CONTENTS

Preface

Copyright 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 may 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://support.sonicwall.com>

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 may not apply to you. Where liability may not be limited under applicable law, SonicWALL's

liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you may 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.

Caution - Use of controls or adjustments of performance or procedures other than those specified herein may result in hazardous radiation exposure. (GX650 with Gigabit over Fiber Optics Only)

About This Guide

Thank you for purchasing the SonicWALL Internet Security Appliance. The SonicWALL protects your Local Area Network (LAN) 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 guide covers the installation and configuration of the SonicWALL GX250 and GX650.

Organization of the Guide

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

Chapter 2, **SonicWALL QuickStart Installation**, demonstrates how to connect the SonicWALL to your network and perform the initial configuration.

Chapter 3, **Managing Your SonicWALL**, provides a brief overview of the SonicWALL Web Management Interface.

Chapter 4, **Hardware Description**, illustrates and describes the SonicWALL's front and back panel displays.

Chapter 5, **Network Settings**, describes the configuration of the SonicWALL's IP settings, time and password.

Chapter 6, **Logging and Alerting**, illustrates the SonicWALL's logging, alerting and reporting features.

Chapter 7, **Content Filtering and Blocking**, describes SonicWALL's Web content filtering, including subscription updates and customized Web blocking.

Chapter 8, **Web Management Tools**, provides directions to restart the SonicWALL, import and export settings, upload new firmware, and perform diagnostic tests.

Chapter 9, **Network Access Rules**, explains how to permit and block traffic through the SonicWALL, set up servers, and enable remote management.

Chapter 10, **Advanced Features**, describes advanced SonicWALL settings, such as One-to-One NAT, Automatic Web Proxying and DMZ addresses.

Chapter 11, **DHCP Server**, describes the configuration and setup of the SonicWALL's DHCP server.

Chapter 12, **SonicWALL VPN**, explains how to create a VPN tunnel between two SonicWALLs and from the VPN client to the SonicWALL.

Chapter 13, **SonicWALL High Availability**, SonicWALL High Availability eliminates network downtime by allowing the configuration of two SonicWALLs (one primary and one backup) as a High Availability pair.

Chapter 14, **ViewPoint**, SonicWALL ViewPoint is a software application that creates dynamic, Web-based network reports. SonicWALL ViewPoint generates both real-time and historical reports to offer a complete view of all activity through your SonicWALL Internet security appliance.

Chapter 15, **SonicWALL Options and Features**, presents a brief summary of the SonicWALL's subscription services, firmware upgrades and other options.

Chapter 16, **Hardware Description**, illustrates and describes the SonicWALL's front and back panel displays.

Chapter 17, **Appendices**, additional information about the GX series.

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

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

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

Appendix D, **Securing the SonicWALL**, details the steps necessary to safely mount the SonicWALL on a mounting rack.

Appendix E, **Electromagnetic Compatibility**, 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 SonicWALL's Technical Support engineers.

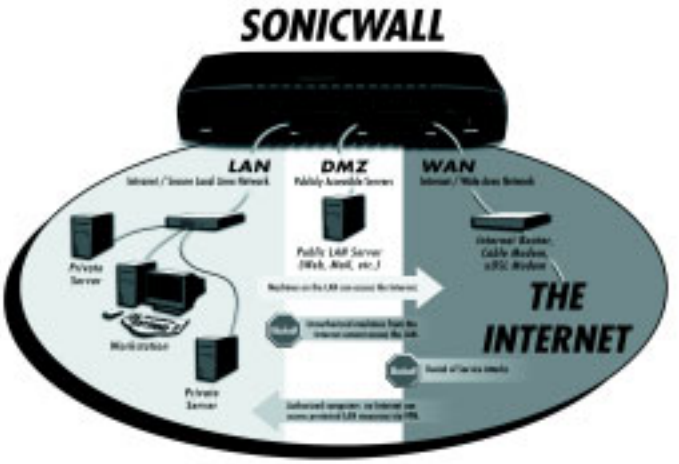
1 Introduction

Your SonicWALL Internet Security Appliance

The SonicWALL is 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. SonicWALL VPN is included with the SonicWALL GX250 and GX650.

The SonicWALL 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.

The following figure illustrates the SonicWALL's security functions.



By default, the SonicWALL allows outbound access from the LAN to the Internet and block 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 on the Internet have full access to the devices on the DMZ.

SonicWALL Internet Security Appliance Features

Internet Security

- **ICSA-Certified Firewall**

  After undergoing a rigorous suite of tests to expose security vulnerabilities, the SonicWALL Internet security appliance has 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 may 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.

- **Auto Update**

  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 send an E-mail with firmware release notes.

- **DMZ Port**

  SonicWALL GX250 and the SonicWALL GX650 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 located on the DMZ are still protected against DoS attacks.

Content Filtering

- **SonicWALL Content Filtering Overview**

  You may use the SonicWALL's Web content filtering to enforce your company's Internet access policies. The SonicWALL blocks specified categories, such as violence or nudity, using a 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 Content Filter List every week to ensure that access restrictions to new and relocated sites are properly enforced.

- **Log and Block or Log Only**

  You may 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's event log. You may view the event log from the SonicWALL's 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 extremely detailed event log information to an external Syslog server. Syslog is the industry-standard method to capture information about network activity.

- **E-mail Alerts**

  The SonicWALL may be configured to send alerts of high-priority events, such as attacks, system errors, and blocked Web sites. When these events occur, alerts may 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's 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.

Installation and Configuration

- **Installation Wizard**

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

- **Online help**

  SonicWALLdocumentation 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 to connect corporate offices and business partners together. By encrypting data, SonicWALL VPN provides private communications between two or more sites without the expense of leased site-to-site lines. SonicWALL VPN comes standard with the SonicWALL the SonicWALL GX250 and the SonicWALL GX650.

- **VPN Client Software for Windows**

  Mobile users with dial-up Internet accounts may 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** and **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

The GX Series of SonicWALL Products

High speed LAN and WAN connections are driving the need for high performance security systems in Internet data centers and large enterprises, but the cost and complexity of currently available gigabit security products has hampered their market acceptance. The new SonicWALL GX Series appeals to organizations seeking Internet security solutions for high-bandwidth networks by offering a scalable solution that integrates performance, reliability and management at a price point not found elsewhere in the market.

All models in the SonicWALL GX Series share a common, scalable chassis, enabling the system to be upgraded over time with additional interfaces, different interface types and higher performance. This unique, scalable system provides enterprise and data center customers with an ability to scale their security solution over time as their bandwidth needs grow.

SonicWALL GX Overview

The Internet boosts business efficiency, improves communications with customers and partners, and allows remote offices and workers to securely connect to the enterprise network. As demand for essential Internet-based services explodes, large central sites and data centers require high performance, integrated security and VPN solutions

designed for the demands of high-bandwidth environments. Security solutions for these sites must meet today's bandwidth requirements as well as provide scalability for future growth.

Internet Security Solution for Enterprises and Data Centers

The SonicWALL GX Series extends SonicWALL's award-winning Internet security solutions to meet the intensive demands of enterprises and data centers. The GX Series delivers industry-leading price/performance in a solution that includes a scalable, robust security platform coupled with a comprehensive management system.

High Performance

The SonicWALL GX Series' high-performance architecture features a maximum firewall throughput of up to 1.0 Gbps and supports up to 500,000 simultaneous connections and 3DES VPN throughput up to 260Mbps to support a maximum of 10,000 VPN tunnels.

Scalability

The chassis-based design of the SonicWALL GX Series provides a scalable path for future performance upgrades, additional interfaces, and different interface types. The SonicWALL GX Series also delivers high availability through failover support and hot swappable power supplies.

Comprehensive Management

The SonicWALL GX Series includes comprehensive security management tools and interface options including Web, SNMP, command line, and global management by SonicWALL GMS. All SonicWALL GX models are bundled with SonicWALL's Global Management System (GMS), which provides an integrated, global security management solution for thousands of SonicWALL Internet security appliances on geographically distributed networks.

Price/Performance Leader

SonicWALL's GX Series extends SonicWALL's industry-leading security technology to meet the demands of high-end security installations. For organizations seeking Internet security solutions for high-bandwidth networks, SonicWALL GX Internet Security appliances deliver an industry leading solution that integrates high performance, reliability, and ease of management.

Features and Benefits of the SonicWALL GX Series

The GX Series Feature Chart

Model	GX250	GX650
Standard Interfaces	(3) 10/100Base-TX	(3) 1000Base-SX
Scalable, Upgradeable Design	20 interfaces	20 interfaces
Firewall Throughput	100 Mbps	1 Gbps
3DES VPN Throughput	100 Mbps	260 Mbps
Simultaneous Connections	250,000	500,000
VPN Tunnels (SAs)	5,000	10,000
High Availability	Yes	Yes
Redundant Power Supplies	Yes	Yes
Management Modes (all included standard)	HTTP, SNMP, CLI, SGMS	HTTP, SNMP, CLI, SGMS
Ethernet Interfaces	Standard	Standard, Fiber (1000-SX), or Copper (1000-baseT) NIC options

- **State-of-the-Art Firewall Security**. SonicWALL GX models use stateful packet inspection technology.
- **High Performance**. SonicWALL GX models support up to 1.0 Gbps firewall throughput and 3DES VPN throughput up to 260Mbps.
- **ICSA Certified**. SonicWALL GX firewalls are certified by the International Computer Security Association (ICSA).
- **IPSec VPN**. SonicWALL VPN, a standard feature on SonicWALL GX models, provides a robust IPSec VPN solution that is compatible with other IPSec VPN gateways, such as Check Point Firewall-1, Cisco PIX, Nortel Contivity and Axent Raptor.
- **Powerful, Scalable Architecture**. SonicWALL GX security systems robust architecture meets the high demands of large-scale security environments and provides a scalable platform for future upgrades.
- **High-Availability**. SonicWALL GX models include high-availability through failover support and dual, hot swappable power supplies.

- **ViewPoint**. SonicWALL ViewPoint is a software application that creates dynamic, Web-based network reports. SonicWALL ViewPoint generates both real-time and historical reports to offer a complete view of all activity through your SonicWALL Internet security appliance.
- **SonicWALL GMS**. SonicWALL GX models include SonicWALL Global Management System (GMS) to enable network administrators to manage their security networks. SonicWALL GMS supports thousands of SonicWALL Internet security appliances from a central location.
- **Industry-Leading Price/Performance**. SonicWALL GX Series security systems deliver scalable, high-performance security, beating existing complex and expensive high-speed security solutions.
- **AutoUpdate**. SonicWALL Internet security appliances maintain the highest level of security by automatically checking for new firmware updates with protection against newly discovered hacker attacks. All firmware updates are FREE for the life of the product.
- **Flexible Management Options**. SonicWALL GX models include multiple management interface options including Web based, SNMP, command line, and SonicWALL GMS.
- **Supports Additional Security Services**. SonicWALL GX models enable administrators to seamlessly add SonicWALL value-added security services including network anti-virus, VPN authentication, vulnerability assessment, and content filtering.

SonicWALL GX Specifications

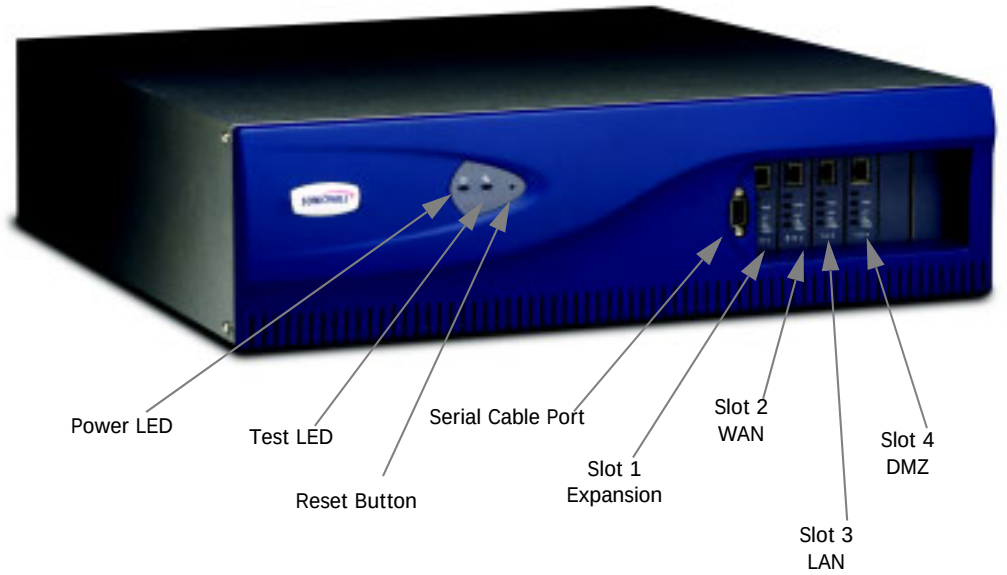
	GX250	GX650
Speeds	Firewall: 100 Mbps VPN: 100 Mbps	Firewall: 1.0 Gbps VPN: 260 Mbps
Maximum Simultaneous Connections - VPN Security Associations	5,000	10,000
Maximum Simultaneous Connections	Three (3) 10/100Base-T (RJ-45) Two (2) expansion slots available for Optional Expansion Cards	Three (3) 1000Base-SX or 1000Base-T
Interfaces	Optional Expansion Cards - Single Port 10/100Base-T Single Port 1000Base-SX Single Port 1000Base-T	
Power	Redundant hot swappable power supplies with PFC 100-240 VAC 50/60 Hz	Redundant hot swappable power supplies with PFC 100-240 VAC 50/60 Hz
Dimensions	19 x 19 x 5.25 inches (3U rack) 48.3 x 48.3 x 13.3 cm Includes 19”rack mounting hardware Weight 30 lb. (13.5 kg.)	19 x 19 x 5.25 inches (3U rack) 48.3 x 48.3 x 13.3 cm Includes 19”rack mounting hardware Weight 30 lb. (13.5 kg.)
Approvals	ICSA Certified, FCC Rules, Part 15, Class A	ICSA Certified, FCC Rules, Part 15, Class A

2 HARDWARE DESCRIPTION

This chapter provides detailed illustrations and descriptions of the SonicWALL GX250 and GX650 front and back panels. Refer to this manual to locate the LEDs, switches, and connectors on the SonicWALL Internet Security Appliances.

SonicWALL GX250 and GX650 Front Panel

The SonicWALL GX250 front panel is shown below, followed by a description of each item. The SonicWALL GX650 is identical to the SonicWALL GX250 except for the GX650 label on the front panel and the types of network interfaces installed.



SonicWALL GX250 and SonicWALL GX650 Front Panel Description

- **Power**

  Lights up green if both power supplies are functioning on the SonicWALL GX250 or SonicWALL GX650. If it is red, one of the power supplies has failed, and an audible alarm also sounds.

- **Test**

  Lights up when the SonicWALL is powered up and performing diagnostic tests for proper operation. These tests take up to 5 minutes. If the Test LED remains lit after this time, the firmware is corrupt and must be reinstalled. This process is described in Appendix C.

- **Serial Port**

  DB-9 RS-232 Serial port for a modem or null-modem cable to support Command Line Interface Management.

There are three network interfaces on the GX250 and GX650 from left to right:

- **WAN**
- **LAN**
- **DMZ**

The GX250 includes three Fast Ethernet network interfaces. The GX650 includes either 1000Base-SX over Fiber or Gigabit Ethernet over Copper network interfaces. A fourth slot for upgrades is available on the GX250.

Three types of network cards are available in the GX series:

- **Fast Ethernet (10/100Base-T)**
- **Gigabit over Fiber (1000Base-SX)**
- **Gigabit over Copper (1000Base-T)**

GX250 Front Panel

Three Fast Ethernet interfaces provide connectivity for either Ethernet and Fast Ethernet networks. The Ethernet ports connect the SonicWALL to the LAN, DMZ, and WAN using category 5 twisted pair cable with RJ-45 connectors. There is an additional slot available for upgrading the appliance. The standard NIC has two LEDs:

- **Link/Activity**

  The **Link** light is green when a twisted pair connection is made to another Ethernet device (usually a switch or a hub) on the port. Note that the device connected to the SonicWALL must support the standard link integrity test. The **Link** LED blinks, indicating **Activity**, when the SonicWALL transmits or receives a packet through the Twisted Pair port onto the network.

- **Network Speed**

  The **Network Speed** LED is not lit if the network speed is 10 Mbps, and the LED is green if the network speed is 100 Mbps.

GX650 Front Panel

Three Gigabit over Fiber or Copper ports provide connectivity for Gigabit networks. Before inserting the cables into the network ports on the fiber optics card, remove the plug from the ports. The 1000Base-SX interface has the following LED lights:

- **Transmit (TX)**

  The **TX** light is lit when the network is transmitting data over the network connection.

- **Receive (RX)**

  The **RX** light is lit when data is received over the network connection.

- **Link**

  The Link LED indicates that the interface is connected to a valid link partner and is receiving link pulses.

The 1000Base-T network interface has the following LEDs:

- **Link**

  The **Link** light is green when a network connection is made to another Ethernet device (usually a hub) on the port.

- **Activity**

  The **Activity** LED blinks, indicating **Activity**, when the SonicWALL transmits or receives a frame.

- **Network Speed**

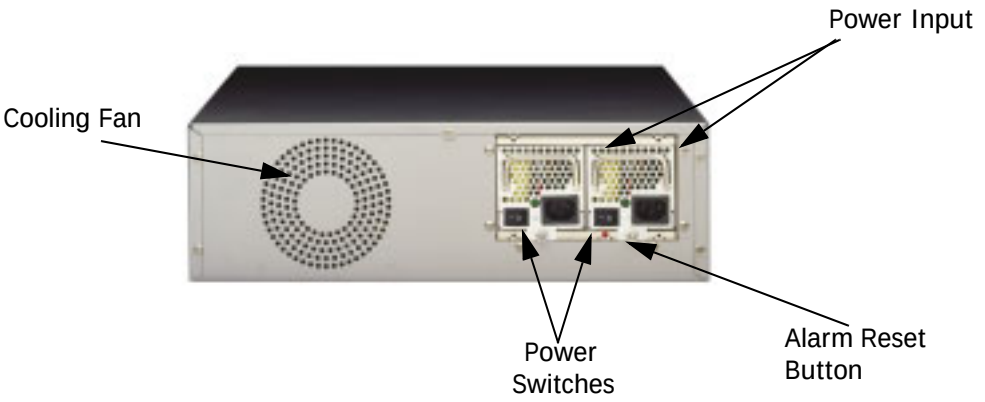
  The **Network Speed** light remains off if there is no connection or if a 10Mbps connection is made. If a 100 Mbps connection is made, the LED is green. If a 1000 Mbps connection is obtained, the LED is yellow.

Reset Switch

Resets the SonicWALL GX250 or the SonicWALL GX650 to its factory clean state. This may be required if you forget the administrator password, or the SonicWALL firmware has become corrupt. Please go to Appendix C for instructions on erasing the SonicWALL firmware.

SonicWALL GX250 and GX650 Rear Panel

The SonicWALL GX250 back panel is shown below, followed by a description of each item. *The SonicWALL GX650 back panel is identical to the SonicWALL GX250.*



SonicWALL GX250 and SonicWALL GX650 Back Panel Description

- **Power Inputs**

  There are two power input receptacles to connect the SonicWALL to the AC power input. The unit comes standard with redundant hot swappable power supplies with active power function correction (100-240 VAC 50/60 Hz).

- **Power Switches**

  One power switch for each hot swappable power supply module. The audible alarm sounds if only one power supply is functioning.

- **Alarm Reset Button**

  The **Alarm Reset** button resets the audible alarm.

- **Cooling Vents**

  The SonicWALL is convection cooled and has an internal fan that is not crucial to the function of the GX, but provides additional cooling to the unit. Do not block the cooling vents on the SonicWALL front and back panels.

3 SonicWALL INSTALLATION

This chapter describes the procedure to install your SonicWALL and perform the initial configuration.

Inspecting the Package

The following items should be included in the package:

- One SonicWALL Internet security appliance
- Two power supplies
- One Category 5 Ethernet crossover cable (labeled "Crossover")
- One Category 5 Ethernet standard cable
- Two fiber optics cables (fiber optics NIC only)
- One Companion CD
- One SonicWALL Internet Security Appliance User's Guide

If an item is missing from the package, contact SonicWALL, Inc. by phone at (408) 752-7819 or submit a Web Support Form at http://www.sonicwall.com/support/.

Overview

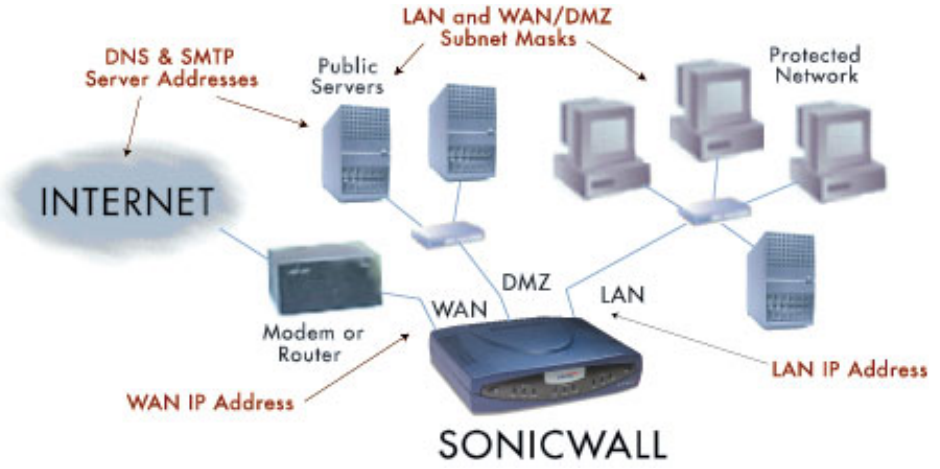
Here are a few helpful guidelines for installing the SonicWALL appliance.

- The **WAN** Ethernet port should be connected to the Internet router or modem.
- The **LAN** Ethernet port should be connected to a network hub or switch on the internal, protected network.
- The **DMZ** Ethernet port, included with the SonicWALL GX250 and GX650, should be connected to publicly accessible servers, such as Web and Mail servers.
- A crossover cable should be used when connecting the SonicWALL directly to another machine or router.
- A standard Ethernet cable should be used when connecting the SonicWALL to a network hub, switch, or modem.
- If using the fiber optics network interface card, remove the plug from the network card to access the network ports on the front of the GX.

***Note**: During the installation, access to the Internet is interrupted. You can minimize this interruption by pre-configuring the SonicWALL before you install it.*

Connecting the SonicWALL to the Network

The following diagram illustrates how the SonicWALL is connected to the network:



The following steps describe integration of the SonicWALL into the network.

Connect the **WAN** Ethernet port on the front of the SonicWALL to the Ethernet port on your Internet router or modem. Use a crossover cable when connecting the SonicWALL to a router. Use a standard Ethernet cable when connecting to a modem or a hub.

Connect the **LAN** Ethernet port to your Local Area Network (LAN). Use a standard Ethernet cable when connecting the SonicWALL to a hub or switch. Use a crossover cable when connecting directly to a computer.

Optional: Connect the **DMZ** Ethernet port to a hub or switch with a standard Ethernet cable. Or connect the **DMZ** port directly to a public server with a crossover cable.

Plug the SonicWALL power supply into an AC power outlet, then plug the power supply output cable into the port on the back labeled **Power**. Use the power adapter supplied with the SonicWALL, do not use another power supply.

***Note**: If you are installing a SonicWALL GX250 or a SonicWALLGX650, connect the SonicWALL to an AC power outlet using a power cable. Then press the power switch to the **On** position.*

Wait for the **Test** LED to turn off. The SonicWALL runs a series of self-diagnostic tests to check for proper operation. During the diagnostic tests, which take about 90 seconds, the **Test** LED remains on.

The SonicWALL is now properly attached to your network.

SonicWALL Installation Checklist

The SonicWALL requires information about the IP address scheme of your network. Your Internet Service Provider (ISP) should be able to provide this information.

- **SonicWALL LAN IP Address**

  The SonicWALL LAN IP address is the address assigned to the SonicWALL LAN port and is used to manage the SonicWALL. It should be a unique IP address from your Local Area Network (LAN) address range.

- **LAN Subnet Mask**

  The LAN Subnet Mask defines the range of IP addresses that are located on your LAN.

- **WAN Gateway (Router) IP Address**

  The WAN Gateway (Router) IP Address is the address of the router that connects your LAN to the Internet. If you have cable or DSL Internet access, the router is probably located at your ISP.

- **DNS Addresses**

  The DNS Addresses are the addresses of Domain Name Servers, either on your LAN or the Internet. These addresses are required for downloading the Content Filter List and for the DNS Name Lookup tool. The DNS addresses should be supplied by your ISP.

- **Mail Server (Optional)**

  The Mail Server address is the name or the IP address of the mail server used to E-mail log messages; it may be a server on your LAN or the Internet. For best results, use the same server used on your LAN for E-mail.

  If you are using Network Address Translation (NAT), then you also need the following information:

- **SonicWALL WAN IP (NAT Public) Address**

  The SonicWALL WAN IP (NAT Public) Address is the valid IP address that your entire network uses to access the Internet. This address should be supplied by your ISP.

- **WAN/DMZ Subnet Mask**

  The WAN Subnet Mask defines which IP addresses are connected to the WAN port of the SonicWALL but not accessed through the WAN router. This subnet mask should be supplied by your ISP.

Performing the Initial Configuration

Setting up your Management Station

All management functions on the SonicWALL are performed from a Web browser. Management can be performed from any computer connected to the LAN port of the SonicWALL. The computer used for management is referred to as the Management Station.

The SonicWALL is pre-configured with the IP address “192.168.168.168", which is used to access it during initial configuration. During the initial configuration, it is necessary to temporarily change the IP address of your Management Station to one in the same subnet as the SonicWALL. For example, set the IP address of your Management Station to “192.168.168.200". It may be necessary to restart the Management Station for the address change to take effect.

***Note**: Appendix A describes how to change the IP address of your Management Station.*

Launching the Web browser

1. Open a Web Browser, such as Internet Explorer 5.0 or Netscape Navigator 3.0 or greater. Then type the default SonicWALL IP address, "192.168.168.168", into the Location or Address field in the Web browser.

***Note**: Your Web browser must be Java-enabled and support HTTP uploads in order to fully manage SonicWALL. Netscape Navigator 3.0 and above is recommended.*

The first time you contact the SonicWALL, the SonicWALL **Installation Wizard** automatically launches and begins the installation process.

The SonicWALL **Installation Wizard** simplifies the initial installation and configuration of the SonicWALL. The **Wizard** provides a series of menu-driven

instructions for setting the administrator password and configuring the settings necessary to access the Internet.

***Note**: To bypass the Wizard, click **Cancel**. Then log into the SonicWALL's **Management Interface** by entering the User Name "admin" and the Password "password".*

To configure your SonicWALL appliance, read the instructions on the Wizard's **Welcome** window and click **Next** to continue.

Settting the Password

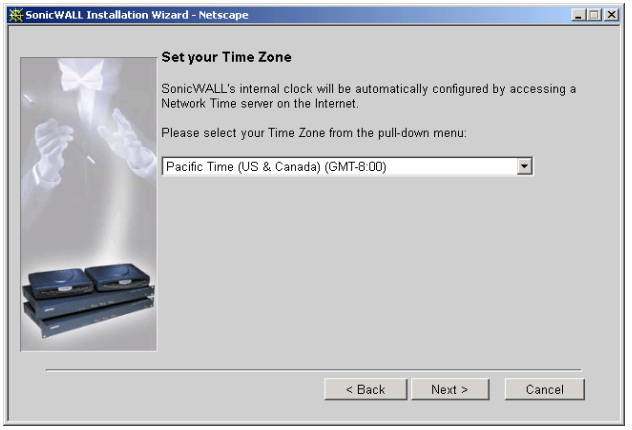
***Note**: The security of the SonicWALL depends on the secrecy of the administrator's password; it is very important to choose a password which cannot be easily guessed by others.*

2. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields.

This window also displays the **Use SonicWALL Global Management System** checkbox. SonicWALL Global Management System (SonicWALL GMS) is a web browser-based security management system. **SonicWALL GMS** allows enterprises and service providers to monitor and manage hundreds of remote SonicWALLs from a central location.

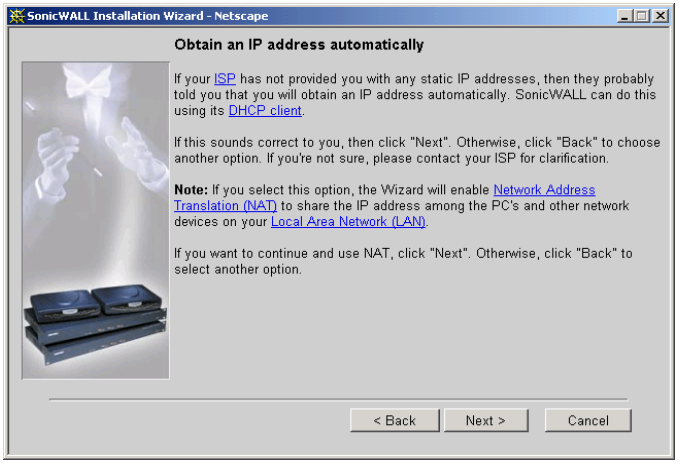
3. Leave the **Use Global Management System** checkbox unchecked unless your SonicWALL is remotely managed by SonicWALL GMS. Click **Next** to continue.

Setting the Time and Date



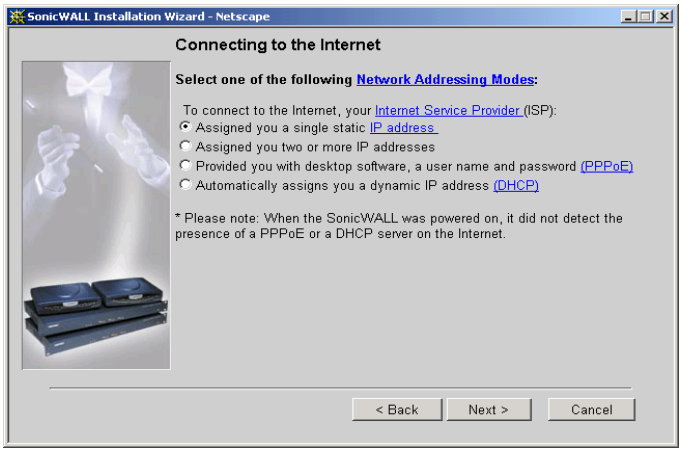
4. From the pull-down menu, select the appropriate **Time Zone**. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next** to continue.

Confirming Network Information



5. Confirm that you have the proper network information needed to configure the SonicWALL to access the Internet. Click the hyperlinks for definitions of the networking terms. Click **Next** to proceed to the next step.

Selecting Your Internet Connection

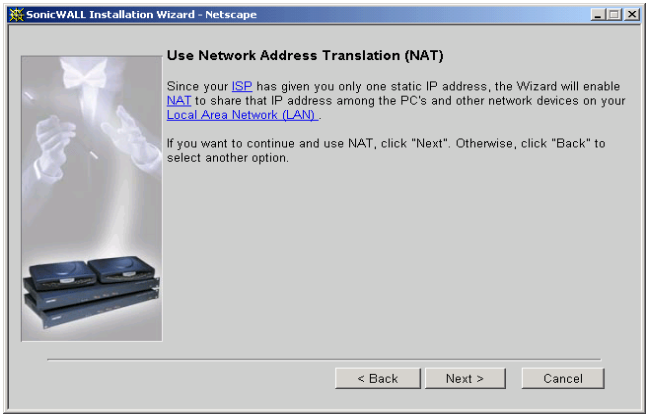


The SonicWALL supports four network addressing modes: **NAT Enabled**, **Standard**, **NAT with PPPoE**, and **NAT with DHCP Client**. Select the appropriate option in the **Connecting to the Internet** window.

6. Select the first option if your ISP has provided you with a single, valid IP address. If you select the first option, your SonicWALL enables **NAT**. Now go to **Step 8**.
7. Select the second option if your ISP has provided you with two or more IP addresses. Either NAT or Standard mode can be enabled if your network has two or more valid IP addresses. If you select the second option, go to **Step 11**.
8. Select the third option, **Provided you with desktop software, a user name, and password (PPPoE)**, if your ISP requires user name and password authentication as well as the installation of login software. If you select the third option, go to **Step 12**.
9. Select the fourth option, **Automatically assigns you a dynamic IP address (DHCP)**, if your ISP automatically assigns you an IP address from their DHCP server. Your SonicWALL enables **NAT with DHCP Client**, a typical network addressing mode for cable and DSL users. If you select the fourth option, go to **Step 13**.

Confirming Network Address Translation (NAT) Mode

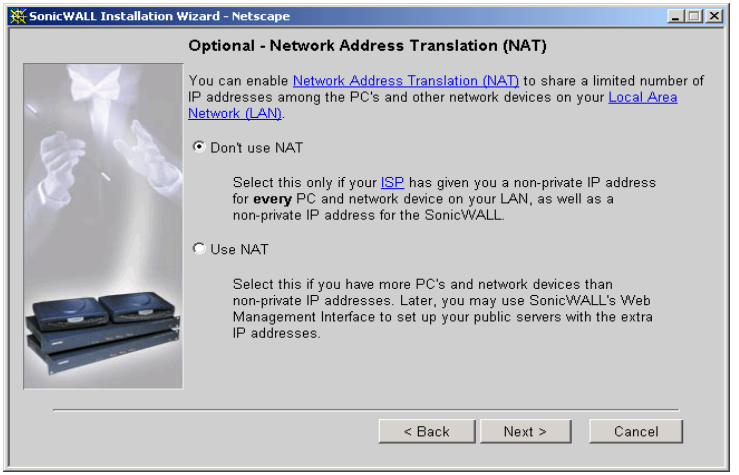
If you select the first option in the **Connecting to the Internet** window, the **Use Network Address Translation (NAT)** window is displayed.



The **Use Network Address Translation (NAT)** window verifies that the SonicWALL has a registered IP address. To confirm this, click **Next** and go to **Step 10**.

Selecting Standard or NAT Enabled Mode

If you selected the **Assigned you a single static IP Address** option in **Step 6**, the **Optional-Network Address Translation** window is displayed.



10. The **Optional-Network Address Translation (NAT)** window offers the ability to enable NAT. Select **Don't Use NAT** if there are enough static IP addresses for your SonicWALL, all PCs, and all network devices on your LAN. Selecting **Don't Use NAT** enables the **Standard** mode. Select **Use NAT** if valid IP addresses are in short supply or to hide all devices on your LAN behind the SonicWALL valid IP address. Click **Next** to continue.

Configuring WAN Network Settings

If you selected either **NAT** or **Standard** mode, the **Getting to the Internet** window is displayed.

11. Enter the valid IP address provided by your ISP in the **Getting to the Internet** window. Enter the **SonicWALL WAN IP Address**, **WAN/DMZ Subnet Mask**, **WAN Gateway (Router) Address**, and **DNS Server Addresses**. Click **Next** to continue. If NAT is disabled, go to **Step 13**. If **Standard** mode is selected, go to **Step 14**.

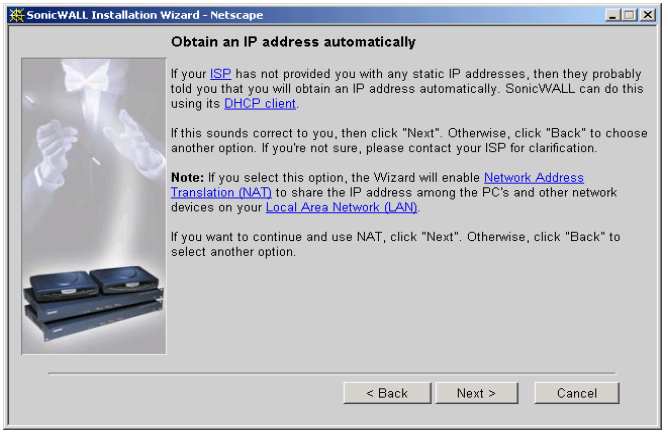
Setting the User Name and Password for PPPoE

If you select **NAT with PPPoE** in the **Connecting to the Internet** window, the **SonicWALL ISP Settings (PPoE)** window is displayed.

12. Enter the **User Name** and **Password** provided by your ISP. The **Password** is case-sensitive. Click **Next** and go to **Step 13**.

Confirming DHCP Client Mode

If you select **NAT with DHCP Client** in **Step 6**, the **Obtain an IP address automatically** window is displayed.

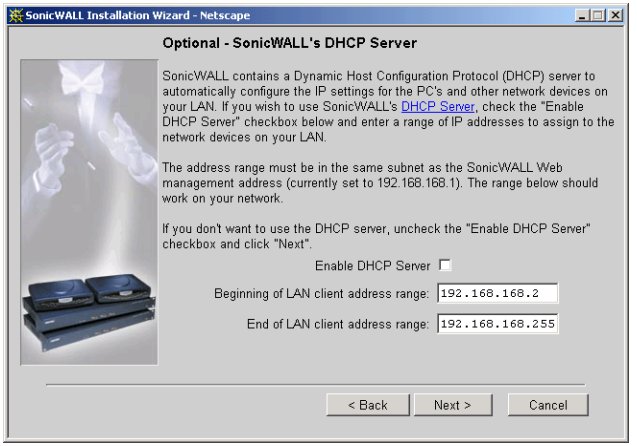


13. The **Obtain an IP address automatically** window states that the ISP dynamically assigns an IP address to the SonicWALL. To confirm this, click **Next** and go to **Step 15**.

Configuring LAN Network Settings

14. The **Fill in information about your LAN** window allows the configuration of the **SonicWALL LAN IP Address** and the **LAN Subnet Mask**.The **SonicWALL LAN IP Address** is the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL work for most networks. Enter the SonicWALL LAN settings and click **Next** to continue.

Configuring the SonicWALL DHCP Server



15. The **Optional-SonicWALL's DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically configures the IP settings of computers on the LAN. To enable the DHCP server, check the **Enable DHCP Server** checkbox, and specify the range of IP addresses that are assigned to computers on the LAN.

    If the **Enable DHCP Server** checkbox is not checked, the DHCP Server is disabled. Click **Next** to continue.

Configuration Summary

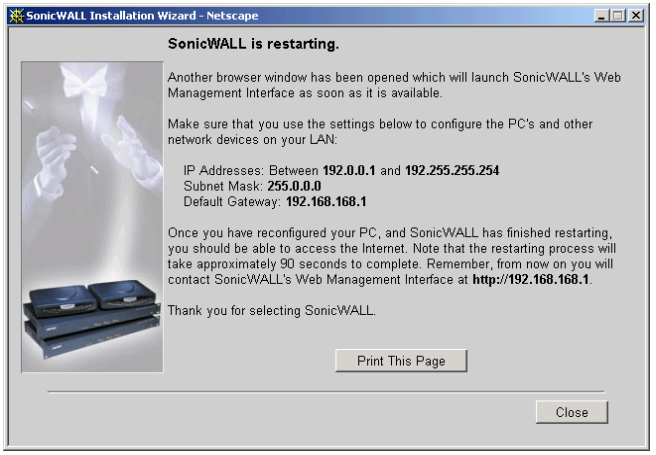
16. The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. If you want to modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next** to proceed to the **Congratulations** window.

Congratulations

***Note**:The new SonicWALL LAN IP address, displayed in the Congratulations window, is used to login and manage the SonicWALL.*

17. Click **Restart** to restart the SonicWALL.

Restarting



***Note**:The final window provides important information to help configure the computers on the LAN. Click **Print this Page** to print the window information.*

The SonicWALL takes 90 seconds to restart. During this time, the yellow **Test** LED is lit. Click **Close** to exit the SonicWALL Wizard.

18. Reset the IP address of the Management Station according to the information displayed in the final window of the **Installation Wizard**.

19. Log into the SonicWALL Management Interface. Once the SonicWALL restarts, contact the SonicWALL Web Management Interface at the new **SonicWALL LAN IP address**. Type the **User Name** “admin” and enter the new administrator password to log into the SonicWALL.
20. Register the SonicWALL. The **Status** window in the SonicWALL **Web Management Interface** displays a link to the online registration form. Registering the SonicWALL provides access to technical support, software updates, and information about new products. Once registered, you receive a free one-month subscription to the SonicWALL **Content Filter List** and a one month trial of SonicWALL Network Anti-Virus.

4 MANAGING YOUR SONICWALL

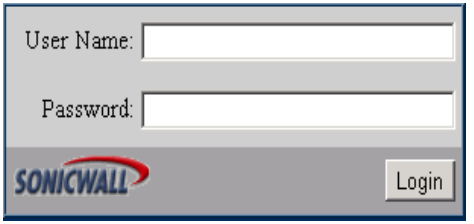
This chapter contains a brief overview of SonicWALL management commands and functions. The commands and functions are accessed through the SonicWALL Web Management Interface. The configuration is the same for all SonicWALL Internet security appliances; any exceptions are noted.

Log into the SonicWALL From a Web Browser

You may 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**: In order to manage the SonicWALL, your Web browser must have Java and Java applets enabled and support HTTP uploads. Netscape Navigator 3.0 and above is recommended. You may download Netscape Navigator at <http://www.netscape.com>.*

1. Open a Web browser, either Netscape Navigator 3.0 or greater, or Internet Explorer 5.0. Type the SonicWALL's 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.



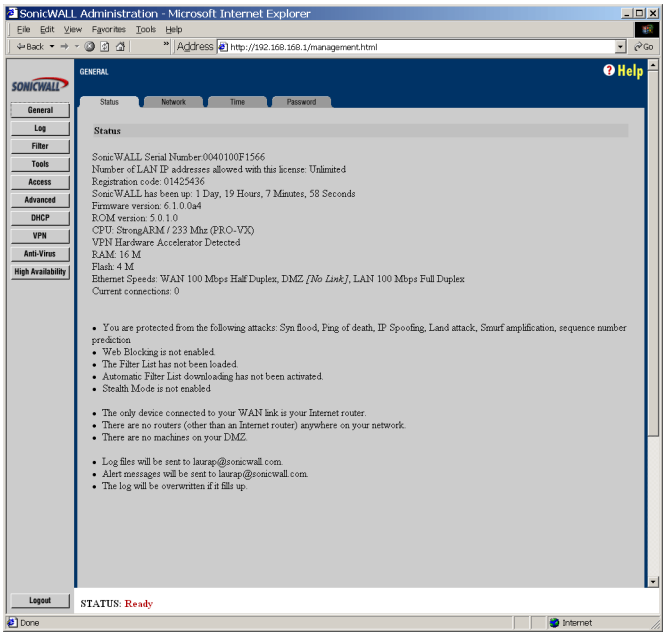
2. Type "admin" in the **User Name** field and the password you defined in the Installation Wizard in the **Password** field. Then click **Login**.

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

If you cannot login to the SonicWALL, it may that 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 logging 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 may be increased on the **Password** tab in the **General** section.

3. Passwords are case-sensitive. Enter the password exactly as defined and click **Login**.



***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 **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, it is necessary to login 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 displays the status of your SonicWALL. It contains an overview of the SonicWALL's 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-width management is now available on SonicWALL appliances using the CLI (Command Line Interface) feature. SonicWALL Internet security appliances can now 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 Frost v.90 modem. CLI communication requires the following modem settings:

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

After the modem is accessed, a telnet 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 Zmodem file transfer.
- **Import** - imports preferences from the SonicWALL using Zmodem file transfer.
- **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 Zmodem file transfer protocol.

The SonicWALL general management and configuration instructions are divided into the following 8 chapters:

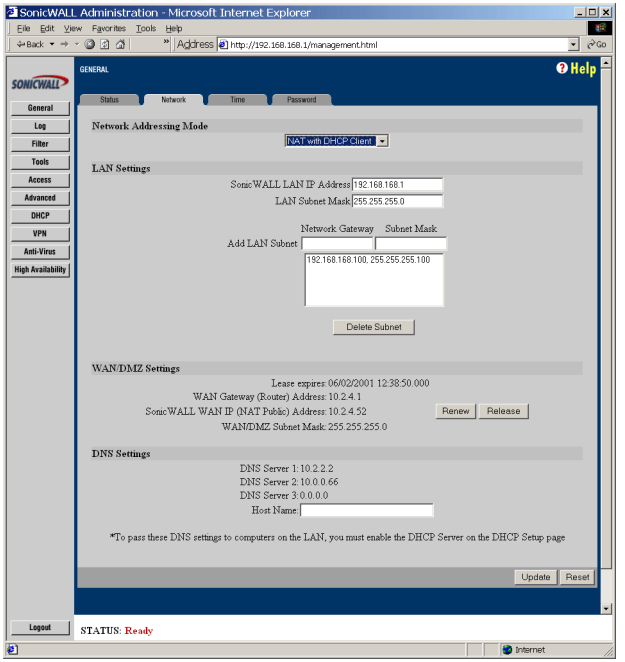
- **Network Settings**
- **Logging and Alerting**
- **Content Filtering and Blocking**
- **Web Management Tools**
- **Network Access Rules**
- **Advanced Features**
- **DHCP Server**
- **SonicWALL VPN**
- **High Availability**
- **ViewPoint**

These chapters describe all the commands and functions necessary to manage your SonicWALL.

5 NETWORK SETTINGS

This chapter describes the configuration of the SonicWALL **Network Settings**. The **Network Settings** include the SonicWALL IP settings, the administrator password, and the time and date.

To configure the SonicWALL **Network Settings**, click **General** on the left side of the browser window, and then click the **Network** tab at the top of the window.



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 your network's private IP addresses to the SonicWALL's single, valid IP address. 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."

WAN Settings

- **WAN Gateway (Router) Address**

  The 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** or **NAT with PPPoE** 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/DMZ Subnet Mask**

  The **WAN/DMZ 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** or **NAT with PPPoE** mode, the WAN/DMZ Subnet Mask is assigned automatically.

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

DNS Settings

- **DNS Servers**

  DNS Servers, or Domain Name 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's 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 need to 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 port and is used for management of the SonicWALL.
3. Enter your network's 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 may be 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 the **Update** button. 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 may 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

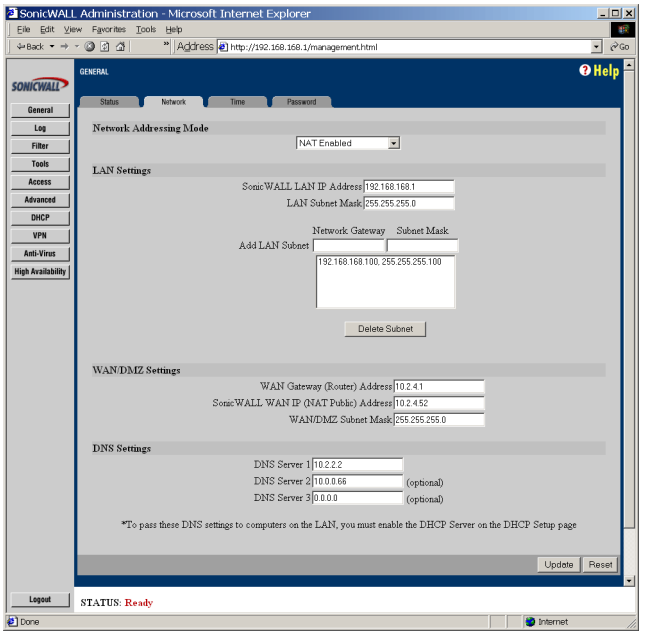
192.168.0.0 - 192.168.255.255

***Note**: If your network address range uses valid TCP/IP addresses, Internet sites within that range will not be 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 will not be 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.



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's LAN port and is used for management of the SonicWALL.
3. Enter your network's 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. Use the **Add LAN Subnet** feature if you have multiple subnets on your network.
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/DMZ 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.

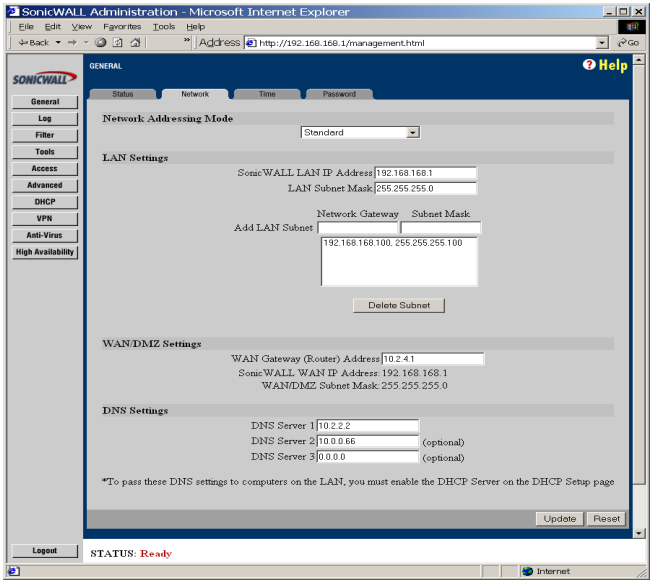
If you enable Network Address Translation, designate the **SonicWALL LAN IP Address** as the gateway address for computers on your LAN. Consider the following example:

- The SonicWALL **WAN Gateway (Router) Address** is "100.1.1.1".
- The SonicWALL **WAN IP (NAT Public) Address** is "100.1.1.25".
- 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**, should be the gateway or router address for all computers on the LAN.

Multiple LAN Subnet Mask Support

Firmware 6.1.0.0 supports multiple subnet masks on the LAN without the use of a second router. Click **General** on the web management interface and then select the **Network** tab. Type in the LAN subnet address into the **Subnet Mask** field and click **Update**. The subnet mask address appears in the list of subnet addresses in the **LAN Settings** section.

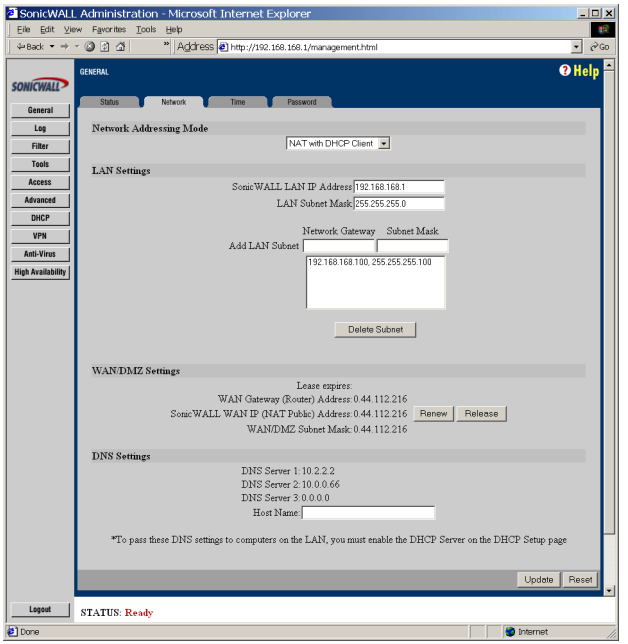


NAT with DHCP Client Configuration

The SonicWALL may receive an IP address from a DHCP server on the Internet. If your ISP did not provide you with a valid IP address, but instructed you 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.



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's LAN port and is used for management of the SonicWALL.
3. Enter your network's 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 the **Update** button. 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 / DMZ Subnet Mask**, and **DNS Servers** is obtained from a DHCP server on the Internet.

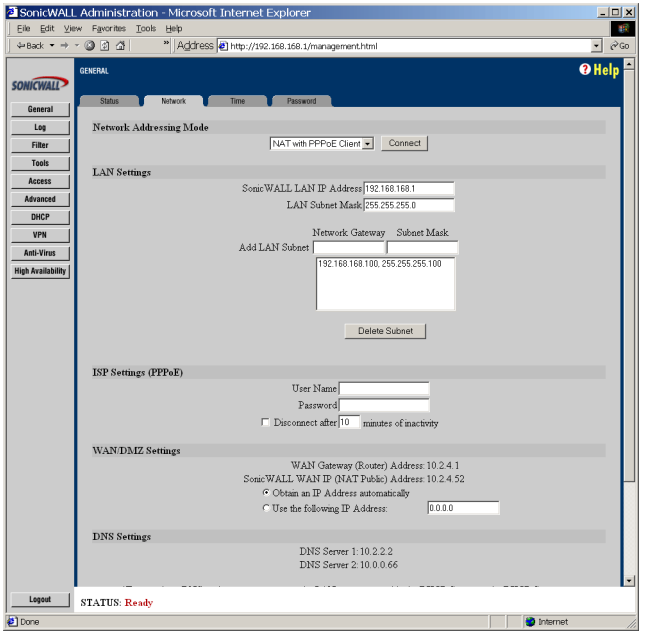
***Note**: The SonicWALL does not relay DNS settings to the LAN; you must enable and configure the SonicWALL's DHCP server or manually configure your computers' DNS settings to obtain DNS name resolution.*

NAT with PPPoE Configuration

The SonicWALL may 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.

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



5. 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's LAN port and is used for management of the SonicWALL.

6. Enter your network's 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. If you have multiple subnets on your network, add the addresses using the **Add LAN Subnet** field.
7. Enter the user name provided by your ISP in the **User Name** field. The user name identifies the PPPoE client.
8. Enter the password provided by your ISP in the **Password** field. The password authenticates the PPPoE session. This field is case sensitive.
9. Check the **Disconnect after __ Minutes of Inactivity** checkbox 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 may range from 1 to 99 minutes.
10. If your ISP does not provide you with an IP address, select **Obtain IP Address automatically**. If your ISP does provide you with a static ISP address, select **Use the following IP address**, and type in the IP address provided into the IP address field. Be sure to type it in exactly as it is provided to you.
11. Click the **Update** button. 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 should be 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/DMZ 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's DHCP server or manually configure your computers' DNS settings to obtain DNS name resolution.*

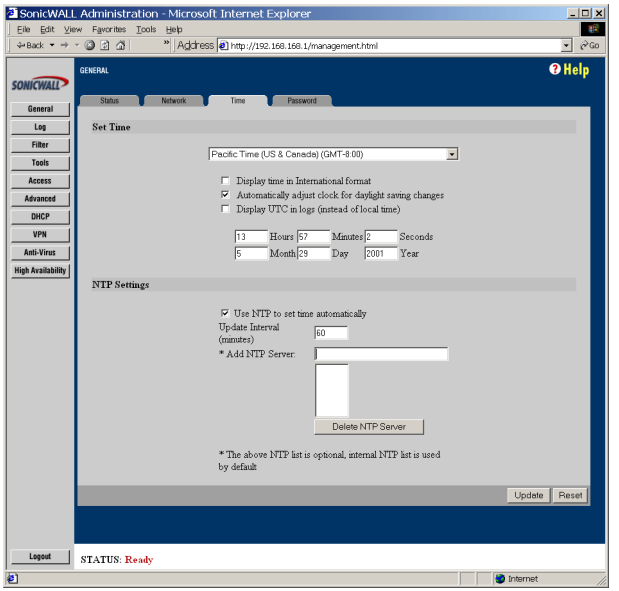
Restart the SonicWALL

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 may 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's LAN IP Address, you also need to change the Management Station's IP address to be in the same subnet as the new LAN IP address.*

Setting the Time and Date

1. Click the **Time** tab at the top of the browser window.



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.

2. Select your time zone from the menu and check the box **Use NTP to set time automatically**. Checking the box allows the SonicWALL to automatically set the local time using **Network Time Protocol (NTP)**.

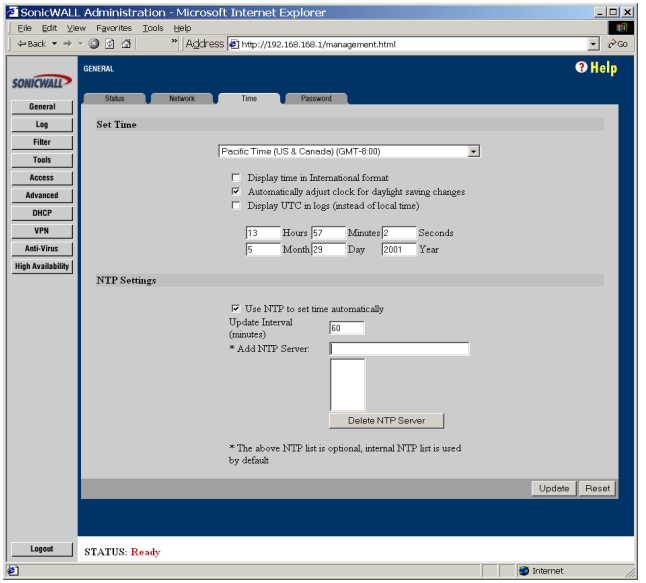
You may also enable automatic adjustments for daylight savings time, use universal time (UTC) rather than local time, and display the date in International format, with the day preceding the month.

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

NTP Settings

Check the box **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL clock. You may also set the **Update Interval** for the NTP server to synchronize the time in the SonicWALL. The default value is 60 minutes. Additionally, it is now possible to add NTP servers to the SonicWALL for time synchronization. This is an optional feature. If there are no NTP Servers added, a predefined list of recognized NTP servers is used. Many atomic clock utilities are

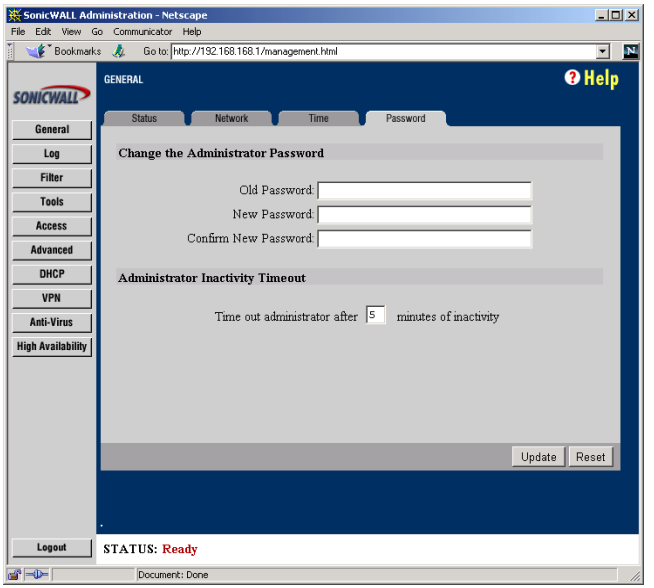
available on the Internet. To remove an NTP server, highlight the IP address and click **Delete NTP Server**.



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

1. Click the **Password** tab at the top of the window.



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

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

If the password is not entered exactly the same in both **New Password** fields, the operation fails. This is done to prevent mistyping a password and getting accidentally locked out of the SonicWALL.

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

Setting the Administrator Inactivity Timeout

The **Administrator Inactivity Timeout** setting allows you to extend the period of inactivity that may elapse before you are automatically logged out of the Web Management Interface. The SonicWALL is preconfigured to logout 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.*

Set the inactivity timeout by entering the desired number of minutes in the **Administrator Inactivity Timeout** section and then click **Update**. The Inactivity Timeout may range from 1 to 99 minutes. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

6 LOGGING AND ALERTING

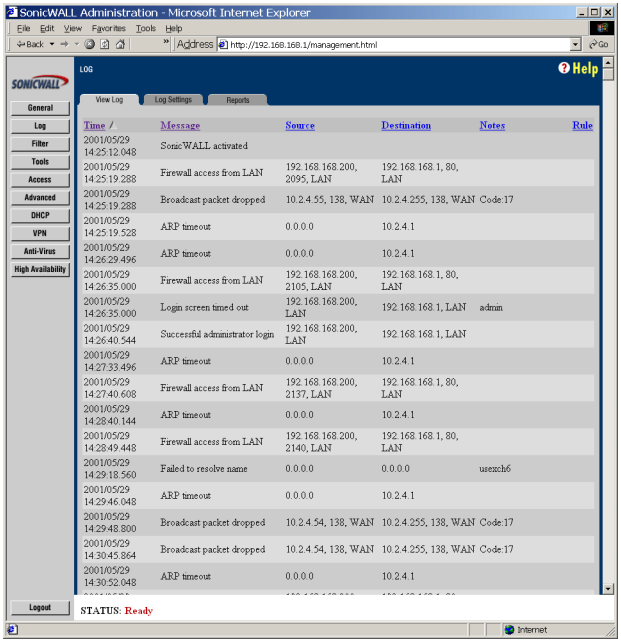
This chapter describes the SonicWALL's logging, alerting and reporting features, which may be viewed in the **Log** section of the SonicWALL Web Management Interface.

View Log

The SonicWALL maintains an **Event** log which displays potential security threats. This log may be viewed with a browser using the SonicWALL Web Management Interface, or it may be automatically sent to an E-mail address for convenience and archiving.

The SonicWALL can also 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.

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



The log is displayed in a table and is sortable by column. Depending on your Web browser, you should be able to copy entries from the log and paste them into documents. Or you may use the E-mail Log function to E-mail the SonicWALL event log.

Each log entry contains the date and time of the event and a brief message describing the event. Some log entries contain additional information.

SonicWALL Log Messages

- **TCP, UDP, or ICMP packets droppe**d

  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 machine attempts to connect to the blocked site or newsgroup, a log event is displayed. The machine'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	g=Satanic/cult
b=Partial Nudity	h=Drug Culture
c=Full Nudity	i=Militant/extremist
d=Sexual Acts	j=sex education
e=gross depictions	k=Gambling/illegal
f=intolerance	l=alcohol/tobacco

- **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.

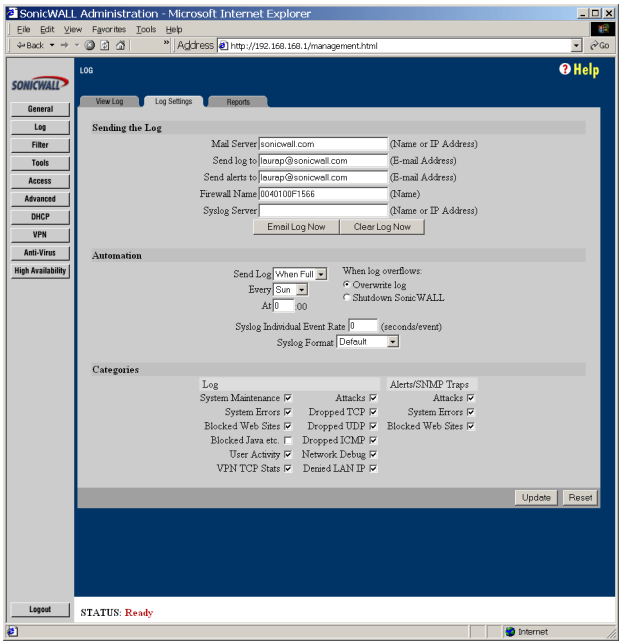
- **Ping of Death, IP Spoof, and SYN Flood Attacks**

  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 at the top of the window.



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 be 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's 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's 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 may be used to sort, analyze, and graph the **Syslog** data. To use ViewPoint for reporting log events, see Chapter 14 for configuration of the SonicWALL.

   Enter the Syslog server name or IP address in the **Syslog Server** field. This field requires restarting the SonicWALL for the change to take effect.

6. **E-mail Log Now** - Clicking **Email 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 **Weekly** or **Daily** 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 without being logged.

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

- **System Maintenance**

  When enabled, log messages showing general system activity, such as administrator logins, automatic downloads of the **Content Filter Lists**, and system activations, is displayed.

- **System Errors**

  When enabled, log messages showing problems with DNS, E-mail, and automatic downloads of the Content Filter List are displayed.

- **Blocked Web Sites**

  When enabled, log messages showing Web sites or newsgroups blocked by the Content Filter List or by customized filtering are displayed.

- **Blocked Java**, **ActiveX**, **and Cookies**

  When enabled, log messages showing Java, ActiveX, and Cookies, which are blocked by the SonicWALL, are displayed.

- **User Activity**

  When enabled, log messages showing successful and unsuccessful login attempts are displayed.

- **VPN TCP Stats**
- **Attacks**

  When enabled, log messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing, are displayed.

- **Dropped TCP**

  When enabled, log messages showing blocked incoming TCP connections are displayed.

- **Dropped UDP**

  When enabled, log messages showing blocked incoming UDP packets are displayed.

- **Dropped ICMP**

  When enabled, log messages showing blocked incoming ICMP packets are displayed.

- **Network Debug**

  When enabled, log messages showing NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems are displayed. **Network Debug** is intended for experienced network administrators.

- **Denied LAN IP**

When checked, any denied TCP or UDP packets from the LAN network are logged.

Alert / SNMP Traps

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

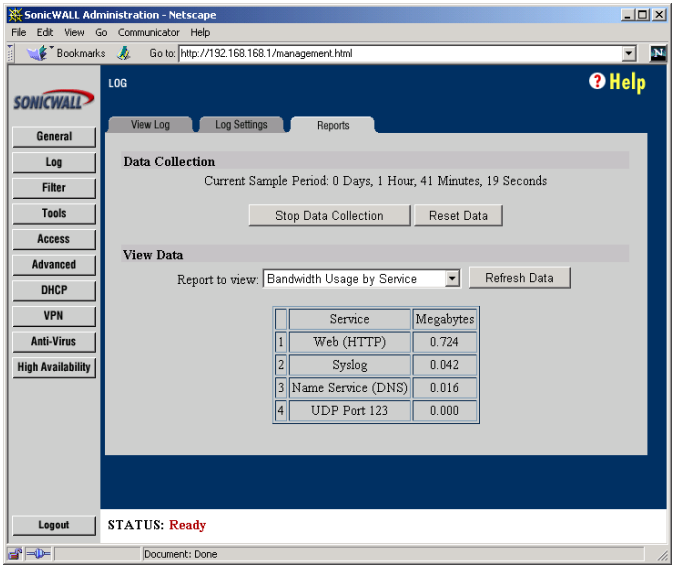
- **Attacks**
  When enabled, log entries categorized as **Attacks** generates an alert message.
- **System Errors**
  When enabled, log entries categorized as System Errors generates an alert message.
- **Blocked Web Sites**
  When enabled, log entries categorized as Blocked Web Sites generates an alert message.

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

Log 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 at the top of the window.



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 that site during the current sample period.

The **Web Site Hits** report can help ensure 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 may choose to block these 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

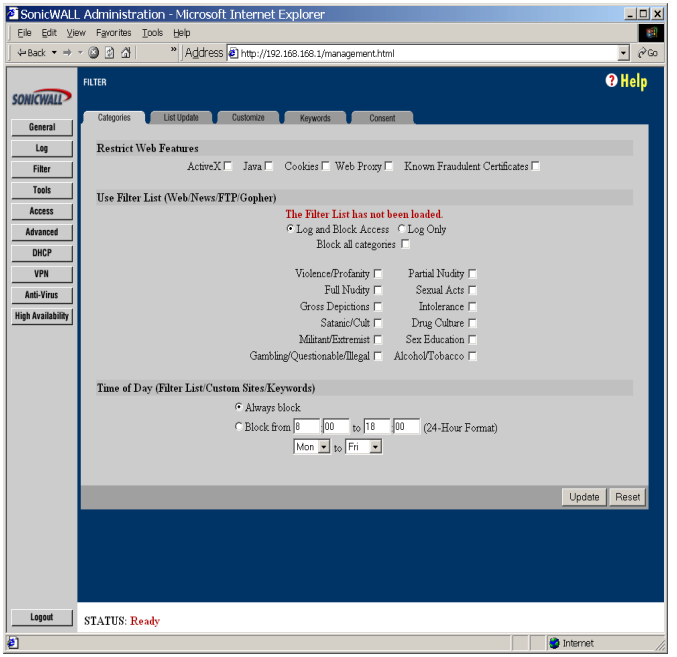
Selecting **Bandwidth Usage by Service** from the **Display Report** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

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 may choose to block these services.

7 CONTENT FILTERING AND BLOCKING

This chapter describes the SonicWALL content filtering features which are configured in the **Filter** section of the SonicWALL Web Management Interface. Content Filtering and Blocking records Web site blocking by Filter List category, domain name, and keyword, and provides instructions to update the SonicWALL Content Filter List.

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



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

Configure the following settings in the **Categories** window:

Restrict Web Features

- **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** checkbox to block ActiveX controls.

- **Java**

  Java is used to embed small programs, called applets, in Web pages. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** checkbox to prevent attacks and other threats created by Java applets.

- **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** checkbox to disable Cookies.

- **Web Proxy**

  When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing to this proxy server. The **Disable Web Proxy** checkbox disables access to proxy servers located on the WAN. It does not block Web proxies located on the LAN.

- **Known Fradulent Certificates**

  Digital certificates help verify that Web content and files originated from an authorized party. If digital certificates are proven fraudulent, then SonicWALL will block Web content and files that use these fraudulent certificates. Enabling this feature protect users on the LAN from downloading malicious programs warranted by these fraudulent certificates.

Use Filter List (Web/News/FTP/Gopher)

- **Log and Block Access**

  When selected, the SonicWALL blocks access to sites on the Content Filter, custom, and keyword lists and log attempts to access these sites.

- **Log Only**

  When selected, the SonicWALL logs and then allows access to all sites on the Content Filter, custom, and keyword lists. The Log Only checkbox allows you to monitor inappropriate usage without restricting access.

- **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. Check the

Block all categories checkbox to block all of these categories. Alternatively, you can select categories individually by selecting the appropriate checkbox.

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

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

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

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 employees' 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, 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**

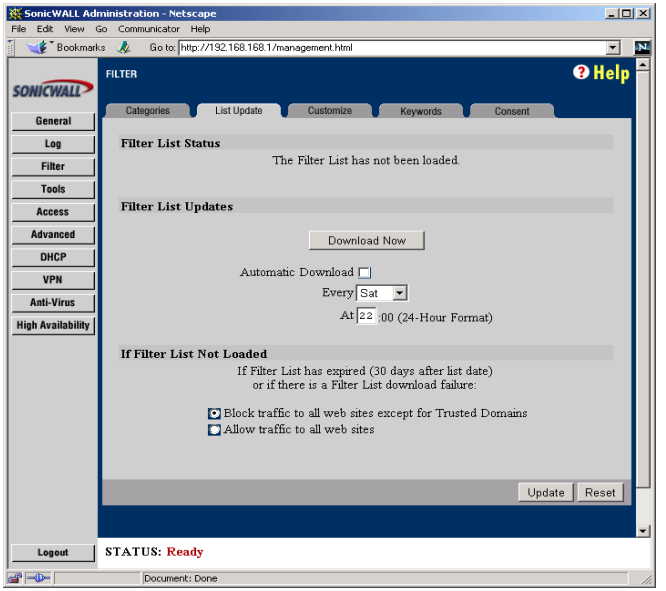
  When selected, **Content Filtering** is enforced during the time and days specified. Enter the time period, in 24-hour format, and select the starting and ending day of the week that Content Filtering is enforced.

Updating the Filter List

Since content on the Internet is constantly changing, the **Content Filter List** needs to be updated regularly. The **List Update** window configures the SonicWALL to automatically download a new list at a specified time every week.

Registering the SonicWALL with SonicWALL, Inc. allows you to receive a one month trial of the Content Filter List subscription at no charge. Please contact SonicWALL Sales at <sales@sonicwall.com> for information about purchasing a SonicWALL Content Filter List subscription.

Click **Filter** on the left side of the browser window, and then click the **List Update** tab at the top of the window.



Configure the following settings in the **List Update** window.

- **Download Now**

  Click **Download Now** to immediately download and install a new **Content Filter List**. This process takes several minutes and requires a current subscription to Content Filter List updates.

- **Automatic Download**

  Check the **Automatic Download** checkbox to enable automatic, weekly downloads of the **Content Filter List**. Then select the day of the week and the time of day when the new list should be retrieved. A current subscription to the Content Filter List updates is required.

  Once loaded, the creation date of the current active list is displayed at the top of the window.

- **If Filter List Not Loaded**

  The **Content Filter List** expires 30 days after it is downloaded. The **Content Filter List** may also be erased if there is a failure while downloading a new list. If the **Content Filter List** expires or fails to download, the SonicWALL can be configured to block all Web sites except for Trusted Domains, or to allow access to all Web sites.

In the **If Filter List Not Loaded** section, select either **Block traffic to all web sites except for Trusted Domains** or **Allow traffic to all web sites**.

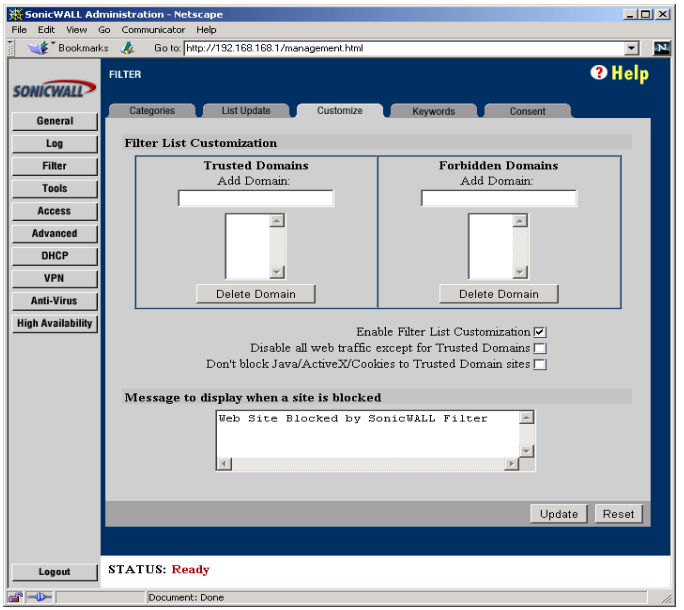
If **Allow traffic to all web sites** is selected, **Forbidden Domains** and **Keywords** are still blocked.

***Note**: The SonicWALL does not ship with the Content Filter List installed. Registering the SonicWALL provides a one month trial subscription to the Content Filter List. Upon registering, a temporary, one-month account is created. Follow the "Download Now" instructions to install the initial Content Filter List.*

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

Customizing the Filter List

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



The **Customize** window allows you to customize the **Content Filter List** by manually blocking or allowing Web site access.

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 **Trusted Domains** fields. 256 entries may be added to the **Trusted 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 may be added to the **Forbidden Domains** list.

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

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

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

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

- **Enable Content Filter List Customization**

  To deactivate **Content Filter List** customization, uncheckthe **Enable Content Filter List Customization** checkbox, and click **Update**. This option allows you to enable and disable customization without removing and re-entering custom domains.

- **Disable Web traffic except for Trusted Domains**

  When the **Disable Web traffic except for Trusted Domains** checkbox is checked, the SonicWALL only allows Web access to sites on the **Trusted Domains** list.

- **Don’t block Java/ActiveX/Cookies to Trusted Domains**

  When this box is checked, SonicWALL permits Java, ActiveX and Cookies from sites on the **Trusted Domains** list to the LAN. This checkbox allows Java, ActiveX or Cookies from sites that are known and trusted.

- **Message to display when a site is blocked**

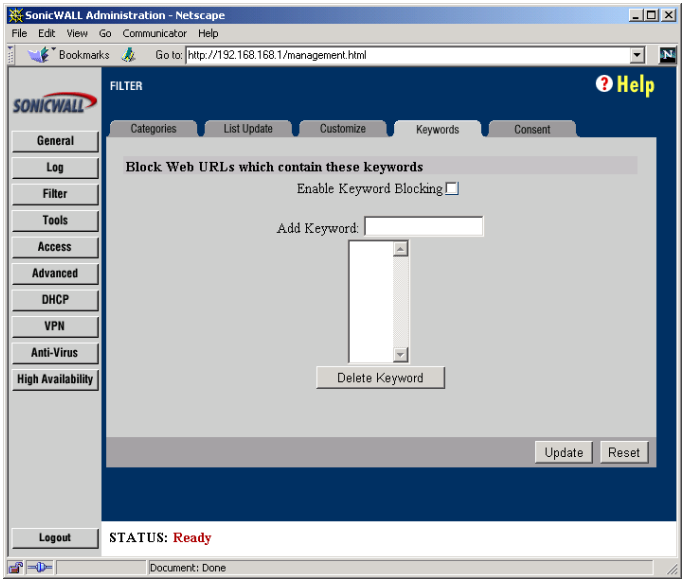
  When a user attempts to access a site that is blocked by the SonicWALL **Content Filter List**, a message is displayed on their screen. The default message is “Web Site Blocked by SonicWALL Filter”. Any message, including embedded HTML, up to 255 characters long, may be defined.

The following example displays a message explaining why the Web site was blocked, with links to the Acceptable Use Policy and the Network Administrator’s E-mail address:

Access to this site was denied because it violates this company’s <A HREF=http://www.your-domain.com/acceptable_use _policy.htm>Acceptable Use Policy</A>. Please contact the <A HREF=”admin@your-domain.com”> Network Administrator</A> if you feel this was in error.

Blocking by Keyword

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



The SonicWALL allows you to block Web URLs containing keywords. For example, if you add the keyword "XXX", the Web site <http://www.new-site.com/xxx.html> is blocked, even if it is not included in the Content Filter List.

To enable this function, check the **Enable Keyword Blocking** checkbox.

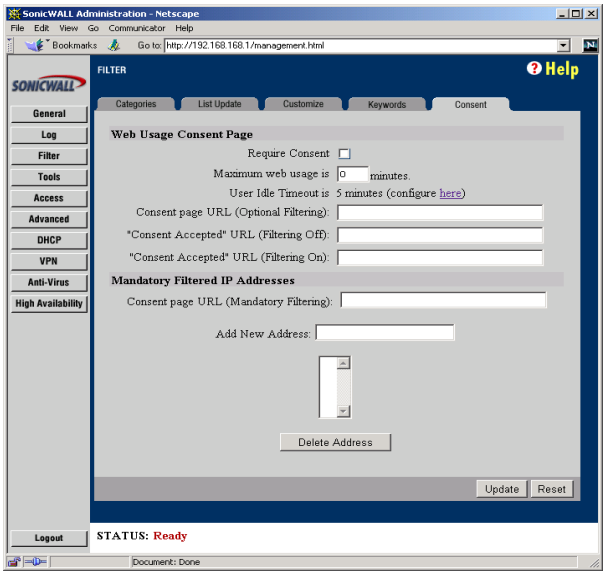
Enter the keyword to block in the **Add Keyword** field, and click **Update**. Once the keyword has been added, a message confirming the update is displayed at the bottom of the browser window.

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.

Consent Features

Consent allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent may 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 at the top of the window.



- **Require Consent**

  Select the **Require Consent** checkbox to enable the **Consent** features.

- **Maximum Web usage**

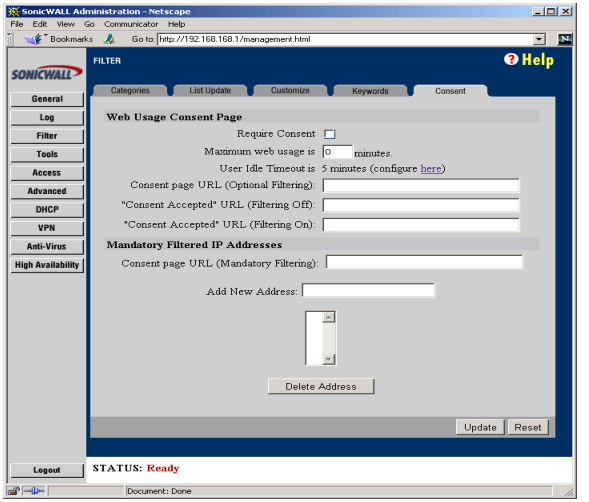
  In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL can be used to remind users when their time has expired by displaying the page defined in the Consent page URL field. Enter the time limit, in minutes, in the Maximum Web usage field. When the default value of zero (0) is entered, this feature is disabled.

- **Maximum idle time**

  After a period of inactivity, the SonicWALL requires the user to agree to the terms outlined in the Consent page before any additional Web browsing is allowed. 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. An example of this page is shown below:



You must create this Web (HTML) page. It may 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.

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

  When a user opens a Web browser on a computer with mandatory content filtering they are shown a consent page. You need to create this Web page. It may contain the 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, which, when selected, tell the SonicWALL 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 may 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 may be entered.

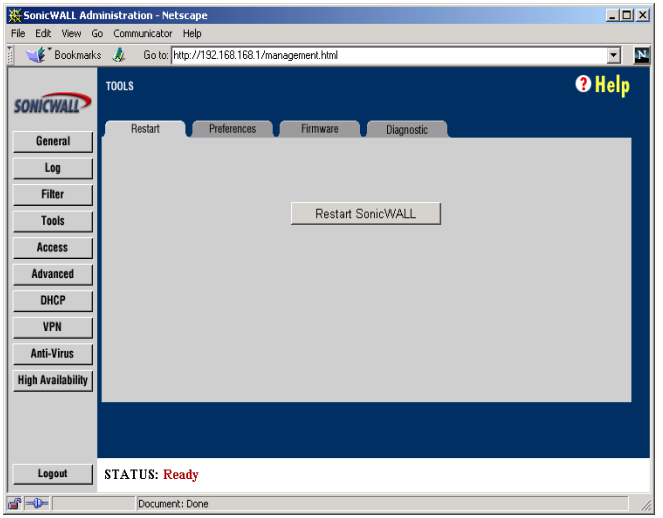
  To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete Address**.

8 WEB MANAGEMENT TOOLS

This chapter describes the SonicWALL **Management Tools**, which may be accessed 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.

Restarting the SonicWALL

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

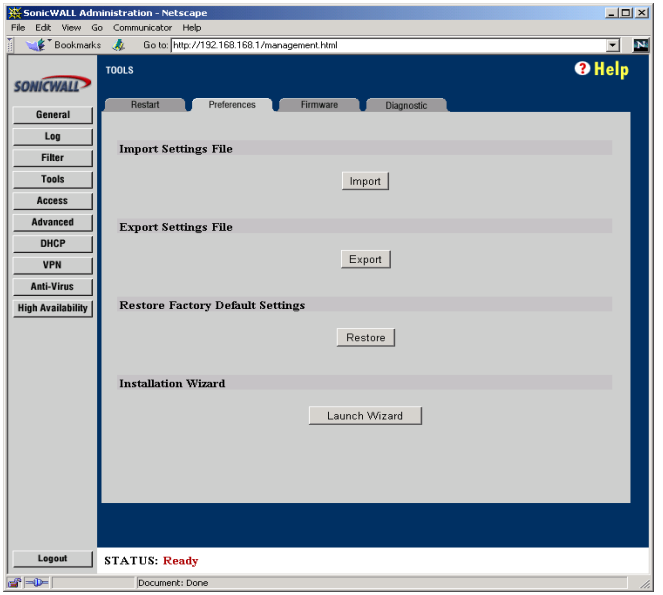


The SonicWALL may be restarted from the Web Management Interface. Click **Restart** SonicWALL, and then click **Yes** to confirm the restart.

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

Preferences

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



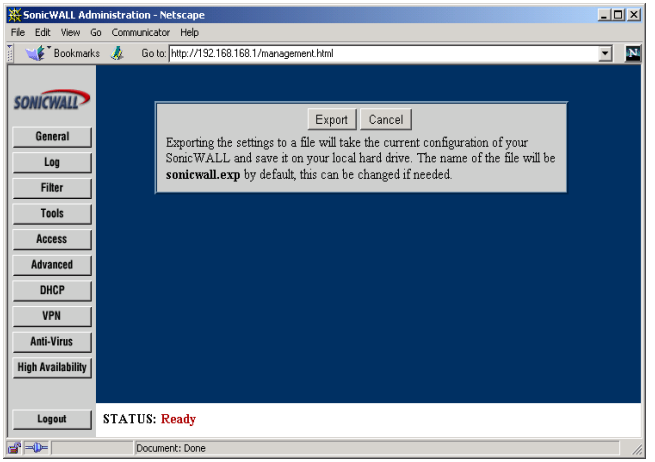
You can save the SonicWALL settings, and then retrieve them later for backup purposes. It is recommended to save the SonicWALL settings when upgrading the firmware.

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 to a “preferences file” to your computer, and then to load it back into the SonicWALL later.

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

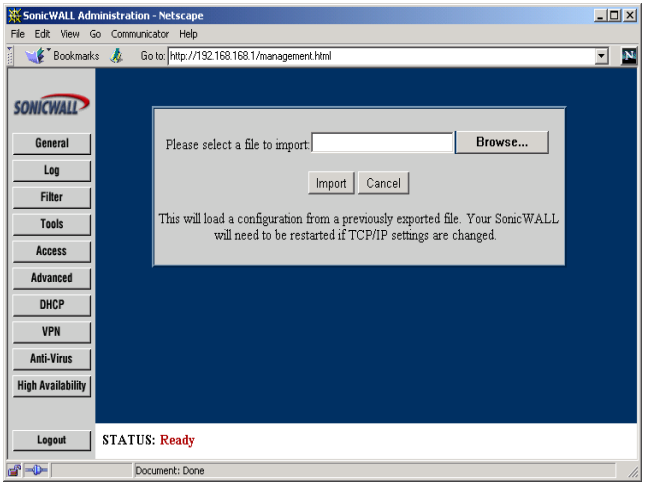


2. Click **Export** again to download the settings file. Then choose the location to save the settings file. The file is named “sonicwall.exp” by default, but may be renamed.
3. Click **Save** to save the file. This process may take up to a minute.

Importing the Settings File

After exporting a settings file, it is possible to import it back to the SonicWALL.

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



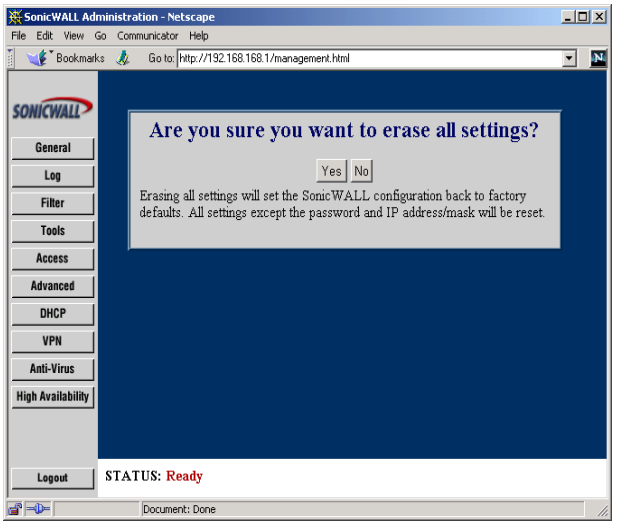
2. Click **Browse** to locate a settings file which was saved using **Export**.
3. Once the file is selected, click **Import**.
4. Restart the SonicWALL for the settings to take effect.

***Note**: The Web browser used to Import Settings must support HTTP uploads. Netscape Navigator 3.0 and above is recommended. Netscape Navigator may be downloaded at <http://www.netscape.com>.*

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.



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

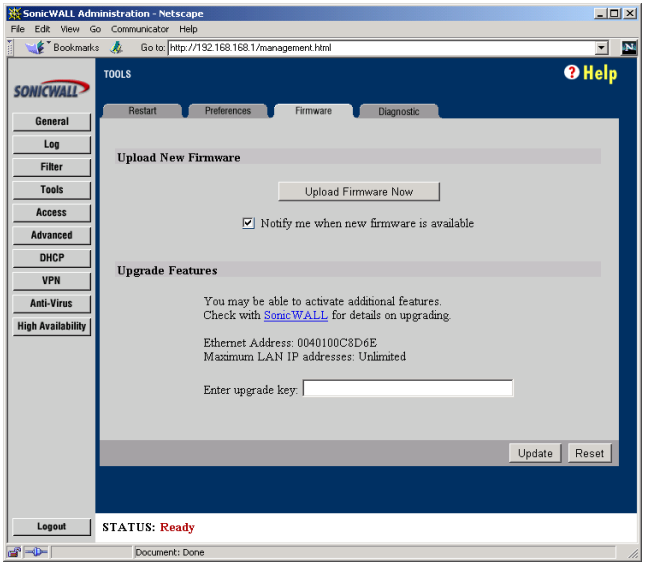
***Note**: The SonicWALL LAN IP Address, LAN Subnet Mask, and the Administrator Password is not reset.*

Updating Firmware

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

***Note**: Firmware updates are only available to registered users. You may 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 at the top of the window.



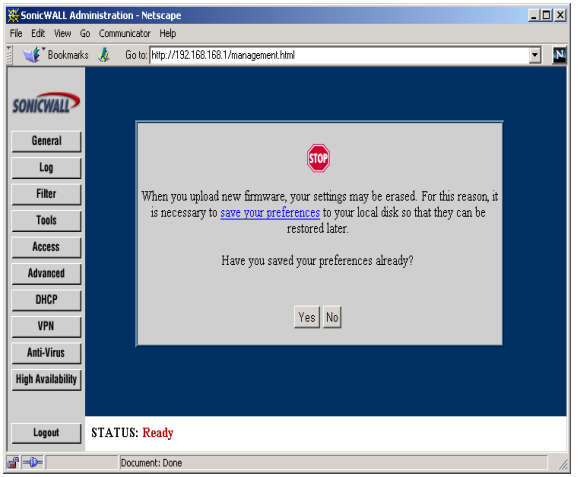
To be automatically notified when new firmware is available, check the **Notify me when new firmware is available** checkbox. Then click **Update**. If you enable firmware notification, your SonicWALL sends a status message to SonicWALL, Inc. Firmware Server on a daily basis. The status message includes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

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 quickly update the firmware.

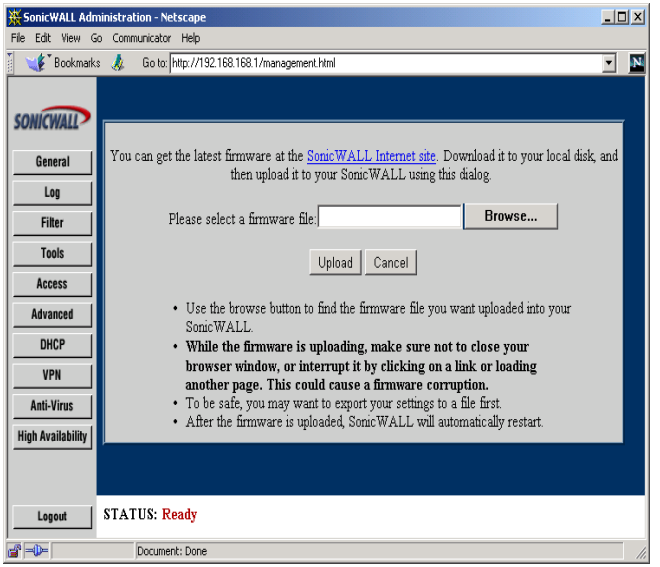
Updating Firmware Manually

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



***Note**: The Web browser used to upload new firmware into the SonicWALL must support HTTP uploads. Netscape Navigator 3.0 and above is recommended.*

When firmware is uploaded, the SonicWALL settings may be erased. It is recommended to save the SonicWALL's preferences so that they can be restored later. Once the settings have been saved, click **Yes**.



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, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the SonicWALL's firmware.*

Upgrade Features

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

Chapter 15, **SonicWALL Options and Upgrades**, provides a summary of the SonicWALL firmware upgrades, subscription services, and support offerings. You may 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 that are included with the upgrade for configuration.

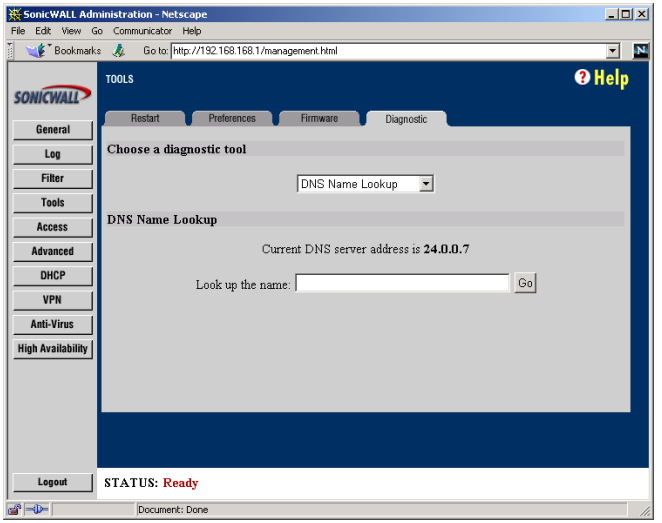
Diagnostic Tools

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 at the top of the window.

DNS Name Lookup

The SonicWALL has a DNS lookup tool that returns the numerical IP address of a domain name.

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



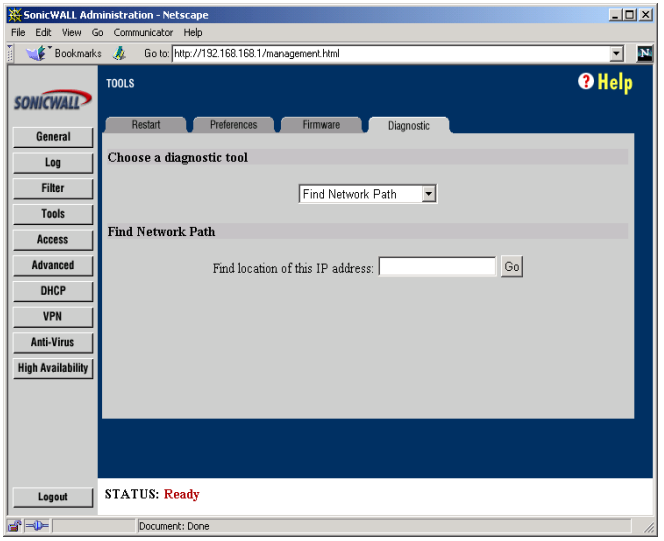
2. Enter the host name to lookup in the **Look up the name** field and click **Go**. Do not add the prefix "http://". The SonicWALL then query the DNS server and display the result at the bottom of the screen.

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, the WAN or the DMZ. This is helpful to determine if the SonicWALL is properly configured. For example, if the SonicWALL “thinks” that a machine on the Internet is located on the LAN port, then the SonicWALL Network or Intranet settings may 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 which gateway the device is using which helps isolate configuration problems.

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



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.

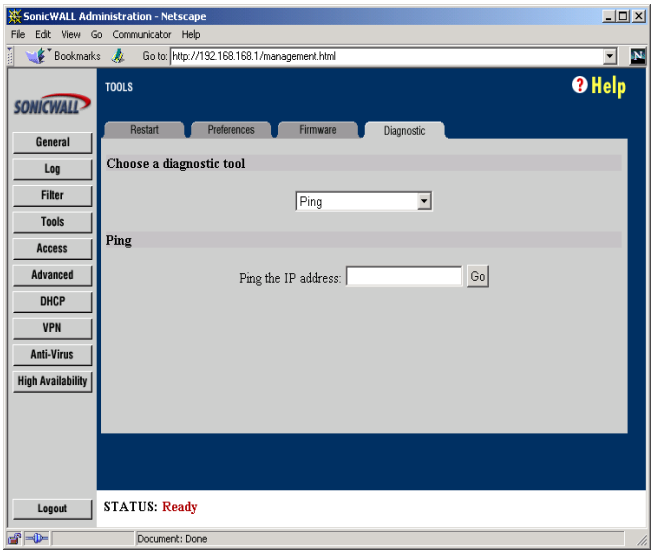
If the network path is incorrect, check the SonicWALL Intranet and Static Routes settings.

***Note**: **Find Network Path** requires an IP address. The SonicWALL **DNS Name Lookup** tool may 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.



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 may 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's 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]

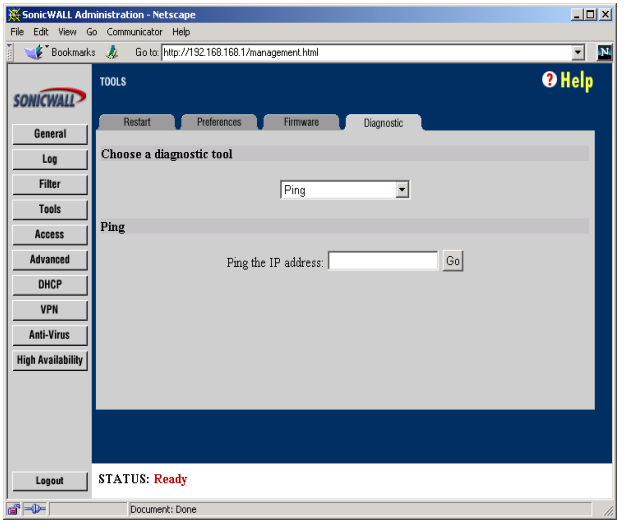
   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e

   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 start of data transfer.

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.



***Note**: **Packet Trace** requires an IP address. The SonicWALL **DNS Name Lookup** tool may 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.

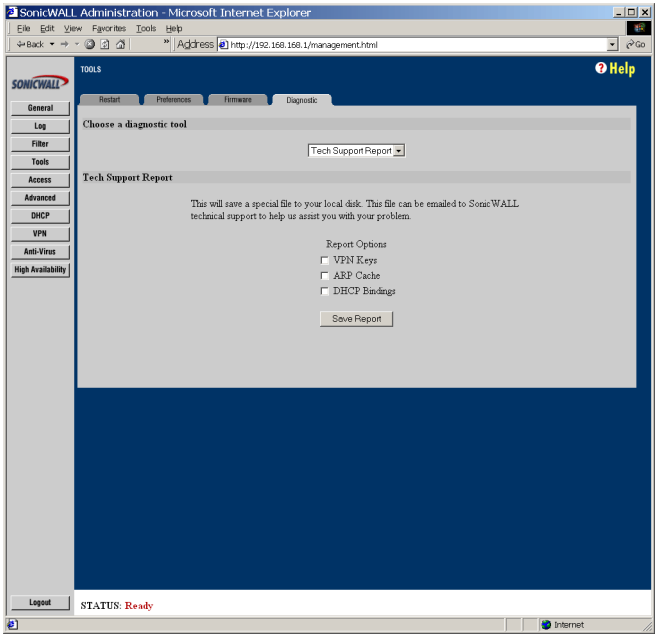
Tech Support Report

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, please 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. In the **Tech Support Report** section, there are three **Report Options** that can be selected to E-mail with your **Tech Support Report**:

- **VPN Keys**
- **ARP Cache**
- **DHCP Bindings**



1. Select the **Report Options** to be included in the Tech Support Report. Click **Save Report** to save the report as a text file to the local disk.A message is displayed to notify you that you are saving your SonicWALL settings in a plaintext file format.

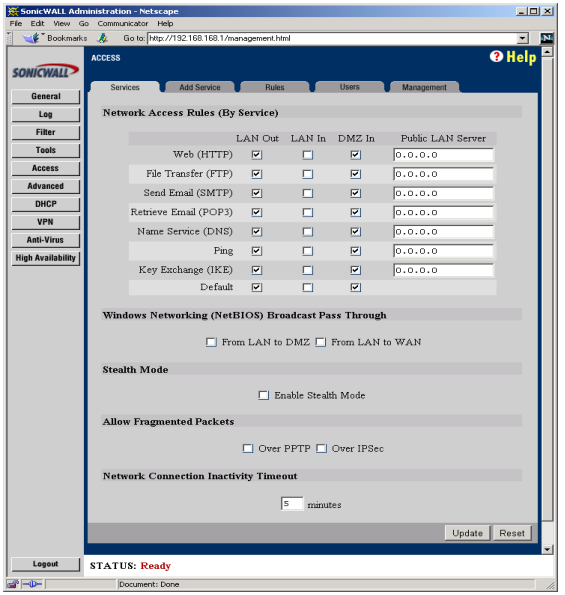
2. The report contains all of the information about your SonicWALL configuration in plaintext.

9 NETWORK ACCESS RULES

This chapter describes the SonicWALL **Network Access Rules**, which determine inbound and outbound access policy, user authentication and remote management. **Network Access Rules** are configured in the **Access** section of the SonicWALL Web Management Interface

Services

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



***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** checkbox is checked, users on your LAN are able to access that service on the Internet. Otherwise, they are blocked from accessing that service. By default, **LAN Out** checkboxes are checked.

LAN In

If a **LAN In** checkbox is checked, users on the Internet may access all computers on your LAN for that service. By default, **LAN In** checkboxes are not checked; use caution when enabling. The **LAN In** column is not displayed if NAT is enabled.

DMZ In (Optional)

If a **DMZ In** checkbox is checked, users on the Internet may access that service on the DMZ. Otherwise, they are blocked from accessing that service on the DMZ. By default, DMZ In checkboxes are checked.

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

Public LAN Server

A **Public LAN Server** is a LAN server that is designated to receive inbound traffic for a specific service, such as Web or E-mail. You may 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. See **Creating a Public LAN Server** on the following page for more information.

Windows Networking Pass Through

Computers running Microsoft Windows® communicate with one another through NetBIOS broadcast packets. By default, the SonicWALL blocks these broadcasts. If you check the **Windows Networking** checkbox, 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 on 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** checkbox 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 checkbox 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 may increase the **Inactivity Timeout** if applications, such as Telnet and FTP, are frequently disconnected.

Creating a Public LAN Server

A Public LAN Server is a server on your LAN that is accessible to users on the Internet. **Creating a Public LAN Server** in the **Services** window is the easiest way to set up a mail server, Web server or other public server, on your LAN.

To create a Public LAN Server, complete the following instructions.

1. Determine what type of service your server uses, such as FTP, Web, or Mail. Locate this service in the Services window. If the service does not appear in the **Services** window, you need to define it in the **Add Service** window.
2. Enter the server's IP address in the **Public LAN Server** field for the appropriate service.

***Note**: If NAT is enabled, this IP address should be a private LAN address. Users on the Internet accesses the Public LAN Server at the SonicWALL WAN IP (NAT Public) Address.*

3. You do not need to check the **LAN IN** checkbox (for **Standard network Addressing Mode**) or remove the **Deny Default * to LAN Rule** in the **Rules** window to allow inbound access to a Public LAN Server.
4. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

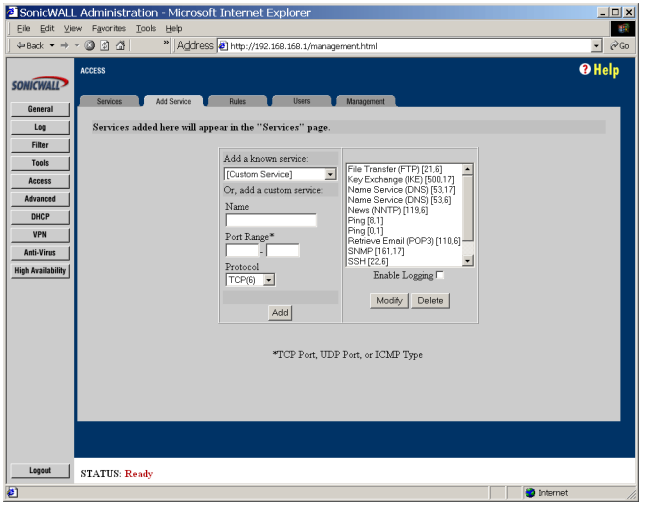
Repeat these instructions to configure additional Public LAN Servers.

Additional Notes:

- In **Standard Network Addressing Mode**, users on the Internet access Public LAN Servers at their valid, LAN IP addresses.
- If NAT is enabled, users on the Internet access Public LAN Servers at the SonicWALL WAN IP (NAT Public) Address.
- If users on the Internet cannot access Public LAN Servers, make sure that the Public LAN Servers have been configured properly and have Internet connectivity. Also, confirm that the DNS MX record points to the correct IP address--the WAN IP (NAT Public) Address, if NAT is enabled.
- If you have multiple LAN servers of the same service, such as multiple Web servers, and your SonicWALL has been configured for **Standard Network Addressing Mode**, you will need to create additional rules in the **Rules** window for the remaining Public LAN Servers.
- If you have multiple LAN servers of the same service, such as multiple Web servers, and you have enabled NAT, you will need to configure One-to-One NAT.

Add Service

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



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 may 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** menu.
2. Click **Add**. The new service appears in the listbox on the right side of the browser window. Note that some services add more than one entry to the listbox.

Add a Custom Service

1. Select **[Custom Service]** from the **Add** a known service menu.
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** menu.
5. Click **Add**. The new service appears in the listbox 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 may not function as expected.*

Disable Logging

You may disable logging of events in the SonicWALL **Event Log**. For example, if LINUX's authentication messages are filling up your log, you may disable logging of LINUX authentication.

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

Delete a Service

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

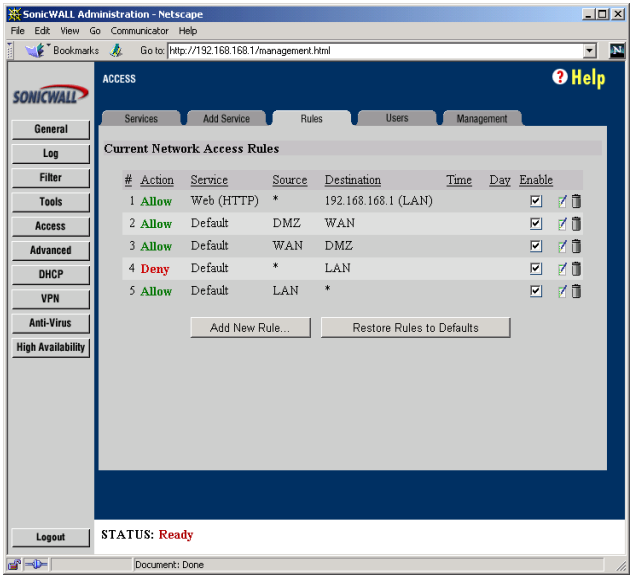
Rules

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 overrides the SonicWALL's 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 may be created to modify the default rules. For example, rules may 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.

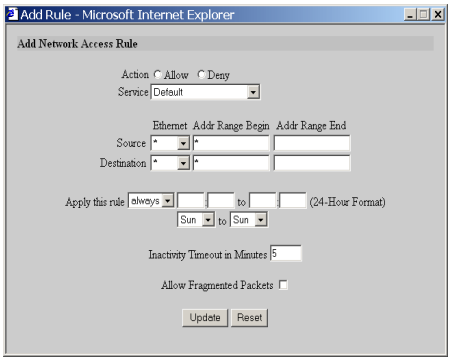
To create custom **Network Access Rules**, click **Access** on the left side of the browser window, and then click the **Rules** tab at the top of the window.



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

Add A New Rule

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



2. Select **Allow or Deny** in the **Action** menu 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** menu. If the service is not listed, you need to 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, WAN, DMZ, or *, 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, WAN, DMZ, 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 **Apply this rule "always"** if the rule is always in effect.

   Select **Apply this rule "from"** 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 will need to make additional rules for each time period.*

***Note**: Although custom rules may 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.*

7. In the **User Idle Timeout** section, define a value in minutes for the network connection to timeout if a connection becomes inactive. 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.
8. To allow fragmented data packets over the connection, check the **Allow Fragmented Packets** box.
9. Click **Update** to add the rule to **Current Network Access Rules** list.

Current Network Access Rules List

All of your 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, uncheck the **Enable** checkbox to the right of the rule. To enable a disabled rule, check the **Enable** checkbox. 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	DMZ	WAN			☑
5	Allow	Default	WAN	DMZ	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 menu, you need 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** in the menu.
11. Click **Update** to add your new Rule.

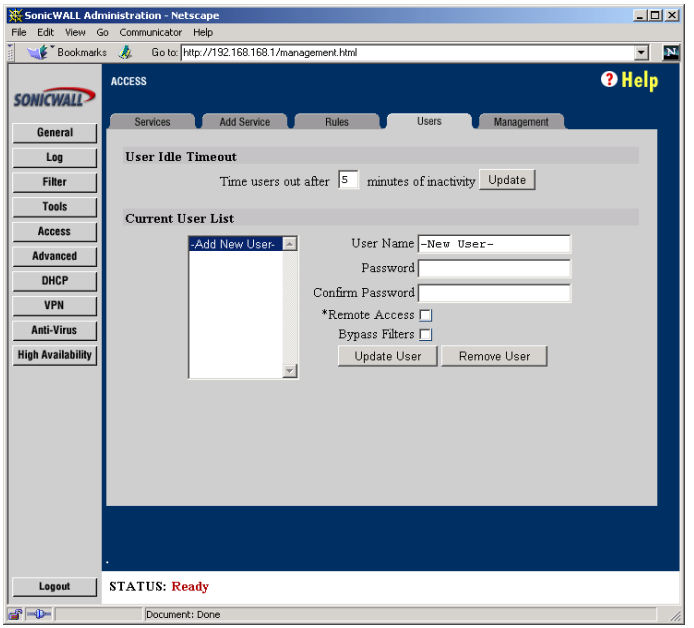
Enabling Ping

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 **Apply** this rule "always" to ensure continuous enforcement.
9. Click **Update** to add your new Rule.

User Authentication

The SonicWALL provides an authentication method that gives authorized users on the Internet access to LAN resources and that allows users on the LAN to bypass Web content filtering.



User Settings

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

- **User Idle Timeout**

This sets the maximum period of inactivity before a user is required to re-establish an Authenticated Session. The inactivity timeout applies to both Remote Access and Bypass Filters. This value may range from 5 to 99 minutes.

- **Current User List**

The **Current User List** is a list that displays all currently defined users.

To add a new user, complete the following instructions.

1. Highlight the **-Add New User-** entry in the **Current User List** box.
2. Enter the user's login name in the **User Name** field.
3. Enter the user's password in the **Password** and **Confirm Password** fields. It is important to use a password that could not be guessed by someone else. Avoid

using names of friends, family, pets, etc. The password should consist of random characters, such as “a*$#7fe2j%42”. The password is case sensitive.

4. Choose the privileges to be enabled for the user by selecting one or both check-boxes. Two options are available:

   A. **Remote Access**

   This option provides unrestricted access to the LAN from a remote location on the Internet. Only **Standard** mode supports Remote Access. If NAT is enabled, VPN client remote access is recommended.

   B. **Bypass Filters**

   This option provides unrestricted access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.

5. Click **Update User**.

***Note**: The SonicWALL supports up to 100 users.*

Edit User Settings

To change a user’s password or privileges, highlight the name in the **Current User List**, make the changes and click **Update User**. To delete a user, highlight the name and click **Remove User**.

Establishing an Authenticated User Session

In order to establish an **Authenticated User Session**, a user must enter the SonicWALL LAN IP Address into the **Location** or **Go to** field in their Web browser.

***Note**: The Web browser used to establish an authenticated session must support Java and JavaScript.*

The user sees the SonicWALL authentication window, asking for their user name and password. After completing these fields and clicking **Login**, their password is verified using MD5 authentication. The password is never sent "in the clear" over the Internet, preventing password theft.

***Note**: User names are not case sensitive (“john” is equivalent to “JOHN” or “John”), but passwords are case sensitive (“password” is not the same as “Password”).*

Once authenticated, remote users are able to access all IP resources on the LAN, and users on the LAN are able to bypass the **Content Filter Lists**. The connection closes if user inactivity on the connection exceeds the configured time-out period. If the connection is closed, the remote user needs to re-authenticate.

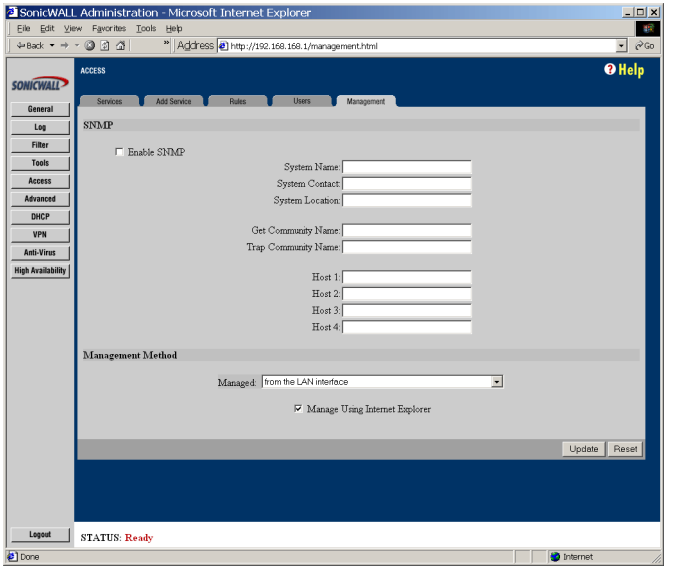
***Note**: **Authenticated Sessions** create a log entry when established. However, user activity is not logged.*

Remote Management

SonicWALL SNMP Support

SNMP (Simple Network Management Protocol) is a network protocol over User Datagram Protocol (UDP) that provides network administrators with the ability to monitor the status of the SonicWALL 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 MIBII for generating trap messages.

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.



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 may 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, type in the necessary information in the following fields:

- **Enable SNMP** - To enable the SNMP agent, select **Enabled SNMP**.
- **System Name** - This is the hostname of the SonicWALL appliance.
- **System Contact** - Type in the name of the network administrator for the SonicWALL appliance.
- **System Location** - The network administrator's contact information is placed into this field. Type in an E-mail address, telephone number, or pager number.
- **Get Community Name** - Create a name for a group or community of administrators who can view SNMP data. The default value is **Public**.
- **Trap Community Name** - Create a name for a group or community of administrators who can view SNMP traps. A name must be entered.
- **Host 1 through 4** - Enter the IP address or hostname of the SNMP management system receiving the SNMP traps. 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 is 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 into the trusted network. SNMP trap messages may be sent via the LAN, WAN, or DMZ interface.

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

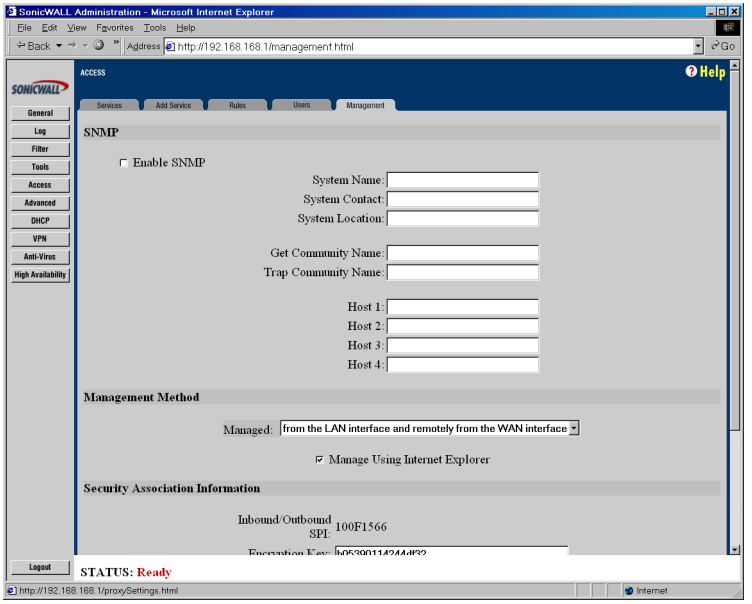
Remote Management

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 may be managed remotely using a **Management SA** or with a **VPN SA**.*

To enable secure remote management, click **Access** on the left side of the browser window, and click the **Management** tab at the top of the browser window. Then select

Managed: "from the LAN interface and remotely from the WAN interface" to enable secure remote management.



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 Managment** 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. A valid encryption key may be 1234567890ABCDEF. Or you may 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. A valid authentication key may be 1234567890ABCDEF1234567890ABCDEF. Or you may 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. In contrast, when connecting to a **VPN SA**, the remote SonicWALL is managed at the SonicWALL LAN IP Address.*

4. Click **Help** in the upper right corner of the SonicWALL Management Interface to access detailed instructions for configuring the VPN client.

Note: The **Management Method** menu 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**. Refer to **SonicWALL GMS** documentation for set up instructions.

Manage Using Internet Explorer

Under the **Management** tab of the **Access** section, there is a check box labeled **Manage Using Internet Explorer**. This box is checked by default and enables Internet Explorer web browsers to quickly load the SonicWALL Web Management Authentication web page. With the IE checkbox enabled, the SonicWALL appliance LAN port responds to NetBIOS name request on port 137.

Users can disable the LAN port response to port 137 by unchecking the IE checkbox, however, this slows down the login process into the SonicWALL Management station.

10 ADVANCED FEATURES

This chapter describes the SonicWALL **Advanced Features**, such as Web Proxy Forwarding, DMZ Address settings, One-to-One NAT, and Ethernet. The **Advanced Features** may be accessed in the **Advanced** section of the SonicWALL Web Management Interface.

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.

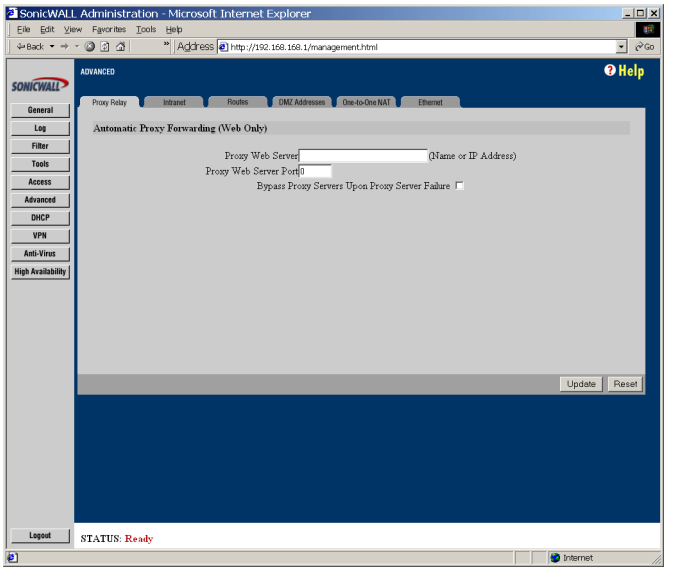
If you have a proxy server on your network, instead of configuring each computer to point to the proxy server, you may move the server to the WAN and enable Web Proxy Forwarding. The SonicWALL automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the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

Configuring 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 may 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.

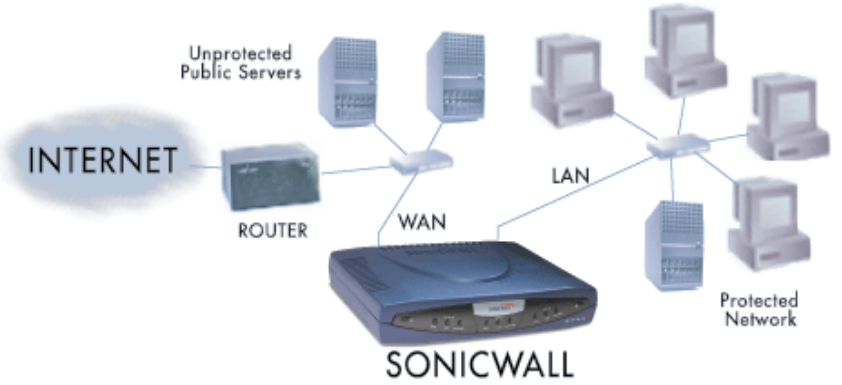


3. Enter the name or IP address of the proxy server in the **Proxy Web Server** field, and the proxy's IP port in the **Proxy Web Server Port** field. Select the **Bypass Proxy Servers Upon Proxy Server Failure** checkbox to allow access to the Internet in the event that the proxy server fails. Click **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. In the **Intranet** tab, enter the proxy server's IP address in the **Add Range** field.
6. 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.

Intranet

The SonicWALL may 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 need to 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

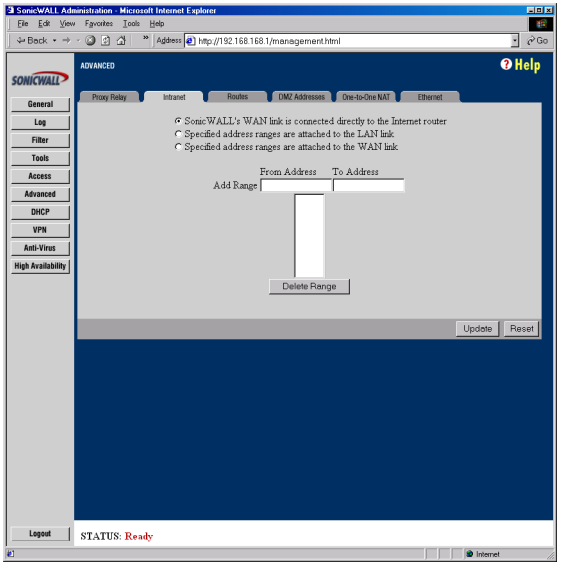
1. Connect the LAN Ethernet port on the back of the SonicWALL to the network segment to be protected against unauthorized access.
2. Connect the WAN Ethernet port on the back of the SonicWALL to the rest of the network.

***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 GX250 and SonicWALL GX650, press the Power Switch to the **ON** position.

Configuration

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



To enable Intranet firewalling, 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 need 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 three options:

- **SonicWALL's 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 will be inaccessible to users on your LAN.

- **Add Range**

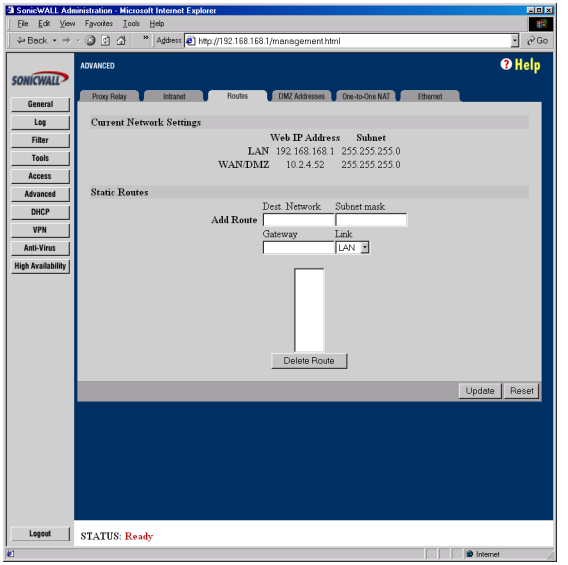
  To add a range of addresses, such as "199.2.23.50" to "199.2.23.54", enter the starting address in the **From Address** field and the ending address in the **To Address** field. An individual IP address should be entered in the **From Address** field only.

***Note**: Up to 64 address ranges may 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, you have to configure the **Static Routes** section of the SonicWALL.



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

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 LAN, WAN or DMZ, from the **Link** menu.

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 64 static route entries.*

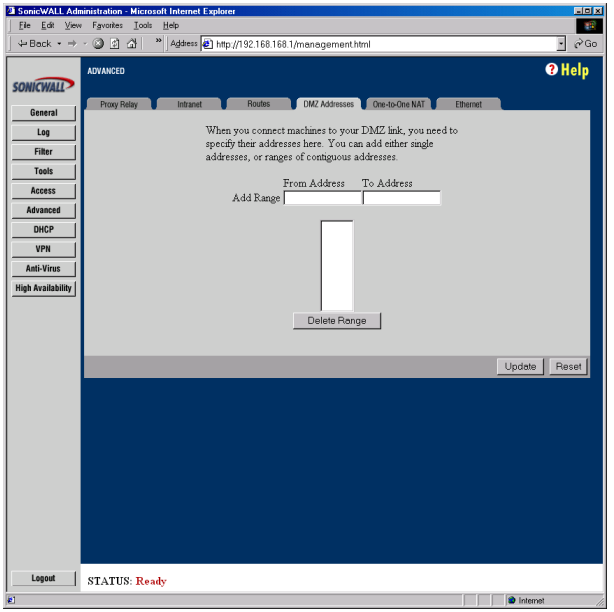
DMZ Addresses

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.

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

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



Servers on the **DMZ** need 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.

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 may 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.*

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.

***Note**: Network Address Translation (NAT) does not apply to servers on the DMZ.*

One-to-One NAT

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

You may 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.

In the following example, a business has been assigned valid IP addresses ranging from 209.19.28.16 to 209.19.28.31, with 209.19.28.16 assigned as the **NAT Public Address**. The address range of 192.168.168.2 to 192.168.168.255 is used by computers on the LAN. Typically, only computers that have been designated as Public LAN Servers are accessible from the Internet. However, with **One-to-One NAT**,

computers with private IP addresses of 192.168.168.2 to 192.168.168.16 may be accessed at the corresponding external IP address, as shown in the diagram below.

LAN Address	Corresponding WAN Address	Accessed Via
192.168.168.1	209.19.28.16	Inaccessible: NAT Public IP Address
192.168.168.2	209.19.28.17	Accessed at 209.19.28.17
[…]	[…]	[…]
192.168.168.16	209.19.28.31	Accessed at 209.19.28.31
192.168.168.33	No corresponding valid IP Address	Inaccessible except as Public LAN Server
[…]	[…]	[…]
192.168.168.255	No corresponding valid IP Address	Inaccessible except as Public LAN Server

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

1. Check the **Enable One-to-One NAT** checkbox.
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 may not exceed the number of valid IP addresses. Up to 64 ranges may 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.*

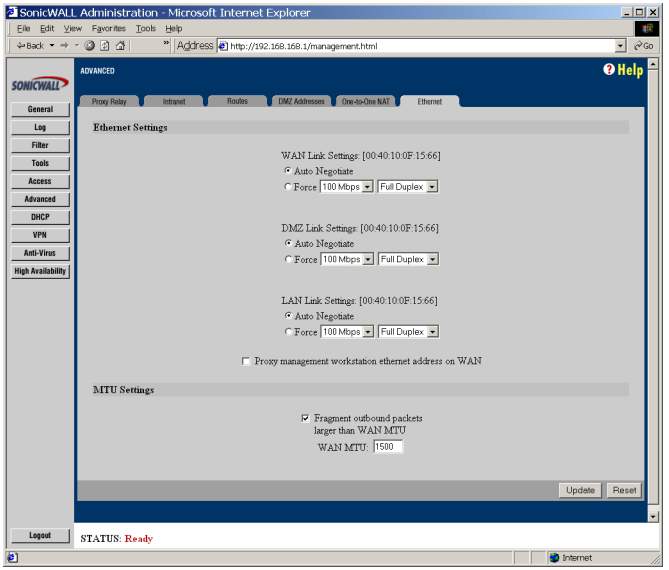
*A rule must be created in the **Rules** section to allow access to LAN servers. Once **One-to-One NAT** has been configured, create an **Allow** rule to permit traffic from the Internet to the private IP address(es) on the LAN.*

The Ethernet Tab

In the **Advanced** section of the SonicWALL management interface, a new tab labeled **Ethernet** has been added. The **Ethernet** tab allows you to manage your Ethernet settings and is divided into two sections:

- **Ethernet Speed / Duplex Settings**
- **Ethernet Address Settings**

The **Ethernet** tab is displayed below:



Ethernet Speed / Duplex Settings

This section has the following settings:

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

The default setting for all of the link settings is **Auto Negotiate** which means that the Ethernet links automatically negotiate the speed and duplex mode. The other choice, **Force** with drop down menus for choices of **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

This checkbox may be checked if you are managing the Ethernet from the LAN side of your network. The SonicWALL appliance takes the Ethernet address of the computer that is managing the SonicWALL appliance and proxies that address on the WAN port of the SonicWALL. If you are not managing the SonicWALL appliance from the LAN side of your network, the firmware looks for a random computer on the LAN which can be a lengthy search process.

MTU Settings

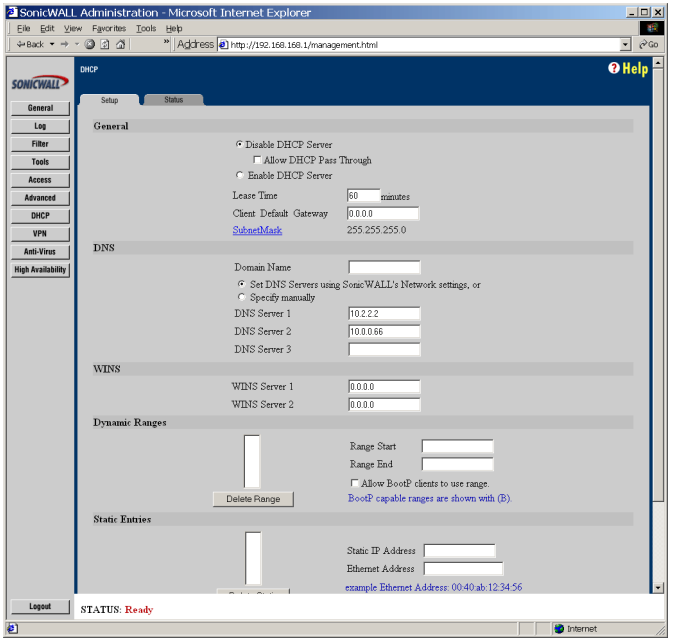
A network administrator may set the MTU (Maximum Transmission Unit) allowed over the over a packet or frame-based network such as TCP/IP. If the MTU size is too large, it may require more transmissions if the packet encounters a router unable to handle a larger packet. If the packet size is too small, 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.

11 DHCP SERVER

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

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.



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

1. Select **Enable DHCP Server**. If you want to have a DHCP server located outside the SonicWALL appliance, check the **Allow DHCP Pass Through** checkbox.

***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 may range from 1 to 9999 minutes.

3. Enter the gateway address used by LAN computers to access the Internet in the **Client Default Gateway** field. Enter the SonicWALL LAN IP Address if NAT is enabled.

4. 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.

5. 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 need to enter one DNS Server address, but multiple DNS entries improve performance and reliability.

6. 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.

7. **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.

   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** checkbox 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** will not assign an IP address from the dynamic range if the address is already being used by a computer on your LAN.*

8. 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. 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.

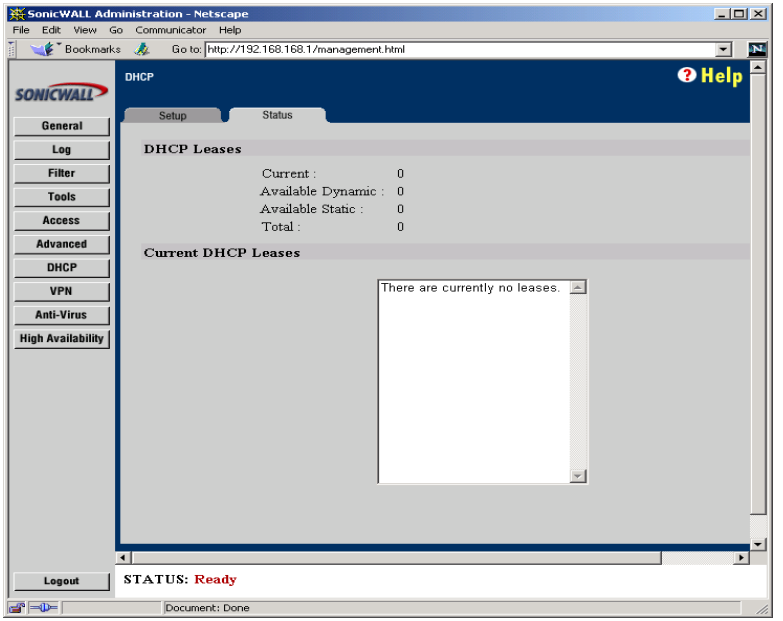
***Note**: The SonicWALL DHCP server may assign a total of 254 dynamic and static IP addresses.*

Deleting Dynamic Ranges and Static Entries

1. 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.
2. 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 Status

Click the **Status** tab at the top of the browser window.



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 may be necessary because Web pages are not automatically refreshed, and new bindings may have been issued since the page was first loaded.

12 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. Visit SonicWALL's Web site at <http://www.sonicwall.com/products/documentation/WhitePapers.html> for information about VPN interoperability. SonicWALL VPN is included with the SonicWALL GX250 and the SonicWALL GX650.

This chapter is organized into the following sections:

- **The VPN Summary Tab**

  This section describes the **Summary** tab and settings.

- **Enabling Group VPN on the SonicWALL**

  This section demonstrates the configuration of SonicWALL Group VPN settings using the Group VPN Security Association.

- **Configuring VPN using Manual Key**

  This section describes the configuration of a SonicWALL appliance and a VPN client using the Manual Key Security Association.

- **SonicWALL VPN between two SonicWALLs**

  This section 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 GX250 and a SonicWALL TELE2.

- **Testing a VPN Tunnel Connection**

  This section describes testing a VPN tunnel configuration by using "ping" to send data packets to a remote computer.

- **Enhanced VPN Logging Settings**

  This section describes logging settings for both the SonicWALL appliance and the VPN client for troubleshooting VPN problems.

- **XAUTH/RADIUS Server Configuration**

  This section describes using a RADIUS server for authentication of VPN Clients.

- **Deleting and Disabling Security Associations**

  This section describes deleting and disabling Security Associations for VPN access.

- **Basic VPN Terms and Concepts**

  This section provides a glossary defining applicable VPN terms such as encryption methods, authentication methods, and IPSec keying modes.

VPN Applications

- **Linking Two or More Networks Together**

  SonicWALL VPN is the perfect way for you to connect to your branch offices and business partners over the Internet. SonicWALL VPN offers an affordable, high-performance alternative to leased site-to-site lines. If NAT is enabled, SonicWALL VPN also provides access to remote devices that have been assigned private IP addresses.

- **Remotely Managing the SonicWALL**

  The SonicWALL GX series includes a free VPN client for remote administration and 100 VPN clients for remote users. The SonicWALL VPN client, installed on Windows 95, 98, NT, and 2000, allows you securely manage the SonicWALL over the Internet.

- **Accessing Network Resources from a VPN Client**

  VPN client remote access allows your employees to connect to your network from any location. The VPN client remote access solution is easy to deploy and supports hundreds of remote users.

VPN Feature Chart

	GX250	GX650
3DES VPN Throughput	100 Mbps	260 Mbps
Simultaneous Connections	250,000	500,000
VPN Tunnels (SAs)	5,000	10,000

***Note**: Simultaneous VPN Client Connections represents the maximum number of VPN clients that should connect to the SonicWALL at the same time. Although the number of VPN clients configured and deployed may exceed this limit, only the number*

specified in the VPN Feature Chart may connect at the same time without affecting the performance of the SonicWALL.

The VPN Interface

Click **VPN** on the left-side of the SonicWALL management station interface. There are four tabs in the VPN interface:

- **Summary**
- **Configure**
- **RADIUS**
- **Certificates**

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

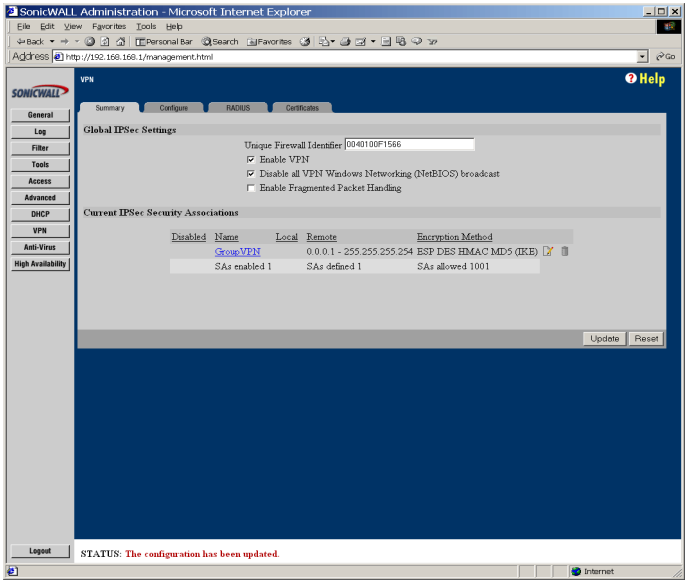
Global IPSec Settings

The **Global IPSec Settings** section displays the **Unique Firewall Identifier** which defaults to the serial number of the SonicWALL appliance. You may change the **Identifier**, but the default value should be used for configuring VPN tunnels. The **Enable VPN** check box must be checked to allow VPN security associations. The **Disable all VPN Windows Networking (NetBIOS) broadcast** check box is also checked. This check box disables NetBIOS broadcasts for every Security Association configuration. The **Enable Fragmented Packet Handling** check box should be checked if the VPN log report shows the log message "Fragmented IPSec packet dropped". Leave it unchecked until the VPN tunnel is established and in operation.

Current IPSec Security Associations

This section displays all of the VPN configurations in the SonicWALL appliance. If you click on the name of the security association, the security association settings are displayed. Alternatively, click on the **Notepad** icon to edit a VPN configuration. You may also delete a configuration by clicking on the **Trashcan** icon.

Also, you can view the number of Security Associations enabled, the number of SAs defined, and the number of SAs allowed. Each Security Association configured is listed in this section. An asterisk appears next to a Security Association that is disabled.



SonicWALL VPN Client for Remote Access and Management

When you register the SonicWALL GX250 or the SonicWALL GX650 at <http://www.mysonicwall.com>, you receive a single VPN Client for Windows and a VPN Client serial number. Using the VPN client software, you may establish a secure VPN tunnel to remotely manage the SonicWALL. Contact your SonicWALL reseller for information about purchasing additional VPN client licenses for remote access.

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

Group Configuration uses IKE (Internet Key Exchange) and requires few 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.

IKE using pre-shared secret

IKE using pre-shared secret is a VPN configuration between two SonicWALL Internet security appliance.

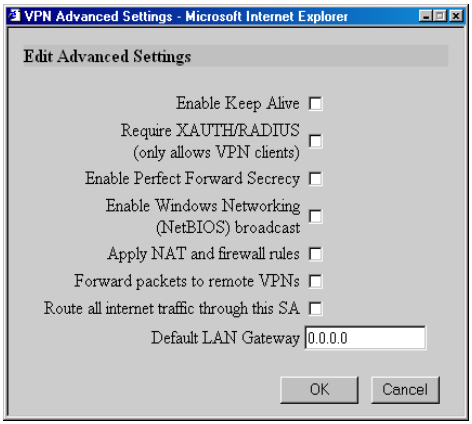
Manual Key Configuration requires matching encryption and authentication keys. Each Manual Key SA allows 64 VPN clients sharing the same configuration. The number of VPN Clients that may be configured using Manual Key is 64 times the total number of Security Associations. For example, 5000 SAs or a total of 320,000 VPN clients may be configured to connect to the SonicWALL GX. However, only 100 VPN clients should connect to the SonicWALL PRO simultaneously (See the VPN Feature Chart at the beginning of this chapter for more information). Because **Manual Key Configuration** supports multiple SAs, it enables individual control over remote users.

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

VPN Advanced Settings

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

- **Enable Keep Alive**
- **Require XAUTH/RADIUS (only allows VPN clients)**
- **Enable Perfect Forward Secrecy**
- **Enable Windows Networking (NetBIOS) broadcast**
- **Apply NAT and firewall rules**
- **Forward packets to remote VPNs**
- **Route all internet traffic through this SA**
- **Default LAN Gateway**



Enable Keep Alive

Checking the **Enable Keep Alive** checkbox allows the VPN tunnel to remain active or maintain its current connection. A proprietary dead peer detection is now implemented that detects whether or not the remote Security Gateway has a valid IKE tunnel. This checkbox cannot be used with the Group VPN Security Association.

Require XAUTH/RADIUS (only allows VPN clients)

An IKE Security Association may be configured to require RADIUS authentication before allowing VPN clients to access LAN resources. This authentication provides an additional layer of VPN security while simplifying and centralizing management. RADIUS authentication allows many VPN clients to share the same VPN configuration, but requires each client to authenticate with a unique user name and password. And because a RADIUS server controls network access, all employee privileges may be created and modified from one location

Enable Perfect Forward Secrecy

A new checkbox is available for the **Security Association** "IKE using Pre-shared Secret" between two SonicWALL appliances. The **Enable Perfect Forward Secrecy** checkbox 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 the two appliances, an additional Diffie-Hellmen key exchange is performed. **Perfect Forward Secrecy** adds incremental security between gateway.

Enable Windows Networking (NetBIOS) broadcast

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

Apply NAT and firewall rules

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

If the SonicWALL uses the **Standard** network configuration, using this checkbox applies the firewall access rules and checks for attacks. It does not apply NAT as the SonicWALL is not configured for it. If the SonicWALL uses **NAT** network configuration, then checking the **Apply NAT and firewall rules** checkbox performs normal firewall checks, access rules, and applies NAT.

Forward Packets to Remote VPNs

Checking the **Forward Packets to Remote VPNs** checkbox 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's local 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** checkbox for each Security Association, including the remote SAs, in your SonicWALL. Additionally, destination networks must be configured the same in

both the central office SA and the remote site SA. Traffic is now able to go from branch office to branch office via the corporate office.

Route all internet traffic through this SA

Checking this box allows a network administrator to force all network traffic to the WAN 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 checkbox. 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. This checkbox is used for configuration of remote site Security Associations.

Note: *Only one SA may have this checkbox enabled.*

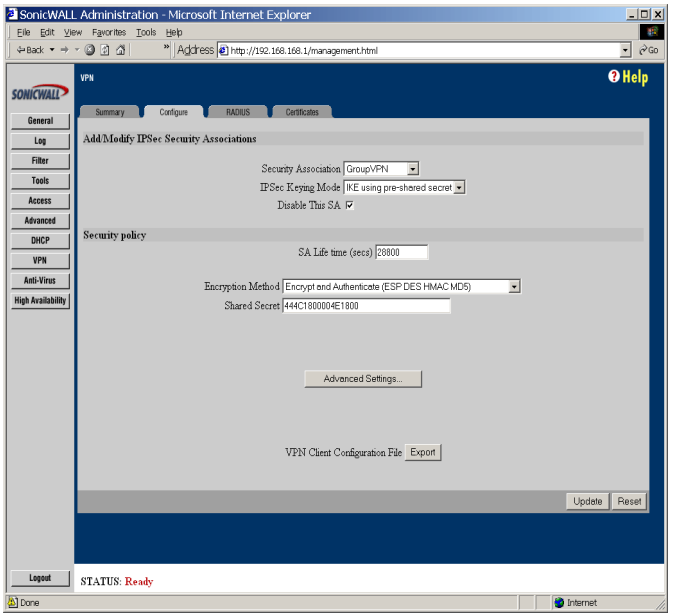
Default LAN Gateway

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** checkbox. 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 may 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. This checkbox is used if configuring a central site Security Association for a VPN tunnel.

Enabling Group VPN on the SonicWALL

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



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 as it eliminates the need 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 Preshared Secrets** or **IKE using Certificates**. To use certificates, an **Authentication Service** upgrade must be purchased.
4. Enter the **SA Life Time** value in minutes. A value of 28800 minutes (8 hours) is recommended.

5. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** from the **Encryption Method** menu.
6. Type the **Shared Secret** in the **Shared Secret** text box. 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.
7. Click **Advanced Settings.**
8. Leave **Require XAUTH/RADIUS (only allows VPN clients)** unchecked.
9. Check **Enable Perfect Forward Secrecy** if an additional level of security is desired.
10. Check **Enable Windows Networking (NetBIOS) broadcast** if remote sites browse the network using Windows Network Neighborhood.
11. Check **Apply NAT and firewall rules** if applicable.
12. Check **Forward Packets to remote VPNs** if configuring a "hub and spoke" network.
13. Click **OK** to close the **Advanced Settings** window.
14. Click **Update** to enable the changes.

To export the **Group VPN** settings to remote VPN clients, click **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.

***Note**: You must use the **Group VPN Security Association** even if you have only one VPN client to deploy. The **Group VPN Security Association** defaults to the **Simple Configuration** previously available in firmware version 5.1.1. If you have only one client to deploy, you may want to consider **Manual Key Configuration** for your appliance and client.*

Installing the VPN Client Software

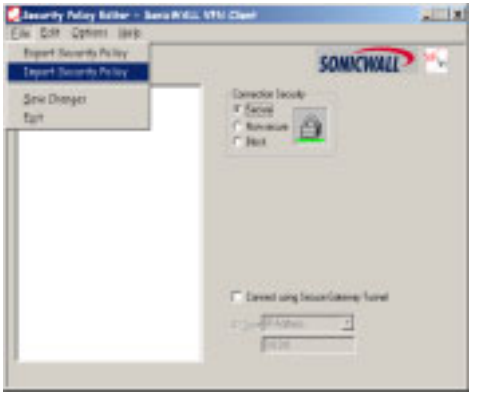
1. When you register your SonicWALL or SonicWALL VPN Upgrade at <http://www.mysonicwall.com>, a unique VPN client serial number and link to download the SonicWALL VPN Client zip file is displayed.
2. Unzip the SonicWALL VPN Client zip file.
3. Double-click **setup.exe** and follow the VPN client setup program step-by-step instructions. Enter the VPN client's 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/vpn-center/vpn-setup.html>

Group VPN Client Configuration

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

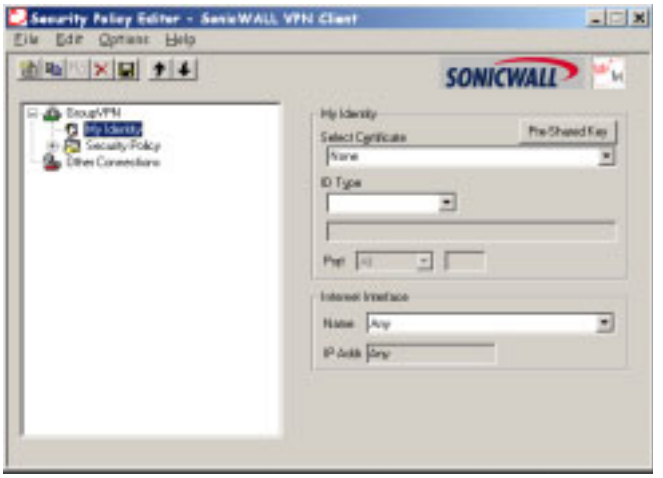
1. Open the **VPN Client**. Click **File**, and then **Import Security Policy**.



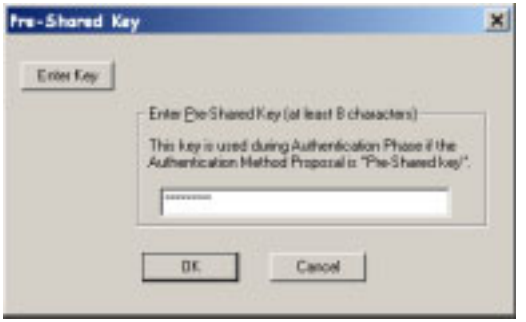
2. A file location box appears which allows searching for the location of the saved security file. Select the file, and click **Open**.

3. A dialogue box asking to import the security file appears. 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.

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

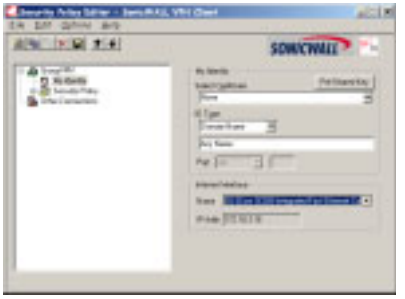


5. Click **Pre-Shared Key** to enter the **Pre-Shared Secret** created in the **Group VPN** settings in the SonicWALL appliance. Click **OK**.



6. Select **None** in the **Select Certificate** menu, and select **Domain Name** in the **ID Type** menu. Enter any word or phrase in the field below the **ID Type** menu. Do not leave this field blank.

7. In the **Internet Interface** box, select the adapter used to access the Internet. Select **PPP Adapter** in the **Name** menu if you have a dial-up Internet account. Select your **Ethernet adapter** if you have a dedicated Cable, ISDN, or DSL line.



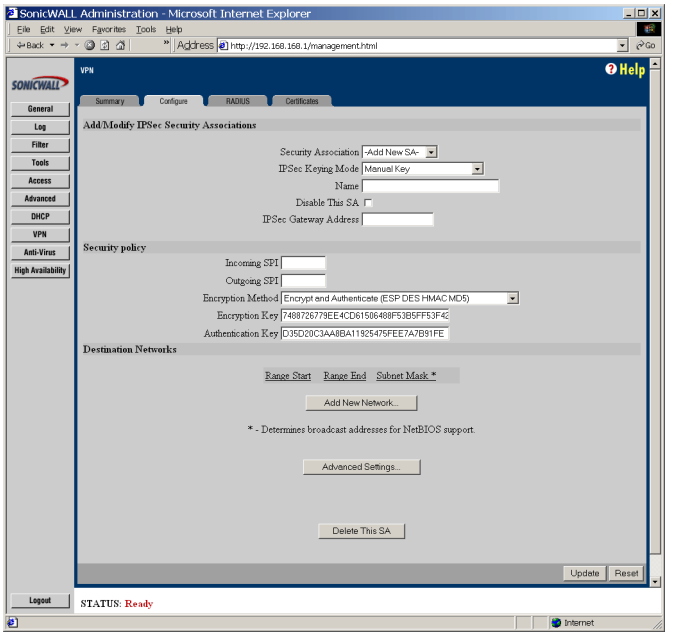
8. Click **File**, then **Save Changes** to save the settings to the security policy.

There is no need to configure the **Security Policy** as it is imported directly into the **Client** application. Exporting the security association to a file facilitates configuration of a large number of VPN clients and eliminates the need to configure each client individually.

Group VPN may 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/products/documentation.html.

Manual Key Configuration for the VPN Client

To configure the SonicWALL appliance, click **VPN** on the left side of the browser window, and check the **Enable VPN** checkbox to allow the VPN connection.



1. Check the **Disable VPN Windows Networking (NetBIOS) broadcast** checkbox. Leave the **Enable Fragmented Packet Handling** checkbox unchecked until the VPN logs show many fragmented packets transmitted.
2. Click the **Configure** tab and select **Manual Key** from the **IPSec Keying Mode** menu.
3. In the **Add/Modify IPSec Security Association** section, create a new **Security Association** by selecting **-Add New SA-** from the **Security Association** menu.
4. Enter a descriptive name that identifies the VPN client in the **Name** field, such as the client's location or name.
5. Enter "0.0.0.0" in the **IPSec Gateway Address** field.
6. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and may range from 3 to 8 characters in length.

***Note**: SPIs should range from 3 to 8 characters in length and include only 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). If you enter an invalid SPI, an error message is 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's Incoming SPI may be the same as the Outgoing SPI.*

7. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** from the **Encryption Method** menu.
8. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL client's encryption key, therefore, write it down to use while configuring the client.
9. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the 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.*

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 "0.0.0.0" in the **Range Start**, **Range End,** and **Destination Subnet Mask for NetBIOS broadcast** fields.
12. Click **Advanced Settings.**
13. Check **Enable Windows Networking (NetBIOS) broadcast** if the remote site is allowed access to network resources by browsing the Windows Network Neighborhood.
14. Check **Apply NAT and firewall rules** if applicable.
15. Check **Forward Packets to Remote VPNs** if configuring a "hub and spoke"network.
16. Check **Route all Internet Traffic through this SA** if configuring a remote site Security Association with access to the Internet via the VPN tunnel. If configuring a central site Security Association, this checkbox does not apply.
17. Enter the **Default LAN Gateway** if **Route all Internet traffic through this SA** is checked for a remote site Security Association and you are configuring a corresponding central site Security Association.
18. Click **OK** to close the **Advanced Settings** window.
19. 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.

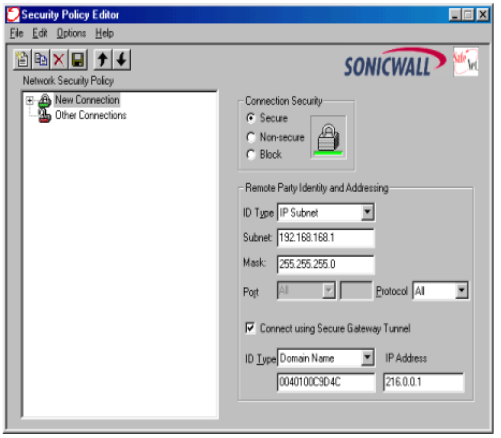
Installing the VPN Client Software

1. When you register your SonicWALL or 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.
2. Unzip the SonicWALL VPN Client zip file.
3. Double-click setup.exe and follow the VPN client setup program's step-by-step instructions. Enter the VPN client's 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**.

Select **Add > New Connection** in the **Edit** menu at the top of the **Security Policy Editor** window.



***Note**: The security policy may be renamed by highlighting **New Connection** in the **Network Security Policy** box and typing the desired security policy name.*

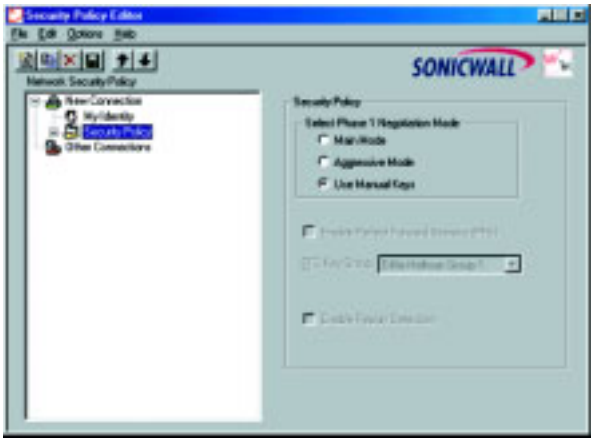
Configuring VPN Security and Remote Identity

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. Type the SonicWALL LAN IP Address in the **Subnet** field.
4. Type 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. Check the **Connect using Secure Gateway Tunnel** checkbox.
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.

Configuring VPN Client Security Policy

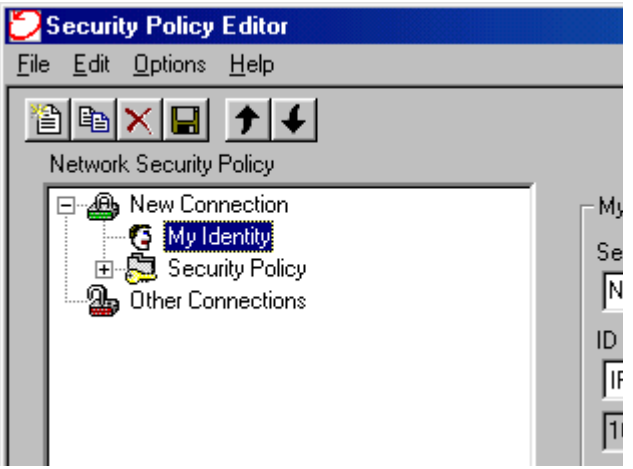
1. Double click **New Connection** in the **Network Security Policy** box on the left side of the **Security Policy Editor** window. **My Identity** and **Security Policy** should appear below **New Connection**.



2. Select **Security Policy** in the **Network Security Policy** box. The **Security Policy** interface appears.
3. Select **Use Manual Keys** in the **Select Phase 1 Negotiation Mode** box.

Configuring VPN Client Identity

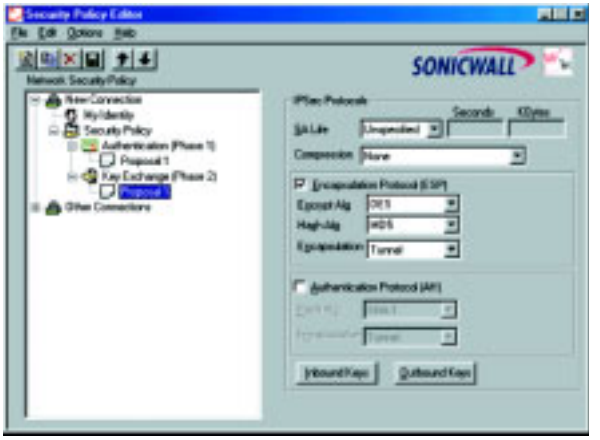
1. Click **My Identity** in the **Network Security Policy** box on the left side of the **Security Policy Editor** window.



2. Choose **None** in the **Select Certificate** menu on the right side of the **Security Policy Editor** window.
3. Select **IP Address** in the **ID Type** menu.
4. In the **Internet Interface** box, select the adapter you use to access the Internet. Select **PPP Adapter** in the **Name** menu if you have a dial-up Internet account. Select your **Ethernet** adapter if you have a dedicated Cable, ISDN, or DSL line.

Configuring VPN Client Key Exchange Proposal

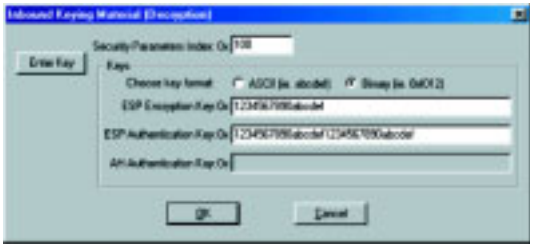
1. Double click **Key Exchange** in the **Network Security Policy** box. Then select **Proposal 1** below **Key Exchange**.



2. Select **Unspecified** in the **SA Life** menu.
3. Select **None** in the **Compressed** menu.
4. Check the **Encapsulation Protocol (ESP)** checkbox.
5. Select **DES** in the **Encryption Alg** menu.
6. Select **MD5** in the **Hash Alg** menu.
7. Select **Tunnel** in the **Encapsulation** menu.
8. Leave the **Authentication Protocol (AH)** checkbox unchecked.

Configuring Inbound VPN Client Keys

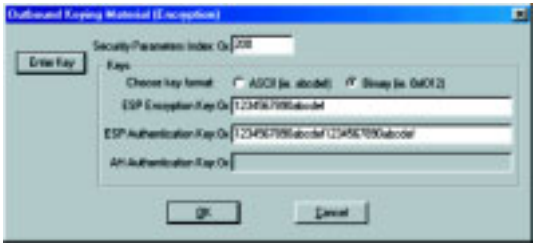
1. Click **Inbound Keys** . The **Inbound Keying Material box** appears.



2. Click **Enter Key** to define the encryption and authentication keys.
3. Type 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.



2. Click **Enter Key** to define the encryption and authentication keys.
3. Type the SonicWALL **Incoming SPI** in the **Security Parameter Index** field.
4. Select **Binary** in the **Choose key format** options.
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

1. Select **Save Changes** in the **File** menu in the top left corner of the **Security Policy Editor** window.

Instructions for testing the VPN tunnel and configuring WINS for browsing a remote network are found in the section Testing the VPN Tunnel.

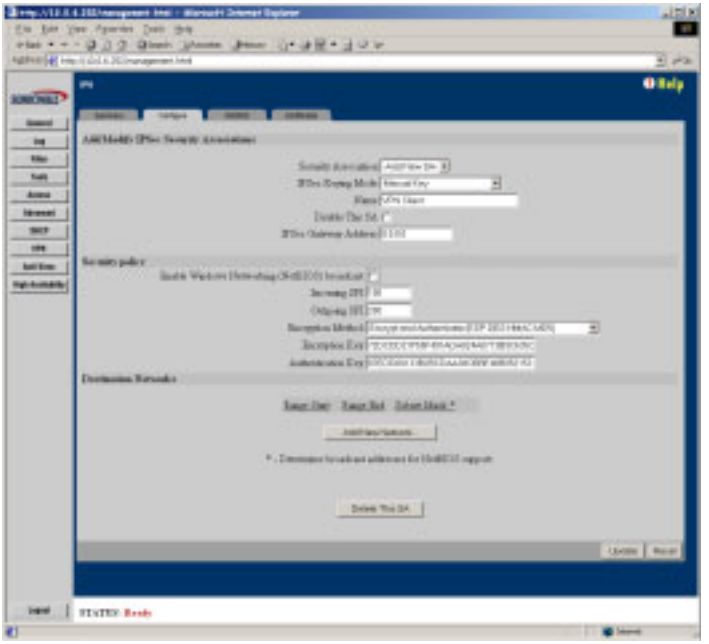
VPN between Two SonicWALLs

VPN between two SonicWALLs allows users to securely access files and applications at remote locations. The first step to set up a VPN between two SonicWALLs is creating corresponding **Security Associations** (**SAs**). The instructions below describe how to create an **SA** using **Manual Keying and Internet Key Exchange (IKE)**. These instructions are followed by an example illustrating a VPN tunnel between two SonicWALLs.

Manual Key between Two SonicWALLs

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

1. Select **Manual Key** 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 "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.

***Note**: SPIs should range from 3 to 8 characters in length and include only 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). 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's **Incoming SPI** may 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 for Check Point (ESP 3DES)** is similar to **Strong Encrypt (ESP 3DES)** but is interoperable with Check Point Firewall-1.
- **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 and Authenticate (ESP 3DES HMAC SHA-1)** is similar to **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** but uses HMAC SHA-1 instead of HMAC-MD5.
- **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.
- **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.
- **Encrypt and Authenticate (ESP DES HMAC SHA-1)** similar to MD5 but uses SHA-1.
- **Authenticate (AH MD5)** uses AH to authenticate VPN communications but it does not encrypt data.
- **Authenticate (AH SHA-1)** uses SHA-1 instead of MD5.
- **Authenticate (ESP MD5)** does not provide data confidentiality (no data encryption), but it uses MD5 for authentication.
- **Authenticate (ESP SHA-1)** similar to MD5 but uses SHA-1 for authentication.

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. Enter a 40 character hexadecimal key if you are using SHA-1. This encryption key must match the remote SonicWALL's encryption key.

   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 may 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 if using MD5. If uisng SHA-1, enter a 40 character hexadecimal key in the **Authentication Key** field.

   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 may 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's 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 checked. Otherwise, enter "0.0.0.0" in the field.
14. Click **Advanced Settings.**
15. Check **Enable Windows Networking (NetBIOS) broadcast** if the remote site is allowed access to network resources by browsing the Windows Network Neighborhood.
16. Check **Apply NAT and firewall rules** if applicable.
17. Check **Forward Packets to Remote VPNs** if configuring a “hub and spoke”network.
18. Check **Route all Internet Traffic through this SA** if configuring a remote site Security Association with access to the Internet via the VPN tunnel. If configuring a central site Security Association, this checkbox does not apply.
19. Enter the **Default LAN Gateway** if **Route all Internet traffic through this SA** is checked for a remote site Security Association and you are configuring a corresponding central site Security Association.
20. Click **OK** to close the **Advanced Settings** window.
21. 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.

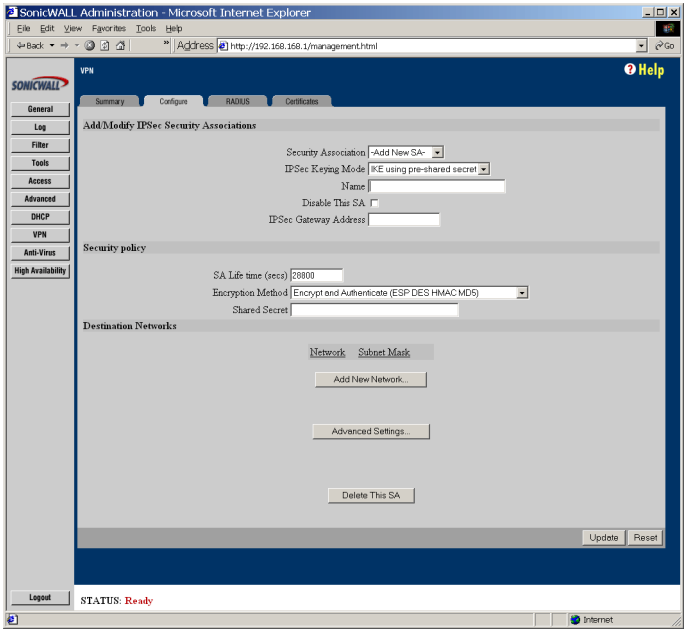
Configuring the Second SonicWALL Appliance

To configure the second SonicWALL appliance, follow the same configuration steps as the first SonicWALL. You must, however, enter the same SPIs and Encryption keys as the first SonicWALL appliance into the settings of the second SonicWALL appliance.

IKE Configuration between 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 at the top of the window.



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 Names for both SonicWALLs must match the opposite SonicWALLs' Unique Firewall Identifiers. This requirement adds another layer of authentication to maximize security.*

5. Define the length of time before an IKE Security Association automatically renegotiates in the **SA Life Time (secs)** field. The **SA Life Time** may range from 120 to 2,500,000 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.*

6. Select the appropriate encryption algorithm from the **Encryption Method** menu. The SonicWALL supports the following encryption algorithms:

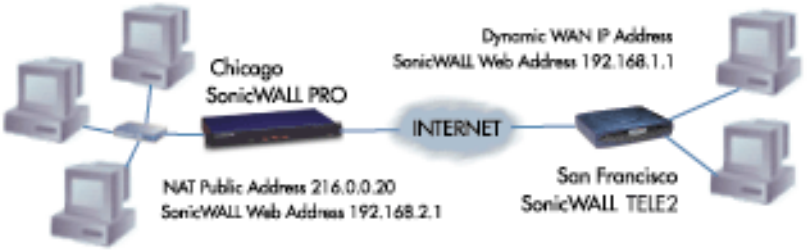
- **Tunnel Only (ESP NULL)** does not provide encryption or authentication, but offers access to machines at private addresses behind NAT. It also allows unsupported services through the SonicWALL.
- **Encrypt (ESP DES)** uses 56 bit DES to encrypt data. DES is an extremely secure encryption method, 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 for Check Point (ESP 3DES)** is similar to **Strong Encrypt (ESP 3DES)** but is interoperable with Check Point Firewall-1.
- **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 and Authenticate (ESP 3DES HMAC SHA-1)** is similar to **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** but uses HMAC SHA-1 instead of HMAC-MD5.
- **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.
- **Encrypt and Authenticate (ESP DES HMAC SHA-1)** similar to MD5 but uses SHA-1.
- **Authenticate (AH MD5)** uses AH to authenticate the VPN communications but it does not encrypt data.

- **Authenticate (AH SHA-1)** uses SHA-1 instead of MD5.
- **Authenticate (ESP MD5)** does not provide data confidentiality (no data encryption), but it uses MD5 for authentication.
- **Authenticate (ESP SHA-1)** similar to MD5 but uses SHA-1 for authentication.

7. Enter a alphanumeric "secret" in the **Shared Secret** field. The **Shared Secret** must match the corresponding field in the remote SonicWALL. This field may range from 4 to 128 characters in length and is case sensitive.
8. 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.
9. 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.
10. Enter the subnet mask of the remote network in the **Subnet mask** field.
11. Click **Advanced Settings.**
12. Check **Enable Keep Alive** if you want the SA to check for an active VPN tunnel while the tunnel is connected.
13. Check **Enable Perfect Forward Secrecy** for added security.
14. Check **Enable Windows Networking (NetBIOS) broadcast** if the remote site is allowed access to network resources by browsing the Windows Network Neighborhood.
15. Check **Apply NAT and firewall rules** if applicable.
16. Check **Forward Packets to Remote VPNs** if configuring a “hub and spoke”network.
17. Check **Route all Internet Traffic through this SA** if configuring a remote site Security Association with access to the Internet via the VPN tunnel. If configuring a central site Security Association, this checkbox does not apply.
18. Enter the **Default LAN Gateway** if **Route all Internet traffic through this SA** is checked for a remote site Security Association and you are configuring a corresponding central site Security Association.
19. Click **OK** to close the **Advanced Settings** window.
20. 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.

Example: Linking Two SonicWALLs

The following example illustrates the steps needed to create an IKE VPN tunnel between a SonicWALL GX250 and a SonicWALL TELE2.



A company wants to use VPN to link two offices together, one in Chicago and the other in San Francisco. To do this, the SonicWALL GX250 in Chicago and the SonicWALL TELE2 in San Francisco must have corresponding Security Associations.

Configuring a SonicWALL GX250 in Chicago

1. Enter the SonicWALL GX250 **Unique Firewall Identifier** in the **VPN Summary** window; in this example, "Chicago Office."
2. Create a new **Security Association** by selecting **-Add New SA-** from the **Security Association** menu in the **VPN Configure** window.
3. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
4. Because the SonicWALL TELE2 does not have a permanent WAN IP address, the SonicWALL GX250 needs to authenticate the VPN session by matching the **Name of the SA** with the TELE2 Unique Firewall Identifier. Enter the TELE2 Unique Firewall Identifier in the **Name** field, in this example, "San Francisco Office."
5. Enter the WAN IP address of the remote SonicWALL in the **IPSec Gateway Address** field. In this example, the San Francisco SonicWALL TELE2 has a dynamic IP address, therefore enter "0.0.0.0" in the **IPSec Gateway Address** field

***Note**: Only one of the two IPSec gateways may have a dynamic IP address when using SonicWALL VPN.*

6. Enter "86,400" in the **SA Life time (secs)** field to renegotiate IKE encryption and authentication keys every day.
7. Select a VPN method from the **Encryption Method** menu. Since data throughput and security are the primary concern, select **ARCFour**.

8. Define a **Shared Secret**. Write down this key as it is required when configuring the San Francisco Office SonicWALL TELE2.
9. Click **Add New Network...** to open the **VPN Destination Network** window and enter the destination network addresses.
10. Enter the IP address and subnet mask of the destination network, the San Francisco office, in the **Network** and **Subnet Mask** fields. Since NAT is enabled at the San Francisco office, enter a private LAN IP address. In this example, enter "192.168.1.1" and subnet mask "255.255.255.0."

***Note**: The **Destination Network Address** must NOT be in the local network's address range. Therefore, the San Francisco and Chicago offices must have different LAN IP address ranges.*

11. Click **Advanced Settings.**
12. Check **Enable Keep Alive** if you want the SA to check for an active VPN tunnel while the tunnel is connected.
13. Check **Enable Perfect Forward Secrecy** for added security.
14. Check **Enable Windows Networking (NetBIOS) broadcast** if the remote site is allowed access to network resources by browsing the Windows Network Neighborhood.
15. Check **Apply NAT and firewall rules** if applicable.
16. Check **Forward Packets to Remote VPNs** if configuring a “hub and spoke”network.
17. Check **Route all Internet Traffic through this SA** if configuring a remote site Security Association with access to the Internet via the VPN tunnel. If configuring a central site Security Association, this checkbox does not apply.
18. Enter the **Default LAN Gateway** if **Route all Internet traffic through this SA** is checked for a remote site Security Association and you are configuring a corresponding central site Security Association.
19. Click OK to close the **Advanced Settings** window.
20. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL GX250 is updated, a message confirming the update is displayed at the bottom of the browser window.

Configuring a SonicWALL TELE2 in San Francisco

1. Enter the SonicWALL TELE2 **Unique Firewall Identifier** in the **VPN Summary** window, in this example, "San Francisco Office."
2. Select **-Add New SA-** from the **Security Association** menu.
3. Select **IKE using pre-shared secret** from the IPSec Keying Mode menu.

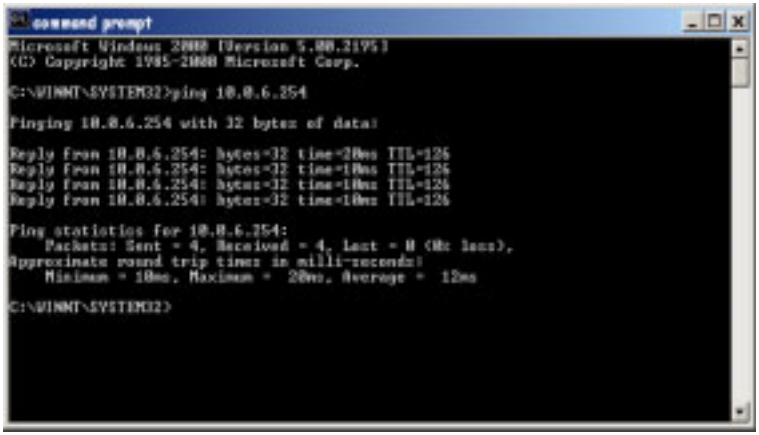
4. Enter the SonicWALL GX250 **Unique Firewall Identifier** in the SonicWALL TELE2 **Name** field, in this example, "Chicago Office."
5. Enter the SonicWALL GX250 WAN IP Address in the **IPSec Gateway Address** field. This address must be valid, and is the SonicWALL GX250 NAT Public Address, or "216.0.0.20."
6. Enter "86,400" in the **SA Life time (secs)** field to renegotiate keys daily.
7. Select the encryption algorithm from the **Encryption Method** menu. The San Francisco office **Encryption Method** must match Chicago, so **ARC Four** must be selected.
8. Enter the same **Shared Secret** used in the Chicago Office SonicWALL GX250 into the SonicWALL TELE2 **Shared Secret** field.
9. Click **Add New Network...** to open the **VPN Destination Network** window and define the destination network addresses.
10. 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."
11. Click **Advanced Settings.**
12. Check **Enable Keep Alive** if you want the SA to check for an active VPN tunnel while the tunnel is connected.
13. Check **Enable Perfect Forward Secrecy** for added security.
14. Check **Enable Windows Networking (NetBIOS) broadcast** to allow the remote site access to network resources by browsing the Windows Network Neighborhood.
15. Check **Apply NAT and firewall rules** if applicable.
16. Check **Forward Packets to Remote VPNs** if configuring a "hub and spoke"network.
17. Check **Route all Internet Traffic through this SA** if configuring a remote site Security Association with access to the Internet via the VPN tunnel. If configuring a central site Security Association, this checkbox does not apply.
18. Enter the **Default LAN Gateway** if **Route all Internet traffic through this SA** is checked for a remote site Security Association and you are configuring a corresponding central site Security Association.
19. Click OK to close the **Advanced Settings** window.
20. Click **Update** to add the remote network and close the **VPN Destination Network** window. Once the SonicWALL TELE2 has been updated, a message confirming the update is displayed at the bottom of the browser window.

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

Testing a VPN Tunnel Connection Using PING

To verify that your VPN tunnel is working properly, it is useful 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 un-successful ping returns a message of **Request Timed Out**.



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

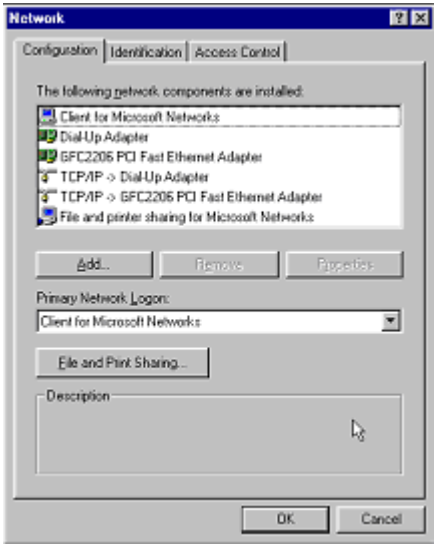
After you have successfully pinged the remote host and confirmed that your VPN tunnel is working, your administrator may ask you to configure your computer for Windows Networking. By configuring your computer for Windows Networking, you are able to

browse the remote network using **Network Neighborhood.** Before logging into the remote network, you need to following information from your administrator:

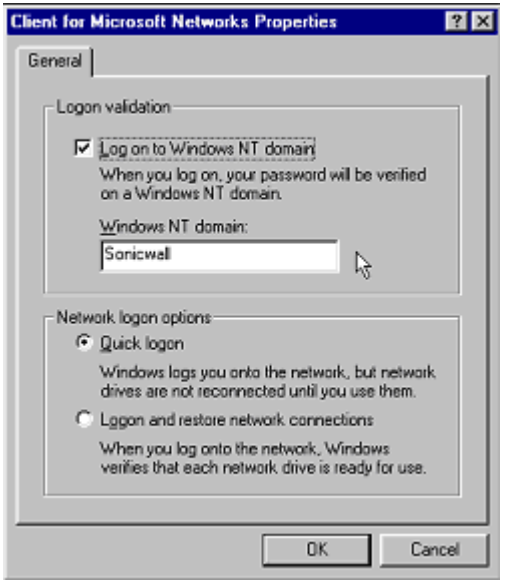
- **NT Account information including your username and password**
- **NT Domain Name**
- **WINS Server IP Address**
- **Internal DNS (optional)**

Use the following steps to configure **Windows Networking** on your computer (Windows98):

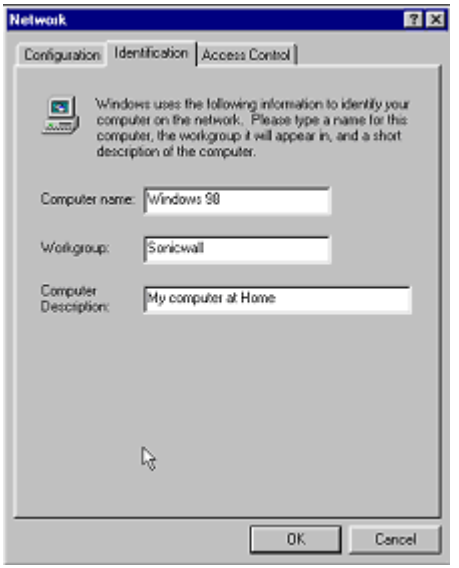
1. Click **Start**, then **Control Panel**. Locate the **Network** icon and double-click it.
2. Select **Client for Microsoft Networks** from the list, and then click **Properties**.



3. Check the **Logon to Windows NT Domain** checkbox, and enter the domain name provided by your administrator into the **Windows NT domain** text box. Select **Quick Logon** under **Network logon options** section.



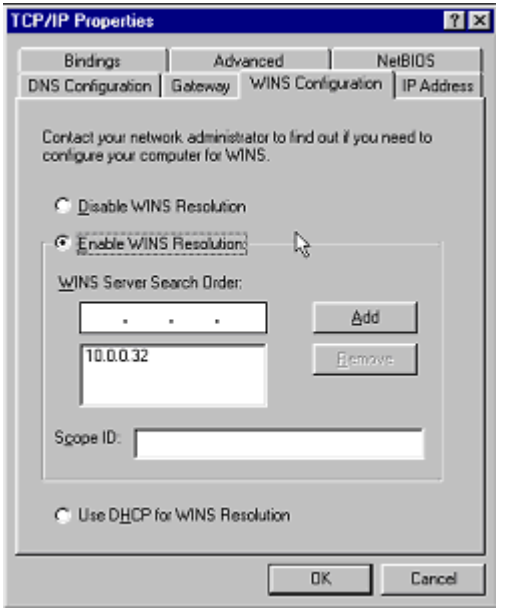
4. Click on the **Identification** tab, and enter the domain name provided by your administrator in the **Workgroup** text box.



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 serv-

er 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.



7. Windows98 users must restart their computer for the settings to take effect, and then log into the remote domain.

Windows2000 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 setup a WINS server and browse the network using Network Neighborhood.

To access shared resources on remote computers, you need to 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 may 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 menu and click the **Delete This SA** button. To modify an **SA**, select it from the menu, 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, may 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 may access the SQL server by using the server's 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's registry
- Configure a **WINS Server** to resolve a name to a remote IP address.

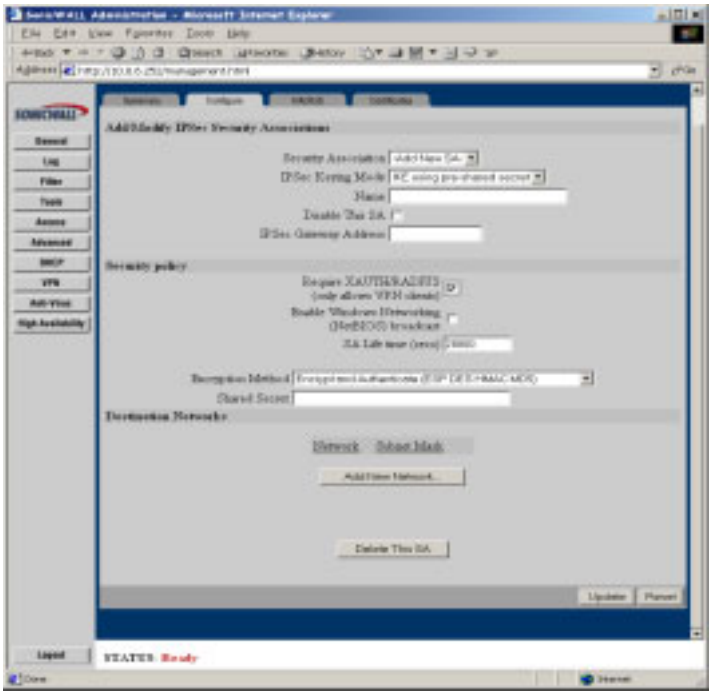
Radius and Xauth Authentication

An IKE Security Association may be configured to require RADIUS authentication before allowing VPN clients to access LAN resources. This authentication provides an additional layer of VPN security while simplifying and centralizing management. RADIUS authentication allows many VPN clients to share the same VPN configuration, but requires each client to authenticate with a unique user name and password. And because a RADIUS server controls network access, all employee privileges may be created and modified from one location.

***Note**: SonicWALL's RADIUS implementation supports Steel-Belted RADIUS by Funk Software. A 30-day demo version of Steel-Belted RADIUS may be downloaded from <http://www.funk.com>.*

To enforce RADIUS authentication, complete the following instructions.

1. Click **VPN** on the left side of the browser window and then click the **Configure** tab at the top of the window.

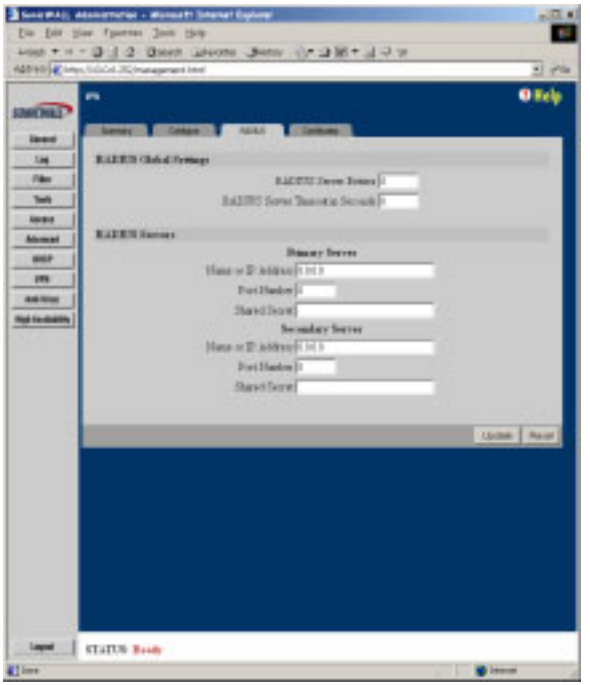


2. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** menu.
3. Check the **Require XAUTH/RADIUS (only allows VPN clients)** checkbox. This forces inbound VPN clients to connect to this Security Association to authenticate to a RADIUS server.
4. Configure the **Security Association** as specified in the **IKE Configuration** for the **VPN Client** section.

***Note**: Only SonicWALL VPN Clients may authenticate to a RADIUS server. Users tunneling from another VPN gateway, such a second SonicWALL, is not able to complete the VPN tunnel if the Require XAUTH/RADIUS checkbox is checked.*

Configuring the RADIUS Settings

Click **VPN** on the left side of the browser window, and then click the **RADIUS** tab at the top of the window.



To configure RADIUS settings, complete the following instructions.

1. Check the **Enable RADIUS** checkbox.
2. Define the number of times the SonicWALL attempts to contact the RADIUS server in the **RADIUS Server Retries** field. If the RADIUS server does not respond within the specified number of retries, the VPN connection is dropped. This field may range between 0 and 30, however 3 RADIUS server retries is recommended.
3. Enter the number of seconds between attempts to contact the RADIUS server in the **RADIUS Server Timeout in Seconds** field. The RADIUS server timeout may range from 0 to 60 seconds, but 5 seconds is recommended.

RADIUS Servers

Specify the settings of the primary RADIUS server in the **RADIUS servers** section. An optional secondary RADIUS server may be defined if a backup RADIUS server exists on the network.

1. Enter the IP address or domain name of the RADIUS server in the **IP Address/ name** field.

2. Enter the UDP port number that the RADIUS server listens on. The Steel- Belted RADIUS server is set, by default, to listen on port 1645.
3. Enter the RADIUS server's administrative password or "shared secret" in the **Shared Secret** field. The alphanumeric **Shared Secret** may range from 1 to 30 characters in length. The **Shared Secret** is case sensitive.

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

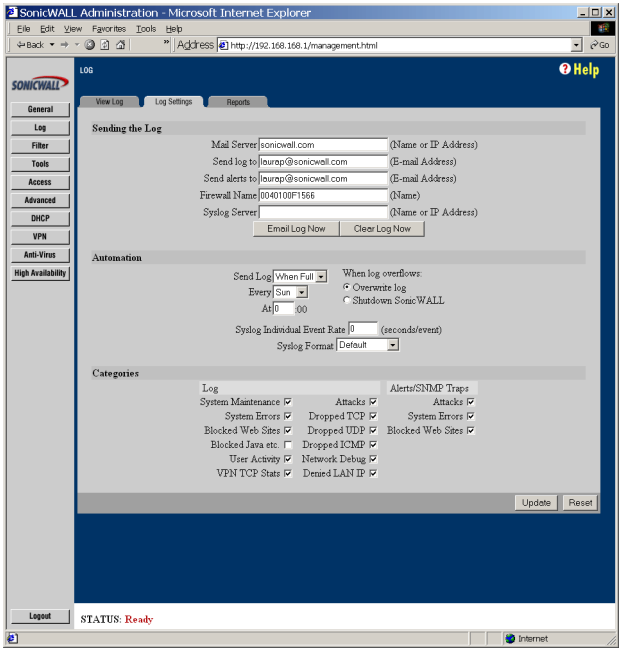
The **User Name** and **Password** is relayed to the RADIUS server for verification. Once the VPN client is authenticated, the client can access network resources.

SonicWALL Enhanced VPN Logging

If **Network Debug** is checked 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 may occur with the connections.

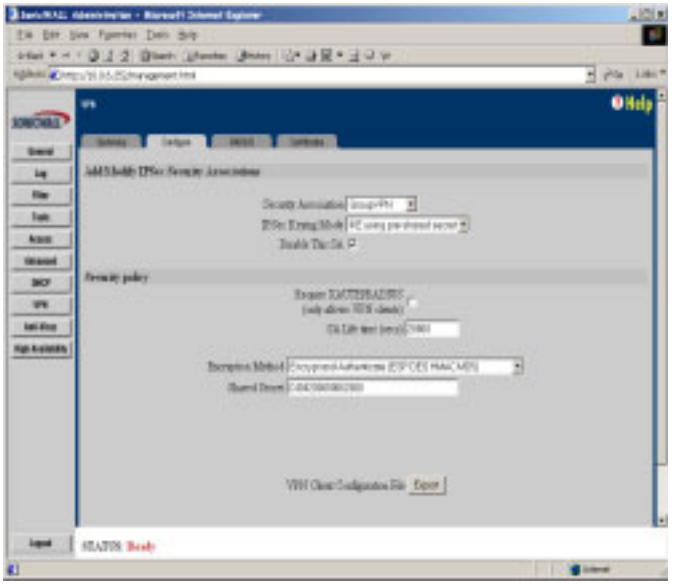
To use the enhanced VPN Logging feature, perform the following steps:

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.



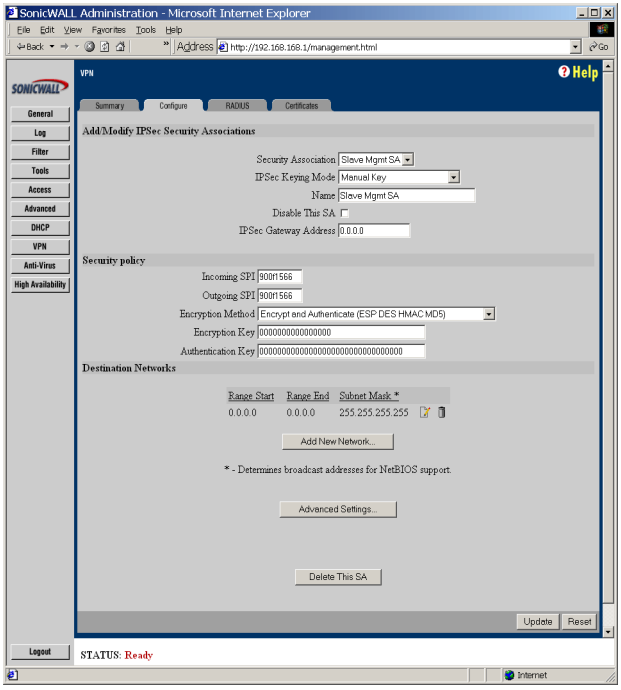
Disabling Security Associations

Administrators may 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.



Editing and Deleting Security Associations

In the **Current IPSec Security Associations** section of the VPN Summary tab, VPN Security Associations may be edited by either clicking on the hyperlinked name of the Security Associaton or by clicking the **Notepad** icon located after the **Encryption Method**. Security Associations may be deleted from the **Current IPSec Security Associations** section of the **Summary** tab by clicking on the Trash Can icon located next to the Notepad icon. Or, click on the hyperlinked name of the Security Association to go to the **Configure** tab, and delete the Security Association by clicking **Delete this SA** at the bottom of the page.



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 are typically 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 need 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 the necessary settings needed to create a VPN tunnel. Different SAs may 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 Encryption and Authentication Keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass IP traffic. The initial exchange occurs on UDP port 500, so when an IKE SA is created, the SonicWALL will automatically open up port 500 to allow the IKE key exchange.

- **Manual Keying**

  Manual keying allows you to specify the Encryption and Authentication keys. 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 may 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 will also increase 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.

  SonicWALL VPN's 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.

  SonicWALL VPN's 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.

  SonicWALL's 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.

13 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 mission 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 PRO-VX and the GX product line. It is available as an upgrade for the SonicWALL PRO. 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:

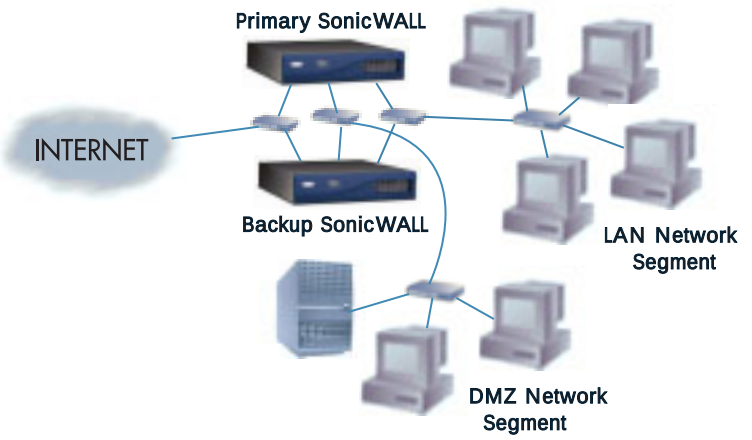
- You have two (2) SonicWALL GX 250, two (2) GX650, two (2) PRO, or two (2) PRO-Vx Internet Security Appliances. The **High Availability** pair must consist of two identical SonicWALL models.
- You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (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 will not be 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:

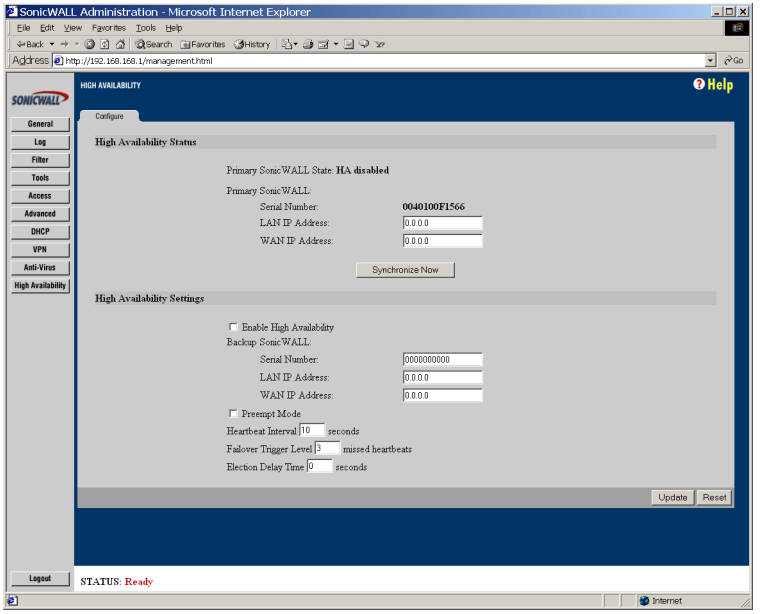


All SonicWALL ports being used must be connected together with a hub or switch. Each SonicWALL must have a unique LAN IP Address on the same LAN subnet. If each SonicWALL has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

***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 together.*

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.



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 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 a primary SonicWALL becomes active after bootup, it looks for the backup SonicWALL on the network. In some cases, there may be a delay in locating the backup firewall due to

network delays built into some switches. Configure the primary SonicWALL to allow an increment of time (in seconds) to look for the backup SonicWALLon the network. the default value of 0 is correct.

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 that during initial configuration, the backup SonicWALL has not been 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.

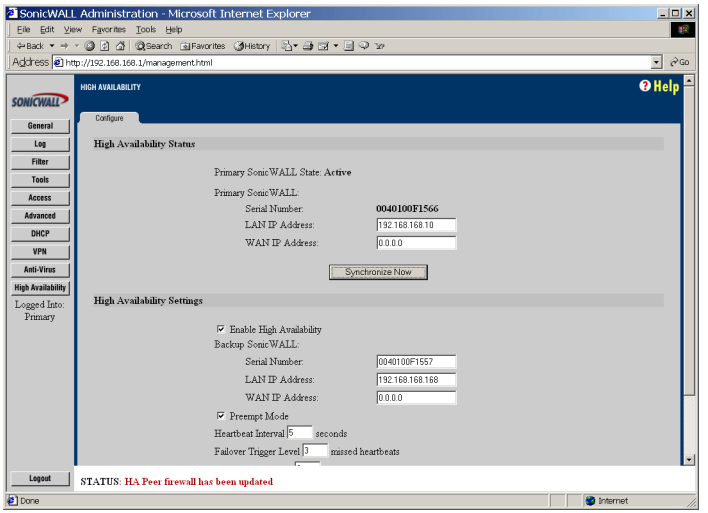
To check the backup SonicWALL firmware version or serial number, log into the backup SonicWALL, click **General** on the left side of the browser window and then click **Status** at the top of the window. Both the firmware version and the SonicWALL serial number are displayed at the top of the window.

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 maintain 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.



***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 Availiability configuration.*

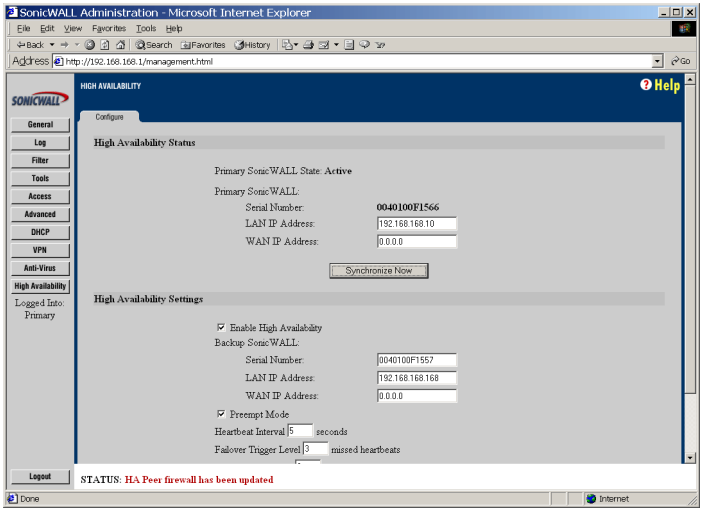
High Availability Status

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.

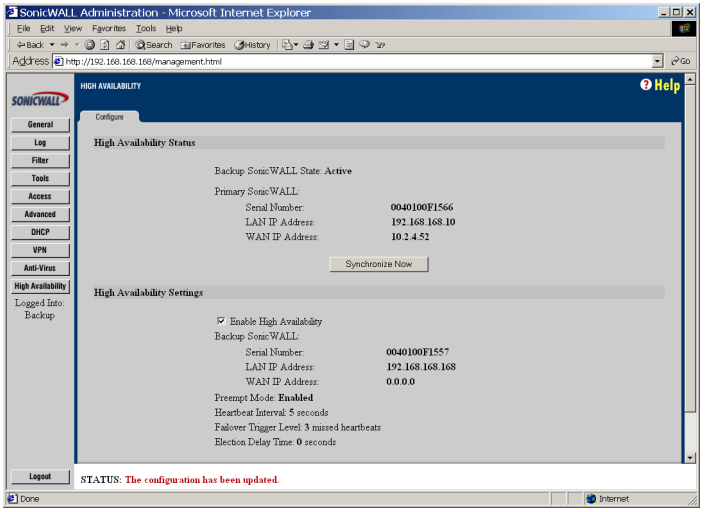
High Availability Status Window

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, iyou 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**.



If the backup SonicWALL is active, the first line changes to reflect the active status of the backup as shown below:



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.*

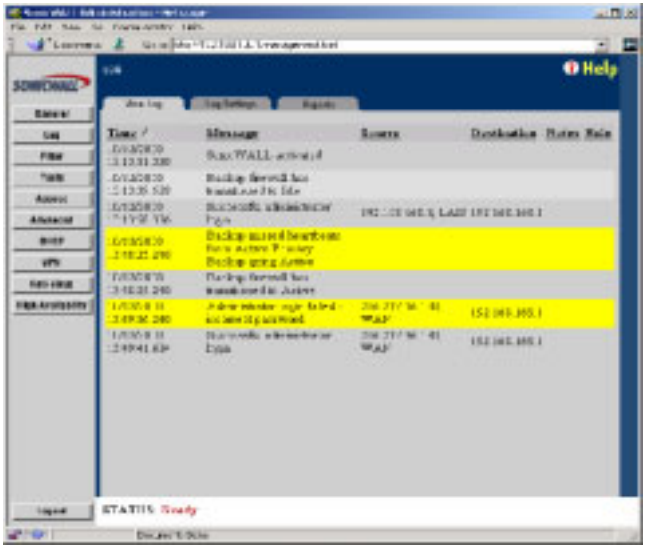
E-mail Alerts Indicating Status Change

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.

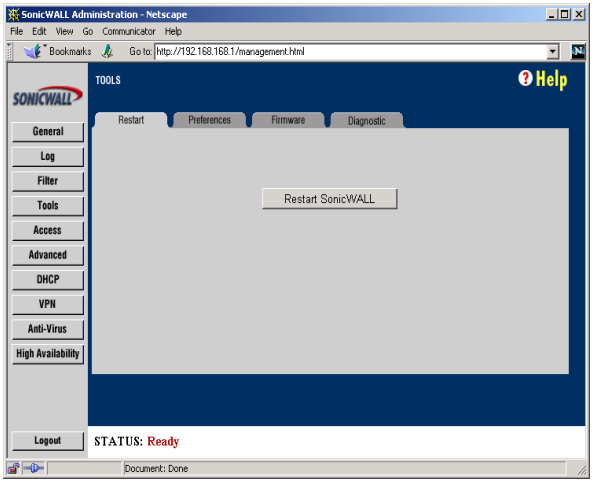


Forcing Transitions

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 preventative maintenance on the primary SonicWALL.

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

To restart the active SonicWALL, log into the primary SonicWALL LAN IP Address and click **Tools** on the left side of the browser window and then click **Restart** at the top of the window.



Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **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.*

14 VIEWPOINT

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 SonicWALL's Internet security offerings by providing detailed and comprehensive reports of network activity.

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

SonicWALL ViewPoint:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site

SonicWALL ViewPoint software may be installed on a server running Windows 2000 or NT located on the SonicWALL's LAN. SonicWALL ViewPoint is available as a standard feature for the SonicWALLGX series.

Getting Started with ViewPoint

SonicWALL ViewPoint is a software reporting solution that may be installed on any computer on the SonicWALL's LAN. The computer used to host the reporting software is referred to as the “ViewPoint Server.”

Minimum System Requirements

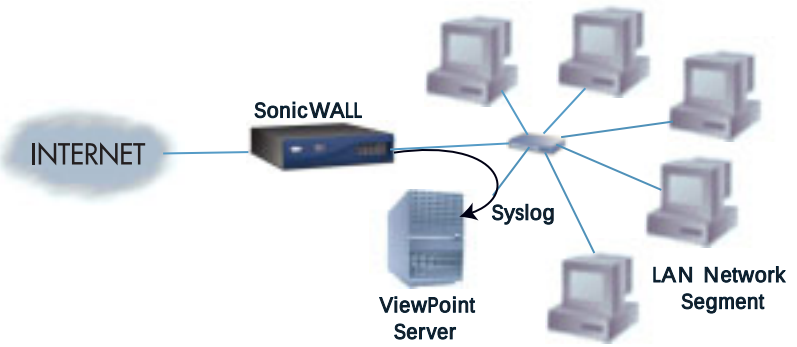
The following is a list of the minimum requirements for the ViewPoint Server:

- Microsoft Windows 2000 or NT 4.0 Service Pack 4 or greater
- 500 MHz Processor
- 512 MB available disk space
- 256 MB memory
- Internet Explorer 4.0 or later or Netscape Navigator 4.x

***Note**: More disk space may be required to analyze large networks.*

Network Configuration for ViewPoint

The following diagram illustrates the network configuration for SonicWALL ViewPoint:



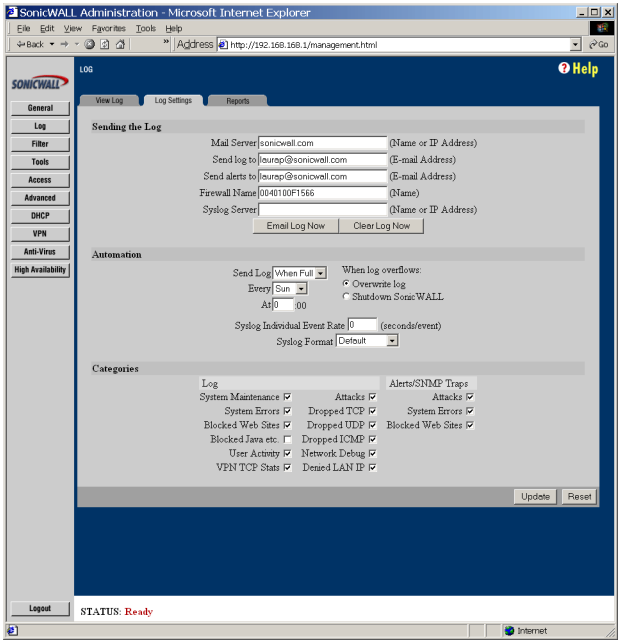
The SonicWALL ViewPoint Server may be any computer or server located on the SonicWALL's LAN running Windows 2000 or Windows NT 4.0 SP 4 or greater and meeting the minimum system requirements.

***Note**: The ViewPoint Server must have a static, permanent IP address.*

Configuring the SonicWALL for ViewPoint

This page describes the configuration of the SonicWALL to direct the syslog to the ViewPoint Server.

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



2. Enter the IP address or domain name of the ViewPoint Server in the **Syslog Server** field.

***Note**: The ViewPoint Server must have a static IP address. Confirm that the server has a permanent IP address in the ViewPoint Server TCP/IP Properties window.*

3. Enter “0”in the **Syslog Individual Event Rate** field to send all syslog messages without filtering.

4. Confirm that the **Syslog Format** is set to **Default**.

5. Click **Update**, and then restart the SonicWALL to update the changes.

Installing ViewPoint Software

You may download the ViewPoint software file from the SonicWALL, Inc. Web site. When ViewPoint version 1.1 is available, the ViewPoint software will be included on a CD-ROM. If your SonicWALL GX series included a ViewPoint CD, you may skip the following instructions and instead run the ViewPoint setup program from the ViewPoint CD.

Internet Download Installation

To download and install the software from the Internet, save the ViewPoint executable file to your hard drive and then double click the file to run the executable.

The ViewPoint server must be running Windows 2000 or Windows NT SP 4 or greater and it must have a static IP address.

Note: *The Windows DNS configuration must also be properly configured, or domain and host names are not be displayed in ViewPoint's Web-based reports.*

Software License Agreement

Before the program files are copied to your system, the Software License Agreement is presented.

- If you agree to the stated terms, click **Yes**.
- If you do not agree, click **No** to exit the setup program without installing.

Note: *When you install ViewPoint, be sure to close all other applications on the ViewPoint Server.*

The installation wizard guides you through the set up program and installs ViewPoint reporting software and a syslog server, Tomcat Web Server, and MySQL Database.

The ViewPoint setup program detects whether the default Web, syslog or MySQL ports are in use. If the default Web port is active, the setup program automatically recommends an alternative Web port, port 8080. If either syslog port 514 or MySQL port 3306 are active, the ViewPoint setup program displays an error message.

Note: *If you have a syslog server already installed on your computer, you must remove the existing program and install the syslog server provided with SonicWALL ViewPoint.*

The Installation Wizard prompts you to define the ViewPoint Web Server port. The default Web (HTTP) port is port 80.

Note: If you have a Web server already installed on the ViewPoint Server, then configure the ViewPoint's Web server to run on an unused HTTP port, such as the recommended port, 8080.

The Installation Wizard prompts you to define additional settings, such as the SonicWALL LAN IP address and the SonicWALL administrator password.

Once the programs are installed, you may close the ViewPoint Installation Wizard window. You need to restart your computer for the changes to take effect.

Managing ViewPoint

Logging into the ViewPoint Web Interface

You must configure several settings in the ViewPoint Web Interface in order to view network reports.

Login to the ViewPoint Web Interface. Type http://LocalHost or http://<ViewPoint Server IP Address> into the **Location** or **Address** field of your Web browser or launch ViewPoint from the **SonicWALL** folder in the Windows **Start** menu. An authentication window is displayed.

Note: *If you configured the ViewPoint Web server to use a different port than port 80, then add the port number to the URL, for example,* http://LocalHost:8080*.*

1. Type the **User Name** and **Password**.

Note: *The default* ***User Name*** *is "admin" and the default* ***Password*** *is "password."*

Note*: The password that was configured during the ViewPoint installation is used to authenticate to your SonicWALL Internet security appliance, it does not provide access to ViewPoint.*

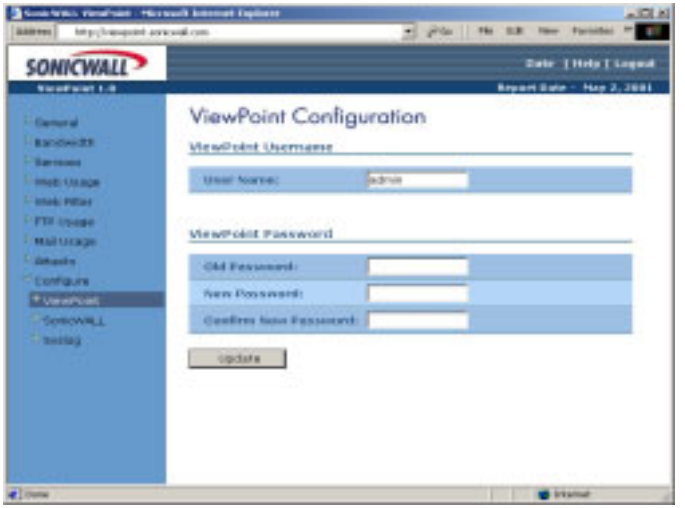
2. Click the **Login** button to login to the Web Interface.

Note*: Confirm that the authentication screen has finished loading before attempting to log in. Also note that the ViewPoint password is case-sensitive.*

Configuring ViewPoint Settings

ViewPoint requires that clients successfully authenticate to access reports. This authentication mechanism prevents unknown users from viewing sensitive network data. The ViewPoint Configuration window allows you to modify the ViewPoint user name and password.

1. From the ViewPoint Web Interface, expand the **Configure** option on the left side of the browser window and then click **ViewPoint**.



2. To change the ViewPoint user name, highlight the text in the **User Name** field and replace it with your new user name.
3. To change the ViewPoint password, enter your current ViewPoint password in the **Old Password** field.
4. Enter the new ViewPoint password in the **New Password** and **Confirm New Password** fields.

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

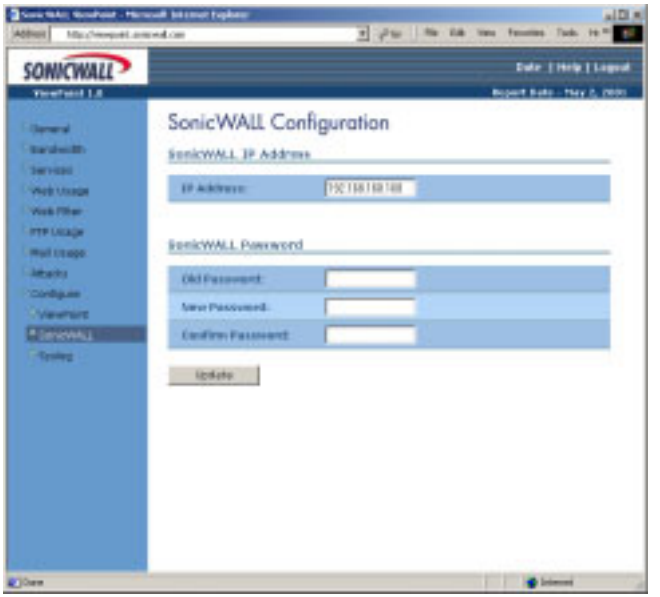
5. Click the **Update** button to update the configuration.

Note: *If you lose or forget the ViewPoint user name or password, you will need to uninstall and then reinstall the ViewPoint software.*

Configuring SonicWALL Settings for Viewpoint

ViewPoint transparently authenticates to your SonicWALL Internet security appliance for status and state information. ViewPoint uses the SonicWALL administrator password and IP address configured during ViewPoint installation to authenticate. If the SonicWALL IP address or password is changed, you will need to modify the ViewPoint settings to reflect these changes.

1. From the ViewPoint Web Interface, expand the **Configure** option on the left side of the browser window and then click **SonicWALL**.



2. Enter the LAN IP Address of your SonicWALL Internet security appliance in the **IP Address** field.
3. Enter the current SonicWALL administrator password in the **Old Password** field.
4. Enter the new SonicWALL administrator password in the **New Password** and **Confirm New Password** fields.

Note: *This password must match the password of your SonicWALL appliance.*

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

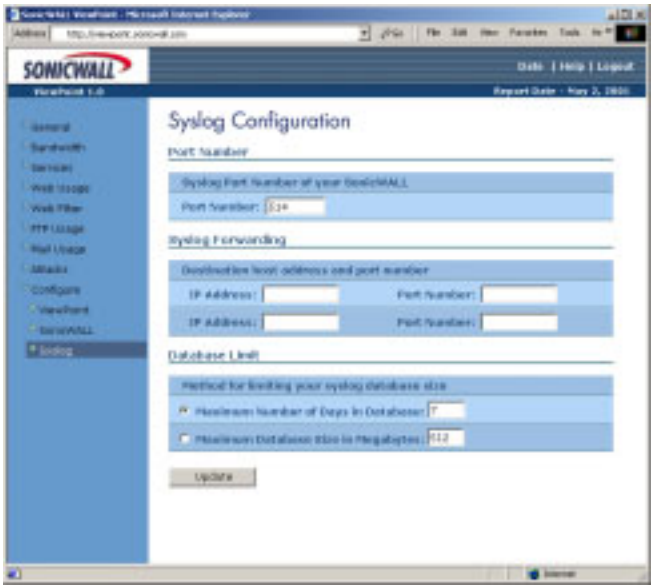
5. Click the **Update** button to update the configuration. Then logout of ViewPoint and reauthenticate in order for these changes to take effect.

Note: *If you lose or forget the password that had been defined in the SonicWALL Configuration window and ViewPoint cannot authenticate to your SonicWALL, you will need to uninstall and reinstall the ViewPoint software, and then define the correct SonicWALL administrator password.*

Configuring Syslog Settings

The Syslog Configuration window allows you to change the UDP port number that ViewPoint syslog server listens on, to configure ViewPoint to forward syslog data to other servers, and to limit the database size.

1. From the ViewPoint Web Interface, expand the **Configure** option on the left side of the browser window and then click **Syslog**.



2. To change the UDP port number that the ViewPoint syslog server listens on, enter the new port number in the **Port Number** field.

Note: *SonicWALL Internet security appliances write syslog traffic on port number 514.*

3. To forward syslog data to a backup server, enter the IP address of the secondary server in the **IP Address** field.

4. Enter the port number that the syslog data uses to send data in the **Port Number** field.

5. You may configure the maximum size of the ViewPoint database. To limit the database by number of days, select the **Maximum Number of Days in Database** radio button and enter the number of days that syslog messages should be saved in the corresponding field.

   To limit the database by size, select the **Maximum Database Size in Megabytes** radio button and enter the number of megabytes of memory that the database will store in the corresponding field.

Note: *By default, Viewpoint saves database records for seven days.*

6. Click **Update** and restart the ViewPoint server for syslog settings changes to take effect.

Note: *Maintenance on the ViewPoint database is completed every night, after midnight. Changes to the database size do not take effect until database maintenance is performed.*

Setting the ViewPoint Report Date

You may change the ViewPoint report date quickly and easily.

1. To change the report date, click the **Date** option in the top right corner of the browser window.

2. The current report date is highlighted in the ViewPoint date calendar. Select the desired month and year from the **Month** and **Year** menus.
3. Select the desired day in the ViewPoint date calendar. The new report date will be displayed in the upper right corner of the ViewPoint Report window. The ViewPoint report table and chart is also updated to show the new report date.
4. Click **Close** to close the ViewPoint Date Selector window.

ViewPoint Web Interface

This section briefly describes the ViewPoint Web Interface and the Web-based help options. The ViewPoint Web Interface may be accessed from any computer located on the same network as the ViewPoint Server from a Web browser.

Note: *Please use Internet Explorer 4.0 or greater or Netscape Navigator 4.x to login and manage ViewPoint. Confirm that your Web browser is configured to allow cookies and Java code.*

General, **Bandwidth**, **Services**, **Web Usage**, **Web Filter**, **FTP Usage**, **Mail Usage**, **Attacks**, and **Configure** options appear on the left side of the window. You may navigate through the Web-based ViewPoint reports by selecting and expanding the menu options on the left side of browser window and then selecting the desired ViewPoint report.

The ViewPoint Web Interface also includes links at the top right corner of the browser window. These options are: **Date**, **Help**, and **Logout**.

- The **Date** option opens a new window. This window allows you to change the report date from a Web-based calendar.
- The **Help** option displays comprehensive, Web-based instructions for installing, configuring and troubleshooting ViewPoint.
- The **Logout** option on the upper right side of the browser window terminates the management session and redisplays the Authentication window. If the **Logout** option is clicked, it is necessary to re-login and authenticate to use ViewPoint.

Note: *The ViewPoint administrator is automatically logged out of the ViewPoint User Interface after 5 minutes of inactivity.*

The current report date is displayed at the top right of the ViewPoint window.

ViewPoint Report Layout

Most ViewPoint reports include a chart and a table. The chart displays information such as the amount of bandwidth through the SonicWALL over time. The table provides a summary of the data displayed in the chart. Several reports deviate from this layout: the **General Status** report presents state information retrieved directly from the SonicWALL, the **Bandwidth Monitor** and **Service Monitor** display dynamic, real-time graphs of network activity through the SonicWALL, and the **Admin Login**, **User Login**, **Failed Login**, **VPN Events**, and **System Events** reports display a list of all pertinent events sorted by time.

Next / Previous

Some reports may contain thousands of records; more data than can be displayed in a single table. These reports include **Next** and **Previous** links at the top of the table which allow you to view the subsequent or preceding report data.

Source

The **Source** is the domain or host name or the IP address of the device that initiated an event.

Destination

The **Destination** is the domain or host name or the IP address that the event was directed towards.

Event / Hit

There are two primary methods to measure network activity through the SonicWALL, the amount of data transferred in bytes or the number of individual events. Depending upon the report type, events may be called "hits", "events", or "connections". All of these terms describe a single IP connection from one location to another location through the SonicWALL.

KBytes / MBytes

Most ViewPoint reports display data in terms of KBytes or MBytes. KBytes, an abbreviation for kilobytes, and MBytes, an abbreviation for megabytes, describe the amount of data that was transferred through the SonicWALL.

ViewPoint Report Descriptions

General Reports

Status

The **General Status** report displays comprehensive information about the current status of the SonicWALL. The Status report includes the SonicWALL serial number, firmware version, ROM version, enabled upgrades and subscriptions, the number of users connected to the SonicWALL, and other state information.

Admin Login

The Administrative Login report displays successful administrative authentications to the SonicWALL that occurred during the report period. The Administrative Login report helps identify misuse and unauthorized management of your SonicWALL Internet security appliance.

The Administrative Login report table displays the time and the name or IP address of the machine that authenticated to the SonicWALL.

User Login

The User Login report lists successful authentications to the SonicWALL to bypass content filtering or to remotely access local network resources. User names, passwords and user privileges are defined on the Users window in the SonicWALL Web Management Interface. The User Login report illustrates the location and frequency of authenticated user sessions.

The User Login report table displays the time and the name or IP address of the machine that authenticated to the SonicWALL.

Failed Login

The Failed Login report lists all attempts to login into your SonicWALL Internet security appliance. Failed authentication attempts include unsuccessful administrative and user logins. The Failed Login report identifies unauthorized authentication attempts and uncovers malicious activity.

The Failed Login report table displays the time and the name or IP address of the machine that attempted to authenticate to the SonicWALL.

VPN Events

The VPN Events report lists all VPN events, including VPN SA negotiation attempts, VPN key exchanges, VPN heartbeat messages and VPN connection errors. The VPN Events report helps illustrate the cause of VPN negotiation failures. It also identifies unknown or suspicious VPN activity.

The VPN Events table displays the time, the source and destination of the event, and the type of event that occurred.

System Events

The System Events report lists events and errors that occurred to the SonicWALL Internet security appliance during the report period. System events include successful downloads of the Content Filter List, SonicWALL activations, DHCP and PPPoE informational messages, and High Availability backup firewall activation. System errors listed include problems downloading the Content Filter List, difficulties obtaining a DHCP Client or PPPoE Client Lease, deactivation of the SonicWALL because the log was full, and the number of simultaneous connections exceeding the limit.

The System Events table displays the time, the source name or IP address, and the type of system event. Since many system events are created by the SonicWALL, the SonicWALL will be the most common source of events. Most events are results of normal SonicWALL operation, and do not indicate network or SonicWALL problems.

Bandwidth Reports

Bandwidth Summary Report

The Bandwidth Summary report shows the level of traffic traveling through your SonicWALL over time. This report helps to determine when to perform system maintenance on the SonicWALL. It also displays peak bandwidth usage times and predicts future bandwidth needs.

The Bandwidth Summary Report displays a bar graph of all IP traffic through the SonicWALL in MBytes transferred. The table displays the hour of the day, the number of events that occurred during the hour, the number of MBytes transferred, and the MBytes as a percentage of the total MBytes for the report day. Both the chart and the table include inbound and outbound traffic through the LAN, WAN, and DMZ interfaces.

Bandwidth Monitor

The Bandwidth Monitor report displays a real-time graph of all network activity through the SonicWALL. The Bandwidth Monitor displays inbound and outbound IP traffic through the SonicWALL in either KBytes or MBytes per second over the past 5 minutes. The Bandwidth Monitor includes traffic through the LAN, WAN, and DMZ interfaces.

Top Users of Bandwidth

The Top Users of Bandwidth report shows the top users of bandwidth in KBytes per second. This report illustrates which users on the LAN, the WAN, or the DMZ are using the greatest amount of bandwidth. This data helps identify inappropriate bandwidth use.

The Top Users of Bandwidth report includes a pie chart of the top users of bandwidth as a percentage of total MBytes transferred. The colors in the pie chart correspond with the users listed in the table. The report table displays the IP address, host or domain name of the top 10 users, the number of connections initiated by or directed to the users, the number of MBytes transferred by the users, and the MBytes transferred as a percentage of all MBytes transferred.

Services Reports

Service Summary

The Service Summary Report shows the amount of bandwidth used by a service. This report reveals inappropriate use of Internet bandwidth and can help determine network access policies enforced by your SonicWALL.

The Service Summary Report displays a graph of FTP, HTTP, ICMP, NetBIOS, DNS, NTP, SMTP and other service traffic by the number of events or IP connections that have occurred. The report table lists the services displayed in the graph, the number of events per service, the number of KBytes transferred, and the KBytes as a percentage of the total KBytes for the report period.

Service Monitor

The Service Monitor report displays a real-time graph of network activity by a service over the past 5 minutes. The Service Monitor shows FTP, HTTP, ICMP, NetBIOS, DNS, NTP, SMTP, and other services in KBytes or MBytes transferred per second. The Service Monitor includes traffic through the LAN, WAN, and DMZ interfaces.

Web Usage Reports

Web Usage Summary Report

The Web Usage Summary report shows the amount of Web (HTTP) traffic traveling through your SonicWALL over time. This report displays peak bandwidth usage times of Web traffic and provides information about the number of Web site hits and bandwidth use during the report period.

The Web Usage Summary report displays a bar graph of Web traffic through the SonicWALL in MBytes transferred. The table displays the hour of the day, the number of Web hits that occurred during the hour, the number of MBytes transferred, and the MBytes as a percentage of the total MBytes for the report period.

Top Web Sites

The Top Web Sites report identifies the most popular Web sites accessed through your SonicWALL. This report provides a snapshot of the Web sites located on the LAN, WAN, or DMZ that users are visiting.

The Top Web Sites report displays a bar graph of the top 20 Web sites visited by the number of hits to the site. The table displays the name of the Web site, the number of hits to the Web site, the number of KBytes transferred, and the number of hits as a percentage of the total hits during the report period.

Note: *Each Web site listed in the table includes a link to the site, so that the ViewPoint administrator may view and evaluate the top Web sites.*

Top Users of Web

The Top Users of Web report shows the most active users accessing Web sites on the Internet or on the LAN or DMZ network segments. This report displays the number of Web site hits and the amount of bandwidth transferred, identifying inappropriate or excessive Web usage.

The Top Users of Web report displays a pie chart of the top 10 users by the number of Web site hits. The report table lists the top 10 users displayed in the chart, the number of MBytes transferred by the user, the number of hits generated by the user, and the number of hits as a percentage of the total Web hits during the report period.

Top Web Sites by User

The Top Web Sites By User report shows the top 5 Web sites visited by user. This report provides clear and in-depth information about Web activity by network user.

The Top Web Sites By User report displays a table listing the top users of Web, the top 5 Web sites visited by each user, and the KBytes transferred from the Web site to the user. Additional users' Web activity may be displayed by clicking the **Next 5** link at the top of the report table. This report includes LAN users accessing Internet sites, as well as WAN users accessing Web sites hosted on the LAN or DMZ.

Note: *Each Web site displayed in the table includes a link to the site, so that the ViewPoint administrator may view and evaluate the listed Web sites.*

Web Filter Reports

Web Filter Summary Report

The Web Filter Summary report shows the number of attempts to access blocked Web sites over time. The Web Filter Summary report includes Web sites blocked by the SonicWALL's Content Filter List or by customized Keyword or Domain Name filtering. This report also includes blocked Java, blocked cookies and blocked ActiveX attempts.

The Web Filter Summary report displays a bar graph of attempts to access objectionable Web sites by the number of blocked attempts. The table displays the hour of the day, the number of attempts to access objectionable Web content during the hour, and the number of attempts as a percentage of the total attempts during the report period.

Top Objectionable Web Sites

The Top Objectionable Web Sites report presents the top Web site destinations that were blocked by the SonicWALL. This report allows you to see which sites users are attempting to access.

The Top Objectionable Web Sites report displays a pie chart of the top 20 objectionable Web sites by the number of attempts to access the site. The table lists the top objectionable Web sites, the number of attempts to access the site, and the number of attempts as a percentage of the total attempts during the report period.

***Note**: The Web sites displayed in the table include links to the blocked sites, so that the ViewPoint administrator may view and evaluate blocked Web sites. The ViewPoint administrator may also be blocked from accessing these sites if he or she does not have privileges to bypass the SonicWALL's Content Filter List.*

Top Users Attempting to Access Objectionable Web Sites

The Top Users Attempting to Access Objectionable Web Sites report shows the users most frequently blocked by the SonicWALL's Content Filtering policies. This report presents a list of users that are trying to access inappropriate or objectionable material on the Internet.

The Top Users Attempting to Access Objectionable Web Sites report displays a pie chart of the top 10 users by the number of connection attempts. The report table lists the top 10 users displayed in the chart, the number of Web attempts by the user, and the number of attempts as a percentage of the total blocked attempts during the report period.

Top Objectionable Web Sites By User

The Top Objectionable Web Sites By User report shows the top 5 filtered Web sites by user. This report describes the Web sites users attempted to visit that were blocked by the SonicWALL's Web Content Filtering policies.

The Top Objectionable Web Sites By User report displays a table of the users blocked by the SonicWALL, the top 5 Web sites the users attempted to access, and the number of attempts to access each Web site. If more than 5 users attempted to access objectionable Web sites, the additional users' Web activity may be displayed by clicking the Next 5 link at the top of the report table.

FTP Usage Reports

FTP Usage Summary Report

The FTP Usage Summary Report shows the amount of inbound and outbound FTP traffic traveling through the SonicWALL in KBytes per second. This report displays peak bandwidth usage times for FTP traffic and provides detailed information about bandwidth use and the number of FTP sessions.

The FTP Usage Summary Report displays a bar graph of FTP traffic through the SonicWALL in MBytes transferred. The table displays the hour of the day, the number of FTP events that occurred during the hour, the number of MBytes transferred for FTP, and the number of MBytes as a percentage of the total MBytes for the report period.

Top Users of FTP

The Top Users of FTP report shows the most active users on the LAN, WAN, or DMZ transferring FTP files. This report shows the number of FTP events and the amount of data transferred by individual users.

The Top Users of FTP report displays a pie chart of the top 10 users of FTP by the number of KBytes transferred. The report table lists the top 10 users displayed in the chart, the number of FTP events generated by the user, the number of KBytes transferred by the user, and the number of KBytes as a percentage of total KBytes of FTP during the report period.

Mail Usage Reports

Mail Usage Summary Report

The Mail Usage Summary Report shows the amount of E-mail traveling through the SonicWALL. The report displays peak bandwidth usage times for E-mail.

The Mail Usage Summary Report displays a bar graph of Mail traffic through the SonicWALL in KBytes transferred. The table displays the hour of the day, the number of Mail events that occurred during the hour, the number of KBytes transferred for Mail, and the number of KBytes as a percentage of the total KBytes for the report period.

Note: *Mail Usage includes SMTP, POP3, and IMAP traffic*.

Top Users of Mail

The Top Users of Mail report shows the most active users on the LAN, WAN, or DMZ sending or receiving E-mail messages. This report shows the number of E-mail files transferred by user in KBytes and the total number of E-mail events through the SonicWALL.

The Top Users of Mail report displays a pie chart of the top 10 users by the number of Mail Events. The report table lists the top 10 users displayed in the chart, the number of KBytes transferred by the user, the number of mail events generated by the user, and the number of events as a percentage of the total Mail Events during the report period.

Attack Reports

Attack Summary Report

The Attack Summary Report shows the number of attacks the SonicWALL received over the report period. It displays Denial of Service attacks, intrusions, probes, and all other malicious activity targeted against the SonicWALL or computers on the LAN or DMZ.

The Attack Summary Report displays a bar graph of the number of attacks received by the SonicWALL. The table displays the hour of the day, the number of attacks that occurred during the hour and the number of attacks as a percentage of the total attacks during the report period.

Top Sources of Attacks

The Top Sources of Attacks report shows the top users that attacked the SonicWALL or devices on the network over the report period. Top sources of attacks reveal the IP addresses or host names of devices that generated the most attacks.

The Top Sources of Attacks report displays a pie chart of the top 10 sources by the number of attacks. The report table lists the top 10 sources displayed in the chart, the number of attacks generated by the source, and the number of attacks as a percentage of the total attacks during the report period.

Number of Attacks by Category

The Number of Attacks by Category report presents attacks against the SonicWALL by category over the report period. Attack categories include IP spoof, Ping of Death, SYN flood, land, smurf, probe, and Trojan.

The Number of Attacks by Category report displays a pie chart of the top attack categories by number of attacks. The report table lists the top 10 attack categories displayed in the chart, the number of attacks for the category, and the number of attacks for the category as a percentage of the total attacks during the report period.

Dropped Packets

The Dropped Packets report displays all IP packets dropped by your SonicWALL. IP packets dropped by the SonicWALL include: TCP Packets, UDP Packets, ICMP Packets, IPSec Packets, PPTP Packets, Broadcast Packets, and Fragmented Packets. The Dropped Packets report includes blocked NetBIOS packets and other normal Internet activity and it also signals unusual or suspicious connection attempts.

The Dropped Packets Report displays a bar graph of the number of IP packets dropped by the SonicWALL. The table displays the hour of the day, the number of dropped packets during the hour and the number of dropped packets as a percentage of the total dropped packets during the report period.

Accessing ViewPoint Remotely

Because the ViewPoint Interface is Web browser-based, any user on the SonicWALL's LAN may login and look at ViewPoint network reports. Even users located across a VPN or accessing network resources through applications such as pcAnywhere should be able to contact the ViewPoint Web Interface.

To access ViewPoint, the remote user should launch a Web browser, then type http://<ViewPoint Server IP Address> into the **Location** or **Address** field of the Web browser.

Note: *If the ViewPoint Web Interface uses a different port than port 80, add the port number after the IP address, for example, type http://<IP Address>:8080.*

Note: *Internet Explorer 4.0 or greater or Netscape Navigator 4.x should be used to login and manage ViewPoint. The Web browser must also be enabled for Java and cookies and support Java applets.*

1. Type the ViewPoint **User Name** and **Password**.
2. Click **Login** to access to the Web Interface.

The remote user can now view network reports and perform all management functions.

Uninstalling ViewPoint

Uninstall the ViewPoint program and all of its components from your system by relaunching the ViewPoint setup program.

1. If you installed ViewPoint from a CD, load the CD into your server and run the ViewPoint setup program.

   If you downloaded the ViewPoint executable file from the SonicWALL Web site, then select and launch the ViewPoint executable file from your local disk. If you can not locate the ViewPoint executable file, you may download it from http://www.sonicwall.com.

2. The ViewPoint setup program automatically detects ViewPoint and displays a window to confirm deletion of the software. To remove the ViewPoint software application and all of its components, select **OK**.

3. The ViewPoint uninstall program prompts you to remove the MySQL Server and Clients 3.23. To remove this software, click **Yes**.

4. The ViewPoint uninstall program also prompts you to delete the ViewPoint database data. To remove the data, click **Yes**. To keep the data for future use, click **No**.

5. Click **Finish** to complete the uninstallation process.

ViewPoint Server Across a VPN

While it is recommended that the ViewPoint Server be located on the SonicWALL's LAN for performance issues, it may also be located remotely, across a VPN. The only requirement is that the ViewPoint Server must be able to access and login to the SonicWALL Web Management Interface.

Note: *If your VPN tunnel is interrupted or temporarily disabled, report data may be lost.*

ViewPoint Software Components

The ViewPoint software program consists of several different components. These components include: MySQL Database version 3.2.3, Tomcat Web server, a syslog server, and SonicWALL ViewPoint software files.

MySQL Database

MySQL is a relational database management system. It is open source software that uses SQL, or Structured Query Language, the most common standardized language used to access databases. To learn more about the MySQL database system, visit http://www.mysql.com.

Tomcat Web Server

Tomcat is a Web server and Java servlet engine developed by the Apache Software Foundation. More specifically, Tomcat is a Java server that invokes servlets when JSP

pages are requested. To learn more about Tomcat software or the Apache Software Foundation, visit http://www.apache.org.

SonicWALL ViewPoint Software

SonicWALL ViewPoint software includes proprietary HTML, Java and servlet files as well as a Syslog Daemon. The SonicWALL Syslog Daemon receives syslog messages from a SonicWALL Internet security appliance on UDP port 514 and then forwards the messages to the MySQL database.

ViewPoint software operates on Windows 2000 or Windows NT 4.0 Service Pack 4 or greater.

Active ViewPoint Services

For maintenance or other reasons, it may be necessary to start or stop ViewPoint services. ViewPoint-related services in the "Control Panel/Administrative Tools/ Services" directory include **ViewPoint**, **Syslogd**, and **MySql**.

Processes initiated by ViewPoint that appear in the Windows Task Manager include **mysqld-nt.exe,** two instances of **java.exe**, and two instances of **srvany.exe**.

15 SONICWALL OPTIONS AND FEATURES

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 Network Anti-Virus Subscription**
- **SonicWALL Content Filter List Subscription**
- **SonicWALL Authentication Service**
- **SonicWALL Vulnerability Scanning Service**
- **Per Incident Support**
- **Extended Warranty**

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 myCIO.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 may be purchased in 10, 50 and 100 license annual subscriptions.

SonicWALL Content Filter List Subscription

Inappropriate online content may 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 needs 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 may be given a password to bypass the filter, giving them unrestricted access to the Internet.

SonicWALL Authentication Service

SonicWALL Authentication Service provides extra security for VPN tunnels and users.

SonicWALL Vulnerability Scanning Service

You can scan your network for any security vulnerabilities using the SonicWALL Vulnerability Scanning Service.

SonicWALL Per Incident Support

SonicWALL **Per Incident Support** offers fast, personal assistance for a single technical support issue. SonicWALL **Per Incident Support** is ideal if you have a single problem that requires a quick resolution. This support program minimizes network downtime by offering immediate technical assistance for your configuration issues.

SonicWALL Premium Support

The SonicWALL **Premium Support** Program, based on a yearly subscription, provides the best possible service to SonicWALL customers. It minimizes potential network downtime by offering priority assistance from our knowledgeable support staff who provide expert advice for setting up SonicWALLs in even the most complex networks. It also includes advance swap shipment of defective products. SonicWALL **Premium Support** is an excellent program if you rely heavily on network and Internet connectivity and cannot afford network downtime.

SonicWALL Extended Warranty

SonicWALL **Extended Warranty** provides one additional year of warranty coverage and continued access to SonicWALL Technical Support resources. There is no limit to how many times the warranty may be extended. Once the warranty expires, additional warranty coverage cannot be purchased.

SonicWALL Global Management System

SonicWALL **Global Management System** is a scalable, cost-effective solution that extends the SonicWALL ease of administration, giving you the tools to manage the security policies of remote, distributed networks. SonicWALL GMS is included as a standard feature on the GX250 and GX650. 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.

Please 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

16 APPENDICES

APPENDIX A- 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 B- CONFIGURING TCP/IP SETTINGS

The following steps describe how to configure the Management Station's 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 may be helpful when configuring the SonicWALL's IP settings.

From a Windows 95 or 98 computer, do the following:

1. From the **Start** menu, 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 Macintosh computer, do the following:

1. From the Apple menu, choose **Control Panel**, and then choose **TCP/IP** to open the **TCP/IP Control Panel**.
2. From the **Configure** menu, choose **Manually**.
3. Enter "192.168.168.200" in the **IP address** field.
4. 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 C- ERASING THE FIRMWARE

It may be necessary to reset the SonicWALL to its factory clean state if the administrator password is forgotten, or the firmware has become corrupt. 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 will be necessary to follow the initial configuration procedures detailed in this manual's QuickStart section to reconfigure the SonicWALL.

1. Turn off the SonicWALL and disconnect it from the network.
2. Locate the recessed Reset Switch on the back panel of the SonicWALL.
3. Press and hold down 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.

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 D- SECURING THE SONICWALL

Mounting the SonicWALL GX250 and SonicWALL GX650

The SonicWALL **GX250** and SonicWALL **GX650** 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.

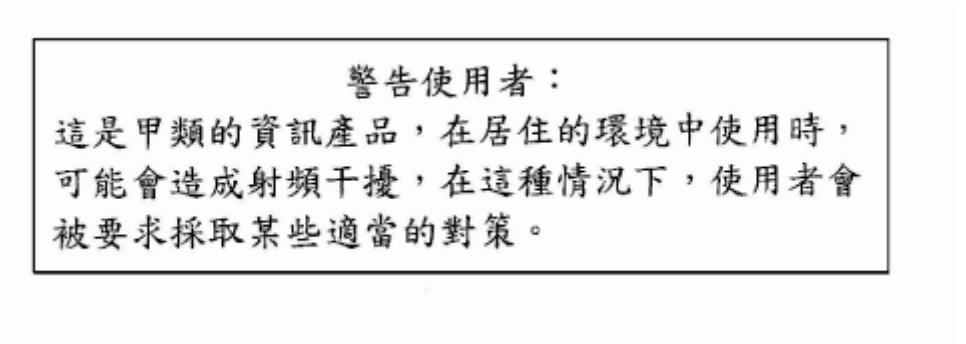
APPENDIX E- ELECTROMAGNETIC COMPATIBILITY

SonicWALL GX250 and SonicWALL GX650

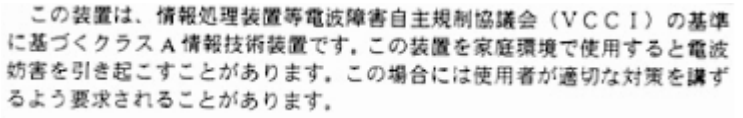
FCC Statement

This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may 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 may 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 may violate FCC rules.

BSMI Statement



VCCI Statement



CSA Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

NOTES

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

WARNINGS AND NOTICES

Lithium Battery Disposal Warning

The Lithium Battery used in the SonicWALL Internet Security appliance must 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 the SonicWALL Internet Security appliance requires disposal, it must be done in accordance with the manufacturer's instructions.

UL Power Supply Compliance Notice

Caution: Disconnect power cord before servicing power supply. To disconnect all power and current to the system, unplug both power cords from system.

Radiation Warning

Caution: Use of controls or adjustments of performance or procedures other than those specified herein may result in hazardous radiation exposure.