

SonicWALL Internet Security Appliances

SonicWALL TZ 170 SP/W/SPW

SonicOS Standard 2.2

Administrator's Guide



Table of Contents

Preface	1
Copyright Notice	1
Limited Warranty	1
Introduction	1
SonicWALL SonicOS Standard Overview	1
SonicWALL Management Interface.....	1
Accessing the Management Interface.....	1
Navigating the Management Interface	2
Applying Changes	2
Getting Help	2
Logging Out	2
About this Guide.....	3
Organization of this Guide	3
Guide Conventions	4
Icons Used in this Manual.....	4
SonicWALL Technical Support.....	5
North America Telephone Support.....	5
International Telephone Support	5
More Information on SonicWALL Products and Services	5
Internet Connectivity Using the Setup Wizard	7
Configuring a Static IP Address with NAT Enabled.....	7
Setup Wizard	8
Step 1: Change Password	8
Step 2: Change Time Zone	9
Step 3: WAN Network Mode	9
Step 4: WAN Network Mode: NAT Enabled.....	10
Step 5: LAN Settings.....	10
Step 6: LAN DHCP Settings	11
Step 7: SonicWALL Configuration Summary	11
Storing SonicWALL Configuration	12
Setup Wizard Complete	12
Configuring DHCP Networking Mode.....	13
Step 1: Change Password	13
Step 2: Change Time Zone	14
Step 3: WAN Network Mode	14
Step 4: WAN Network Mode: NAT with DHCP Client	15
Step 5: LAN Settings.....	15
Step 6: DHCP Settings	16

Configuration Summary.....	16
Storing SonicWALL Configuration.....	17
Setup Wizard Complete	17
Configuring NAT Enabled with PPPoE	18
Step 1: Change Password.....	18
Step 2: Change Time Zone	19
Step 3: WAN Network Mode	19
Step 4: WAN Network Mode: NAT with PPPoE Client	20
Step 5: LAN Settings	20
Step 6: DHCP Server	21
Step 7: SonicWALL Configuration Summary	21
Storing SonicWALL Configuration	22
Setup Wizard Complete	22
Configuring PPTP Network Mode.....	23
Step 1: Change Password.....	23
Step 2: Change Time Zone	24
Step 3: WAN Network Mode	24
Step 4: WAN Network Mode: NAT with PPTP Client	25
Step 5: LAN Settings	25
Step 6: DHCP Server	26
Step 7: SonicWALL Configuration Summary	26
Storing SonicWALL Configuration	27
Setup Wizard Complete	27
System Settings	29
System>Status.....	29
System Messages.....	29
System Information	29
Security Services.....	30
Registering Your SonicWALL	30
mySonicWALL.com.....	30
Latest Alerts	31
Network Interfaces	31
System>Licenses.....	31
Security Services Summary	31
Manage Security Services Online	31
Manual Upgrade.....	32
System>Administration	32
Firewall Name	32
Name/Password	33
Administrator Name	33
Changing the Administrator Password.....	33

Login Security	33
Enable Administrator/User Lockout	33
Management Protocol	34
Advanced Management	34
Enable SNMP	34
Enable Management Using SonicWALL GMS	35
System>Time	36
Set Time.....	36
NTP Settings.....	37
System>Settings	37
Settings	37
Import Settings	37
Export Settings	37
Firmware Management	38
New Firmware	38
Updating Firmware Manually	39
Firmware Management Settings.....	39
SafeMode - Rebooting the SonicWALL	39
System Information.....	40
Firmware Management.....	40
System>Diagnostics	41
DNS Name Lookup	41
Find Network Path	41
Ping.....	42
Packet Trace.....	42
Tech Support Report.....	43
Generating a Tech Support Report	44
Trace Route	44
System>Restart.....	44
Network.....	45
Network>Settings	45
Network Addressing Modes	46
Interfaces	46
Configuring WAN Settings	47
WAN Properties>General	47
Configuring LAN Settings.....	48
LAN Properties>General	48
Multiple LAN Subnet Support	48
Configuring OPT/DMZ Settings	50
Configuring the OPT/DMZ Port in Transparent Mode.....	50
Configuring the OPT/DMZ Port in NAT Mode.....	51
Configuring the SonicWALL in Transparent Mode.....	52

Configuration Example.....	53
Configuring NAT with DHCP Client.....	53
Configuring LAN Settings.....	55
LAN Properties>General.....	55
Configuring NAT with PPPoE Client.....	56
Configuring LAN Properties for NAT with PPPoE Client.....	58
Configuring NAT with L2TP Client.....	59
Configuring LAN Properties for NAT with L2TP Client.....	61
Configuring NAT with PPTP Client.....	62
Configuring LAN Properties for NAT with PPTP Client.....	64
DNS Settings.....	65
Network>One-to-One NAT.....	65
One-to-One NAT Configuration Example.....	66
Network>Web Proxy.....	68
Configuring Automatic Proxy Forwarding (Web Only).....	68
Bypass Proxy Servers Upon Proxy Failure.....	69
Network>Intranet.....	69
Installation.....	69
Intranet Settings.....	70
Network>Routing.....	71
Static Routes.....	71
Static Route Configuration Example.....	72
Route Advertisement.....	72
Route Table.....	73
Network>ARP.....	74
Network>DHCP Server.....	75
DHCP Settings.....	75
Configuring DHCP Server for Dynamic Ranges.....	75
The General Tab.....	76
The DNS/WINS Tab.....	77
Configuring Static DHCP Entries.....	77
The General Tab.....	78
The DNS/WINS Tab.....	78
Current DHCP Leases.....	79
Configuring the TZ 170 Wireless.....	81
Considerations for Using Wireless Connections.....	81
Recommendations for Optimal Wireless Performance.....	82
Adjusting the TZ 170 Wireless Antennas.....	82
Wireless Guest Services (WGS).....	82
Wireless Node Count Enforcement.....	82
MAC Filter List.....	83
WiFiSec Enforcement.....	83

SonicOS Standard Wireless Features and Enhancements	83
Wireless Status Page Updates	83
TZ 170 Wireless Deployment Scenarios	84
Configuring the TZ 170 Wireless as an Office Gateway	85
Welcome to the SonicWALL Setup Wizard	85
Selecting the Deployment Scenario	85
Changing the Password	86
Selecting Your Time Zone	86
Configuring the WAN Network Mode	86
Configuring WAN Settings	87
Configuring LAN Settings	87
Configuring WLAN 802.11b Settings	87
Configuring WiFiSec - VPN Client User Authentication	88
Configuring Wireless Guest Services	88
SonicWALL Configuration Summary	88
Storing SonicWALL Configuration	89
Congratulations!	89
Configuring the TZ 170 Wireless as a Secure Access Point	90
Welcome to the SonicWALL Setup Wizard	90
Selecting the Deployment Scenario	90
Changing the Password	90
Selecting Your Time Zone	91
Configuring the WAN Network Mode	91
Configuring WAN Settings	92
Configuring the LAN Settings	92
Configuring WLAN 802.11b Settings	92
Configuring WiFiSec - VPN Client User Authentication	93
Configuring Wireless Guest Services	93
SonicWALL Configuration Summary	93
Storing SonicWALL Configuration	94
Congratulations!	94
Configuring the TZ 170 Wireless as a Guest Internet Gateway	95
Welcome to the SonicWALL Setup Wizard	95
Selecting the Deployment Scenario	95
Changing the Password	95
Selecting Your Time Zone	96
Configuring the WAN Network Mode	96
Configuring WAN Settings	96
Configuring the LAN Settings	97
Configuring WLAN 802.11b Settings	97
Configuring Wireless Guest Services	97
SonicWALL Configuration Summary	98
Storing SonicWALL Configuration	98
Congratulations!	98
Configuring the TZ 170 Wireless using a Custom Deployment	99
Welcome to the SonicWALL Setup Wizard	99

Selecting the Deployment Scenario	99
Changing the Password	99
Selecting Your Time Zone	100
Configuring the WAN Network Mode	100
Configuring WAN Settings	100
Configuring LAN Settings	101
Configuring WLAN 802.11b Settings	101
Configuring WiFiSec - VPN Client User Authentication	101
Configuring Wireless Guest Services	102
SonicWALL Configuration Summary	102
Storing SonicWALL Configuration	102
Congratulations!	103
Using the Wireless Wizard	103
Welcome to the SonicWALL Wireless Configuration Wizard ..	103
WLAN Network	104
WLAN 802.11b Settings	104
WLAN Security Settings	105
WiFiSec - VPN Client User Authentication	105
Wireless Guest Services	106
Wireless Configuration Summary	106
Updating the TZ 170 Wireless!	107
Congratulations!	107
Access Point Status	109
WLAN Statistics	109
Station Status	110
Wireless > Settings	111
Wireless Radio Mode	111
WiFiSec Enforcement	111
Secure Wireless Bridging	113
Wireless Bridging (without WiFiSec)	113
Configuring a Secure Wireless Bridge	114
Network Settings for the Example Network	115
Configuring VPN Policies for the Access Point and Wireless Bridge	115
Advanced Configuration for both VPN Policies	115
Wireless > WEP Encryption	117
WEP Encryption Settings	117
WEP Encryption Keys	118
Beaconing & SSID Controls	119
Wireless Client Communications	119
Advanced Radio Settings	119
Configurable Antenna Diversity	119
Wireless>MAC Filter List	121
Wireless Intrusion Detection Services	122
Wireless Bridge IDS	122
Access Point IDS	122
Enable Client Null Probing	123

Sequence Number Analysis	123
Association Flood Detection	123
Rogue Access Point Detection	123
Authorizing Access Points on Your Network	124
Wireless Guest Services.....	125
Wireless Guest Services	126
Bypass Guest Authentication	126
Dynamic Address Translation (DAT)	126
URL Allow List	127
IP Deny List	128
Configuring Wireless Guests	129
Enable Account	129
Auto-Prune Account	129
WGS Login Uniqueness	129
Activate Account Upon First Login	129
Automated Account Generation	129
Account Lifetime	129
Session Lifetime	130
Idle Timeout.....	130
Comment	130
Account Detail Printing	130
Flexible Default Route.....	130
Secure Access Point with Virtual Adapter Support.....	130
Secure Access Point with Wireless Guest Services	132
Modem.....	1
Modem > Status	1
Modem Status.....	1
Modem > Settings	2
Configuring Profile and Modem Settings	2
Modem > Failover.....	3
Modem Failover Settings	3
Configuring Modem Failover	4
Modem > Dialup Profiles	5
Dial-Up Profiles	5
Configuring a Dialup Profile	5
Modem > Dialup Profiles > Modem Profile Configuration	6
Configuring a Dialup Profile	6
Chat Scripts	9
Custom Chat Scripts.....	9
Firewall	11
Using Bandwidth Management with Access Rules	11

Firewall>Access Rules.....	12
Restoring Default Network Access Rules.....	12
Adding Rules using the Network Access Rule Wizard	13
Step 1: Access Rule Type.....	13
Configuring a Public Server Rule	14
Step 2: Public Server	14
Configuring a General Network Access Rule	15
Step 1: Access Rule Type.....	15
Step 2: Access Rule Service.....	16
Step 3: Access Rule Action	16
Step 4: Access Rule Source Interface and Address	17
Step 5: Access Rule Destination Interface and Address	17
Step 6: Access Rule Time.....	18
Completing the Network Access Rule Wizard	18
Adding Rules Using the Add Rule Window	19
Rule Examples	20
Blocking LAN Access for Specific Services	20
Enabling Ping.....	21
Access Rules> Advanced	21
Windows Networking (NetBIOS) Broadcast Pass Through.....	21
Detection Prevention	22
Enable Stealth Mode.....	22
Randomize IP ID	22
Dynamic Ports.....	22
Source Routed Packets.....	22
TCP Connection Inactivity Timeout	22
Firewall>Services.....	23
User Defined (Custom) Services.....	23
VPN	25
VPN>Settings	25
VPN Global Settings.....	25
VPN Policies.....	26
Currently Active VPN Tunnels.....	26
Configuring GroupVPN Policy on the SonicWALL.....	26
Configuring IKE using Preshared Secret.....	26
General	27
Proposals	27
Advanced	28
Client.....	29
Configuring GroupVPN with IKE using 3rd Party Certificates	30
General	30
Proposals	30
Advanced	30

Client	31
Export a GroupVPN Client Policy	32
Site to Site VPN Configurations	33
VPN Planning Sheet for Site-to-Site VPN Policies	34
Site A	34
Router	34
Additional Information	34
Configuring Site to Site VPN Policies	
Using the VPN Policy Wizard	35
Creating a Typical IKE using Preshared Secret VPN Policy.....	35
Creating a Custom VPN Policy using IKE and a Preshared Secret	35
Creating a Manual Key VPN Policy with the VPN Policy Wizard ...	36
Configuring IKE using 3rd Party Certificates with the VPN Policy Wizard	37
Creating VPN Policies Using the VPN Policy Window	38
Configuring a VPN Policy using IKE with Preshared Secret	38
..... Configuring a VPN Policy using Manual Key	41
Configuring a VPN Policy with IKE using a Third Party Certificate	44
VPN>Advanced	46
Advanced VPN Settings.....	46
VPN Single-Armed Mode (stand-alone VPN gateway).....	47
Configuring a SonicWALL for VPN Single Armed Mode	48
VPN User Authentication Settings	49
VPN Bandwidth Management.....	49
VPN>DHCP over VPN	50
DHCP Relay Mode.....	50
Configuring the Central Gateway for DHCP Over VPN	51
Configuring DHCP over VPN Remote Gateway	52
Device Configuration.....	52
Current DHCP over VPN Leases	53
VPN>L2TP Server.....	53
General	54
L2TP Server Settings	54
IP Address Settings	55
Adding L2TP Clients to the SonicWALL	55
Currently Active L2TP Sessions	55
Digital Certificates	55
Overview of X.509 v3 Certificates	55
SonicWALL Third Party Digital Certificate Support.....	55
VPN>Local Certificates	56
Importing Certificate with Private Key	56
Certificate Details	56
Delete This Certificate	57

Generating a Certificate Signing Request	57
VPN>CA Certificates	58
Importing CA Certificates into the SonicWALL	58
Certificate Details	58
Delete This Certificate	58
Certificate Revocation List (CRL)	59
Importing a CRL List	59
Automatic CRL Update	59
Users	61
Users>Status	61
Active User Sessions	61
Users>Settings	62
Authentication Method.....	62
Global User Settings	62
Acceptable Use Policy.....	63
Configuring RADIUS Authentication.....	63
Users>Local Users	65
Settings	65
Security Services.....	67
Security Services>Summary.....	68
Security Services Summary	68
Manage Services Online	68
If Your SonicWALL is Not Registered	69
Security Services Settings.....	69
SonicWALL Content Filtering Service.....	69
Security Services>Content Filter	70
Content Filter Status.....	70
Activating SonicWALL CFS	71
Activating a SonicWALL CFS FREE TRIAL.....	71
Content Filter Type.....	71
Restrict Web Features.....	71
Trusted Domains	72
Message to Display when Blocking.....	73
Configuring SonicWALL Filter Properties	73
.....Custom List	73
Enable Keyword Blocking	74
Disable all Web traffic except for Allowed Domains.....	74
Settings	74
Consent.....	75
Mandatory Filtered IP Addresses	76

Consent Page URL (mandatory filtering).....	76
Adding a New Address	76
SonicWALL Network Anti-Virus	76
Security Services>Anti-Virus	77
Activating SonicWALL Network Anti-Virus	77
Activating a SonicWALL Network Anti-Virus FREE TRIAL	77
Network Anti-Virus E-Mail Filter	78
Intrusion Prevention Service	78
SonicWALL IPS Features	78
SonicWALL Deep Packet Inspection	79
How SonicWALL's Deep Packet Inspection Architecture Works ...	79
SonicWALL IPS Terminology.....	80
SonicWALL IPS Activation	81
mySonicWALL.com.....	81
Activating SonicWALL IPS.....	81
Activating the SonicWALL IPS FREE TRIAL	82
Log	83
Log>View.....	83
SonicWALL Log Messages.....	84
Clear Log	84
E-mail Log	84
Log>Categories	85
Log Categories.....	85
Alerts & SNMP Traps.....	86
Log>Automation	87
E-mail.....	87
Syslog Servers.....	87
Log>Reports.....	88
Data Collection.....	89
View Data.....	89
Web Site Hits.....	89
Bandwidth Usage by IP Address	89
Bandwidth Usage by Service.....	89
Log>ViewPoint	90
SonicWALL ViewPoint	90
Appendices	91
Appendix A - SonicWALL Support Solutions.....	91
Knowledge Base	91
Internet Security Expertise.....	91
SonicWALL Support Programs	91

Warranty Support - North America and International	91
Appendix B- Configuring the Management Station	
TCP/IP Settings	92
Windows 98	92
Windows NT	93
Windows 2000	94
Windows XP	95
Macintosh OS 10	95

Preface

Copyright Notice

© 2004 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL 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 OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

1 Introduction

Thank you for purchasing the SonicWALL Internet Security Appliance. Organizations of all kinds face an array of security threats -- and must react quickly with limited IT resources. That means that SonicWALL offers security solutions for specific business applications such as networking, site-to-site communications, telecommuting, POS transactions, or secure web-sites. SonicWALL offers solutions that are specifically designed to meet the objectives of today's Internet connected business.

SonicWALL Internet firewall/VPN security appliances support an array of security applications and deliver powerful firewall and VPN performance. SonicWALL appliances are built on stateful inspection firewall technology, and a dedicated security ASIC designed to ensure maximum performance for VPN enabled applications. With integrated support for firewall, VPN, Anti Virus, content filtering, and an award-winning Global Management System (GMS), IT administrators can trust SonicWALL to protect their network while securely and reliably connecting their remote businesses or personnel.

SonicWALL SonicOS Standard Overview

SonicWALL SonicOS Standard is the standard operating system for the SonicWALL TZ 170, SonicWALL 2040, and SonicWALL 3060, which provides a complete security solution to protect your network from attacks, intrusions, and malicious tampering. In addition, SonicOS provides secure, encrypted communications via IPSec VPN to business partners and branch offices as well as support for a growing number of SonicWALL Security Services, such as SonicWALL Content Filtering Service and SonicWALL Network Anti-Virus.



Tip! SonicWALL SonicOS Standard can be upgraded to SonicOS Enhanced. For detailed instructions on upgrading to SonicOS Enhanced, see the **Upgrading SonicOS Standard to SonicOS Enhanced** Technote available on the PRO 2040 Product CD or at <http://www.sonicwall.com/services/documentation.html>.

SonicWALL Management Interface

The SonicWALL's Web Management Interface provides a easy-to-use graphical interface for configuring your SonicWALL. SonicWALL management functions are performed through a Web browser.



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

Accessing the Management Interface

To access the SonicWALL Management Interface, you need to configure the Management Station TCP/IP settings in order to initially contact the SonicWALL. A computer used to manage the SonicWALL is referred to as the "Management Station." Any computer on the same network as the SonicWALL can be used to access the management interface.

MD5 authentication is used to secure communications between your Management Station and the SonicWALL Web Management Interface. MD5 Authentication prevents unauthorized users from detecting and stealing the SonicWALL password as it is sent over your network.

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



Note: For instructions on setting up your Management Station for accessing the SonicWALL Management Interface, see Appendix B.

Navigating the Management Interface

Navigating the SonicWALL Management Interface includes a hierarchy of menu buttons on the navigation bar (left side of window). The SonicOS Standard menu buttons on the navigation bar include:

- **System**
- **Network**
- **Firewall**
- **VPN**
- **Users**
- **Security Services**
- **Log**
- **Help**
- **Wizards**
- **Logout**

When you click a menu button, related management functions are displayed as submenu items in the navigation bar. To navigate to a submenu page, click the link. When you click a menu button, the first submenu item page is displayed.

Applying Changes

Click the **Apply** button at the top right corner of the SonicWALL Management Interface to save any configuration changes you made on the page.

If the settings are contained in a secondary window within the Management Interface, when you click **OK**, the settings are automatically applied to the SonicWALL.

Getting Help

Each SonicWALL includes Web-based online help available from the Management Interface.

Clicking the question mark ? button on the top right corner of every page accesses the context-sensitive help for the page.



Alert! SonicWALL online help requires Internet connectivity.

Logging Out

The Logout button at the bottom of the menu bar terminates the Management Interface session and displays the Authentication page.

About this Guide

Welcome to the *SonicWALL SonicOS Standard Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS Standard 2.2 for the SonicWALL TZ170, PRO 2040, and PRO 3060 Internet Security Appliances.

This manual is updated and released with SonicOS Standard 2.2. Always check <http://www.sonicwall.com/services/documentation.html> for the latest version of this manual as well as other SonicWALL Security Service and upgrade manuals.



Tip! *The **Quick Start Guide** for your SonicWALL provides instructions for quickly installing and configuring your SonicWALL for connecting your network through the SonicWALL for secure Internet connectivity.*

Organization of this Guide

The *SonicOS Standard Administrator's Guide* organization follows the SonicWALL Web Management Interface structure.

Chapter 1, **Introduction** - Overview of SonicOS Standard, the SonicWALL Web-based Management Interface, and this manual's conventions.

Chapter 2, **Internet Connectivity Using the Setup Wizard** - explains how to get your network securely connected to the Internet with the SonicWALL using the Setup Wizard.

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

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

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

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

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

Chapter 8, **Security Services** - provides configuration instructions for SonicWALL Content Filtering Service and Anti-Virus features.

Chapter 9, **Logging and Alerts** - illustrates the SonicWALL logging, alerting, and reporting features.

Chapter 10, **Appendices**

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

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

Guide Conventions

The following Conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select on the SonicWALL Management Interface.
<i>Italic</i>	Highlights a value to enter into a field. For example, “type <i>192.168.168.168</i> in the IP Address field.”
Menu Item>Menu Item	Indicates a multiple step Management Interface menu choice. For example, “ Security Services>Content Filter means select Security Services, then select Content Filter.

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:



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



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



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

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/services/support.html>. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada - 888.777.1476 or +1 408.752.7819

International Telephone Support

Australia - + 1800.35.1642

Austria - + 43(0)820.400.105

EMEA - +31(0)411.617.810

France - + 33(0)1.4933.7414

Germany - + 49(0)1805.0800.22

Hong Kong - + 1.800.93.0997

India - + 8026556828

Italy - +39.02.7541.9803

Japan - + 81(0)3.5460.5356

New Zealand - + 0800.446489

Singapore - + 800.110.1441

Spain - + 34(0)9137.53035

Switzerland - +41.1.308.3.977

UK - +44(0)1344.668.484



Note: Please visit <http://www.sonicwall.com/services/contact.html> for the latest technical support telephone numbers.

More Information on SonicWALL Products and Services

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

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

E-mail: sales@sonicwall.com

Phone: (408) 745-9600

Fax: (408) 745-9300

2 Internet Connectivity Using the Setup Wizard

The **Setup Wizard** takes you step by step through network configuration for Internet connectivity. There are four types of network connectivity available: Static IP, DHCP, PPPoE, and PPTP.

The first time you log into the SonicWALL, the **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any time from the Management Interface, log into the SonicWALL. Click **Wizards** and select **Setup Wizard**.



Note: *The Wizard pages shown in this chapter are for the SonicWALL TZ170 but they are identical to Wizard pages for the PRO 2040 and PRO 3060.*



Tip! *You can also configure all your WAN and network settings on the **Network>Settings** page of the SonicWALL Management Interface*

Configuring a Static IP Address with NAT Enabled

Using NAT to set up your SonicWALL eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

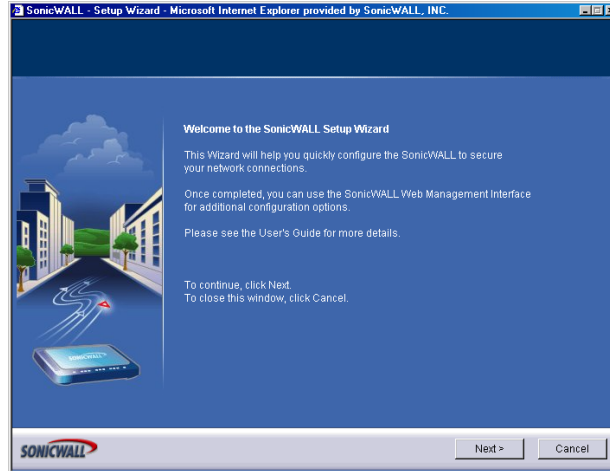
Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a SonicWALL with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

This section describes configuring the SonicWALL appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.



Tip! *Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.*

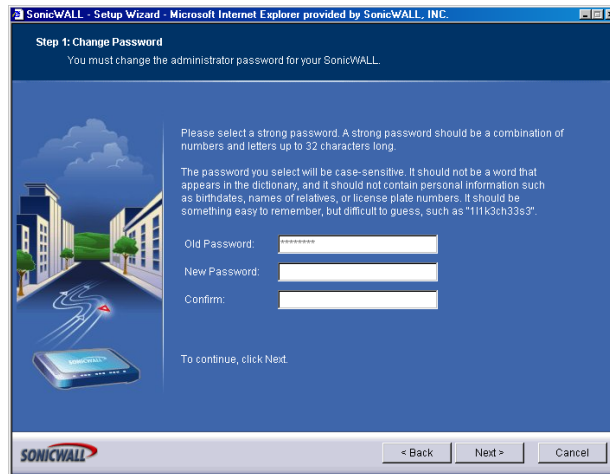
Setup Wizard



Note: Your Web browser must be Java-enabled and support HTTP uploads in order to fully manage SonicWALL. Internet Explorer 5.0 and above as well as Netscape Navigator 4.0 and above are recommended.

1. Click the **Setup Wizard** button on the **Network>Settings** page. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password

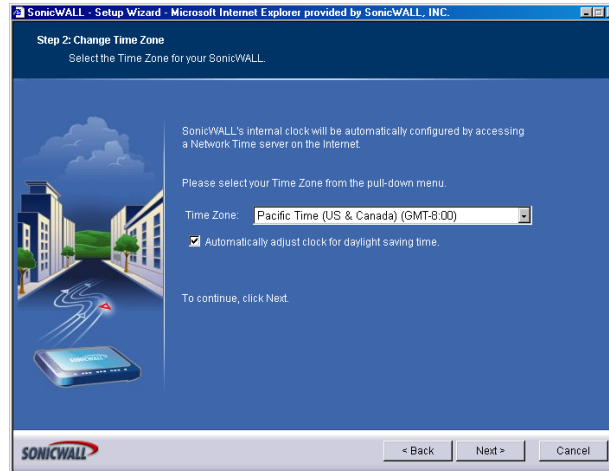


2. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



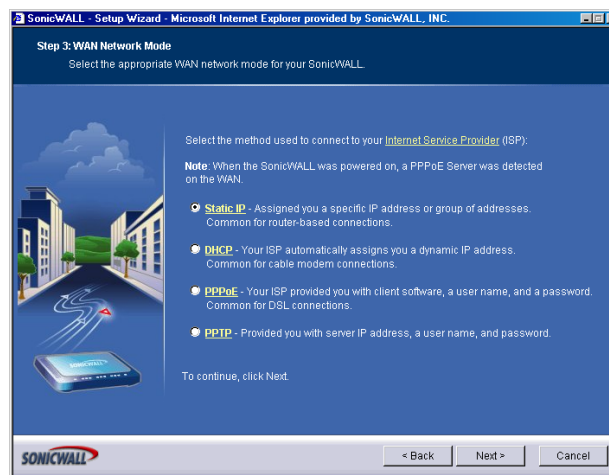
Tip! It is very important to choose a password which cannot be easily guessed by others.

Step 2: Change Time Zone



3. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode



4. Confirm that you have the proper network information necessary to configure the SonicWALL to access the Internet. Click the hyperlinks for definitions of the networking terms.

You can choose:

- Static IP**, if your ISP assigns you a specific IP address or group of addresses.
 - DHCP**, if your ISP automatically assigns you a dynamic IP address.
 - PPPoE**, if your ISP provided you with client software, a user name, and a password.
 - PPTP**, if your ISP provided you with a server IP address, a user name, and password.
5. Choose **Static IP** and click **Next**.

Step 4: WAN Network Mode: NAT Enabled

SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode: NAT Enabled
Fill in the following network settings to get to the Internet.

You will need to fill in the following fields to connect to the Internet.
All these values must be entered as numerical IP addresses (such as 10.50.128.52).
If you do not have the information, please contact your ISP.

SonicWALL WAN IP Address: 10.0.93.17
WAN/OPT Subnet Mask: 255.255.255.0
Gateway (Router) Address: 10.0.0.254
DNS Server Address: 10.50.128.52
DNS Server Address #2 (optional): 10.50.128.53

To continue, click Next.

< Back Next > Cancel

6. Enter the public IP address provided by your ISP in the **SonicWALL WAN IP Address**, then fill in the rest of the fields: **WAN/OPT/DMZ Subnet Mask**, **WAN Gateway (Router) Address**, and **DNS Server Addresses**. Click **Next**.

Step 5: LAN Settings

SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings
Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.
You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.168.1).
The default values below will work well for most networks.

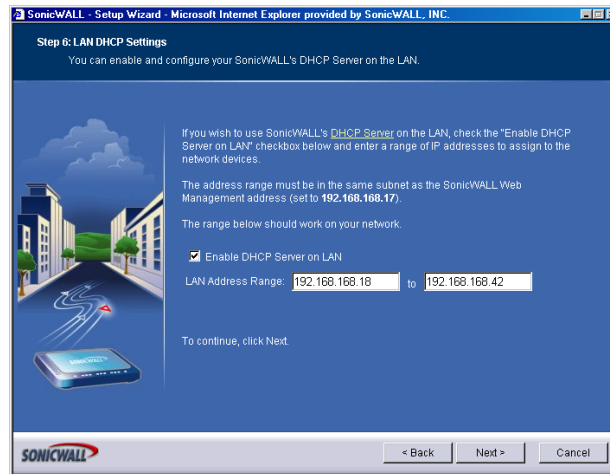
SonicWALL LAN IP Address: 192.168.168.17
LAN Subnet Mask: 255.255.255.0
 Enable Windows Networking Support

To continue, click Next.

< Back Next > Cancel

7. The **LAN** page allows the configuration of the **SonicWALL LAN IP Addresses** and the **LAN Subnet Mask**. The **SonicWALL LAN IP Addresses** are 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. If you do not use the default settings, enter your preferred private IP address and subnet mask in the fields. Click **Next**.

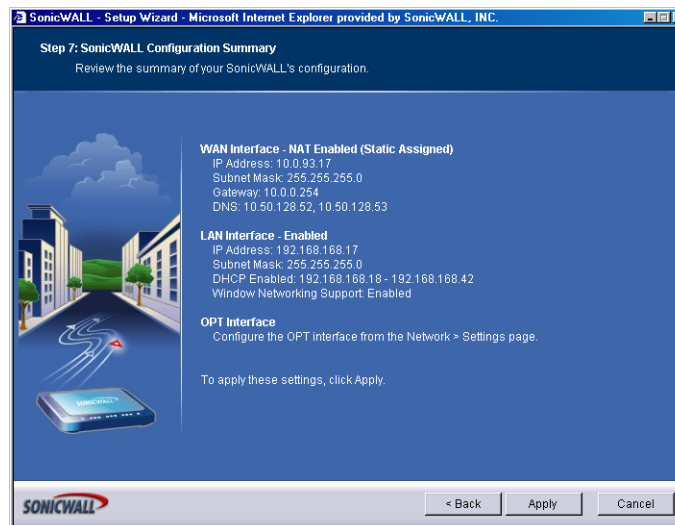
Step 6: LAN DHCP Settings



8. The **Optional-SonicWALL 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, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

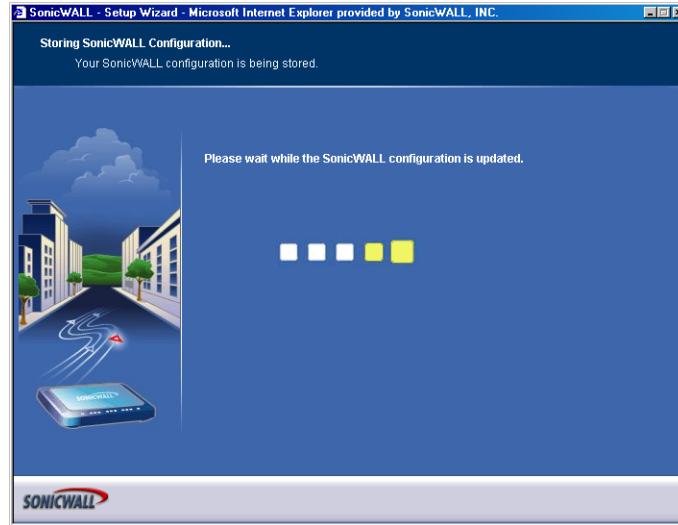
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 7: SonicWALL Configuration Summary

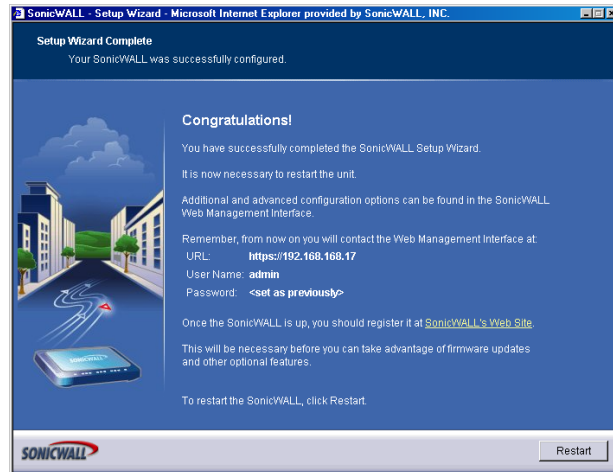


9. The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.

Storing SonicWALL Configuration



Setup Wizard Complete

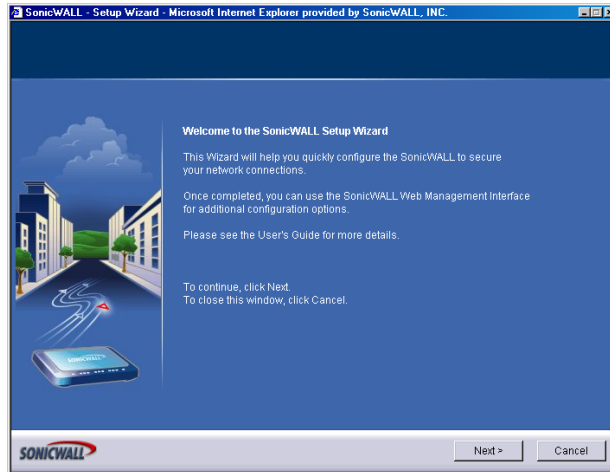


10. The SonicWALL stores the network settings.
11. Click **Restart** to restart the SonicWALL. The SonicWALL takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

Configuring DHCP Networking Mode

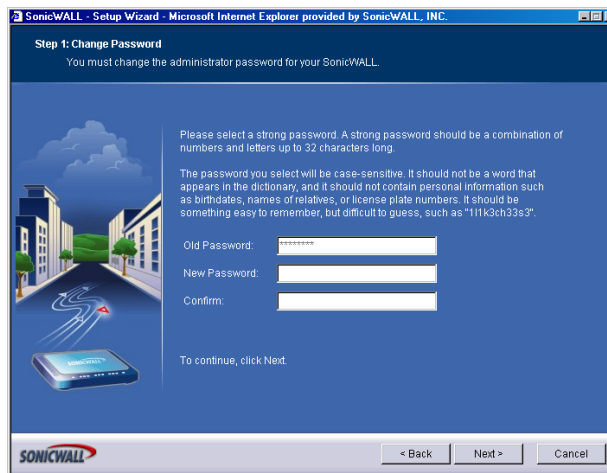
DHCP is a networking mode that allows you to obtain an IP address for a specific length of time from a DHCP server. The length of time is called a lease which is renewed by the DHCP server typically after a few days. When the lease is ready to expire, the client contacts the server to renew the lease. This is a common network configuration for customers with cable or DSL modems. You are not assigned a specific IP address by your ISP.

1. Click the **Setup Wizard** button on the **Network>Settings** page.



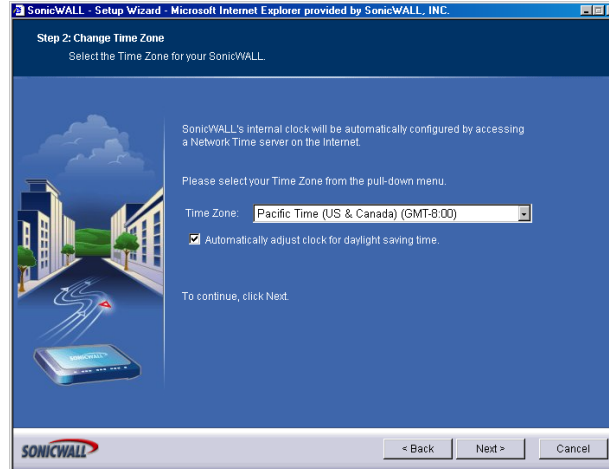
2. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password



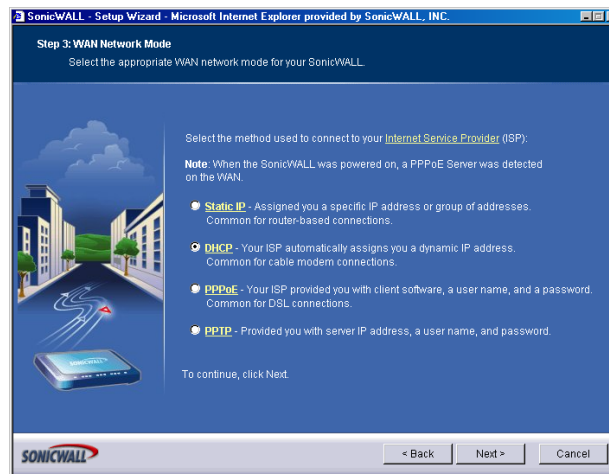
3. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

Step 2: Change Time Zone



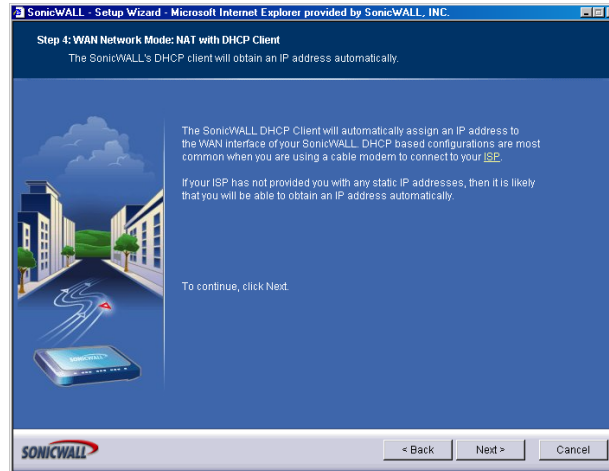
4. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode



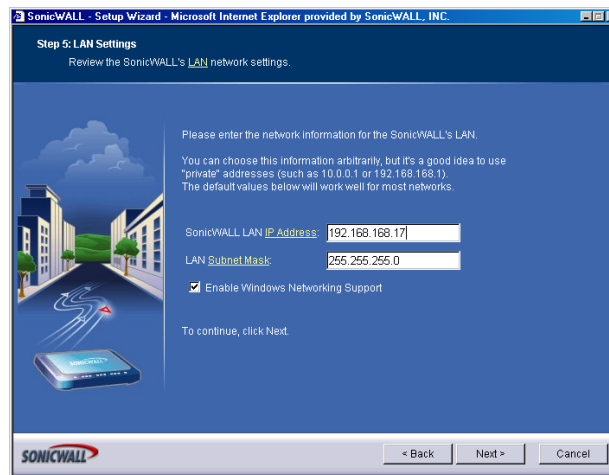
5. Select **DHCP**, the **Obtain an IP address automatically** window is displayed. Click **Next**.

Step 4: WAN Network Mode: NAT with DHCP Client



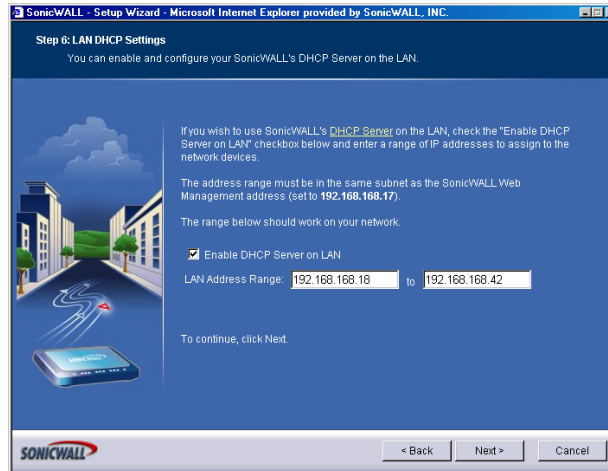
6. The **Obtain an IP address automatically** window states that the ISP dynamically assigns an IP address to the SonicWALL. To confirm this, click **Next**. DHCP-based configurations are most common with cable modem connections.

Step 5: LAN Settings



7. The **Fill in information about your LAN** page allows the configuration of SonicWALL LAN IP Addresses and Subnet Masks. SonicWALL LAN IP Addresses are the private IP addresses assigned to the LAN of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the networks. The default values provided by the SonicWALL are useful for most networks. Click **Next**.

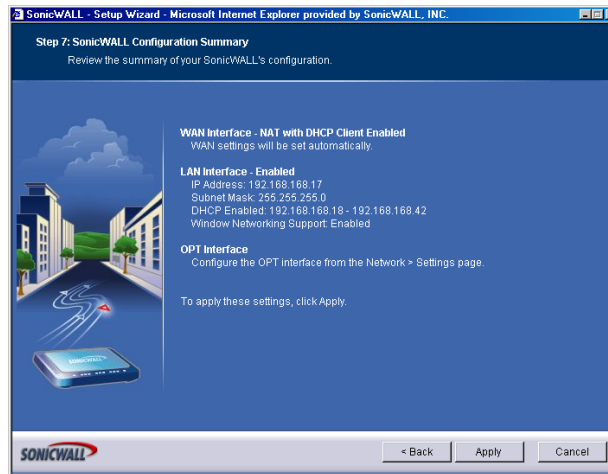
Step 6: DHCP Settings



8. The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses assigned to computers on the LAN.

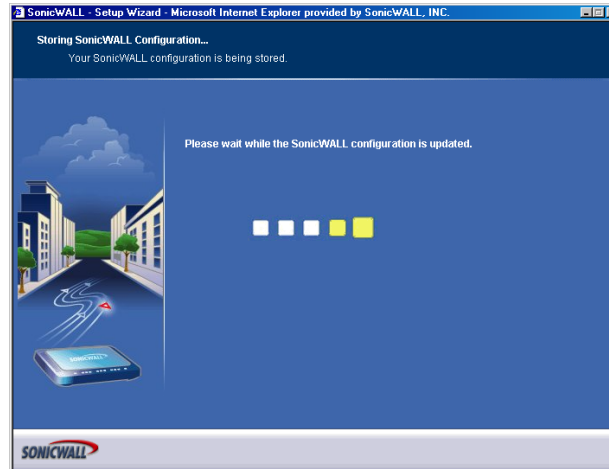
If **Disable DHCP Server** is selected, the DHCP Server is disabled. Click **Next** to continue.

Configuration Summary

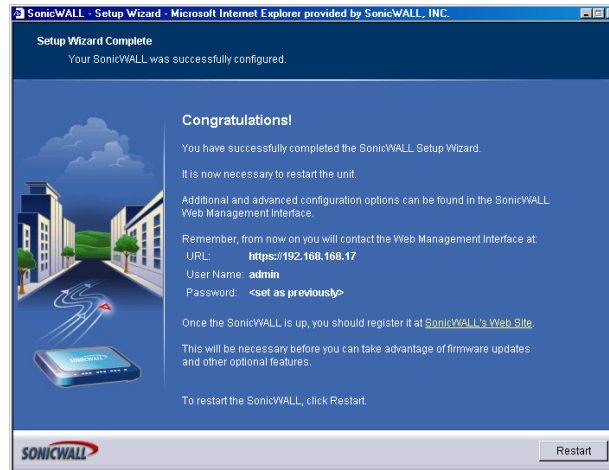


9. The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Apply**.

Storing SonicWALL Configuration



Setup Wizard Complete



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

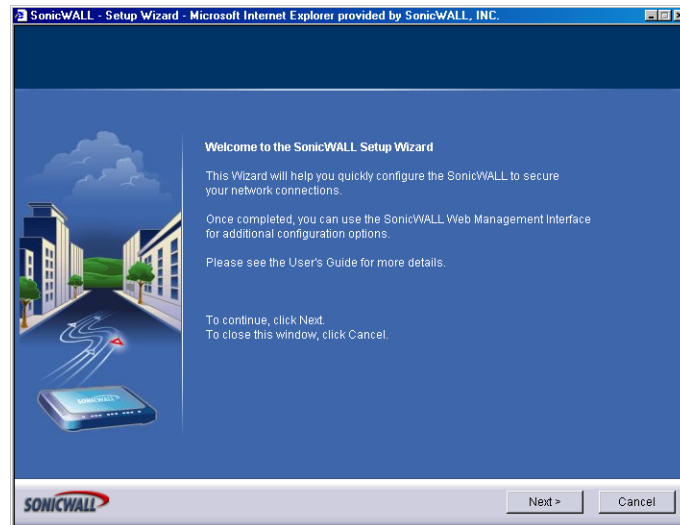


Tip! The new SonicWALL LAN IP address, displayed in the **URL** field of the **Congratulations** window, is used to log in and manage the SonicWALL.

Configuring NAT Enabled with PPPoE

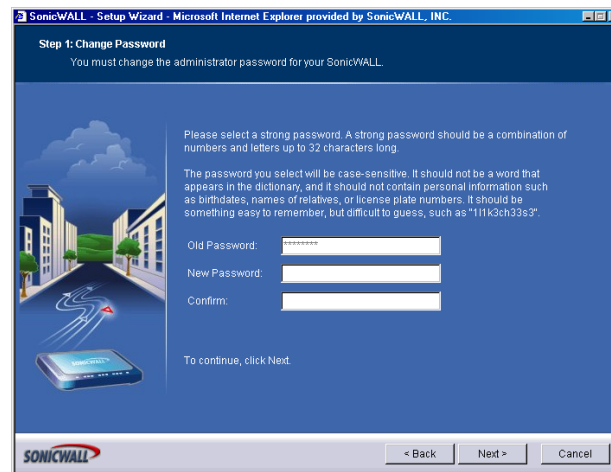
NAT with PPPoE Client is a network protocol that uses Point to Point Protocol over Ethernet to connect with a remote site using various Remote Access Service products. This protocol is typically found when using a DSL modem with an ISP requiring a user name and password to log into the remote server. The ISP may then allow you to obtain an IP address automatically or give you a specific IP address.

1. Click the **Setup Wizard** button on the **Network>Settings** page.



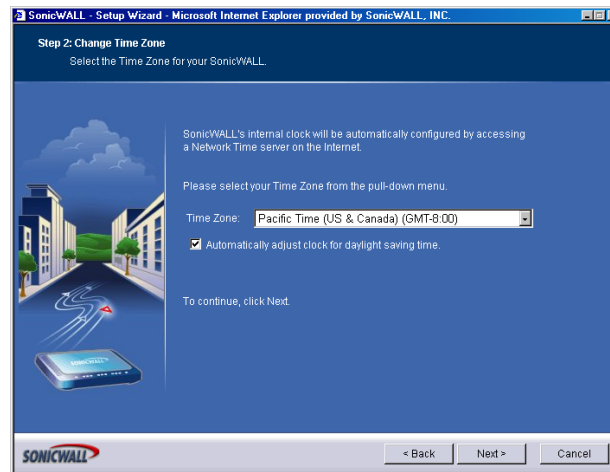
2. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password



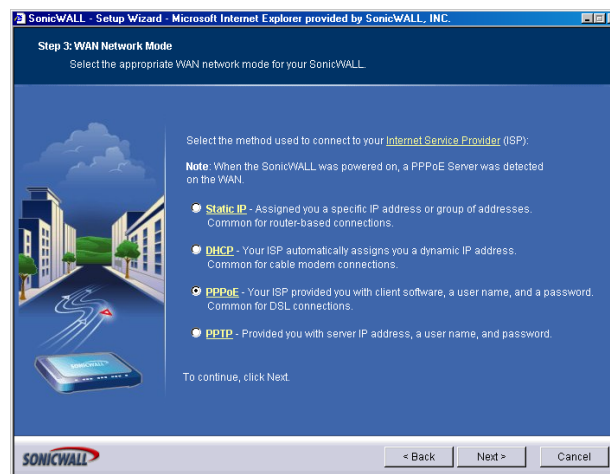
3. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

Step 2: Change Time Zone



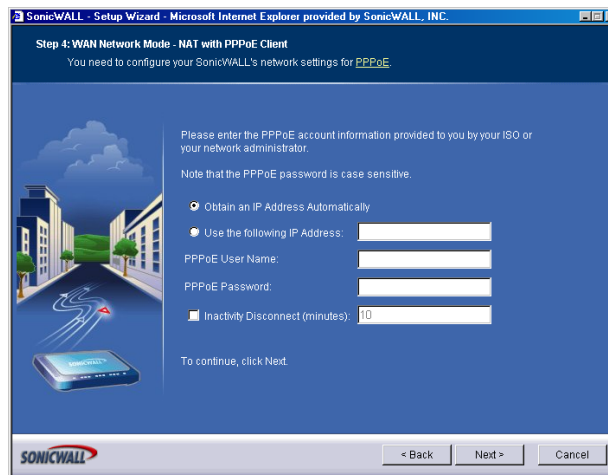
4. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode



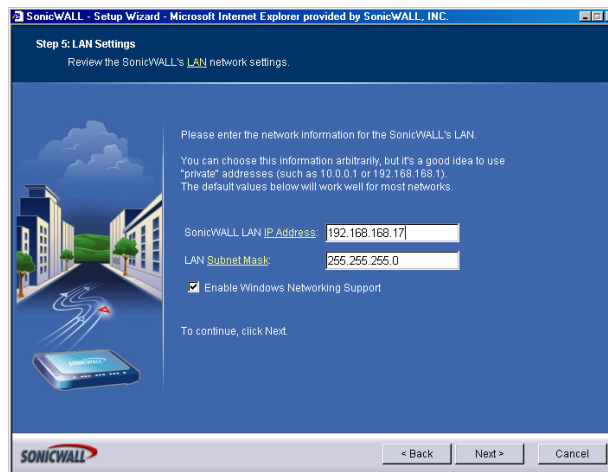
5. The SonicWALL automatically detects the presence of a PPPoE server on the WAN. If not, then select **PPPoE: Your ISP provided you with desktop software, a user name and password**. Click **Next**.

Step 4: WAN Network Mode: NAT with PPPoE Client



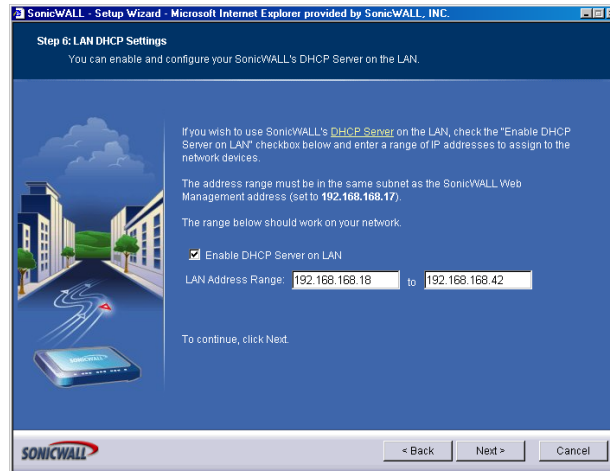
6. Enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

Step 5: LAN Settings



7. The **LAN Settings** page allows the configuration of SonicWALL LAN IP Addresses and 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 are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

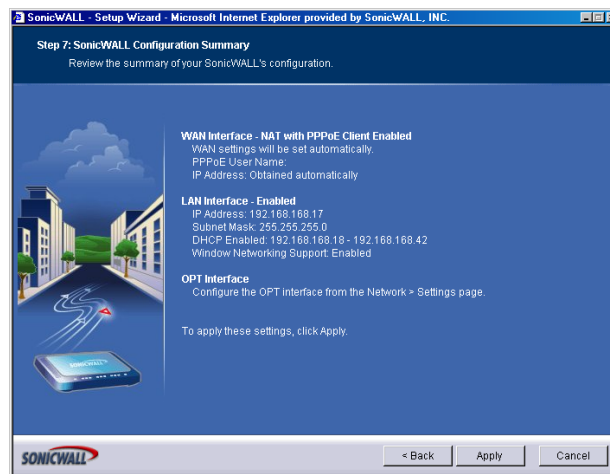
Step 6: DHCP Server



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

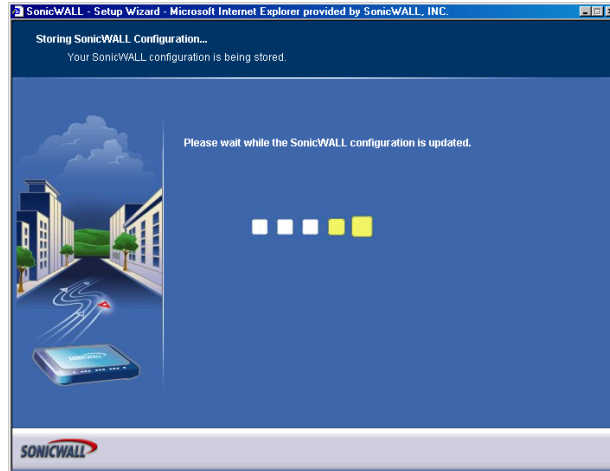
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 7: SonicWALL Configuration Summary



9. The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to the **WAN Settings** window. If the configuration is correct, click **Next** to proceed to the **Congratulations** window.

Storing SonicWALL Configuration



Tip! The new SonicWALL LAN IP address, displayed in the **URL** field of the **Congratulations** window, is used to log in and manage the SonicWALL.

Setup Wizard Complete

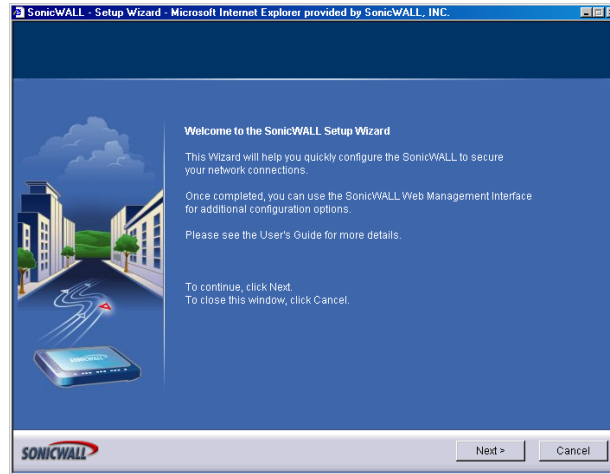


10. Click **Restart** to restart the SonicWALL.
11. The SonicWALL takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

Configuring PPTP Network Mode

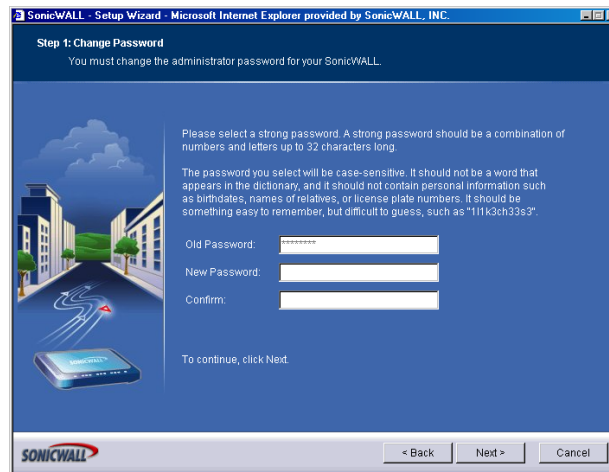
NAT with PPTP Client mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.

1. Click the **Setup Wizard** button on the **Network>Settings** page.



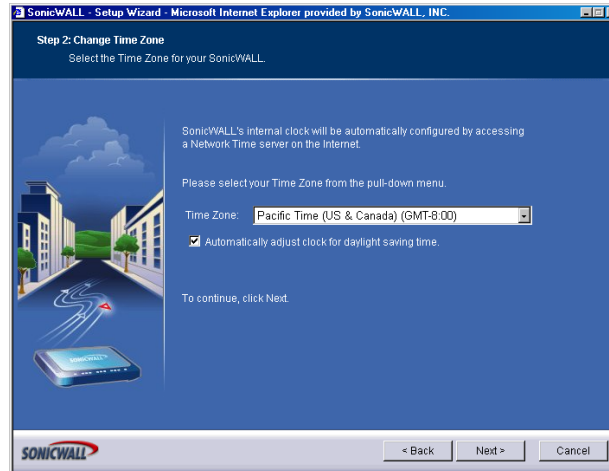
2. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password



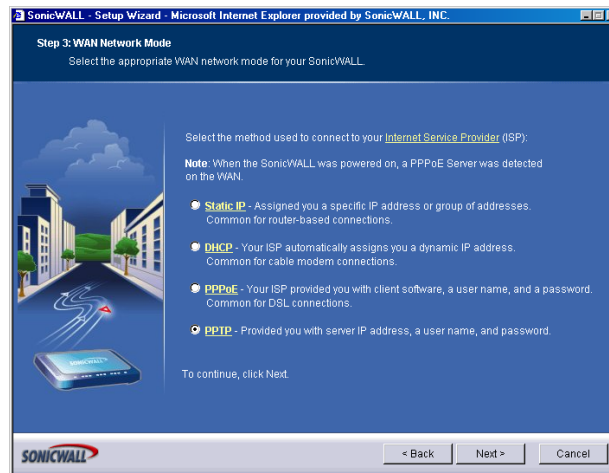
3. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

Step 2: Change Time Zone



4. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode



5. Select **PPTP: Provided you with a server IP address, a user name and password**. Click **Next**.

Step 4: WAN Network Mode: NAT with PPTP Client

SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode: NAT with PPTP Client

You need to configure your SonicWALL's ISP settings for PPTP.

PPTP Server IP Address:

PPTP User Name:

PPTP Password:

Obtain an IP Address Automatically

Use the following IP Address

SonicWALL WAN IP Address:

WAN/OPT Subnet Mask:

Gateway (Router) Address:

To continue, click Next.

< Back Next > Cancel

6. Enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

Step 5: LAN Settings

SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.

You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.168.1). The default values below will work well for most networks.

SonicWALL LAN IP Address:

LAN Subnet Mask:

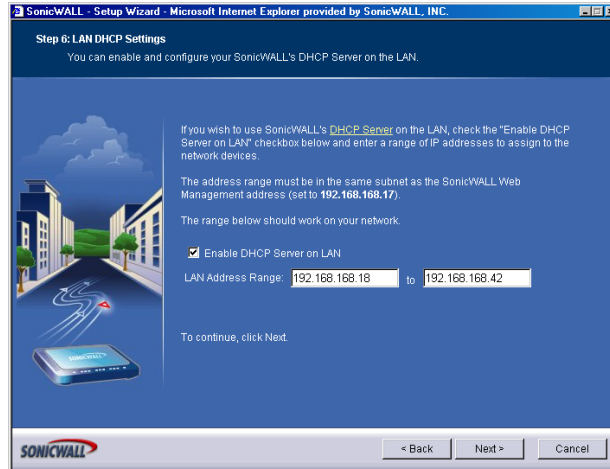
Enable Windows Networking Support

To continue, click Next.

< Back Next > Cancel

7. The **LAN Settings** page allows the configuration of SonicWALL LAN IP Addresses and 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 are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

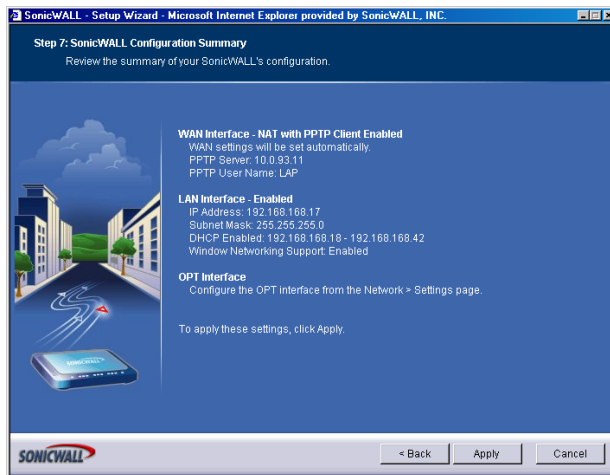
Step 6: DHCP Server



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

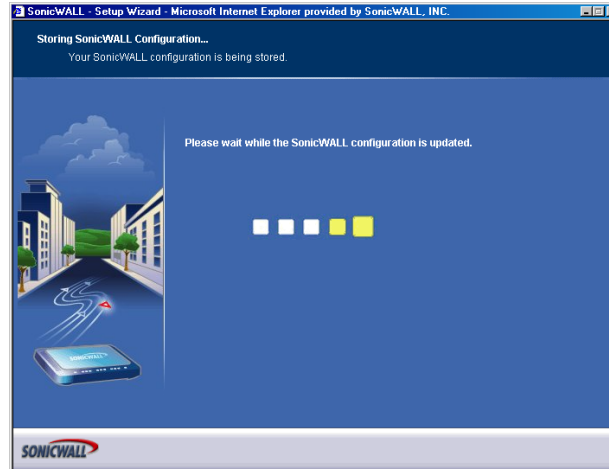
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 7: SonicWALL Configuration Summary



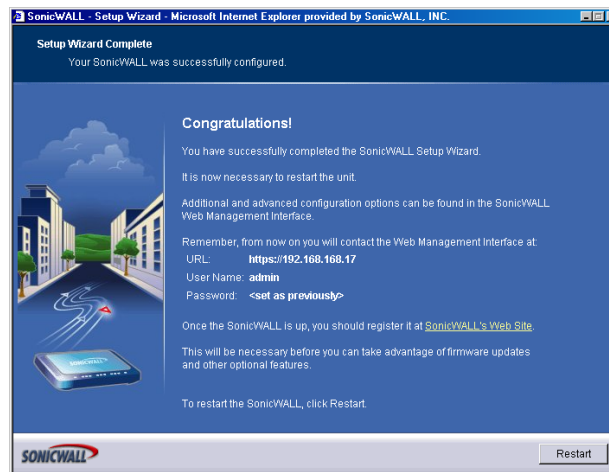
9. The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next** to proceed to the **Storing SonicWALL Configuration** window.

Storing SonicWALL Configuration



Tip! The new SonicWALL LAN IP address, displayed in the **URL** field of the **Congratulations** window, is used to log in and manage the SonicWALL.

Setup Wizard Complete



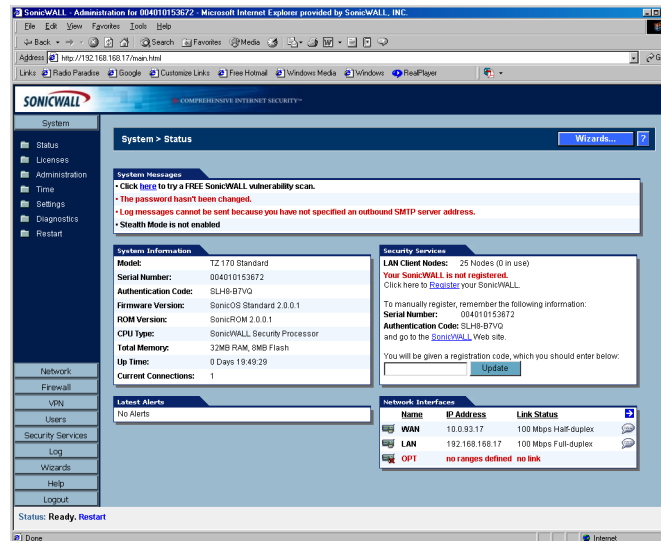
10. Click **Restart** to restart the SonicWALL. The SonicWALL takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

3 System Settings

This chapter describes the configuration of the SonicWALL IP settings, time, and password as well as providing instructions to restart the SonicWALL, import and export settings, upload new firmware, and perform diagnostic tests.

System>Status

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



System Messages

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

System Information

The following information is displayed in this section:

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

Security Services

A list of available SonicWALL Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column displays the number of licenses and the number of licenses in use. Clicking the **Arrow** icon displays the **System>Licenses** page in the SonicWALL Web Management Interface. SonicWALL Security Services and Internet Security Appliance registration is managed by mySonicWALL.com.

Registering Your SonicWALL

If your SonicWALL is not registered at mySonicWALL.com, the following message is displayed in the **Security Services** folder: Your SonicWALL is not registered. Click here to Register your SonicWALL.



Note: You need a mySonicWALL.com account to register your SonicWALL or activate security services. You can create a mySonicWALL.com account directly from the SonicWALL Management Interface.

You can manually register your SonicWALL at the mySonicWALL.com site using the **Serial Number** and **Authentication Code** displayed in the **Security Services** folder. Click the SonicWALL link to access your mySonicWALL.com account. You will be given a registration code after you have registered your SonicWALL. Enter the registration code in the field below **You will be given a registration code, which you should enter below**, then click **Update**.

If you have a mySonicWALL.com account, follow these steps to register your SonicWALL:

1. Click the here link to automatically register your SonicWALL. The **mySonicWALL.com Login** page is displayed.
2. Type your mySonicWALL.com username and password in the **User Name** and **Password** fields and click **Submit**.
3. Type in a “friendly name” for your SonicWALL in the **Friendly Name** field. A friendly name is used to help identify your SonicWALL, such as its location.
4. Click **Submit**. Your SonicWALL is now registered.

mySonicWALL.com

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

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

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

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



Tip! For more information on [mySonicWALL.com](https://www.mysonicwall.com), access the online help available at <https://www.mysonicwall.com>.



Note: [mySonicWALL.com](https://www.mysonicwall.com) registration information is not sold or shared with any other company.

Latest Alerts

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

Network Interfaces

The following information is contained in this section:

- **WAN** - network speed, for example 100 Mbps, and devices connected to the WAN link.
- **LAN** - network speed and network address mode
- **OPT/DMZ** - network speed and network address mode

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

System>Licenses

The **System>Licenses** page provides links to activate, upgrade, or renew SonicWALL Security Services and upgrades.



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

Security Services Summary

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

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

Manage Security Services Online

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**. Click the link in **To synchronize licenses with mySonicWALL.com click here** to synchronize your [mySonicWALL.com](https://www.mysonicwall.com) account with the **Security Services Summary** table.

You can also get free trial subscriptions to SonicWALL Content Filter Service and Network Anti-Virus by clicking the **For Free Trials click here link**. When you click these links, the **mySonicWALL.com Login** page is displayed. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields and click **Submit**. The **Manage Services Online** page is displayed with licensing information from your mySonicWALL.com account.

Manual Upgrade

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

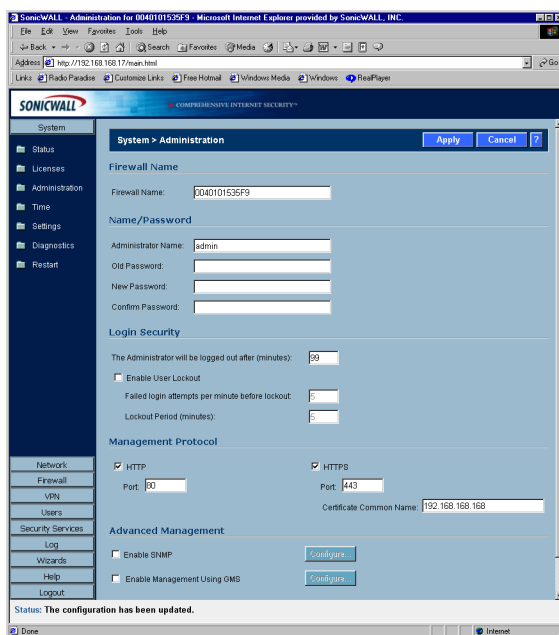


Tip! You must have a mysonicwall.com account to upgrade and activate services through the SonicWALL.



Note: If your SonicWALL is deployed in a high-security environment that does not allow direct Internet connectivity from the SonicWALL, you can enter the encrypted license key information manually in the enter keyset field. See the SonicWALL TechNote **Manual Upgrades for Closed Environments using License Keyset** at <www.sonicwall.com/services/SonicOS_FW_documentation.html> for instructions.

System>Administration



Firewall Name

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

Name/Password

Administrator Name

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

Changing the Administrator Password

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

Login Security

The **Administrator Inactivity Timeout** setting allows you to set the length of inactivity time that elapses before you are automatically logged out of the Web Management Interface. By default, the SonicWALL logs out the administrator after 5 minutes of inactivity.



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

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

Enable Administrator/User Lockout

You can configure the SonicWALL to lockout an administrator or a user if the login credentials are incorrect. Select the **Enable Administrator/User Lockout** check box to prevent users from attempting to log into the SonicWALL without proper authentication credentials. Enter the number of failed attempts before the user is locked out in the **Lock out user after __ failed login attempts in a 1 minute** period field. Enter the length of time that must elapse before the user attempts to log into the SonicWALL again in the **Lockout Period (minutes)** field.



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

Management Protocol

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

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

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

Advanced Management

Enable SNMP

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

To enable SNMP on the SonicWALL, select the **Enable SNMP** check box, and then click **Configure** in the System>Administration page.



Note: v1 traps are not supported on the SonicWALL.

1. Enter the host name of the SonicWALL in the **System Name** field.
2. Enter the network administrator's name in the **System Contact** field.

3. Enter an e-mail address, telephone number, or pager number in the **System Location** field.
4. Enter a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.
5. Enter a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
6. Enter the IP address or host name of the SNMP management system receiving SNMP traps in the Host 1 through Host 4 fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.
7. Click **OK**.

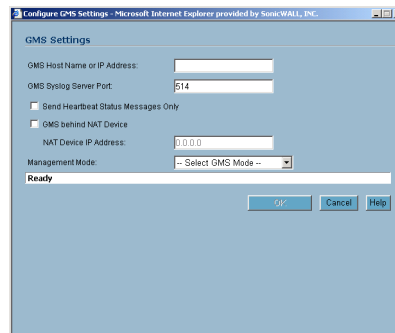
Trap messages are generated only for the alert message categories normally sent by the SonicWALL. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Log>Settings** page, then no trap messages are generated.

By default, the SonicWALL responds only to **Get SNMP** messages received on its LAN interface. Appropriate rules must be configured to allow SNMP traffic to and from the WAN interface. SNMP trap messages can be sent via the LAN or WAN. See Chapter 5, **Firewall**, for instructions on adding services and rules to the SonicWALL.

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

Enable Management Using SonicWALL GMS

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



To configure the SonicWALL for GMS management:

1. Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
2. Enter the port in the **GMS Syslog Server Port** field. The default value is 514.
3. Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
4. Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.
5. Select one of the following GMS modes from the **Management Mode** menu.

IPSEC Management Tunnel - Use the IPsec management tunnel included with the SonicWALL. The default IPsec VPN settings are displayed.

Existing Tunnel - Use an existing tunnel for GMS management of the SonicWALL.

HTTPS - Use HTTPS for GMS management of the SonicWALL. The following configuration settings for HTTPS management mode are displayed:

Send Syslog Messages in Cleartext Format - Sends Syslog messages as cleartext.

Send Syslog Messages to a Distributed GMS Reporting Server - Sends Syslog Messages to a GMS Reporting Server separated from the GMS management server.

GMS Reporting Server IP Address - Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.

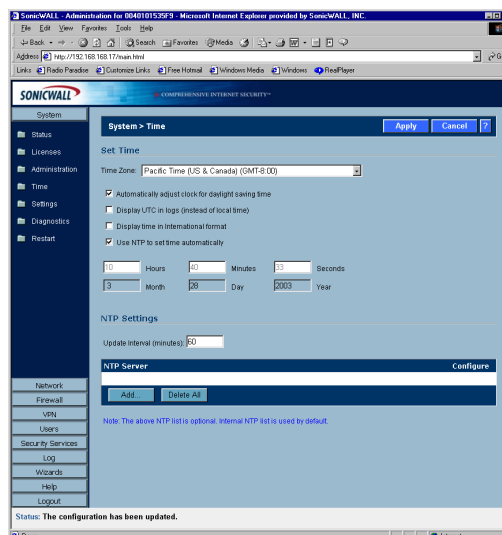
GMS Reporting Server Port - Enter the port for the GMS Reporting Server. The default value is 514

6. Click **OK**.

System>Time

Set Time

The SonicWALL uses the time and date settings to time stamp log events, to automatically update SonicWALL Security Services, and for other internal purposes. By default, the SonicWALL uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.



To select your time zone and automatically update the time, choose the time zone from the **Time Zone** menu. The **Use NTP to set time automatically** is activated by default to use the NTP (Network Time Protocol) to set time automatically. If you want to set your time manually, uncheck this setting. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus. **Automatically adjust clock for daylight saving changes** is activated by default to enable automatic adjustments for daylight savings time.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display time in International format** displays the date in International format, with the day preceding the month.

After selecting your System Time settings, click **Apply**.

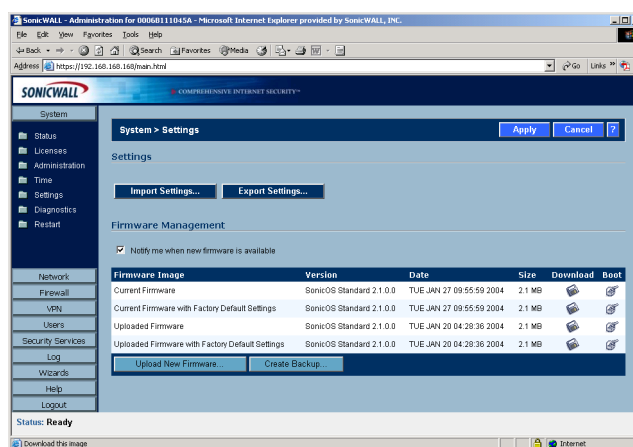
NTP Settings

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

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

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

System>Settings



Settings

Import Settings

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

1. Click **Import Settings** to import a previously exported preferences file into the SonicWALL. The **Import Settings** window is displayed.
2. Click **Browse** to locate the file which has a *.exp file name extension.
3. Select the preferences file.
4. Click **Import**, and restart the firewall.

Export Settings

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

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

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

Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

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



Note: *SonicWALL SafeMode, which uses the same settings used in the Firmware Management section, provides quick recovery from uncertain states.*

New Firmware

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

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

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Standard 2.0.0.2	TUE OCT 21 11:38:21 2003	2.1 MB		
Current Firmware with Factory Default Settings	SonicOS Standard 2.0.0.2	TUE OCT 21 11:38:21 2003	2.1 MB		
Current Firmware with Backup Settings	SonicOS Standard 2.0.0.2	TUE OCT 21 11:38:21 2003	2.1 MB		
Uploaded Firmware - New!	SonicOS Standard 2.0.0.2	TUE OCT 21 11:36:58 2003	2.1 MB		
Uploaded Firmware with Factory Default Settings - New!	SonicOS Standard 2.0.0.2	TUE OCT 21 11:36:58 2003	2.1 MB		
Uploaded Firmware with Backup Settings - New!	SonicOS Standard 2.0.0.2	TUE OCT 21 11:36:58 2003	2.1 MB		

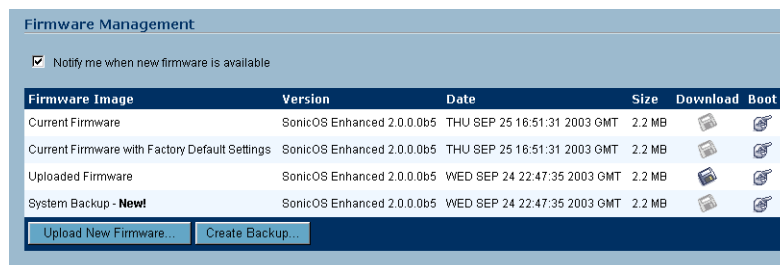


Alert! *After the initial 90 days from purchase, firmware updates are available only to registered users with a valid support contract. You must register your SonicWALL at <<https://www.mysonicwall.com>>.*

Updating Firmware Manually

Click **Upload New Firmware** to load new firmware in the SonicWALL. A dialogue box is displayed warning you that your current firmware version is overwritten by the uploaded version. You should export your current SonicWALL settings to a preferences file before uploading new firmware. Click **Browse** to locate the new firmware version. Once you locate the file, click **Upload** to load the new firmware onto the SonicWALL.

Firmware Management Settings



The screenshot shows the 'Firmware Management' section of a web interface. At the top, there is a checkbox labeled 'Notify me when new firmware is available' which is checked. Below this is a table with the following columns: 'Firmware Image', 'Version', 'Date', 'Size', 'Download', and 'Boot'. The table contains four rows of data. At the bottom of the table, there are two buttons: 'Upload New Firmware...' and 'Create Backup...'.

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 2.0.0.0b5	THU SEP 25 16:51:31 2003 GMT	2.2 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 2.0.0.0b5	THU SEP 25 16:51:31 2003 GMT	2.2 MB		
Uploaded Firmware	SonicOS Enhanced 2.0.0.0b5	WED SEP 24 22:47:35 2003 GMT	2.2 MB		
System Backup - New!	SonicOS Enhanced 2.0.0.0b5	WED SEP 24 22:47:35 2003 GMT	2.2 MB		

The **Firmware Management** table has the following columns:

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



Alert! *When uploading firmware to the SonicWALL, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.*

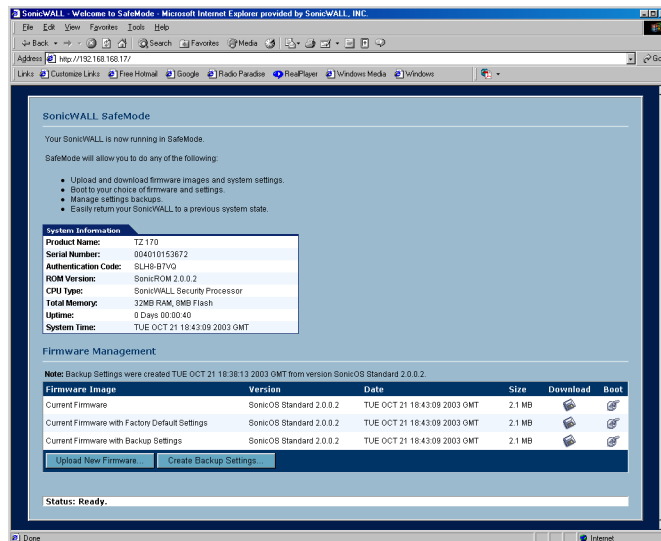


Note: *Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the Current Firmware image. On the TZ170, the uploaded firmware images are removed from the table after rebooting the SonicWALL.*

SafeMode - Rebooting the SonicWALL

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. It is no longer necessary to reset the firmware by pressing and holding the Reset button on the appliance. Pressing the Reset button for one second launches the SonicWALL into SafeMode. SafeMode allows you to select the firmware version to load and reboot the SonicWALL.

Because there are hardware differences between the TZ 170 and the PRO 2040/PRO 3060, Safe Mode on the TZ 170 cannot store as many firmware images as the PRO 2040/3060. After rebooting, the TZ 170 does not retain uploaded firmware images. To access the SonicWALL using SafeMode, press the Reset button for 1 second. After the SonicWALL reboots, open your Web browser and enter the current IP address of the SonicWALL or the default IP address: *192.168.168.168*. The SafeMode page is displayed:



SafeMode allows you to do any of the following:

- Upload and download firmware images to the SonicWALL.
- Upload and download system settings to the SonicWALL.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your SonicWALL to a previous system state.

System Information

System Information for the SonicWALL is retained and displayed in this section.

Firmware Management

The **Firmware Management** table has the following columns:

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

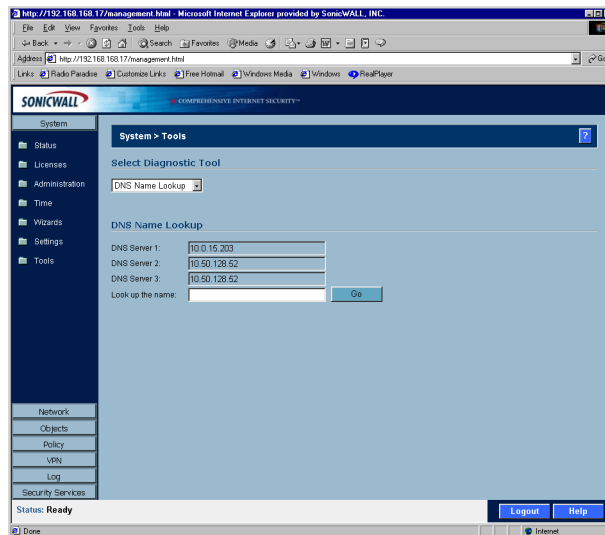


Note: Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image.

Click **Boot** in the firmware row of your choice to restart the SonicWALL.

System>Diagnostics

The SonicWALL has several diagnostic tools which help troubleshoot network problems on the **System>Diagnostics** page. You select the diagnostic tool from the menu in the **Select Diagnostic Tool** section.



DNS Name Lookup

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

1. Enter the host name or IP address in the **Look up name** field. Do not add *http* to the host name.
2. The SonicWALL queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.

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

Find Network Path

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

Ping

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

1. Select **Ping** from the **Diagnostic Tool** menu.
2. Enter the IP address or host name of the target device and click **Go**.
3. If the test is successful, the SonicWALL returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Packet Trace

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

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

1. TCP received on LAN [SYN]
From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)
To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL receives SYN from LAN client.

2. TCP sent on WAN [SYN]
From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)
To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL forwards SYN from LAN client to remote host.

3. TCP received on WAN [SYN,ACK]
From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)
To 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

The SonicWALL receives SYN,ACK from remote host.

4. TCP sent on LAN [SYN,ACK]
From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)
To 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

The SonicWALL forwards SYN,ACK to LAN client.

5. TCP received on LAN [ACK]
From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)
To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

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

6. TCP sent on WAN [ACK]
From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)
To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

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

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

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



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

7. 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". The **Trace is off** turns from red to green with Trace Active displayed.
8. Contact the remote host using an IP application such as Web, FTP, or Telnet.
9. Click **Refresh** and the packet trace information is displayed.
10. Click **Stop** to terminate the packet trace, and **Reset** to clear the results.

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

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

Tech Support Report

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



Alert! *You must register your SonicWALL on [mySonicWALL.com](https://www.mysonicwall.com) to receive technical support.*

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

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

- **VPN Keys** - saves shared secrets, encryption, and authentication keys to the report.
- **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses.
- **DHCP Bindings** - saves entries from the SonicWALL DHCP server.
- **IKE Info** - saves current information about active IKE configurations.

Generating a Tech Support Report

1. Select **Tech Support Report** from the **Choose a diagnostic tool** menu.
2. Select the **Report Options** to be included with your e-mail.
3. Click **Save Report** to save the file to your system. When you click **Save Report**, a warning message is displayed.
4. Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.

Trace Route

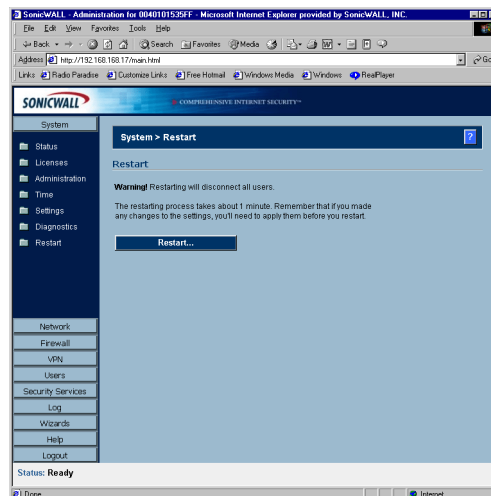
Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther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

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

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

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

System>Restart



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

The SonicWALL takes approximately 60 seconds to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

4 Network

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

- **Settings** - select your network mode and manually configure the network settings on the SonicWALL.
- **One-to-One NAT** - map internal IP addresses to public IP addresses using One-to-One NAT.
- **Web Proxy** - A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests.
- **Intranet** - The SonicWALL can be configured as an Intranet firewall to prevent network users from accessing sensitive servers.
- **Routing** - view the **Route Table**, **ARP Cache** and configure **Static Routes**.
- **ARP** - view the ARP settings and clear the ARP cache as well as configure ARP cache time.
- **DHCP Server** - configure the SonicWALL as a DHCP Server on your network to dynamically assign IP addresses to computers on your network.

Network>Settings

The **Network>Settings** page allows you to configure the your network and Internet connectivity settings. You can configure your WAN (Internet), LAN, and DMZ interfaces.



Tip!

If you are unsure about configuring network settings manually, click **Setup Wizard**. The **Setup Wizard** offers a easy-to-use method for configuring your SonicWALL. See Chapter 2 for complete **Setup Wizard** instructions.

