from the **Security Association** menu. Then select **Manual Key** from the **IPSec Keying Mode** menu.

3. Enter a descriptive name that identifies the VPN client in the **Name** field, such as the client’s location or name.

4. Enter "0.0.0.0" in the **IPSec Gateway Address** field.

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

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

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

__Note__: It is important to remember the __Encryption Method__ selected as you need to select the same parameters in the VPN Client configuration.

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

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

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

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

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

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

Installing the VPN Client Software

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

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

2. Unzip the SonicWALL VPN Client zip file.

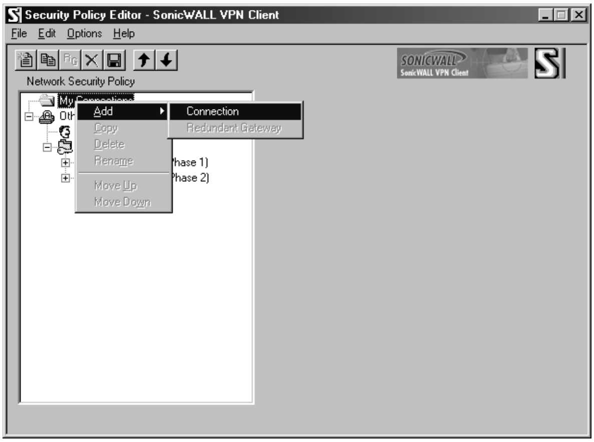
3. Double-click **setup.exe** and follow the VPN client setup program step-by-step instructions. Enter the VPN client serial number when prompted.

4. Restart your computer after installing the VPN client software.

Launching the SonicWALL VPN Client

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

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

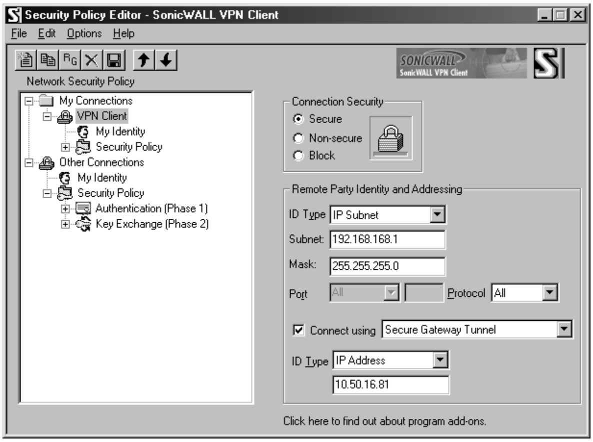


***Note**: The security policy is renamed to match the SA name created in the SonicWALL. You can rename the security policy by highlighting **New Connection** in the **Network Security Policy** box and typing the security policy name.*

Configuring VPN Security and Remote Identity

1. Select **Secure** in the **Network Security Policy** box on the right side of the **Security Policy Editor** window.
2. Select **IP Subnet** in the **ID Type** menu.
3. Enter the SonicWALL LAN IP Address in the **Subnet** field.
4. Enter the LAN Subnet Mask in the **Mask** field.
5. Select **All** in the **Protocol** menu to permit all IP traffic through the VPN tunnel.
6. Select the **Connect using Secure Gateway Tunnel** check box.
7. Select **IP Address** in the **ID Type** menu at the bottom of the **Security Policy Editor** window.

8. Enter the SonicWALL WAN IP Address in the field below the **ID Type** menu. Enter the NAT Public Address if NAT is enabled.



Connection Security
● Secure
○ Non-secure
○ Block

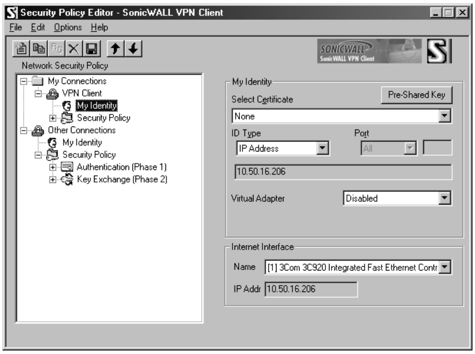
Remote Party Identity and Addressing

ID Type: IP Subnet
Subnet: 192.168.168.1
Mask: 255.255.255.0
Port: All
Protocol: All
☑ Connect using: Secure Gateway Tunnel
ID Type: IP Address
10.50.16.81

Configuring VPN Client Identity

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

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



My Identity

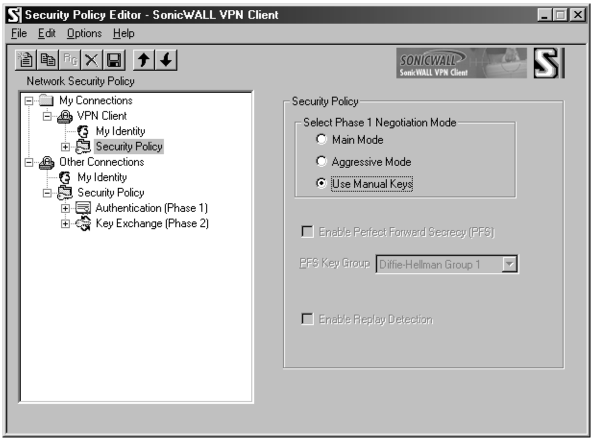
Select Certificate: None
ID Type: IP Address
Port: All
10.50.16.206
Virtual Adapter: Disabled

Internet Interface

Name: [1] 3Com 3C920 Integrated Fast Ethernet Contr
IP Addr: 10.50.16.206

Configuring VPN Client Security Policy

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



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

○ Aggressive Mode

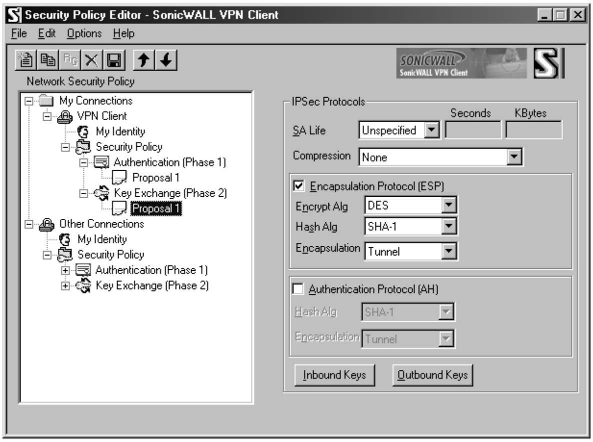
● Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

□ Enable Replay Detection

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



IPSec Protocols

		Seconds	KBytes
SA Life	Unspecified		
Compression	None		

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

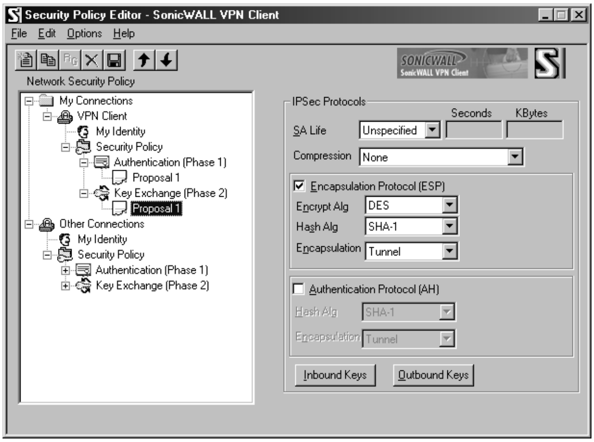
□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Configuring VPN Client Key Exchange Proposal

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



SA Life: Unspecified

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

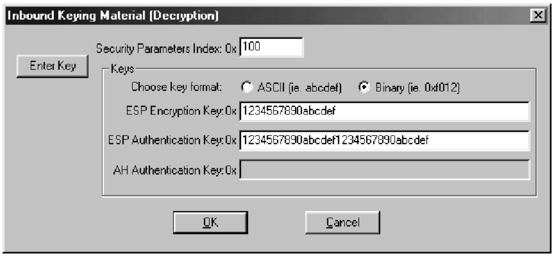
Hash Alg: SHA-1

Encapsulation: Tunnel

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

Configuring Inbound VPN Client Keys

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



Security Parameters Index: 0x 100

Choose key format: ○ ASCII (ie. abcdef) ● Binary (ie. 0x012)

ESP Encryption Key: 0x 1234567890abcdef

ESP Authentication Key: 0x 1234567890abcdef1234567890abcdef

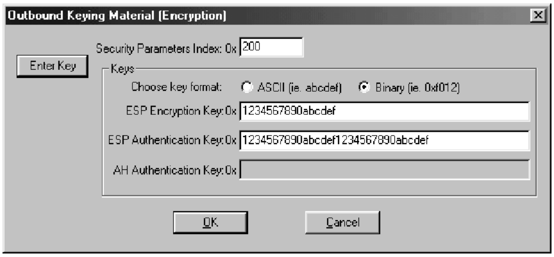
AH Authentication Key: 0x

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

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

Configuring Outbound VPN Client Keys

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



Security Parameters Index: 0x 200

Choose key format: ○ ASCII (ie. abcdef) ● Binary (ie. 0xf012)

ESP Encryption Key: 0x 1234567890abcdef

ESP Authentication Key: 0x 1234567890abcdef1234567890abcdef

AH Authentication Key: 0x

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

Saving SonicWALL VPN Client Settings

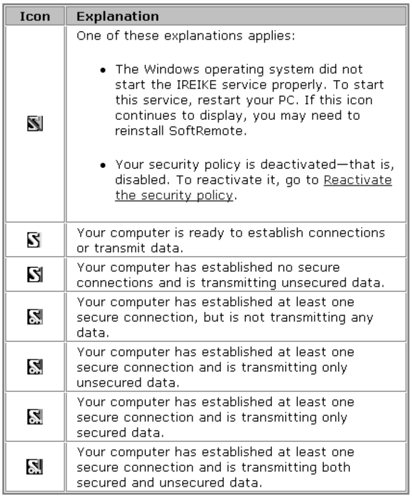
Select **Save Changes** in the **File** menu in the top left corner of the **Security Policy Editor** window.

Verifying the VPN Tunnel as Active

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

Verifying the VPN Client Icon in the System Tray

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



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

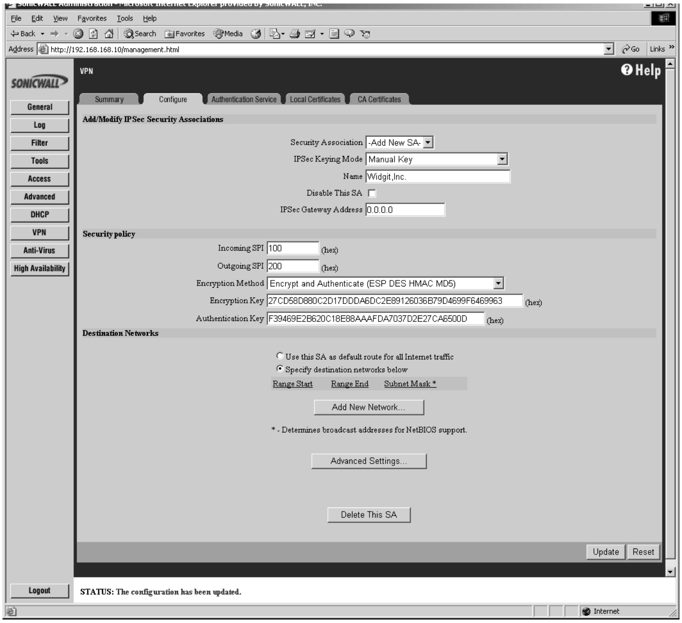
VPN for Two SonicWALLs

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

Manual Key for Two SonicWALLs

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

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



http://192.168.168.10/management.html

Add/Modify IPSec Security Associations

Security Association: -Add New SA-

IPSec Keying Mode: Manual Key

Name: Widgit,Inc.

Disable This SA: □

IPSec Gateway Address: 0.0.0.0

Security policy

Incoming SPI: 100 (hex)

Outgoing SPI: 200 (hex)

Encryption Method: Encrypt and Authenticate (ESP DES HMAC MD5)

Encryption Key: 27CD58D880C2D17DDDA6DC2E89126036B79D4699F6469963 (hex)

Authentication Key: F39469E2B620C18E88AAAFDA7037D2E27CA6500D (hex)

Destination Networks

○ Use this SA as default route for all Internet traffic

● Specify destination networks below

Range Start	Range End	Subnet Mask *

* - Determines broadcast addresses for NetBIOS support.

STATUS: The configuration has been updated.

3. Enter a descriptive name for the **Security Association**, such as "Chicago Office" or "Remote Management", in the **Name** field.
4. Enter the IP address of the remote VPN gateway, such as another SonicWALL VPN gateway, in the **IPSec Gateway Address** field. This must be a valid IP address and is the remote VPN gateway NAT Public Address if NAT is enabled. Enter "0.0.0.0" if the remote VPN gateway has a dynamic IP address.
5. Define an **SPI** (Security Parameter Index) that the remote SonicWALL uses to identify the **Security Association** in the **Incoming SPI** field.

6. Define an **SPI** that the local SonicWALL uses to identify the **Security Association** in the **Outgoing SPI** field.SPIs should range from 3 to 8 characters in length and include only hexadecimal characters.

   Note: *Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). If you enter an invalid **SPI**, an error message will be displayed at the bottom of the browser window. An example of a valid **SPI** is 1234abcd.*

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

7. Select an encryption algorithm from the **Encryption Method** menu. The SonicWALL supports the following encryption algorithms:

- **Tunnel Only (ESP NULL)** does not provide encryption or authentication. This option offers access to computers at private addresses behind NAT and allows unsupported services through the SonicWALL.
- **Encrypt (ESP DES)** uses 56-bit DES to encrypt data. DES is an extremely secure encryption method, supporting over 72 quadrillion possible encryption keys that can be used to encrypt data.
- **Fast Encrypt (ESP ARCFour)** uses 56-bit ARCFour to encrypt data. ARCFour is a secure encryption method and has little impact on the throughput of the SonicWALL.
- **Strong Encrypt (ESP 3DES)** uses 168-bit 3DES (Triple DES) to encrypt data. 3DES is considered an almost "unbreakable" encryption method, applying three DES keys in succession, but it significantly impacts the data throughput of the SonicWALL.
- **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** uses 168 bit 3DES encryption and HMAC MD5 authentication. 3DES is an extremely secure encryption method, and HMAC MD5 authentication is used to verify integrity. This method significantly impacts the data throughput of the SonicWALL.
- **Encrypt for Check Point (ESP DES rfc1829)** is interoperable with Check Point Firewall-1. In **Manual Keying** mode, **Encrypt for Check Point** uses 56-bit DES as specified in RFC 1829 as the encryption method.
- **Authenticate (AH MD5)** uses AH to authenticate VPN communications and MD5 to generate a 128-bit digest.
- **Authenticate (AH SHA1)** uses AH to authenticate VPN communications and SHA1 to generate a 160-bit message digest.
- **Authenticate (ESP MD5)** authenticates using ESP as the security protocol, no encryption, and MD5 to generate a 128-bit message digest.
- **Authenticate (ESP SHA1)** authenticates using ESP as the security protocol, no encryption, and SHA1 to generate a 160-bit message digest.

- **Encrypt and Authenticate (ESP DES HMAC MD5)** uses 56-bit DES encryption and HMAC MD5 authentication. This method impacts the data throughput of VPN communications. SonicWALL VPN client software supports this method.

8. Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. Enter a 48-character hexadecimal key if you are using Triple DES encryption. This encryption key must match the remote SonicWALL's encryption key.

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

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

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

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

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

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

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

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

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

14. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.
15. Click **Advanced Settings** and check the boxes that apply to your SA:

- **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.
- **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
- **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
- **VPN Terminated at LAN** - select one of the three terminating points for the VPN tunnel.

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

Configuring the Second SonicWALL Appliance

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

Example of Manual Key Configuration for Two SonicWALLs

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

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

The remote office has the following network settings:

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

- WAN subnet mask - 255.255.255.248

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

1. Configure the network settings for the firewall using the **Network** tab located in the **General** section.
2. Click **Update** and restart the SonicWALL if necessary.
3. Click **VPN**, then the **Configure** tab.
4. Create a name for the main office SA, for example, **Main Office**.
5. Type in the branch office WAN IP address for the **IPSec Gateway Address**.
6. Create an **Incoming SPI** using alphanumeric characters.
7. Create an **Outgoing SPI** using alphanumeric characters.
8. Select **Strong Encrypt (ESP 3DES)** as the **Encryption Method**.
9. Write the **Encryption Key** down or use cut and paste to copy it to a Notepad window.
10. Click **Add New Network**. Type the IP address, “192.168.22.1” in the **Range Start** field. Type the IP address, “192.168.22.254” in the **Range End** field. This **Range End** value is appropriate even if NetBIOS broadcast support is enabled. Leave the subnet mask field blank. Click **Update**.
11. Click **Advanced Settings** and select the features that apply to the SA.

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

12. Click **OK**, and then click **Update**.

To configure the remote SonicWALL, use the following steps:

1. Configure the network settings for the firewall using the **Network** tab located in the **General** section.
2. Click **Update** and restart the SonicWALL if necessary.
3. Click **VPN**, then the **Configure** tab.
4. Create a name for the remote office SA, for example, **Remote Office**.

5. Type in the main office WAN IP address for the **IPSec Gateway Address**.
6. Create an **Incoming SPI** using alphanumeric characters.
7. Create an **Outgoing SPI** using alphanumeric characters.
8. Select **Strong Encrypt (ESP 3DES)** as the **Encryption Method**.
9. Enter the **Encryption Key** from the Main Office configuration.
10. Click **Add New Network**. Enter the IP address, “192.168.11.1” in the **Range Start** field. Enter the IP address, “192.168.11.254” in the **Range End** field. This **Range End** value is appropriate even if NetBIOS broadcast support is enabled. Leave the subnet mask field blank. Click **Update**.
11. Click **Advanced Settings** and select the features that apply to the SA.

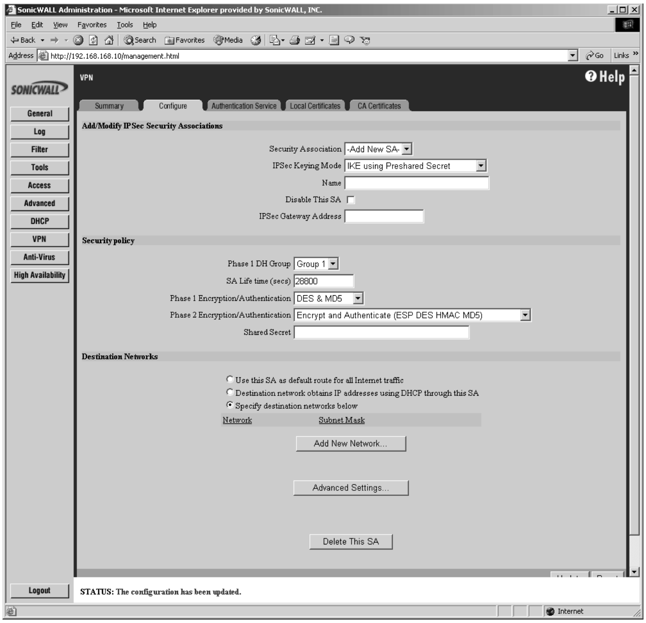
- **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.
- **Apply NAT and firewall rules** - to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Forward packets to remote VPNs** - if creating a “hub and spoke” network configuration
- **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
- **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.

12. Click **OK**, and then click **Update**.

IKE Configuration for Two SonicWALLs

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

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



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address http://192.168.168.10/management.html

VPN

Add/Modify IPSec Security Associations

Security Association -Add New SA-

IPSec Keying Mode IKE using Preshared Secret

Name

□ Disable This SA

IPSec Gateway Address

Security policy

Phase 1 DH Group Group 1

SA Life time (secs) 28800

Phase 1 Encryption/Authentication DES & MD5

Phase 2 Encryption/Authentication Encrypt and Authenticate (ESP DES HMAC MD5)

Shared Secret

Destination Networks

○ Use this SA as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this SA

● Specify destination networks below

Network	Subnet Mask

STATUS: The configuration has been updated.

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

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

5. Select **Group 2** from the **Phase 1 DH Group** menu.

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

   ***Note**: A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, users accessing remote resources are disconnected. Therefore, the default SA Life Time of 28,800 seconds (8 hours) is recommended.*

7. Select **DES & SHA1** from the **Phase 1 Encryption/Authentication** menu.
8. Select the appropriate encryption algorithm from the **Phase 2 Encryption/Authentication** menu. The SonicWALL supports the following encryption algorithms:

- **Tunnel Only (ESP NULL)** does not provide encryption or authentication, but offers access to machines at private addresses behind NAT. It also allows unsupported services through the SonicWALL.
- **Encrypt (ESP DES)** uses 56-bit DES to encrypt data. DES is an extremely secure encryption method, supporting over 72 quadrillion possible encryption keys that can be used to encrypt data.
- **Fast Encrypt (ESP ARCFour)** uses 56-bit ARCFour to encrypt data. ARCFour is a secure encryption method, and has less impact on throughput than DES or Triple DES. This encryption method is recommended for all but the most sensitive data.
- **Strong Encrypt (ESP 3DES)** uses 168-bit 3DES (Triple DES) to encrypt data. 3DES is considered an almost "unbreakable" encryption method, applying three DES keys in succession, but it significantly impacts the data throughput of the SonicWALL.
- **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** uses 168-bit 3DES encryption and HMAC MD5 authentication. 3DES is an extremely secure encryption method, and HMAC MD5 authentication is used to verify integrity. This method significantly impacts the data throughput of the SonicWALL.
- **Strong Encrypt for Checkpoint (ESP 3DES)** uses 168-bit 3DES encryption but does not use an authentication protocol.
- **Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)** uses 168-bit 3DES encryption and HMAC SHA1 authentication. 3DES is an extremely secure encryption method, and HMAC SHA1 authentication is used to verify integrity. This method significantly impacts the data throughput of the SonicWALL.
- **Encrypt for Check Point (ESP DES HMAC MD5)** uses 56-bit DES to encrypt data and is compatible with Check Point Firewall-1. This method impacts the data throughput of the SonicWALL.
- **Encrypt and Authenticate (ESP DES HMAC MD5)** uses 56-bit DES encryption and HMAC MD5 authentication. This method impacts the data throughput of VPN communications. SonicWALL VPN client software supports this method.
- **Authenticate (AH MD5)** uses AH to authenticate VPN communications and MD5 to generate a 128-bit digest.

- **Authenticate (AH SHA1)** uses AH to authenticate VPN communications and SHA1 to generate a 160-bit message digest.
- **Authenticate (ESP MD5)** authenticates using ESP as the security protocol, no encryption, and MD5 to generate a 128-bit message digest.
- **Authenticate (ESP SHA1)** authenticates using ESP as the security protocol, no encryption, and SHA1 to generate a 160-bit message digest.
- **Encrypt and Authenticate (ESP DES HMAC SHA1)** uses 56-bit DES encryption and HMAC SHA1 authentication.

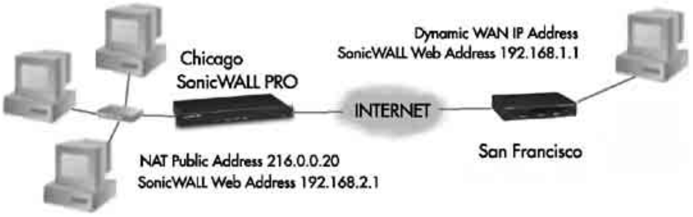
9. Enter a alphanumeric “secret” in the **Shared Secret** field. The **Shared Secret** must match the corresponding field in the remote SonicWALL. This field can range from 4 to 128 characters in length and is case sensitive.
10. Click **Add New Network...** to define the destination network addresses. Clicking **Add New Network...** updates the VPN configuration and opens the **VPN Destination Network** window.
11. Enter the IP address of the remote network in the **Network** field. This address is a private address if the remote LAN has enabled NAT.
12. Enter the subnet mask of the remote network in the **Subnet mask** field.
13. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.
14. Click **Advanced Settings** and select the boxes that apply to your SA:

- **Use Aggressive Mode** - requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange.
- **Enable Keep Alive** - if you want to maintain the current connection by listening for traffic on the network segment between the two connections.
- **Enable Windows Networking (NetBIOS) broadcast** - if remote clients use Windows Network Neighborhood to browse remote networks.
- **Apply NAT and firewall rules -** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Forward packets to remote VPNs -** if creating a “hub and spoke” network configuration
- **Enable Perfect Forward Secrecy** - if you want to add another layer of security by adding an additional Diffie-Hellman key exchange.
- **Phase 2 DH Group** - select the level of Phase 2 DH key exchange if **Perfect Forward Secrecy** is enabled.
- **Default LAN Gateway** - if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.

15. Click **OK** to close the **Advanced Settings** window. Click **Update** to upload the changes in the SonicWALL.

Example: Linking Two SonicWALLs using IKE

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


Chicago
SonicWALL PRO
Dynamic WAN IP Address
SonicWALL Web Address 192.168.1.1
INTERNET
San Francisco
NAT Public Address 216.0.0.20
SonicWALL Web Address 192.168.2.1

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

Configuring a SonicWALL PRO 200 in Chicago

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

   Note*: Only one of the two IPSec gateways can have a dynamic IP address when using SonicWALL VPN.*

6. Select **Group 2** from the **Phase 1 DH Group** menu.
7. Enter "86400" in the **SA Life time (secs)** field to renegotiate IKE encryption and authentication keys every 24 hours.
8. Select **DES & SHA1** from the **Phase 1 DH Group** menu.

9. Select a VPN encryption method from the **Phase 2 Encryption/Authentication** menu. Since data throughput and security are the primary concern, select **Encrypt and Authenticate (ESP DES HMAC SHA1)**.

10. Define a **Shared Secret**. Write down this key as it is required when configuring the San Francisco Office SonicWALL TELE3 SP.

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

12. Enter the IP address and subnet mask of the destination network, the San Francisco office, in the **Network** and **Subnet Mask** fields. Since NAT is enabled at the San Francisco office, enter a private LAN IP address. In this example, enter "192.168.1.1" and subnet mask "255.255.255.0." Click **OK** to add the destination network address.

    ***Note**: The **Destination Network Address** must NOT be in the local network address range. Therefore, the San Francisco and Chicago offices must have different LAN IP address ranges.*

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

- **Use Aggressive Mode** - requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange.
- **Enable Keep Alive** - if you want to maintain the current connection by listening for traffic on the network segment between the two connections.
- **Enable Windows Networking (NetBIOS) broadcast** - if remote clients use Windows Network Neighborhood to browse remote networks.
- **Apply NAT and firewall rules -** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Forward packets to remote VPNs -** if creating a “hub and spoke” network configuration
- **Enable Perfect Forward Secrecy** - if you want to add another layer of security by adding an additional Diffie-Hellman key exchange.
- **Phase 2 DH Group** - select the type of DH key exchange in Phase 2 for **Perfect Forward Secrecy**.
- **Default LAN Gateway** - if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.

14. Click **Update** to add the Security Association. Once the SonicWALL PRO 200 is updated, a message confirming the update is displayed at the bottom of the browser window.

Configuring a SonicWALL TELE3 in San Francisco

1. Enter the SonicWALL TELE3 **Unique Firewall Identifier** in the **VPN Summary** window, in this example, "San Francisco Office."
2. Select **-Add New SA-** from the **Security Association** menu.
3. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
4. Enter the SonicWALL PRO 200 **Unique Firewall Identifier** in the SonicWALL TELE3 **Name** field, in this example, "Chicago Office."
5. Enter the SonicWALL PRO 200 WAN IP Address in the **IPSec Gateway Address** field. This address must be valid, and is the SonicWALL PRO 200 NAT Public Address, or "216.0.0.20."
6. Select **Group 2** from the **Phase 1 DH Group** menu.
7. Enter 86400 in the **SA Life time (secs)** field to renegotiate keys daily.
8. Select **DES & SHA1** from the **Phase 1 Encryption/Authentication** menu.
9. Select the encryption algorithm from the **Phase 2 Encryption/Authentication** menu. The San Francisco office **Phase 2 Encryption/Authentication** must match Chicago, so **Encrypt and Authenticate (ESP DES HMAC SHA1)** must be selected.
10. Enter the same **Shared Secret** used in the Chicago Office SonicWALL PRO 200 into the SonicWALL TELE3 **Shared Secret** field.
11. Click **Add New Network...** to open the **VPN Destination Network** window and define the destination network addresses.
12. Enter the IP address and subnet mask of the destination network, the Chicago office, in the **Network** and Subnet Mask fields. Since NAT is enabled at the Chicago office, enter a private LAN IP address. In this example, enter "192.168.2.1" and subnet mask "255.255.255.0."
13. Click **Advanced Settings**. Select the following boxes that apply to your SA:

- **Use Aggressive Mode** - requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange.
- **Enable Keep Alive** - if you want to maintain the current connection by listening for traffic on the network segment between the two connections.
- **Enable Windows Networking (NetBIOS) broadcast** - if remote clients use Windows Network Neighborhood to browse remote networks.
- **Apply NAT and firewall rules -** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
- **Forward packets to remote VPNs -** if creating a “hub and spoke” network configuration
- **Enable Perfect Forward Secrecy** - if you want to add another layer of security by adding an additional Diffie-Hellman key exchange.

- **Phase 2 DH Group** - select the type of DH key exchange in Phase 2 for **Perfect Forward Secrecy**.
- **Default LAN Gateway** - if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the Route all traffic through this SA check box.

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

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

VPN Third Party Digital Certificate Support

***Note**: 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.

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**.

Certificate Details

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

- **Certificate Authority**
- **Subject Distinguished Name**
- **Certificate Issuer**
- **Certificate Serial Number**
- **Expiration Date**
- **No CRL loaded/CRL Expires on**

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

To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use Third Party Certificates for VPN authentication. Click **Export This CA Certificate** to export the file to your hard drive or a floppy disk

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**, enter the **Certificate Name**.
2. Enter 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.

Note*: 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 enter a URL location of the CRL by entering 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.

Creating a Certificate Signing Request

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

***Note**: 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, enter a name for the certificate in the **Certificate Name** field. Using the drop down menus, enter information for the certificate request. As you enter 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.
9. Now that you have generated the **Certificate Request**, you can send it to your CA service for validation.

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 **Configure**. In the **Add/Modify IPSec Associations** section, Select **IKE using 3rd Party Certificates** from the **IPSec Keying Mode** menu.
2. Enter a Name for the Security Association in the **Name** field.
3. Select a certificate from the **Select Certificate** list.
4. Enter 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. If you are allowing computers at the VPN destination to obtain an IP address dynamically through the VPN tunnel, select **Destination network obtains IP addresses using DHCP through this SA**. If the VPN destination is a specific IP address, select **Specify destination network below** and click **Add New Network...** Enter the network IP address and subnet mask in the fields, and click **OK**.

Advanced Settings

- **Use Aggressive Mode**
- **Enable Keep Alive**
- **Require authentication of local users**
- **Require authentication of remote users**

  - **Remote users behind VPN gateway**
  - **Remote VPN clients with XAUTH**
- **Enable Windows Networking (NetBIOS) broadcast**
- **Apply NAT and firewall rules**
- **Forward packets to remote VPNs**
- **Enable Perfect Forward Secrecy**

- **Phase 2 DH Group**
- **Default LAN Gateway**

Use Aggressive Mode

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

Enable Keep Alive

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

Require authentication of VPN clients via XAUTH

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

Require authentication of local users

Selecting this checkbox requires that all outbound VPN traffic using this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

Require authentication of remote users

Selecting this checkbox requires that all inbound VPN traffic using this SA is from an authenticated user. Unauthenticated traffic not allowed on the VPN tunnel. Select **Remote Users behind VPN gateway** if remote users have a VPN tunnel that terminates on the VPN gateway. Select **Remote VPN Clients with XAUTH** if remote users require authentication using XAUTH and are accessing the SonicWALL via a VPN Client.

Enable Windows Networking (NetBIOS) broadcast

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

Apply NAT and firewall rules

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

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

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

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

Forward Packets to Remote VPNs

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

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

Enable Perfect Forward Secrecy

The **Enable Perfect Forward Secrecy** check box increases the renegotiation time of the VPN tunnel. By enabling **Perfect Forward Secrecy**, a hacker using brute force to break encryption

keys is not able to obtain other or future IPSec keys. During the phase 2 renegotiation between two SonicWALL appliances or a Group VPN SA, an additional Diffie-Hellman key exchange is performed. **Enable Perfect Forward Secrecy** adds incremental security between gateways.

Phase 2 DH Group

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

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

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

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

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

Default LAN Gateway

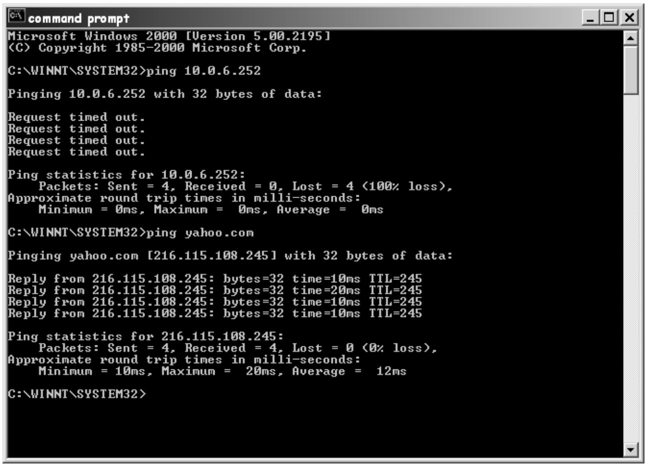
A **Default LAN Gateway** is used at a central site in conjunction with a remote site using the **Route all internet traffic through this SA** check box. The **Default LAN Gateway** field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN network. 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.

Testing a VPN Tunnel Connection Using PING

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

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



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\SYSTEM32>ping 10.0.6.252

Pinging 10.0.6.252 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.6.252:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\WINNT\SYSTEM32>ping yahoo.com

Pinging yahoo.com [216.115.108.245] with 32 bytes of data:

Reply from 216.115.108.245: bytes=32 time=10ms TTL=245
Reply from 216.115.108.245: bytes=32 time=20ms TTL=245
Reply from 216.115.108.245: bytes=32 time=10ms TTL=245
Reply from 216.115.108.245: bytes=32 time=10ms TTL=245

Ping statistics for 216.115.108.245:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum =  20ms, Average =  12ms

C:\WINNT\SYSTEM32>
```

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

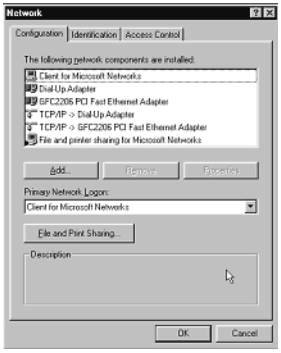
Configuring Windows Networking

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

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

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

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

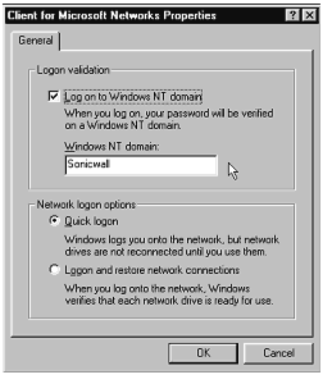


The following network components are installed:

- Client for Microsoft Networks
- Dial-Up Adapter
- GFC2206 PCI Fast Ethernet Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> GFC2206 PCI Fast Ethernet Adapter
- File and printer sharing for Microsoft Networks

Primary Network Logon: Client for Microsoft Networks

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



☑ Log on to Windows NT domain

When you log on, your password will be verified on a Windows NT domain.

Windows NT domain: Sonicwall

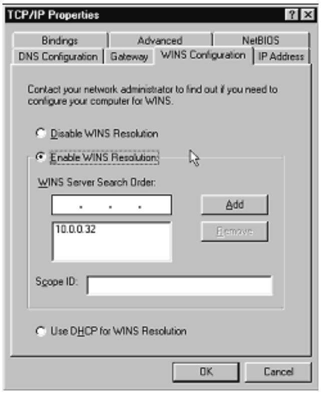
● Quick logon

Windows logs you onto the network, but network drives are not reconnected until you use them.

○ Logon and restore network connections

When you log onto the network, Windows verifies that each network drive is ready for use.

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



Contact your network administrator to find out if you need to configure your computer for WINS.

○ Disable WINS Resolution

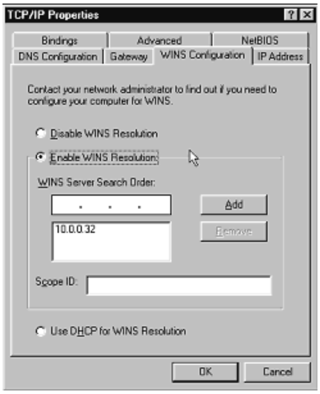
● Enable WINS Resolution:

WINS Server Search Order: 10.0.0.32

Scope ID:

○ Use DHCP for WINS Resolution

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



Contact your network administrator to find out if you need to configure your computer for WINS.

○ Disable WINS Resolution

● Enable WINS Resolution:

WINS Server Search Order: . . .

10.0.0.32

Scope ID:

○ Use DHCP for WINS Resolution

7. Windows 98® users must restart their computer for the settings to take effect, and then log into the remote domain.

Windows 2000® users should consult their network administrators for instructions to set up the remote domain access.

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

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

Adding, Modifying and Deleting Destination Networks

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

Modifying and Deleting Existing Security Associations

The **Security Association** menu also allows you to modify and delete existing **Security Associations**. To delete an **SA**, select it from the list and click the **Delete This SA** button. To modify an **SA**, select it from the list, make the desired changes, and click **Update**. Once the

SonicWALL has been updated, a message confirming the update is displayed at the bottom of the Web browser window. Click **Update** to enable the changes.

Accessing Remote Resources across a Virtual Private Network

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

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

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

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

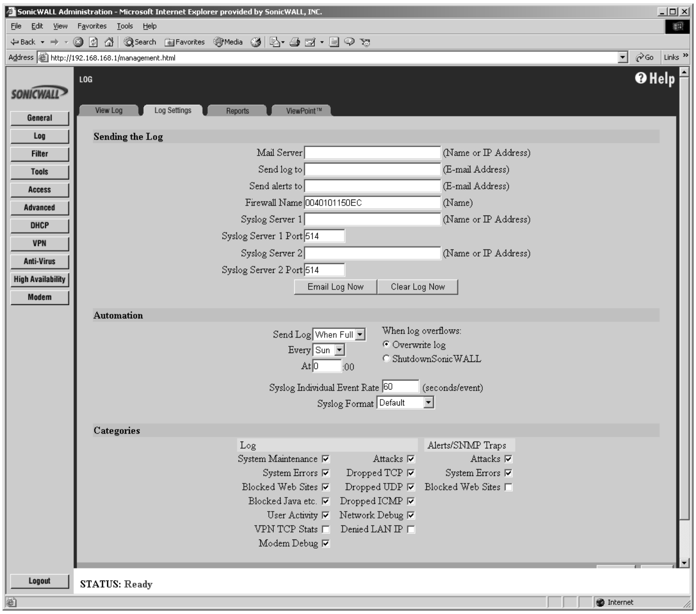
SonicWALL Enhanced VPN Logging

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

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

1. Click **Log** on the left side of the management interface.
2. Click on the **Logging Settings** tab, and locate the **Network Debug** check box.

3. Select the **Network Debug** check box, and then click **Update** to enable the **Network Debug** setting.


SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.1/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Modem
Logout
LOG
Help
View Log
Log Settings
Reports
ViewPoint™
Internet

Sending the Log

Mail Server (Name or IP Address)

Send log to (E-mail Address)

Send alerts to (E-mail Address)

Firewall Name 0040101150EC (Name)

Syslog Server 1 (Name or IP Address)

Syslog Server 1 Port 514

Syslog Server 2 (Name or IP Address)

Syslog Server 2 Port 514

Email Log Now | Clear Log Now

Automation

Send Log When Full

Every Sun

At 0 :00

When log overflows:
● Overwrite log
○ ShutdownSonicWALL

Syslog Individual Event Rate 60 (seconds/event)

Syslog Format Default

Categories

Log		Alerts/SNMP Traps
System Maintenance ☑	Attacks ☑	Attacks ☑
System Errors ☑	Dropped TCP ☑	System Errors ☑
Blocked Web Sites ☑	Dropped UDP ☑	Blocked Web Sites ☐
Blocked Java etc. ☑	Dropped ICMP ☑	
User Activity ☑	Network Debug ☑	
VPN TCP Stats ☐	Denied LAN IP ☐	
Modem Debug ☑		

STATUS: Ready

Disabling Security Associations

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

Basic VPN Terms and Concepts

- **VPN Tunnel**

  A VPN Tunnel is a term that describes a connection between two or more private nodes or LANs over a public network, typically the Internet. Encryption is often used to maintain the confidentiality of private data when traveling over the Internet.

- **Encryption**

  Encryption is a mathematical operation that transforms data from "clear text" (something that a human or a program can interpret) to "cipher text" (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric "key" be supplied along with the clear text. The key and clear text are processed by the encryption operation, which leads to data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms cipher text to clear text.

- **Key**

  A key is an alphanumeric string used by the encryption operation to transform clear text into cipher text. A key is comprised of hexadecimal characters (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). A valid key would be 1234567890abcdef. Keys used in VPN communications can range in length, but typically consist of 16 or 32 characters. The longer the key, the more difficult it is to break the encryption.

- **Asymmetric vs. Symmetric Cryptography**

  Asymmetric and symmetric cryptography refer to the keys used to authenticate, or encrypt and decrypt the data.

  Asymmetric cryptography, or public key cryptography, uses two keys for verification. Organizations, such as RSA Data Security and Verisign, support asymmetric cryptography.

  With symmetric cryptography, the same key is used to authenticate on both ends of the VPN. Symmetric cryptography, or secret key cryptography, is usually faster than asymmetric cryptography. Therefore symmetric algorithms are often used when large quantities of data have to be exchanged. SonicWALL VPN uses Symmetric Cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- **Security Association (SA)**

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

- **Internet Key Exchange (IKE)**

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

- **Manual Key**

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

- **Shared Secret**

  A Shared Secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE SA. This field can be any combination of alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Precautions should be taken when delivering/exchanging this shared secret to assure that a third party cannot compromise the security of a VPN tunnel.

- **Encapsulating Security Payload (ESP)**

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

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

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

- **Authentication Header (AH)**

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

  Using AH increases the processing requirements of VPN and also increases the communications latency. The increased latency is primarily due to the calculation of the authentication data by the sender, and the calculation and comparison of the authentication data by the receiver for each IP packet containing an Authentication Header.

- **Data Encryption Standard (DES)**

  When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. SonicWALL DES encryption algorithm uses a 56 bit key.

  The SonicWALL VPN DES Key must be exactly 16-characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be 1234567890abcdef.

- **ARCFour**

  ARCFour is used for communications with secure Web sites using the SSL protocol. Many banks use a 40 bit key ARCFour for online banking, while others use a 128 bit key. SonicWALL VPN uses a 56 bit key for ARCFour.

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

  The SonicWALL VPN ARCFour key must be exactly 16 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be 1234567890abcdef.

- **Strong Encryption (TripleDES)**

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

  The SonicWALL 3DES Key must be exactly 24 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be 1234567890abcdef12345678.

- **Security Parameter Index (SPI)**

  The SPI is used to establish a VPN tunnel. The SPI is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and keys associated with the SPI to establish the tunnel.

  The SPI must be unique, is from one to eight characters long, and is comprised of hexadecimal characters. Valid hexadecimal characters are "0" to "9", and "a" to "f" inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, valid SPIs would be 999 or 1234abcd.

11 High Availability

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 **High Availability** adds to the award-winning SonicWALL Internet security solution by assuring a highly reliable and secure connection to the Internet.

SonicWALL **High Availability** is standard on the SonicWALL product line. SonicWALL **High Availability** eliminates network downtime by allowing the configuration of two SonicWALLs (one primary and one backup) as a **High Availability** 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.

Getting Started with High Availability

Before Configuring High Availability

Before attempting to configure two SonicWALLs as a **High Availability** pair, check the following requirements:

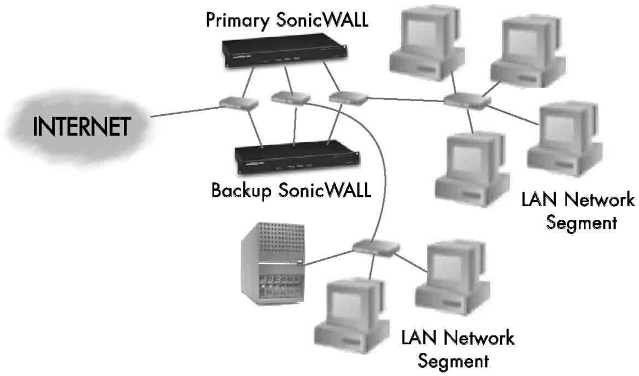
- You have two (2) SonicWALL Internet Security Appliances. The **High Availability** pair must consist of two identical SonicWALL models.
- You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (2) valid, static IP addresses are required to remotely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

***Note**: SonicWALL **High Availability** does not support dynamic IP address assignment from your ISP.*

- Each SonicWALL in the **High Availability** pair must have the same firmware version installed.
- Each SonicWALL in the **High Availability** 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.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a **High Availability** pair:

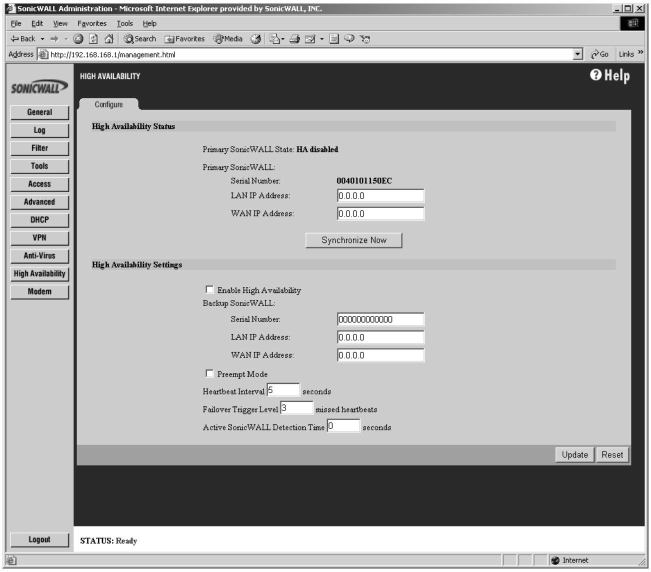


All SonicWALL ports being used must be connected together with a hub or switch. Each SonicWALL must have a unique LAN IP Address on the same LAN subnet. If each SonicWALL has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

***Note**: The two SonicWALLs in the **High Availability** pair sends “heartbeats” over the LAN network segment. The **High Availability** feature does not function if the LAN ports are not connected.*

Configuring High Availability on the Primary SonicWALL

Click **High Availability** on the left side of the SonicWALL browser window, and then click **Configure** at the top of the window.



SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.1/management.html
Go Links
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Modem
Logout
HIGH AVAILABILITY
Help
Configure
Synchronize Now
Update
Reset
Internet

High Availability Status

Primary SonicWALL State: **HA disabled**

Primary SonicWALL:

Serial Number: **0040101150EC**

LAN IP Address: 0.0.0.0

WAN IP Address: 0.0.0.0

High Availability Settings

□ Enable High Availability

Backup SonicWALL:

Serial Number: 000000000000

LAN IP Address: 0.0.0.0

WAN IP Address: 0.0.0.0

□ Preempt Mode

Heartbeat Interval 5 seconds

Failover Trigger Level 3 missed heartbeats

Active SonicWALL Detection Time 0 seconds

STATUS: Ready

The top half of the window displays the primary SonicWALL serial number and network settings. The bottom half of the window displays the backup SonicWALL information boxes. To configure **High Availability**, 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 **High Availability**.

3. Click **High Availability** on the left and begin configuring the following settings for the primary SonicWALL:

- **LAN IP Address** - This is a unique IP address for accessing the primary SonicWALL from the LAN whether it is **Active** or **Idle**.

Note*: This IP address is different from the IP address used to contact the SonicWALL in the General 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**.

Note*: The* ***Synchronize Now*** *button is used for diagnostics and troubleshooting purposes and is not required for initial configuration.*

4. In the Web Management interface for the primary SonicWALL, 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**.

Note: *This IP address is different from the IP address used to contact the SonicWALL in the General 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**.

5. Check the **Preempt mode** checkbox if you want the primary to SonicWALL to takeover 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.

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

6. 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 **High Availability** pair.

7. 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 this number of consecutive missed heartbeats, the backup SonicWALL takes over operation from the active 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 active unit after 10 seconds in the event of a failure in the active unit.

8. 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 High Availability 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 **High Availability** 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.

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

***Note**: 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 using **Restore Factory Default Settings** located in the **Tools** section. Additionally, the password must be changed back to the default password of "password" using the **Password** tab in the **General** section.*

10. Power on the backup SonicWALL used for **High Availability**. 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 **High Availability** 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 **Status** tab. To view the error message on the **Status** tab, click **General** on the left side of the browser and then **Status** at the top of the window.

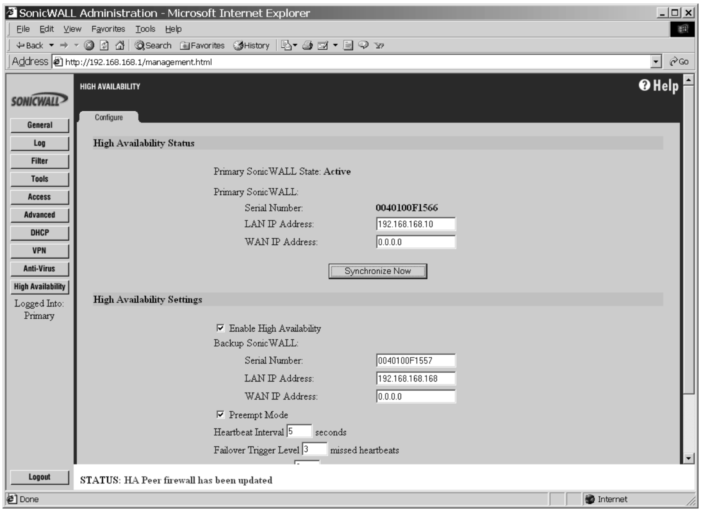
To check the backup SonicWALL firmware version or serial number, log into the backup SonicWALL, click **General** on the left side of the browser window and then click **Status** at the top of the window. Both the firmware version and the SonicWALL serial number are displayed at the top of the window.

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 **High Availability** 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 **High Availability** 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.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.168.1/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
HIGH AVAILABILITY
Help
Configure
Synchronize Now
Done
Internet

High Availability Status

Primary SonicWALL State: Active

Primary SonicWALL:

Serial Number: 0040100F1566

LAN IP Address: 192.168.168.10

WAN IP Address: 0.0.0.0

High Availability Settings

☑ Enable High Availability

Backup SonicWALL:

Serial Number: 0040100F1557

LAN IP Address: 192.168.168.168

WAN IP Address: 0.0.0.0

☑ Preempt Mode

Heartbeat Interval 5 seconds

Failover Trigger Level 3 missed heartbeats

Logged Into: Primary

STATUS: HA Peer firewall has been updated

***Note**: If you change the IP address of either SonicWALL, synchronization cannot occur between the two SonicWALLs without updating the changes manually in the High Availability configuration.*

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.

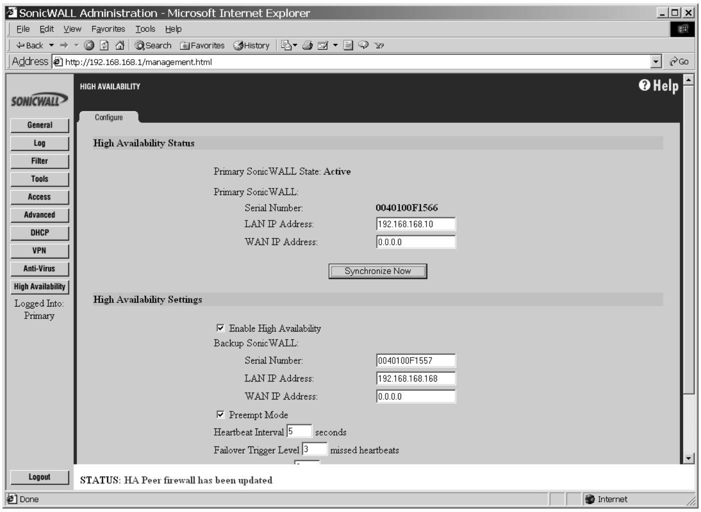
High Availability Status

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 **High Availability Status** window, **E-mail Alerts** and **View Log**. These methods are described in the following sections.

High Availability Status Window

One method to determine which SonicWALL is active is to check the **High Availability Status** page for the **High Availability** pair. To view the **High Availability Status** window, you can log into the primary or backup SonicWALL LAN IP Address. Click **High Availability** on the left side of the browser window and then click **Configure** at the top of the window. If the primary SonicWALL is active, the first line in the status window above indicates that the primary SonicWALL is currently **Active**

.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.168.1/management.html
Go
SONICWALL
HIGH AVAILABILITY
Help
Configure
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Synchronize Now
Done
Internet

High Availability Status

Primary SonicWALL State: **Active**

Primary SonicWALL:

Serial Number:	**0040100F1566**
LAN IP Address:	192.168.168.10
WAN IP Address:	0.0.0.0

High Availability Settings

☑ Enable High Availability

Backup SonicWALL:

Serial Number:	0040100F1557
LAN IP Address:	192.168.168.168
WAN IP Address:	0.0.0.0

☑ Preempt Mode

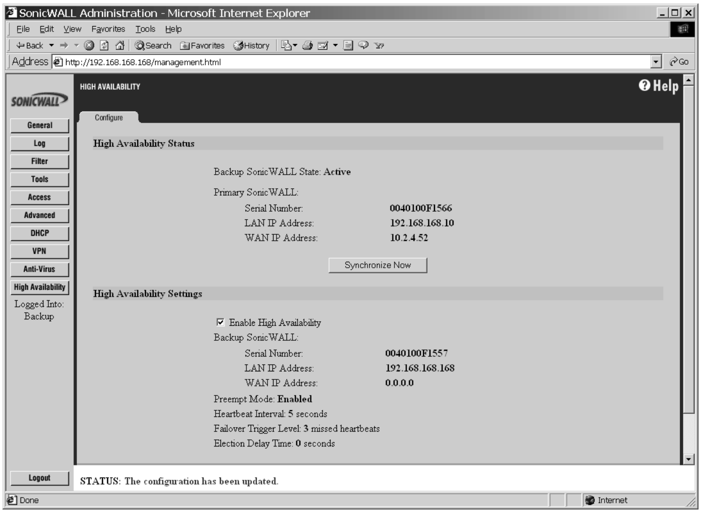
Heartbeat Interval 5 seconds

Failover Trigger Level 3 missed heartbeats

Logged Into: Primary

STATUS: HA Peer firewall has been updated

If the backup SonicWALL is active, the first line changes to reflect the active status of the backup as shown below:


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.168.168/management.html
Go
SONICWALL
HIGH AVAILABILITY
Help
Configure
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Synchronize Now
Done
Internet

High Availability Status

Backup SonicWALL State: **Active**

Primary SonicWALL:

Serial Number:	**0040100F1566**
LAN IP Address:	**192.168.168.10**
WAN IP Address:	**10.2.4.52**

High Availability Settings

☑ Enable High Availability

Backup SonicWALL:

Serial Number:	**0040100F1557**
LAN IP Address:	**192.168.168.168**
WAN IP Address:	**0.0.0.0**

Preempt Mode: **Enabled**

Heartbeat Interval: **5** seconds

Failover Trigger Level: **3** missed heartbeats

Election Delay Time: **0** seconds

Logged Into: Backup

STATUS: The configuration has been updated.

The first line in the status window indicates that the backup 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 window indicates that the backup SonicWALL is currently **Idle**. If the backup has taken over for the primary, this window indicates that the backup is currently **Active**.

***Note**: In the event of a failure in the primary SonicWALL, you may access the Web 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.*

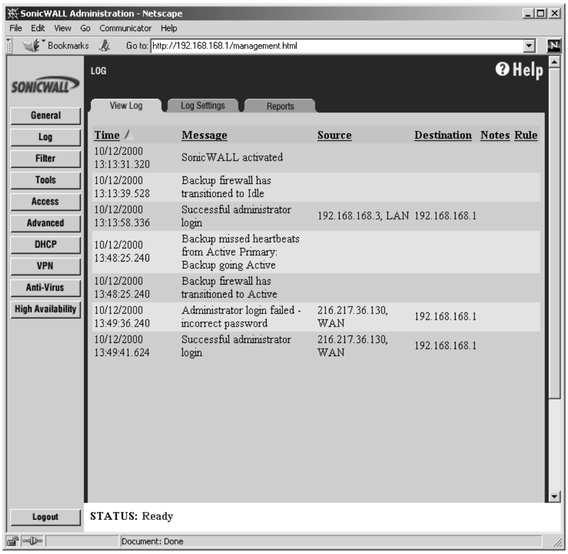
E-mail Alerts Indicating Status Change

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 **High Availability** 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 these **High Availability** events in addition to other status messages and possible security threats. This log may be viewed with a browser using the SonicWALL Web 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 browser window and then click on **View Log** at the top of the window.



Time	Message	Source	Destination	Notes	Rule
10/12/2000 13:13:31.320	SonicWALL activated				
10/12/2000 13:13:39.528	Backup firewall has transitioned to Idle				
10/12/2000 13:13:58.336	Successful administrator login	192.168.168.3, LAN	192.168.168.1		
10/12/2000 13:48:25.240	Backup missed heartbeats from Active Primary: Backup going Active				
10/12/2000 13:48:25.240	Backup firewall has transitioned to Active				
10/12/2000 13:49:36.240	Administrator login failed - incorrect password	216.217.36.130, WAN	192.168.168.1		
10/12/2000 13:49:41.624	Successful administrator login	216.217.36.130, WAN	192.168.168.1		

STATUS: Ready

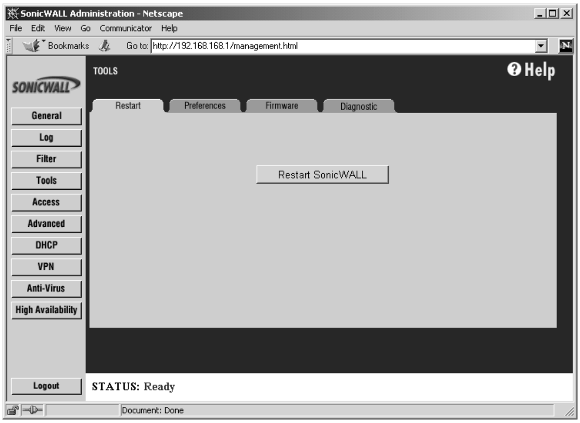
Document: Done

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.



STATUS: Ready

Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **High Availability** pair takes over operation.

***Note**: 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

- **Changing Password** - Do not change the password on the Backup firewall when it is in Idle condition. Changing the password prevents communication between the firewalls.
- If you are configuring the SonicWALL in **Standard** mode on the network, an additional IP address is necessary for the **High Availability** configuration.
- **Auto Update** - If **Auto Update** is enabled 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.

12 SonicWALL Options and Upgrades

SonicWALL, Inc. offers a variety of options and upgrades to enhance the functionality of your SonicWALL Internet security appliance. SonicWALL options and upgrades include the following:

- **SonicWALL VPN Client for Windows**
- **SonicWALL Network Anti-Virus Subscription**
- **Content Filter List Subscription**
- **Vulnerability Scanning Service**
- **Authentication Service**
- **ViewPoint Reporting**
- **SonicWALL Global Management**

SonicWALL VPN Client for Windows

The SonicWALL VPN Client allows remote users to securely access resources on your private LAN from a Dial-up Internet connection. The SonicWALL VPN Client establishes a private, encrypted VPN tunnel to the SonicWALL, allowing users to contact your network servers from any location. The SonicWALL VPN Client is perfect for business travelers and remote users who require access to private resources on the LAN or LAN.

SonicWALL Network Anti-Virus

SonicWALL **Network Anti-Virus** offers a new approach to virus protection by delivering managed anti-virus protection over the Internet. By combining leading-edge anti-virus technology from macafee.com with SonicWALL Internet security appliances, **Network Anti-Virus** ensures that all the computers on your network have a secure defense against viruses.

SonicWALL **Network Anti-Virus** provides constant, uninterrupted protection by monitoring computers for outdated virus software and automatically triggering the installation of new virus software. In addition, the SonicWALL restricts access to the Internet if virus software is not detected, enforcing virus protection. This strategy ensures that current virus software is installed and active on every computer on the network, preventing a rogue user from disabling virus protection and exposing the entire organization to an outbreak.

SonicWALL **Network Anti-Virus** provides centrally managed and enforced virus installation, transparent software updates, and comprehensive Web-based reports. SonicWALL **Network Anti-Virus** is a subscription-based solution that can be purchased in 5-, 10-, 50-, and 100-license annual subscriptions.

Content Filter List Subscription

Inappropriate online content can create an uncomfortable work environment, lead to harassment lawsuits, or expose children to pornography or racially intolerant sites. The SonicWALL Content Filter List Subscription allows businesses to create and enforce Internet access policies tailored to the requirements of the organization.

The SonicWALL Internet security appliance provides you with flexible tools to create and administer Acceptable Use Policies. An annual subscription to the Content Filter List (provided by CyberPatrol) allows you to block or monitor access to undesirable Internet sites, such as pornography or violence. Automatic weekly updates of the customizable Content Filter List ensure proper enforcement of access restrictions to new and relocated sites. Users can be given a password to bypass the filter, giving them unrestricted access to the Internet.

Vulnerability Scanning Service

SonicWALL **Vulnerability Scanning Service** is an automated, subscription that provides network administrators a "hacker's eye view" of a company's network perimeter, including public servers, routers and gateways, and integrates with SonicWALL's industry-leading Internet security appliances.

SonicWALL **Vulnerability Scanning Service** examines a network perimeter for security weaknesses on an ongoing basis. It reports all vulnerabilities detected and provides administrators with in-depth, expert guidance to quickly close up any security holes in a network. This subscription based service offers vulnerability assessment scans that can scheduled on a regular basis or run on demand when policies change or new equipment is deployed.

SonicWALL Authentication Service

SonicWALL **Authentication Service** delivers strong authentication of VPN users across the Internet to protect your organization's valuable and confidential resources. Implemented in collaboration with VeriSign, the leading provider of trusted services, SonicWALL **Authentication Service** is an affordable, easy to administer, end-to-end digital certificate solution for your organization. When combined with SonicWALL VPN, the SonicWALL Authentication Service guarantees that the right people access the right resources.

With SonicWALL **Authentication Service**, organizations can take advantage of the power of public key infrastructure (PKI) and digital certificates without incurring the high cost and complexity of creating the infrastructure themselves. Network administrators manage the **SonicWALL Authentication Service** directly from the SonicWALL Internet security appliance and VPN user certificates are conveniently distributed on a secure, Web-based server.

SonicWALL ViewPoint Reporting

SonicWALL ViewPoint, a Web-based graphical reporting tool, enables administrators to understand and manage their network. ViewPoint compliments and extends SonicWALL's complete security platform by delivering comprehensive, high-level historical reports and real-time monitoring.

SonicWALL ViewPoint includes everything you need to get up and running in one easy-to-install product, including a Web server, syslog server, database and reporting software. ViewPoint uses a Web-based interface and easily installs on any Windows NT or Windows 2000 computer on the network.

SonicWALL Global Management System

SonicWALL **Global Management System** is a scalable, cost-effective solution that extends the SonicWALL's ease of administration, giving you the tools to manage the security policies of remote, distributed networks. SonicWALL **GMS** lets you administer the SonicWALL at your corporate headquarters, branch offices and telecommuters from a central location. SonicWALL **GMS** reduces staffing requirements, speeds up deployment, and lowers delivery costs by centralizing the management and monitoring of security policies. SonicWALL **GMS** uses a hierarchical structure to simplify the management of SonicWALLs with similar security profiles. This gives you the flexibility to manage the security policies of remote SonicWALLs on an individual, group or global level.

Visit SonicWALL's Web site at <http://www.sonicwall.com/products/services.html> for more information about SonicWALL options and upgrades.

Contact your local reseller to purchase SonicWALL upgrades. A SonicWALL sales representative can help locate a SonicWALL-authorized reseller near you.

Web:http://www.sonicwall.com E-mail:sales@sonicwall.com

Phone:(888) 557-6642 or (408) 745-9600 Fax: (408) 745-9300

13 Hardware Description

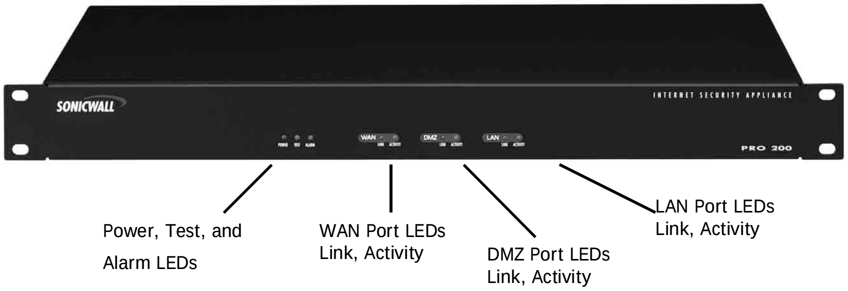
This chapter provides detailed illustrations and descriptions of the SonicWALL Internet Security Appliances front and back panels by model. Refer to this chapter to learn about where the LEDs, switches, and connectors are located.

More information is provided in **Appendix A, Technical Specifications**.

SonicWALL PRO 200 and SonicWALL PRO 300 are described on the following pages; SonicWALL PRO 100, on pages 155-156; and SonicWALL SOHO3 and SonicWALL TELE3 on pages 157-158.

SonicWALL PRO 200 and PRO 300 Front Panel

The SonicWALL PRO 200 front panel is shown below, followed by a description of each item. The SonicWALL PRO 300 is identical to the SonicWALL PRO 200 except for the PRO 300 label on the front panel and the inclusion of VPN accelerator hardware and an additional 8MB of RAM.


SONICWALL
INTERNET SECURITY APPLIANCE
WAN
DMZ
LAN
PRO 200
Power, Test, and Alarm LEDs
WAN Port LEDs Link, Activity
DMZ Port LEDs Link, Activity
LAN Port LEDs Link, Activity

SonicWALL PRO 200 and SonicWALL PRO 300 Front Panel Description

- **Power**

  Lights up when power is applied to SonicWALL PRO or SonicWALL PRO 300.

- **Test**

  Lights up when the SonicWALL is powered up and performing diagnostic tests to check for proper operation. These tests take about 90 seconds. If the Test LED remains lit after this time, the software is corrupt and must be reinstalled.

- **Alarm**

  Lights up and flashes for 10 seconds when an event generates an alert. **Alarm** LED flashes for 10 seconds. Alert events are defined in the **Log Settings** section in Chapter 5.

There are three Ethernet ports; one for each of the LAN, DMZ, and WAN ports:

- **Link**

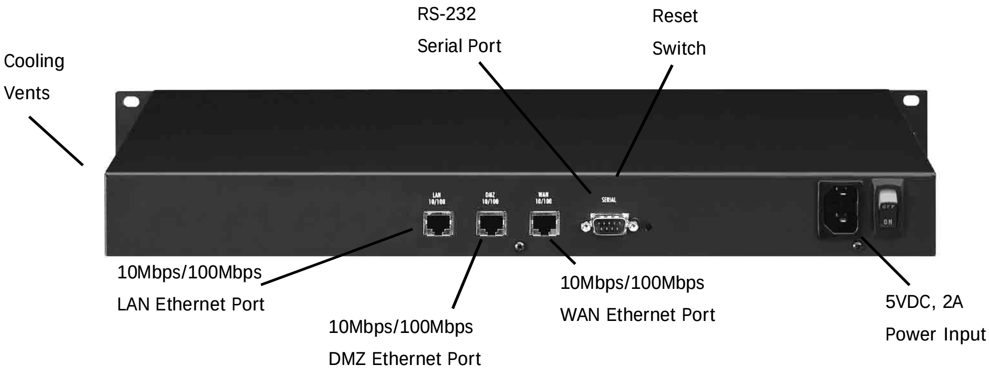
  Lights up when a **Twisted Pair** connection is made to another Ethernet device (usually a hub) on the port. Note that the device connected to the SonicWALL must support the standard Link Integrity test.

- **Activity**

  Lights up when the SonicWALL transmits or receives a packet through the Twisted Pair port onto the network.

SonicWALL PRO 200 and PRO 300 Back Panel

The SonicWALL PRO 200 back panel is shown below, followed by a description of each item. *The SonicWALL PRO 300 back panel is identical to the SonicWALL PRO 200.*



SonicWALL PRO 200 and SonicWALL PRO 300 Back Panel Description

- **(3) Twisted Pair (10Base-T, 100Base-T) Ethernet Ports**

  (3) Auto switching 10Mbps/100Mbps Ethernet ports provide connectivity for both Ethernet and Fast Ethernet networks. The Ethernet ports connect the SonicWALL to the LAN, DMZ, and WAN using Twisted Pair cable with RJ45 connectors.

- **Serial Port**

  DB-9 RS-232 Serial port for Command Line Interface support.

- **Reset Switch**

  Resets the SonicWALL PRO 200 or the SonicWALL PRO 300 to its factory clean state. This can be required if you forget the administrator password, or the SonicWALL firmware has become corrupt.

- **Power Input**

  Connects the SonicWALL to power input. The use of an Uninterruptible Power Supply (UPS) is strongly recommended to protect the SonicWALL against damage, or loss of data due to electrical storms, power failures, or power surges.

- **Power Switch**

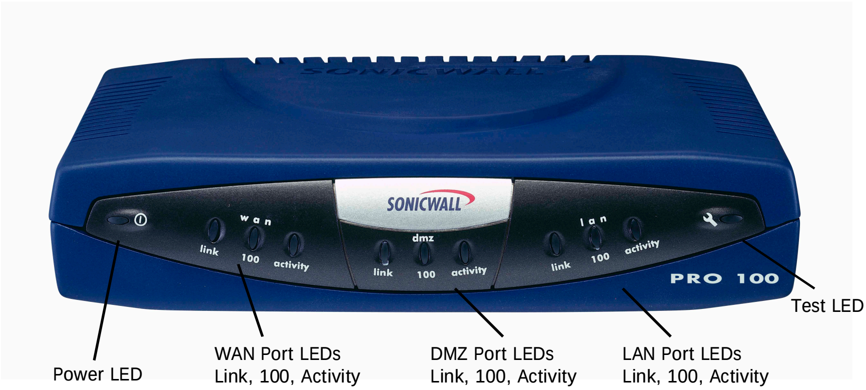
  Powers the SonicWALL on and off.

- **Cooling Vents**

  The SonicWALL is convection cooled; an internal fan is not necessary. Do not block the cooling vents on the SonicWALL side panels.

SonicWALL PRO 100 Front Panel

The SonicWALL PRO 100 front panel is shown below, followed by a description of each item.



SonicWALL PRO 100 Front Panel Description

- **Power**

  Lights up when power is applied to the SonicWALL PRO 100.

- **Test**

  Lights up when the SonicWALL PRO 100 is first powered up and performing diagnostic tests to check for proper operation. These tests take about 90 seconds. If the **Test LED** remains lit after this time, the software is corrupt and must be reinstalled.

There are three Ethernet ports; one for each of the LAN, DMZ, and WAN ports:

- **Link**

  Lights up when the **Twisted Pair** port is connected to a 10Mbps or 100Mbps hub or switch, or directly connected to a computer. Note that the connected Ethernet device must support the standard Link Integrity test.

- **100**

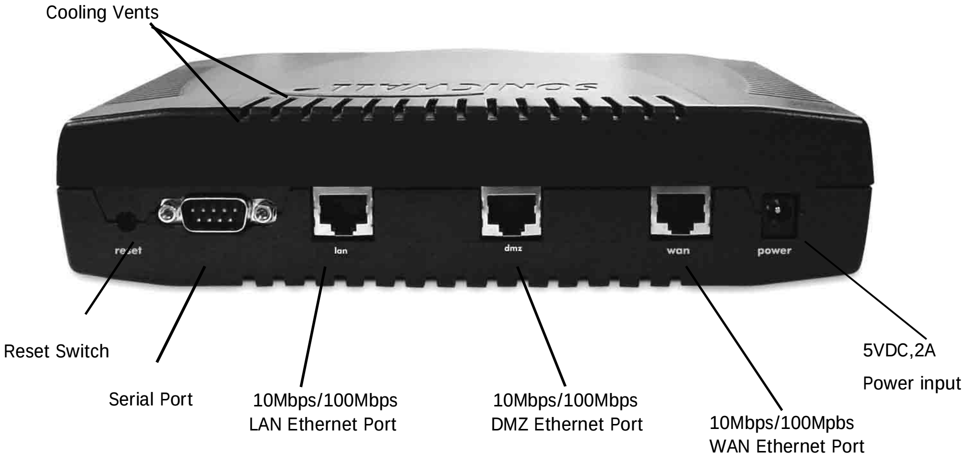
  Lights up when the **Twisted Pair** port is connected to a 100Mbps hub or switch or directly connected to a computer with a 100Mbps network interface.

- **Activity**

  Flashes when the SonicWALL PRO 100 transmits or receives a packet through the **Twisted Pair** port.

SonicWALL PRO 100 Back Panel

The SonicWALL PRO 100 back panel is shown below, followed by a description of each item.



The SonicWALL PRO 100 Back Panel Description

- **Reset Switch**

  Erases the firmware and resets SonicWALL PRO 100 to its factory clean state. This can be necessary if the administrator password is forgotten, or the firmware has become corrupt.

- **Serial Port**

  DB-9 RS-232 Serial port for Command Line Interface support.

- **(3) Twisted Pair (10Base-T, 100Base-T) Ethernet Ports**

  (3) Auto switching 10Mbps/100Mbps Ethernet ports provide connectivity for both Ethernet and Fast Ethernet networks. The Ethernet ports connect the SonicWALL PRO 100 to the LAN, DMZ, and WAN using Twisted Pair cable with RJ45 connectors.

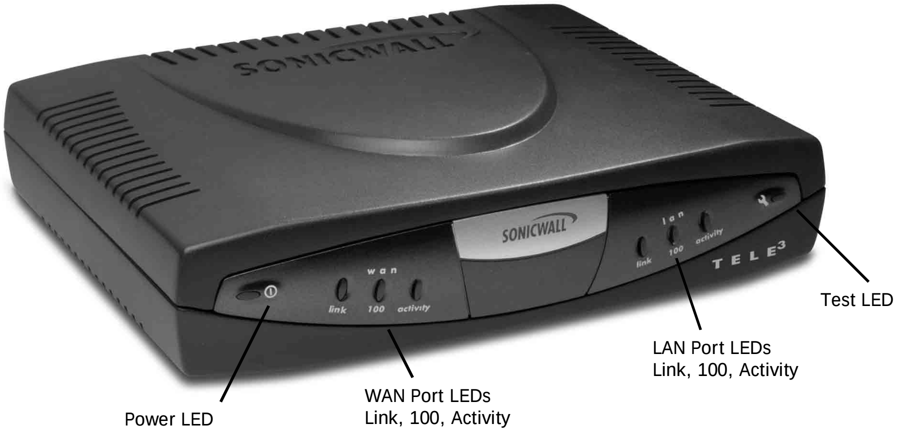
- **Power Input**

  Connects to the external power supply that is provided with the SonicWALL PRO 100. The use of an Uninterruptible Power Supply (UPS) is recommended to protect the SonicWALL PRO 100 against damage or loss of data due to electrical storms, power failures, or power surges.

- **Cooling Vents**
- The SonicWALL PRO 100 is convection cooled; an internal fan is not necessary. Do not block the cooling vents.

SonicWALL SOHO3 and TELE3 Front Panel

The SonicWALL **SOHO3** front panel is shown below, followed by a description of each item. The SonicWALL **TELE3** is identical to the SonicWALL **SOHO3** except for the **TELE3** label on the front panel and the inclusion of SonicWALL VPN.



SonicWALL SOHO3 and SonicWALL TELE3 Front Panel Description

- **Power**

  Lights up when power is applied to the SonicWALL SOHO3 or SonicWALL TELE3.

- **Test**

  Lights up when the SonicWALL is first powered up and performing diagnostic tests to check for proper operation. These tests take about 90 seconds. If the Test LED remains lit after this time, the software is corrupt and must be reinstalled.

There are two Ethernet ports; one of the following for the LAN and WAN ports:

- **Link**

  Lights up when the Twisted Pair port is connected to a 10Mbps or 100Mbps hub or switch or directly connected to a computer. Note that the connected Ethernet device must support the standard Link Integrity test.

- **100**

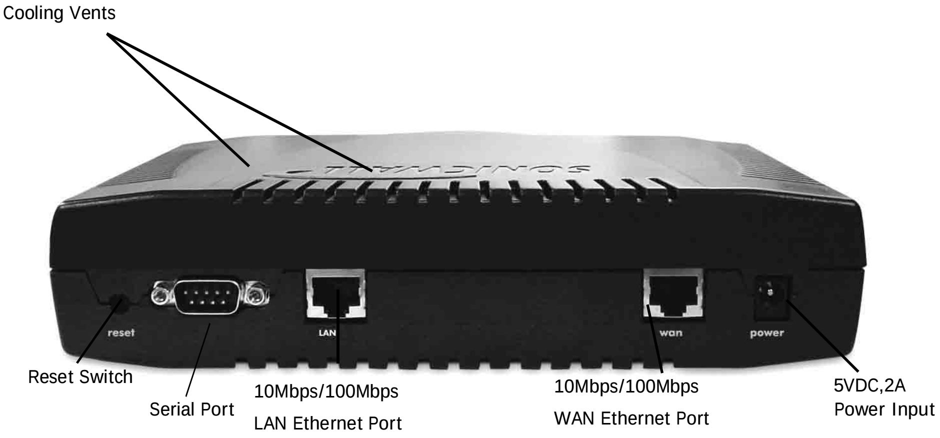
  Lights up when the Twisted Pair port is connected to a 100Mbps hub or switch or directly connected to a computer with a 100Mbps network interface.

- **Activity**

  Flashes when the SonicWALL transmits or receives a packet through the Twisted Pair port.

SonicWALL SOHO3 and TELE3 Back Panel

The SonicWALL SOHO3 back panel is shown below, followed by a description of each item. The SonicWALL TELE3 back panel is identical to the SonicWALL SOHO3.



The SonicWALL SOHO3 and TELE3 Back Panel Description

- **Reset Switch**

  Erases the firmware and resets the SonicWALL to its factory clean state. This can be necessary if you forget the administrator password or the firmware has become corrupt.

- **Serial Port**

  DB-9 RS-232 Serial port for Command Line Interface support.

- **(2) Twisted Pair (10Base-T, 100Base-T) Ethernet Ports**

  (2) Auto switching 10Mbps/100Mbps Ethernet ports provide connectivity for both Ethernet and Fast Ethernet networks. The Ethernet ports connect the SonicWALL to the LAN and WAN using Twisted Pair cable with RJ45 connectors.

- **Power Input**

  Connects to the external power supply which is provided with the SonicWALL SOHO3 and the SonicWALL TELE3. The use of an Uninterruptible Power Supply (UPS) is recommended to protect against damage or loss of data due to electrical storms, power failures, or power surges.

- **Cooling Vents**

  The SonicWALL is convection cooled; an internal fan is not necessary. Do not block the cooling vents on the SonicWALL SOHO3 or the TELE3 side panels.

14 Troubleshooting Guide

This chapter provides solutions for problems that you might encounter when using the SonicWALL. If you are unable to solve your problem, please visit the SonicWALL Tech Support Web site at <http://www.sonicwall.com/support>. There, you will find resources to help you resolve most technical issues, as well as a means to contact one of the SonicWALL Technical Support engineers.

The Link LED is off.

- Make sure the SonicWALL is powered on.
- Make sure the cable connections are secure. Gently moving the cable back and forth should not make the Link LED turn on and off.
- Try replacing the cable with a known good cable.
- Is it the correct cable? Try using a standard Ethernet or crossover cable instead.

A computer on the LAN cannot access the Internet.

- If NAT is enabled, make sure the default router address of the LAN computer is set to the SonicWALL LAN IP Address.
- All computers on the LAN should be able to log into the SonicWALL Management Interface by typing the SonicWALL LAN IP Address into the Location or Go to field from a Web browser. If the SonicWALL authentication screen does not appear, check for Ethernet connectivity problems. Confirm that the computer without Internet access is assigned an IP address in the correct subnet.
- Make sure that the SonicWALL is powered on and responsive.
- If a computer can access the SonicWALL Management Interface, but cannot view Web sites, then check DNS configuration of the computer.
- Try restarting your Internet router and the computer.
- The Internet connection can be down. Disconnect the SonicWALL and try to access the Internet.
- If there are any host devices other than the Internet router connected to the WAN port, they are inaccessible to users on the LAN unless you have configured the SonicWALL Intranet settings.

The SonicWALL does not establish authenticated sessions.

- During initial configuration make sure to change the Management Station's IP address to one in the same subnet as the SonicWALL's, such as "192.168.168.200".
- Check to make sure the Web browser has Java, JavaScript, or ActiveX enabled.
- Make sure the users are attempting to log into the correct IP address. The correct address is the SonicWALL LAN IP Address, and not the NAT Public Address if NAT is enabled.
- Make sure that users are attempting to log in with a valid user name and password.
- Remember that passwords are case-sensitive; make sure the "Caps Lock" key is off.

- If you are using an Internet Explorer browser, you can want to click the **Refresh** button several times to fully load the Java and Java script programs. Also, wait until Java applet has completely loaded before attempting to log in.

The SonicWALL does not save changes that you have made.

- When configuring the SonicWALL, be sure to click **Update** before moving to another window or tab, or all changes will be lost.
- Click **Refresh** or **Reload** in the Web browser. The changes can have occurred, but the Web browser can be caching the old configuration.

Duplicate IP address errors

Duplicate IP address errors occur when the SonicWALL is installed

- Try restarting the router, or restarting LAN computers.
- Make sure the LAN is not connected to the WAN port of the SonicWALL.

Machines on the WAN are not reachable.

- Make sure the Intranet settings in the **Advanced** section are correct.

If these suggestions don't help, please take a look at the current FAQ (Frequently Asked Questions) and Troubleshooting Guide on the SonicWALL Web site:
<http://www.sonicwall.com/support>.

15 Appendices

Appendix A - Technical Specifications

SonicWALL Hardware and Performance

SonicWALL TELE3
SonicWALL SOHO3
SonicWALL PRO 100

- *Processor:* 133Mhz Toshiba TX3927
- *RAM:* 8MB
- *Flash Memory:* 3MB
- *Interfaces:* (2) 10/100Base-T ports (3) 10/100Mbps Ports[4]
- *Concurrent Connections:* 6000
- *Simultaneous VPN Tunnels:* 5[2],10[3], 50[4]
- *Dimensions:* 8.25” x 6.5” x 2”
- *Weight:* 1.1 lb
- *Power:* 100V to 240V AC

SonicWALL PRO 200
SonicWALL PRO 300

- *Processor:* 233Mhz Strong ARM RISC
- *RAM:* 8 MB[5], 16 MB[6]
- *Flash Memory:* 4MB
- *Interfaces:* (3) 10/100Base-T Ports
- *Console:* (1) Serial Port
- *Concurrent Connections:* 30,000[5]; 128,000[6]
- *VPN Tunnels:* 500[5], 1,000[6]
- *Dimensions:* 19” x 8.875” x1.75”
- *Weight:* 6 lbs *Power:* 84V-264V AC
- *Mounting:* Rack Mountable - 3U Rack

[1] All speeds are bi-directional. [2] SonicWALL TELE3 [3] SonicWALL SOHO3 [4] SonicWALL PRO 100 [5] SonicWALL PRO 200 [6] SonicWALL PRO 300

Standards

TCP/IP, UDP, ICMP, HTTP, IPSec, IKE, SNMP, FTP, DHCP, PPPoE

Certifications

FCC, UL, BSMI, VCCI, CSA, ISCA Firewall, ICSA IPSec VPN

Environment

Temperature: 40 - 105°F, 5 - 40°C
Humidity: 5-90% non-condensing

	SonicWALL SOHO3, TELE3, & PRO 100	SonicWALL PRO 200	SonicWALL PRO 300
Firewall			
Firewall Certification	ICSA	ICSA	ICSA
Concurrent Connections	6000	30,000	128,000
Packet Filtering Method	Stateful Packet	Stateful Packet	Stateful Packet
DoS, DDoS Protection	Yes	Yes	Yes
Transparent Mode	Yes	Yes	Yes
Network Address Translation	Yes	Yes	Yes
Port Address Translation	Yes	Yes	Yes
Predefined Services	Yes	Yes	Yes
Customizable Services	Yes	Yes	Yes
Network Access Rules	Yes	Yes	Yes
Number of Users	5-TELE3, 10/50 SOHO3, Unlimited PRO 100	Unlimited	Unlimited
Security Services			
Vulnerability Scanning	Optional	Optional	Optional
Web Content Filtering	Optional	Optional	Optional
Custom Web Blocking	Yes	Yes	Yes
Anti-Virus Management	Optional	Optional	Optional
E-mail Attachment Filtering	EXE, VBS, Custom	EXE, VBS, Custom	EXE, VBS, Custom
Malicious Code Filtering	Java, ActiveX, Proxy, Cookies Digital Certs	Java, ActiveX, Proxy, Cookies Digital Certs	Java, ActiveX, Proxy, Cookies Digital Certs
Network Support			
VPN Client Pass Through	Yes	Yes	Yes
PPPoE Client Support	Yes	Yes	Yes
DHCP Client Support	Yes	Yes	Yes
DHCP Server Support	Yes	Yes	Yes
Total Static Routes	128	128	128
Management			
Management Method	Web Browser	Web Browser	Web Browser
Remote Management	Secure VPN Mgmt	Secure VPN Mgmt	Secure VPN Mgmt
Global Management	SonicWALL GMS	SonicWALL GMS	SonicWALL GMS
SNMP Management	Yes	Yes	Yes
Command Line Interface	Yes	Yes	Yes
Firmware Update Method	Web Browser	Web Browser	Web Browser
Built-in Database Users	100	100	100
Diagnostic Tools	Ping, Trace, NSLookup	Ping, Trace, NSLookup	Ping, Trace, NSLookup
Logging/Reporting	Syslog	Syslog/ViewPoint (Optional)	Syslog/ ViewPoint

	SonicWALL SOHO3, TELE3, & PRO 100	SonicWALL PRO 200	SonicWALL PRO 300
High Availability			
Failover Support	Included	Included	Included
Active-Standby/Mirroring	Yes	Yes	Yes
IPSec VPN			
VPN Encryption	Included TELE3, Optional SOHO3 and PRO 100	Included	Included
Encryption Methods	3DES, DES, ARCFour	3DES, DES, ARCFour	3DES, DES, ARCFour
Authentication	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1
Key Management	IKE, Manual	IKE, Manual	IKE, Manual
VPN Interoperability	IPSec Certified Vendors	IPSec Certified Vendors	IPSec Certified Vendors
VPN Tunnels	TELE3-5,SOHO3-10, PRO 100-50	500	1,000
DES (56-bit) Speed	20 Mbps	26 Mbps	47 Mbps
3DES (168-bit) Speed	20 Mbps	25 Mbps	45 Mbps
Perfect Forward Secrecy	Yes	Yes	Yes
Prevent Replay Attacks	Yes	Yes	Yes
Group VPN Tunnel	Yes	Yes	Yes
User Authentication	RADIUS, SecurID, Internal Database	RADIUS, SecurID, Internal Database	RADIUS, SecurID, Internal Database
PKI/Digital Certificates	Authentication Service	Authentication Service	Authentication Service
VPN Clients Included	Optional	1 License	50 Licenses

Appendix B - 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.

Support Offers

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.

SonicWALL Support 8X5

Designed for customers who need advanced technical support and the additional benefits of ongoing software and firmware updates, SonicWALL Support 8X5 is an annual service that includes

- Factory replacement for defective hardware
- Telephone or electronic technical support during local business hours
- Access to SonicWALL's electronic support and Knowledge Base systems
- All software and firmware updates and upgrades

SonicWALL Support 24X7

For customers with mission-critical network requirements who cannot afford downtime, SonicWALL Support 24X7 is an annual subscription service that offers

- Advanced-exchanged replacement of defective hardware
- Telephone or electronic support, 24 hours, seven days a week
- Enhanced escalation for high priority problems
- Access to SonicWALL's electronic support and Knowledge Base systems

All of SonicWALL Support Services offer a variety of support services to meet your unique needs including fast, responsive service, instant access to electronic support tools, and high quality technical support.

SonicWALL Support Services Features and Benefits

Telephone or Web-based Technical Support. SonicWALL's technical support experts help solve your problems or answer your questions quickly, reducing your risk of Internet attack.

Knowledge Base. Instant access to solutions and documentation provides answers to questions and solves problems electronically.

Firmware/Software Upgrades. Automatic firmware and software upgrades give instant access to new features and capabilities, allowing you to extend your Internet security investment.

Annual Support Agreement. Low, fixed prices for support services allow you to budget accurately and protect you from unexpected technical support expenses.

	SonicWALL Warranty	**SonicWALL Support 8X5**	**Super SonicWALL Support**
Telephone/Web-based technical support	90 days 8:00 a.m. - 5:00 p.m., local time, Monday - Friday	1-year 8:00 a.m. - 5:00 p.m., local time, Monday - Friday	1-year 24 hours by 7 days a week
Hardware Replacement	1 year, return to factory	1 year, return to factory	1 year, advanced exchange
Software/Firmware Updates	90 days	1-year	1-year
Enhanced Escalation			Yes

SonicWALL Support 24X7

Overview

Available for all SonicWALL products, **SonicWALL Support 24X7** includes software/firmware technical support, and factory replacement of defective hardware. Coverage is provided 24 hours a day, seven days a week.

Deliverables

Coverage Hours

Support is provided during standard business hours, 24 hours per day local time, seven days per week, including locally-recognized SonicWALL holidays.

Telephone and Web-based Support

SonicWALL provides technical assistance during standard coverage hours by telephone or through Web-based support tools. A SonicWALL technical specialist works with you to remotely diagnose and identify firmware and hardware not performing to documented specifications. Web-based support includes interactive communication with a SonicWALL technical specialist. SonicWALL also provides general assistance regarding usage and documentation on a limited basis.

Hardware Service

SonicWALL Support 24X7 includes the repair or replacement of failing hardware returned to the SonicWALL factory.

Upon diagnosis of a hardware failure, a SonicWALL technical specialist issues an RMA number and provides instructions for returning the hardware to SonicWALL. SonicWALL ships a replacement appliance to you based upon the RMA information. You are responsible for returning the failed appliance to SonicWALL with 30 days or be charged for the full replacement cost.

SonicWALL does not accept failed appliances without a valid RMA number.

Software/Firmware Support

SonicWALL logs, tracks, prioritizes, and resolves software, firmware and/or documentation bug reports and enhancement requests for software support under this agreement.

SonicWALL Support 24X7 includes priority escalation based on problem severity.

Support for software, firmware, and documentation is limited to the most current version and the immediate prior revision.

Software/Firmware Updates

All software and firmware maintenance releases and updates are included with this agreement. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

SonicWALL Support 24X7 provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

SonicWALL Support 24X7 is an annual service available for sale at the time of product purchase or anytime before warranty expiration.

SonicWALL Support 8X5

Overview

Available for all products, **SonicWALL Support 8X5** includes software/firmware technical support and factory hardware replacement. Coverage is provided during standard business hours.

Deliverables

Coverage Hours

Support is provided during standard business hours, 8:00 a.m. - 5:00 p.m. local time, Monday through Friday, excluding locally-recognized SonicWALL holidays.

Telephone and Web-based Support

SonicWALL provides technical assistance during standard coverage hours by telephone or through Web-based support tools. A SonicWALL technical specialist works with you to remotely diagnose and identify firmware and hardware not performing to documented specifications. Web-based support includes interactive communication with a SonicWALL technical specialist. SonicWALL also provides general assistance regarding usage and documentation on a limited basis.

Hardware Service

SonicWALL Support 8X5 includes the repair or replacement of failing hardware returned to the SonicWALL factory.

Upon diagnosis of a hardware failure, a SonicWALL technical specialist issues an RMA number and provides instructions for returning the hardware to SonicWALL. Upon receipt of the failed appliance, SonicWALL ships a fully functional replacement appliance to you. The replacement appliance is equivalent to a new appliance.

SonicWALL does not accept failed appliances without a valid RMA number.

Software/Firmware Support

SonicWALL logs, tracks, prioritizes, and resolves software, firmware and/or documentation bug reports and enhancement requests for software support under this agreement.

SonicWALL Support 8X5 includes priority escalation based on problem severity.

Support for software, firmware, and documentation is limited to the most current version and the immediate prior revision.

Software/Firmware Updates

All software and firmware maintenance releases and updates are included with this agreement. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

SonicWALL Support 8X5 provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

SonicWALL Support 8X5 is an annual service available for sale at the time of product purchase or anytime before warranty expiration.

Warranty Support - *North America*

Overview

Included with all SonicWALL products, SonicWALL warranty support includes return-to-factory hardware replacement for one year. Warranty Support also includes technical support and software/firmware updates for 90 days. Coverage is provided during normal business hours.

Deliverables

Coverage Hours

Support is provided during standard business hours, 24 hours per day local time, seven days per week, including locally-recognized SonicWALL holidays.

Telephone and Web-based Support

SonicWALL provides technical assistance during standard coverage hours by telephone or through Web-based support tools for 90 days after the date of purchase. A SonicWALL technical specialist works with you to remotely diagnose and identify firmware and hardware not performing to documented specifications. Web-based support includes interactive communication with a SonicWALL technical specialist. SonicWALL also provides general assistance regarding usage and documentation on a limited basis.

Hardware Service

Warranty Support includes the repair or replacement of failing hardware returned to the SonicWALL factory for a period of year following the date of purchase.

Upon diagnosis of a hardware failure, a SonicWALL technical specialist issues an RMA number and provides instructions for returning the hardware to SonicWALL. SonicWALL ships a replacement appliance to you based upon the RMA information. Upon receipt of the failed appliance, SonicWALL ships a fully functional replacement appliance to you. The replacement appliance is equivalent to a new appliance.

SonicWALL does not accept failed appliances without a valid RMA number.

Software / Firmware Support

SonicWALL logs, tracks, prioritizes, and resolves software, firmware and/or documentation bug reports and enhancement requests for software support for a period of 90 days after the date of purchase.

Software / Firmware Updates

All software and firmware maintenance releases and updates are included for 90 days after the date of purchase. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

Warranty Support provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

This warranty is available only in the United States and Canada.

Warranty Support - *International*

Overview

Included with all SonicWALL products, SonicWALL warranty support includes return-to-factory hardware replacement for one year. Warranty Support also includes technical support and software/firmware updates for 90 days. Coverage is provided during normal business hours.

Deliverables

Coverage Hours

Support is provided during standard business hours, 24 hours per day local time, seven days per week, including locally-recognized SonicWALL holidays.

Hardware Service

Warranty Support includes the repair or replacement of failing hardware returned to the SonicWALL factory for a period of year following the date of purchase.

Upon diagnosis of a hardware failure, a SonicWALL technical specialist issues an RMA number and provides instructions for returning the hardware to SonicWALL. Upon receipt of the failed appliance, SonicWALL ships a fully functional appliance. The replacement appliance is equivalent to a new appliance.

SonicWALL does not accept failed appliances without a valid RMA number.

Software / Firmware Updates

All software and firmware maintenance releases and updates are included for 90 days after the date of purchase. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

Warranty Support provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

This warranty applied to products sold in Europe, the Middle East, Africa, Asia, Central and South America.

Appendix C - Introduction to Networking

Overview

This appendix provides a non-technical overview of the network protocols supported by the SonicWALL and includes a discussion of Internet Protocol (IP) addressing.

It can be helpful to review a book on TCP/IP for an overview of protocols such as TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol). The following book is recommended for beginner and intermediate network administrators:

Teach Yourself TCP/IP in 14 Days Second Edition

Timothy Parker, Ph.D

SAMS Publishing

ISBN # 0-672-30885-1

Network Hardware Components

- **Computers** - IBM- compatible, MAC, notebooks, and PDAs
- **Resources** - printers, fax machines, tape backup units, and file storage devices
- **Cables** - crossover, ethernet
- **Connectors** - bridges, routers
- **Network Interface Card (NIC) -** a card installed inside a computer that physically connects a computer to a network and controls the flow of data from the network to the computer. The NIC has a port where the network cable is connected.

Network Types

- **LAN** stands for **Local Area Network**. Local area refers to a network in one location, Local Area Networks connect computers and devices close to each other such as on one floor of a building, one building, or a campus. LANs can connect as few as two computers or as many as 100 computers.
- **WAN** (**Wide Area Network**) connects LANs together. The networks that make up a WAN can be located throughout a country or even around the world. If a single company owns a WAN, it is often referred to as an enterprise network. The Internet is currently the largest WAN.

Firewalls

A firewall is a software or hardware system that prevents unauthorized outside access, theft, deletion, or modification of information stored on a local network. Typically, unauthorized access would be via an organization’s Internet connection.

Gateways

A gateway can be a computer that acts as a connector between a private internal network and another network such as the Internet. A gateway used as a firewall can transmit information from an internal network to the Internet. Also, gateways can examine incoming information and determine if the information is allowed access to the network.

Network Protocols

The method that used to regulate a workstation's access to a computer network to prevent data collisions. The SonicWALL uses the TCP/IP protocol.

- **TCP/IP** - Internet Protocol, or "IP", provides connectionless data transfer over a TCP/IP network. Since IP alone does not provide end-to-end data reliability as well as some other services, other protocols such as TCP (Transmission Control Protocol) can be added to provide these services. In TCP/IP, TCP works with IP to ensure the integrity of the data traveling over the network. TCP/IP is the protocol of the Internet.
- **FTP** - File Transfer Protocol (FTP) is used to transfer documents between different types of computers on a TCP/IP network.
- **HTTP** - HyperText Transfer Protocol (HTTP) is a widely used protocol to transfer information over the Internet. Typically, it is used to transfer information from Web servers to Web browsers.
- **UDP** - User Datagram Protocol (UDP) transfers information using virtual ports between two applications on a TCP/IP network. Slightly faster than TCP, it is not as reliable.
- **DNS** - Domain Name System (DNS) is a protocol that matches Internet computer names to their corresponding IP addresses. By using DNS, a user can type in a computer name, such as www.sonicwall.com, instead of an IP address, such as 192.168.168.168, to access a computer.
- **DHCP** - Dynamic Host Configuration Protocol (DHCP) allows communication between network devices and a server that administers IP numbers. A DHCP server leases IP addresses and other TCP/IP information to DHCP client that requests them. Typically, a DHCP client leases an IP address for a period of time from a DHCP server which allows a larger number of clients to use a set pool of IP addresses.
- **WINS** - Windows Internet Naming System (WINS), used on Microsoft® TCP/IP Networks, matches Microsoft® network computer names to IP addresses. Using this protocol allows computers on the Microsoft® network to communicate with other networks and computers that use the TCP/IP suite.
- **HTTPS** - Secure HyperText Transfer Protocol (HTTPS) is a protocol to transfer information securely over the Internet. HTTPS encrypts and decrypts information exchanged between a Web server and a Web browser using Secure Socket Layer (SSL).
- **SMTP** - Simple Mail Transfer Protocol (SMTP) is used to send and receive e-mail messages. Typically, SMTP is used only to send e-mail while another protocol, POP3, is used to receive e-mail messages.

- **POP3** - Post Office Protocol 3 (POP3) is used to receive e-mail messages and storing messages on a server, referred to as a POP server.
- **ICMP** - Internet Control Messages Protocol (ICMP) reports errors and controls messages on a TCP/IP network. PING uses ICMP protocol to test if a network device is available.

IP Addressing

To become part of an IP network, a network device must have an IP address. An IP address is a unique number that differentiates one device from another on the network to avoid confusion during communication. To help illustrate IP addresses, the following sections compare an IP address to the telephone numbering system, a system that is used every day.

Like a phone number with its long distance "1" and area code, an IP address contains a set of four numbers. While we separate phone number components with dashes, for example 1-408-555-1212, IP address number components are separated by decimal points or dots (called dotted decimal notation), for example 123.45.67.89. Because computers use a binary number system, each number in the set must be less than 255.

There are three components of IP addressing:

- **IP address**
- **Subnet mask**
- **Default gateway**

IP Address

Just as each household or business requires a unique phone number, a networked device (such as a computer, printer, file server, or router) must have a unique IP address. Unlike phone numbers, an IP address requires the entire number when communicating with other devices.

There are three classes of IP addresses: A, B, and C. Like a main business phone number that one can call, and then be transferred through interchange numbers to an individual's extension number, the different classes of IP addresses provide for varying levels of "interchanges" or subnetworks, and "extensions" or device numbers. The classes are based on estimated network size:

- Class A — used for very large networks with hundreds of subnetworks and thousands of devices. Class A networks use IP addresses between 0.0.0.0 and 127.0.0.0.
- Class B — used for medium to large networks with 10–100 subnetworks and hundreds of devices. Class B networks use IP addresses between 128.0.0.0 and 191.0.0.0.
- Class C — used for small to medium networks, usually with only a few subnetworks and less than 250 devices. Class C networks use IP addresses between 192.0.0.0 and 223.0.0.0.

Just as one would go to the phone company for a phone number, there are controlling bodies for IP addresses. The overall controlling body for IP addresses worldwide is InterNIC. Businesses or individuals can request one or many IP addresses from InterNIC. It's a good idea to estimate the network's future growth when requesting the class and number of IP addresses requested.

Subnet Mask

The IP addressing system allows subnetworks or “interchanges” to be created and device numbers or “extensions” to be established within these subnetworks. These numbers are created using a mathematical device called a subnet mask. A subnet mask, like the IP address, is a set of four numbers in dotted decimal notation. Subnet masks typically take three forms:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

The number 255 “masks” out the corresponding number of the IP address, resulting in IP address numbers that are valid for the network. For example, an IP address of 123.45.67.89 and a subnet mask of 255.255.255.0 results in a sub network number of 123.45.67.0 and a device number of 89. The IP address numbers that are actually valid to use are those assigned by InterNIC. Otherwise, anyone could set up IP addresses that are duplicates of those at another company.

The subnet mask used for the network typically corresponds to the class of IP address assigned. If the IP address is Class A, it uses a subnet mask of 255.0.0.0. Class B addresses use a subnet mask of 255.255.0.0, and Class C IP addresses use a subnet mask of 255.255.255.0.

Default Gateway

A default gateway is like a long distance operator. Users can dial the operator to get assistance connecting to the end party. In complex networks with many subnetworks, gateways keep traffic from traveling between different subnetworks unless addressed to travel there. While this helps to keep overall network traffic more manageable, it also introduces another level of complexity.

To communicate with a device on another network, one must go through a gateway that connects the two networks. Therefore, users must know the default gateway IP address. If there is no gateway in the network, use an IP address of 0.0.0.0 in fields that apply to a default gateway.

Network Address Translation (NAT)

NAT hides internal IP addresses by converting all internal host IP addresses to the IP address of the firewall as packets are routed through the firewall. The firewall then retransmits the data payload of the internal host from its own address using a translation table to keep track of which sockets on the exterior interface equate to which sockets on the interior interface. To the Internet, all of the traffic on the network appears to come from the same computer.

Nodes

A node is a device, such as a PC or a printer, on a network with an IP address. The feature chart shows how many node licenses for PCs or printers are included with a SonicWALL Internet Security appliance. The TELE3 has a non-upgradeable 5-node license, but the SOHO3 is upgradeable up to have 10, 50, or an unlimited number of node licenses. The PRO 100, PRO 200, and PRO 300 have an unlimited number of node licenses.

The TELE3, SOHO3-10, and SOHO3-50 allow a maximum of 5, 10, or 50 LAN IP addresses, respectively, to exist on the LAN (Local Area Network). The licenses for the nodes are counted cumulatively, not simultaneously. When the SonicWALL is turned on and configured, the SonicWALL begins to count IP addresses against the license, and continues to count new LAN IP addresses accessing the Internet until the appliance is rebooted.

When a computer or other device connects to the LAN port of the SonicWALL, it is detected via broadcast and stores the computer or other device IP address in memory. If 5, 10, or 50 IP addresses have been stored in the SonicWALL, the SonicWALL does not permit any additional machines to access the Internet. Therefore, the SonicWALL restricts the number of IP addresses on the LAN, not the number of simultaneous connections to the Internet.

If you have fewer than the maximum number of computers or other devices on your LAN, but it appears that the IP license limit is exceeded, download a **Tech Support Report** and review the devices with IP addresses. Rogue devices such as printers are filling up the SonicWALL IP address limit. **Tech Support Reports** are explained in the **Tools** chapter of this manual.

Additionally, computers with two (2) Network Interface Cards (NIC) can take up two IP addresses. You must reconfigure your network to avoid these problems by turning off IP forwarding on Windows® NT or Windows2000® servers using two NICs.

If devices on the LAN receive IP addresses from a DHCP server, see the **DHCP** chapter of this manual.

Appendix D - IP Port Numbers

The port numbers are divided into three ranges: the **Well Known Ports**, the **Registered Ports**, and the **Dynamic and/or Private Ports**.

The **Well Known Ports** range from 0 through 1023.

The **Registered Ports** range from 1024 through 49151.

The **Dynamic and/or Private Ports** range from 49152 through 65535.

Well Known Port Numbers

The **Well Known Ports** are controlled and assigned by the Internet Assigned Numbers Authority (IANA) <http://www.iana.org> and on most systems can only be used by system processes, or by programs executed by privileged users. Many popular services, such as Web, FTP, SMTP/POP3 e-mail, DNS, etc. operate in this port range.

The assigned ports use a small portion of the possible port numbers. For many years the assigned ports were in the range 0-255. Recently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.

Registered Port Numbers

The **Registered Ports** are not controlled by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users.

While the IANA can not control uses of these ports it does list uses of these ports as a convenience.

The **Registered Ports** are in the range 1024-65535.

Visit <http://www.ietf.org/rfc/rfc1700.txt> for a list of IP port numbers.

Appendix E - 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.

From a Windows 95 or 98 computer, do the following:

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 the **Specify an IP Address** radio button.
5. Enter "192.168.168.200" in the **IP Address** field.
6. Enter "255.255.255.0" in the **Subnet Mask** field.
7. Click **OK**, and then click **OK** again.
8. Restart the computer for changes to take effect.

From a Windows2000 computer, do the following:

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 the **Specify an IP Address** radio button.
5. Enter "192.168.168.200" in the **IP Address** field.
6. Enter "255.255.255.0" in the **Subnet Mask** field.
7. Click **OK**, and then click **OK** again.

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. Enter "192.168.168.200" in the **IP address** field.
4. Enter the Subnet Mask address in the Subnet Mask field.
5. Click **OK**.

Follow the SonicWALL Installation Wizard instructions to perform the initial setup of the SonicWALL. Refer to Chapter 2 for instructions on using the Wizard.

Appendix F - Erasing the Firmware

There can be instances when it is necessary to reset the SonicWALL to its factory clean state if the following events happen to the appliance:

- Administrator password is forgotten
- The firmware has become corrupt, and you cannot contact the Management Interface
- The test light comes on and stays on for more than a few minutes.
- During the troubleshooting process, you must start from a “known” state.

Once the firmware is erased, new firmware must be loaded, and the SonicWALL must be reconfigured.

The following procedure erases all settings and reverts the unit to the factory default state. It is necessary to follow the initial configuration procedures detailed in this manual's QuickStart section to reconfigure the SonicWALL. If you need the firmware, download it from <http://firmware.sonicwall.com> or load it from the CD included with the appliance. You can also download firmware by logging into <http://www.mysonicwall.com> as a registered user.

Locating the Reset button on your SonicWALL Internet Security Appliance

SonicWALL SOHO3, PRO 100, TELE3, SOHO 10, SOHO 50, XPRS, SOHO Telecommuter, PRO 200, PRO 300, and newer SonicWALL DMZ models use the small recessed button on the back of the unit for this procedure. If your SonicWALL DMZ unit has a square reset button that is not recessed on the back of the unit, follow the procedure below to locate the blue reset button.

SonicWALL 10 and 50 models, SonicWALL Plus, and older SonicWALL DMZ models have a blue reset button inside. Open the SonicWALL unit by unscrewing the screws on the bottom and gently pulling the top cover off. (The front and back panels remain in place.) Locate the blue button towards the front between the Power, Test, and WAN LEDs.

If your SonicWALL DMZ unit has a circular reset button that is recessed in the back of the unit, then it’s an older DMZ model and you should follow the procedure for locating the reset button inside the unit.

Erasing the Firmware for all Models

1. Turn off the SonicWALL and disconnect all cables to the network.
2. Locate the recessed Reset Switch on the back panel of the SonicWALL.
3. Press and hold the Reset Switch and then apply power to the SonicWALL. Once the Test LED starts to flash, let go of the Reset Switch.

The Test LED flashes for approximately 90 seconds while the firmware is erased. After completing the diagnostic sequence, the Test LED stays lit, indicating that the firmware has been erased. It is normal for the Test LED to stay lit after erasing the firmware. It does not go off until the firmware is installed and loaded into memory by the automatic restart.

4. Log back into the SonicWALL at the default IP address, "http://192.168.168.168". Make sure that the Management Station's IP address is in the same subnet as the SonicWALL--for example, "192.168.168.200".

5. The SonicWALL Management Interface displays a message stating that the firmware has been erased. Click the **Browse** button to locate the SonicWALL firmware file on the Management Station hard drive. Or upload the firmware file that is located on the SonicWALL Companion CD.

6. Reconfigure the SonicWALL as described in Chapter 2.

Appendix G - Securing the SonicWALL

Mounting the SonicWALL PRO 200 and SonicWALL PRO 300

The SonicWALL PRO 200 and SonicWALL PRO 300 are designed to be mounted in a standard 19-inch rack mount cabinet. The following conditions are required for proper installation:

- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application.
- Four mounting screws, compatible with the rack design, must be used and hand tightened to ensure secure installation. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch rack mount cabinet.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.

Appendix H - 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 from 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.

Note: Refer to your Steel Belted RADIUS Administration Guide for complete instructions on adding dictionaries and configuring user privileges.

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**.

   Note: 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 from 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 from 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 on Microsoft 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.

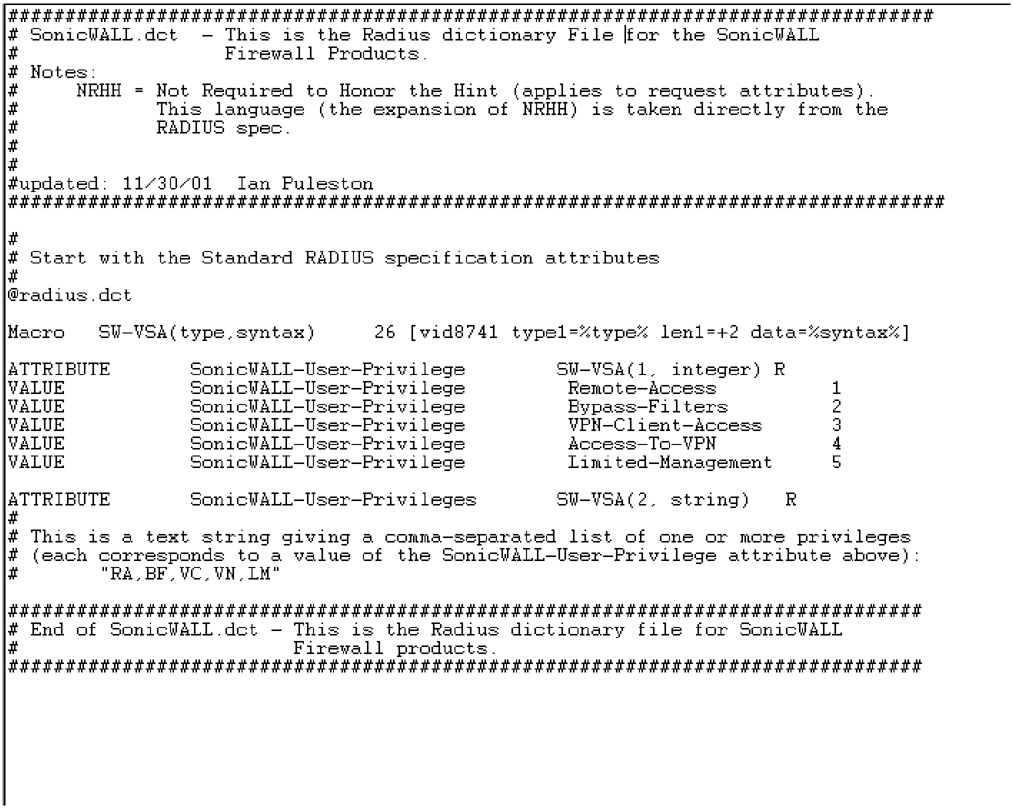
Repeat Steps 5 through 11 for each privilege configured for a policy.

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.

RADIUS Attributes Dictionary

The following is the RADIUS dictionary in the format used with Funk Software’s Steel Belted RADIUS server.



```
#################################################################################
# SonicWALL.dct  - This is the Radius dictionary File for the SonicWALL
#                  Firewall Products.
# Notes:
#     NRHH = Not Required to Honor the Hint (applies to request attributes).
#            This language (the expansion of NRHH) is taken directly from the
#            RADIUS spec.
#
#
#updated: 11/30/01  Ian Puleston
##################################################################################

#
# Start with the Standard RADIUS specification attributes
#
@radius.dct

Macro   SW-VSA(type,syntax)     26 [vid8741 type1=%type% len1=+2 data=%syntax%]

ATTRIBUTE       SonicWALL-User-Privilege        SW-VSA(1, integer) R
VALUE           SonicWALL-User-Privilege         Remote-Access          1
VALUE           SonicWALL-User-Privilege         Bypass-Filters         2
VALUE           SonicWALL-User-Privilege         VPN-Client-Access      3
VALUE           SonicWALL-User-Privilege         Access-To-VPN          4
VALUE           SonicWALL-User-Privilege         Limited-Management     5

ATTRIBUTE       SonicWALL-User-Privileges       SW-VSA(2, string)   R
#
# This is a text string giving a comma-separated list of one or more privileges
# (each corresponds to a value of the SonicWALL-User-Privilege attribute above):
#       "RA,BF,VC,VN,LM"

################################################################################
# End of SonicWALL.dct - This is the Radius dictionary file for SonicWALL
#                        Firewall products.
################################################################################
```

Appendix I - Electromagnetic Compatibility

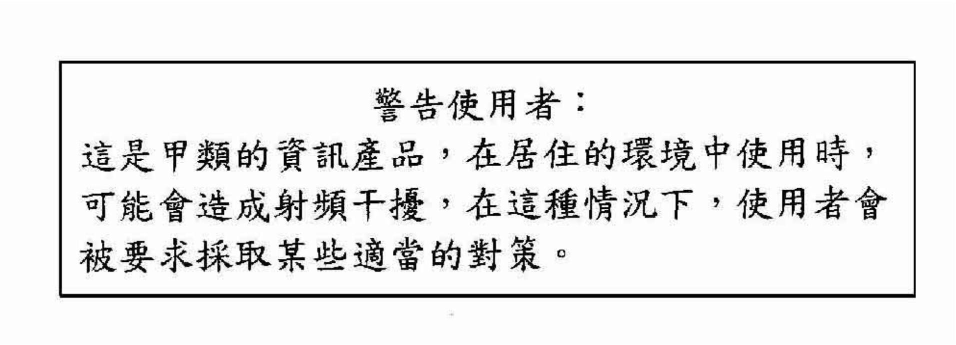
FCC Statement

This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, can cause harmful interference to radio communications. This device has been tested and found to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference, in which case the user, at his own expense, is required to take whatever measures that can be necessary to correct the interference. The cables supplied with this equipment are shielded and created specifically for use on this equipment. The use of shielded I/O cables are mandatory when connecting this equipment to any and all optional peripheral host devices. Failure to do so can violate FCC rules.

Caution*: Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment.*

For more information regarding the above statement, please contact SonicWALL, Inc. at 1160 Bordeaux Dr., Sunnyvale, CA 94089-1209 or 1-408-745-9600.

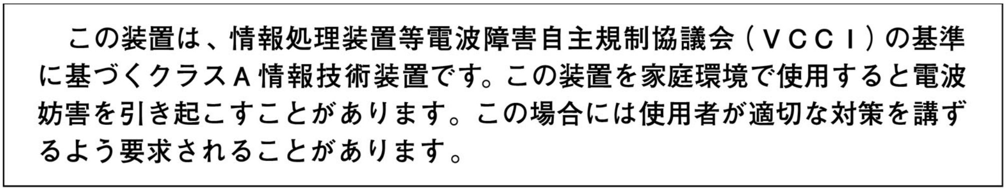
BSMI Statement



警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Statement



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à toutes la norme NMB-003 du Canada.

CISPR 22 (En 55022) Class A

Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Declaration of Conformity

Application of council Directive	**Directive 89/336/EEC (EMC) and 72/23/EEC (LVD)**
Standards to which conformity is declared	**EN 55022 (1998) Class A** **EN 55024 (1998)** **EN 61000-3-2 (1995) + A1, A2, A14** **EN 61000-3-3 (1994)** **EN 60950 (1992) + A1, A2, A4, A11** National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

Lithium Battery Warning

The Lithium Battery used in the SonicWALL Internet security appliance may not be replaced by the user. The SonicWALL must be returned to a SonicWALL authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL Internet security appliance must be disposed of, do so following the battery manufacturer's instructions.

Notes

Notes

Notes

Notes

Notes

Notes

Index

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Tel: (408) 745-9600
Fax: (408) 745-9300
E-mail: info@sonicwall.com
Web: www.sonicwall.com

Part# 232-000219-01
Rev. A 06/02